Tekst KE	Tekst Prez Litewtskiej	Tekst LIBE	Stanowisko MAiC
Article 1 ***Subject matter and objectives*** **1. This Regulation lays down rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data.** **2. This Regulation protects the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data.** **3. The free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.**	*Article 1* *Subject matter and objectives* 1. This Regulation lays down rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data. 2. This Regulation protects (…) fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. 3. The free movement of personal data <u>within the Union</u> shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.	Article 1 Subject matter and objectives 1. This Regulation lays down rules relating to the protection of individuals with regard to the processing of personal data and rules relating to the free movement of personal data. 2. This Regulation protects the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data. 3. The free movement of personal data within the Union shall neither be restricted nor prohibited for reasons connected with the protection of individuals with regard to the processing of personal data.	MAiC nie prezentowało dotąd stanowiska – przedstawiona propozycja jest dla nas do zaakceptowania.
Article 2 **Material scope**	Article 2 Material scope 1. This Regulation applies to the	Article 2 Material scope	**Ust.2 Lit.(b)** – PL wyraźnie opowiadała się za usunięciem wyłączenia dla instytucji unijnych. Jeśli celem ma być harmonizacja, rozporządzenie powinno

1. This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. **2. This Regulation does not apply to the processing of personal data:** **(a) in the course of an activity which falls outside the scope of Union law, in particular concerning national security;** **(b) by the Union institutions, bodies, offices and agencies;** **(c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of the Treaty on European Union;** **(d) by a natural person without any gainful interest in the course of its own exclusively personal or household activity;** **(e) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.** **3. This Regulation shall be**	processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. 2. This Regulation does not apply to the processing of personal data: (a) in the course of an activity which falls outside the scope of Union law (…); (b) (…); (c) by the Member States when carrying out activities which fall within the scope of Chapter 2 <u>of Title V</u> the Treaty on European Union; (d) by a natural person (…) in the course of (…) <u>a</u> personal or household activity; (e) by competent <u>public</u> authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences <u>and, for these purposes, the maintenance of public order,</u> or the execution of criminal penalties 3. (…).	1. This Regulation applies to the processing of personal data wholly or partly by automated means, irrespective of the method of processing, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. 2. This Regulation does not apply to the processing of personal data: (a) in the course of an activity which falls outside the scope of Union law, ~~in particular national security~~; (b) ~~by the Union institutions, bodies, offices and agencies~~; (c) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the Treaty on European Union; (d) by a natural person without any gainful interest in the course of its own an exclusively personal or household activity. This exemption also shall apply to a publication of personal data where it can be reasonably expected that it will be only accessed by a limited number of persons; (e) by competent public authorities for the purposes of prevention, investigation,	mieć zastosowanie do wszystkich podmiotów, również i instytucji europejskich. **Ust.2 Lit. (d)** – PL popiera brzmienie tekstu Rady (wykreślenie *„any gainful interest*" i *exclusively",* jako że te pojęcia są nieostre i powodują wątpliwości interpretacyjne). Rozróżnienie czynności, które mają charakter wyłącznie osobisty i domowy może być problematyczne, w szczególności w odniesieniu do działań w świecie cyfrowym, podobnie niektóre czynności podejmowana w charakterze domowym mogą wiązać się z aspektem zarobkowym. Osoby fizyczne przetwarzające dane w celach osobistych lub domowych nie powinny podlegać wymogom rozporządzenia.

without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.	detection or prosecution of criminal offences or the execution of criminal penalties. 3. This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

Article 3 **Territorial scope** **1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.** **2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:** **(a) the offering of goods or services to such data subjects in the Union; or** **(b) the monitoring of their behaviour.** **3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.**	Article 3 Territorial scope 1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union. 2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment by the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the European Union. 3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.	Article 3 Territorial scope 1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, *whether the processing takes place in the Union or not*. 2. This Regulation applies to the processing of personal data of data subjects ~~*residing*~~ in the Union by a controller *or processor* not established in the Union, where the processing activities are related to: (a) the offering of goods or services*, irrespective of whether a payment of the data subject is required,* to such data subjects in the Union; or (b) the monitoring of *such data subjects* ~~*their behaviour*~~*.* 3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.	PL popiera brzmienie artykułu w tekście PREZ. Polska jest za zastosowaniem przepisów o ochronie danych osobowych w stosunku do podmiotów z państw trzecich w przypadku, gdy przetwarzanie wiąże się z oferowaniem towarów lub usług podmiotom danych w UE lub monitorowaniem zachowania tych osób.

Article 4 **Definitions** **For the purposes of this Regulation:** **(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;** **(2) 'personal data' means any information relating to a data subject;** **(3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction;** **(4) 'filing system' means any**	Article 4 Definitions For the purposes of this Regulation: (1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly (…), in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. (2a) 'pseudonymous data' means personal data processed in such a way that the data cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution; (3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or	Article 4 Definitions For the purposes of this Regulation: ~~*(1) 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;*~~ (2) 'personal data' means any information relating to a*n identified or identifiable natural person ('*data subject*'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, unique identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or gender identity of that person*; *(2a) 'pseudonymous data' means personal data that cannot be attributed to a specific data subject without the use of additional*	Pkt. 2 (definicja danych osobowych) – PL popiera szeroką definicję danych osobowych. Każda bowiem informacja, która przy użyciu rozsądnych środków i przy uwzględnieniu czasu i kosztów pozwala na zidentyfikowanie osoby fizycznej powinna być rozumiana jako dana osobowa (dotyczy to również identyfikatorów internetowych). Tak szeroko rozumiana definicja danych osobowych pozwala na uwzględnienie potencjalnych nowych form identyfikacji, jakie mogą się pojawić w przyszłości w związku z postępem technologicznym.

structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis; **(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data; where the purposes, conditions and means of processing are determined by Union law or Member State law, the controller or the specific** **criteria for his nomination may be designated by Union law or by Member State law;** **(6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;** **(7) 'recipient' means a natural or legal person, public authority, agency or any other body to which the personal data are disclosed;**	combination (…) or erasure; (3a) 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future; (4) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis (5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes (…) and means of the processing of personal data; where the purposes (…) and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law; (6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller; (7) 'recipient' means a natural or legal person, public authority, agency or any other body <u>other than the data subject, the data controller or the data processor</u> to which the personal data are disclosed<u>;</u>	*information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution;* *(2b) 'encrypted data' means personal data, which through technological protection measures is rendered unintelligible to any person who is not authorised to access it;* (3) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction; *(3a) 'profiling' means any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict in particular that natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour;*	Pkt. 2a (definicja danych spseudonimizowanych) – PL popiera wprowadzenie definicji danych spseudonimizowanych.Jednocześnie stoimy na stanowisku, iż dane spseudonimizowane są nadal danymi osobowymi w rozumieniu Rozporządzenia. Pseudonimizacja jest więc jedynie środkiem technicznym, którego zastosowanie może zwalniać administratora danych z niektórych obowiązków, np. z obowiązku zgłaszania naruszeń ochrony danych (data breach).

(8) 'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;	however regulatory bodies and authorities which may receive personal data in the exercise of their official functions shall not be regarded as recipients; (8) 'the data subject's consent' means any freely-given, specific and informed (…)indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;	(4) 'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;	pkt. 7 (definicja odbiorcy) – PL popiera brzmienie definicji odbiorcy w projekcie Rady – postulowaliśmy jej zawężenie poprzez wyłączenie z kategorii odbiorców samych podmiotów danych, administratorów, podmiotów przetwarzających oraz podmiotów publicznych, które mogą otrzymywać dane w ramach konkretnego dochodzenia. Dzięki temu ograniczeniu obowiązek poinformowania odbiorców o operacjach poprawienia lub usunięcia danych, które ujawniono temu odbiorcy nie wydaje się już tak szeroki i znajduje swoje uzasadnienie.
(9) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;	(9) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;	(5) 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes~~, conditions~~ and means of the processing of personal data; where the purposes~~, conditions~~ and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law;	pkt. 8 (definicja zgody) - PL popiera wymóg „zgody wyraźnej" – aby zgoda na przetwarzanie danych nie mogła być dorozumiewana z innych oświadczeń woli, gdyż tylko taka zgoda pozwoli obywatelom zachować kontrolę nad ich danymi i zapewnić autonomię informacyjną. Brak wymogu zgody wyraźnej utrudni również spełnienie przesłanki „zgody poinformowanej" jak i uczyni bardziej skomplikowanym spełnienie przez administratorów wymogu udowodnienia, że podmiot danych wyraził zgodę. Należy mieć na uwadze, że zgoda jest tylko jedną z podstaw przetwarzania danych i wiele z operacji przetwarzania będzie mogło być dokonywanych na podstawie uzasadnionego interesu (np. w
(10) 'genetic data' means all data, of whatever type, concerning the characteristics of an individual which are inherited or acquired during early prenatal development;	(10) 'genetic data' means all personal data relating to the genetic characteristics of an individual that have been inherited or acquired, resulting from an analysis of a biological sample from the individual in question; (11) 'biometric data' means any personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual which allows or confirms the unique identification of that individual, such as facial images, or dactyloscopic data; (12) 'data concerning health' means	(6) 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller; (7) 'recipient' means a natural or legal person, public authority, agency or any other body to which the personal data are disclosed;	

(11) 'biometric data' means any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data; **(12) 'data concerning health' means any information which relates to the physical or mental health of an individual, or to the provision of health services to the individual;** **(13) 'main establishment' means as regards the controller, the place of its establishment in the Union where the main decisions as to the purposes, conditions and means of the processing of personal data are taken; if no decisions as to the purposes, conditions and means of the processing of personal data are taken in the Union, the main establishment is the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place. As regards the processor, 'main establishment' means the place of its central administration**	data related to the physical or mental health of an individual, which reveal information about his or her health status; (12a) 'profiling' means any form of automated processing of personal data intended to create or use a personal profile by evaluating personal aspects relating to a natural person, in particular the analysis and prediction of aspects concerning performance at work, economic situation, health, personal preferences, or interests, reliability or behaviour, location or movements; (13) 'main establishment' means - as regards the controller, the place of its establishment in the Union where the main decisions as to the purposes (…) and means of the processing of personal data are taken; if no decisions as to the purposes (…) and means of the processing of personal data are taken in the Union, (…) the place where the main processing activities in the context of the activities of an establishment of a controller in the Union take place; - as regards the processor, the place of its central administration in the Union and, if it has no central administration in the Union, the place where the main processing activities take place; Where the processing is carried out by a group of undertakings, the main establishment of the controlling	*(7a) 'third party' means any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;* (8) 'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed; (9) 'personal data breach' means ~~*a breach of security leading to*~~ the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. (10) 'genetic data' means all *personal data relating to the genetic characteristics of an individual which have been inherited or acquired as they result from an analysis of a biological sample from the individual in*	przypadku marketingu bezpośredniego) czy też na podstawie umowy i w tych wypadkach nie będzie wymagało udzielania zgody. W polskiej ustawie o ochronie danych osobowych zgoda również jest interpretowana jako „wyraźna". W tym zakresie PL popiera propozycję LIBE, która utrzymuje wymóg zgody „wyraźnej". Pkt.12a (definicja profilowania) – PL popiera wprowadzenie definicji profilowania. Zasady i warunki profilowania określa art. 20. Pkt. 13 (definicja siedziby głównej) – PL jest za jak największym uproszczeniem i obiektywnymi kryteriami definicji siedziby głównej, tak, żeby jej ustalanie nie niosło za sobą wątpliwości. Głównym kryterium powinno być *: The location of the controller or processor's headquarters.* Definicja w obecnym brzmieniu, pozostawiając administratorom możliwość wyboru miejsca, gdzie będą podejmowane decyzje co do celów i środków przetwarzania danych, może skutkować zjawiskiem forum shopping.

in the Union;	undertaking shall be considered as the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking;	*question, in particular by chromosomal, desoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis or analysis of any other element enabling equivalent information to be obtained;*
(14) 'representative' means any natural or legal person established in the Union who, explicitly designated by the controller, acts and may be addressed by any supervisory authority and other bodies in the Union instead of the controller, with regard to the obligations of the controller under this Regulation;	(14) 'representative' means any natural or legal person established in the Union who, (…) designated by the controller in writing pursuant to Article 25, represents the controller with regard to the obligations of the controller under this Regulation (…);	(11) 'biometric data' means any *personal* data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data;
(15) 'enterprise' means any entity engaged in an economic activity, irrespective of its legal form, thus including, in particular, natural and legal persons, partnerships or associations regularly engaged in an economic activity;	(15) 'enterprise' means any natural or legal person engaged in an economic activity, irrespective of its legal form, (…) including (…) partnerships or associations regularly engaged in an economic activity;	(12) 'data concerning health' means any *personal data ~~information~~* which relates to the physical or mental health of an individual, or to the provision of health services to the individual;
(16) 'group of undertakings' means a controlling undertaking and its	(16) 'group of undertakings' means a controlling undertaking and its controlled undertakings;	*(13) 'main establishment' means the place of establishment of the undertaking or group of undertakings in the Union, whether controller or processor, where the main decisions as to the purposes, conditions and means of the processing of personal data are taken. The following objective criteria may be considered among others: The location of the controller or processor's headquarters; the location of the entity within a group of undertakings which is best*
	(17) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State of the Union for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings;	
	(18) (…)	
	(19) 'supervisory authority' means an independent public authority which is	

controlled undertakings; **(17) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State of the Union for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings;** **(18) 'child' means any person below the age of 18 years;** **(19) 'supervisory authority' means a public authority which is established by a Member State in accordance with Article 46.**	established by a Member State pursuant to Article 46; (20) 'Information Society service' means any service as defined by Article 1 (2) of Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services.	*placed in terms of management functions and administrative responsibilities to deal with and enforce the rules as set out in this Regulation; the location where effective and real management activities are exercised determining the data processing through stable arrangements;* (14) 'representative' means any natural or legal person established in the Union who, explicitly designated by the controller, ~~*acts and may be addressed by the supervisory authority and other bodies in the Union instead of the*~~ *represents the* controller~~,~~ with regard to the obligations of the controller under this Regulation; (15) 'enterprise' means any entity engaged in an economic activity, irrespective of its legal form, thus including, in particular, natural and legal persons, partnerships or associations regularly engaged in an economic activity; (16) 'group of undertakings' means a controlling undertaking and its controlled undertakings; (17) 'binding corporate rules' means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State of the Union for transfers or a set of transfers of personal data to a controller or processor in one or more third countries

within a group of undertakings;

(18) 'child' means any person below the age of 18 years;

(19) 'supervisory authority' means a public authority which is established by a Member State in accordance with Article 46.

Article 5 **Principles relating to personal data processing** **Personal data must be:** **(a) processed lawfully, fairly and in a transparent manner in relation to the data subject;** **(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;** **(c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;** **(d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed,**	*Article 5* *Principles relating to personal data processing* 1. Personal data must be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible subject to the conditions and safeguards referred to in Article 83; (c) adequate, relevant and not excessive in relation to the purposes for which they are processed (…); (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed (…) for	Article 5 Principles relating to personal data processing Personal data ~~*must*~~ *shall* be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject *(lawfulness, fairness and transparency)*; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes *(purpose limitation)*; (c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data *(data minimisation)*; (d) accurate and*, where necessary,* kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay *(accuracy).* (e) kept in a form which permits *direct or indirect* identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;	Lit. e) – PL postulowała przywrócenie na końcu punktu (e): „and if a periodic

are erased or rectified without delay; **(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes in accordance with the rules and conditions of Article 83 and if a periodic review is carried out to assess the necessity to continue the storage;** **(f) processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation.**	historical, statistical or scientific (…) purposes <u>pursuant to</u> Article 83 (…); (ee) processed in a manner that ensures appropriate security (…) of the personal data. (f) (…) 2. The controller shall be responsible for compliance with paragraph 1.	personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research *or for archive* purposes in accordance with the rules and conditions of Articles 83 *and 83a* and if a periodic review is carried out to assess the necessity to continue the storage, *and if appropriate technical and organizational measures are put in place to limit access to the data only for these purposes (storage minimisation)*; *(ea) processed in a way that effectively allows the data subject to exercise his or her rights (effectiveness);* *(eb) processed in a way that protects against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity);* (f) processed under the responsibility and liability of the controller, who shall ensure and *be able to* demonstrate ~~*for each processing operation*~~ the compliance with the provisions of this Regulation *(accountability)*.	review is carried out to assess the necessity to continue the storage" (z początkowego tekstu KE), dane osobowe nie powinny być przechowywane bez limitu czasowego. PL popierała dodanie ustępu (ee) (w tekście Rady).

Article 6 **Lawfulness of processing** 1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of their personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested	*Article 6* ***Lawfulness of processing*** 1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given unambiguous consent to the processing of their personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject **(…)**; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;	**Article 6** **Lawfulness of processing** 1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of their personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;	**lit. f)** – rozszerzenie podstawy słusznego interesu na osoby trzecie jest w opinii PL rozwiązaniem zbyt daleko idącym, osłabiającym skuteczną kontrolę podmiotów danych nad przetwarzaniem ich danych osobowych. Obecne brzmienie 23.1.5 uodo to "jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą". ODBIORCA DANYCH, ZGODNIE Z UODO, TO każdy, komu udostępnia się dane osobowe, z wyłączeniem osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, przedstawiciela, o którym mowa w art. 31a u.o.d.o., podmiotu przetwarzającego dane na podstawie umowy z administratorem oraz organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem. PL zaznaczy, iż w toku konsultacji społecznych pojawiły się wątpliwości

in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks. 2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83. 3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in: (a) Union law, or (b) the law of the Member State to which the controller is subject. The law of the Member State must meet an objective of public interest or must be necessary to protect the	(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a controller to which the data are disclosed except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This subparagraph shall not apply to processing carried out by public authorities in the exercise of their public duties . 2. (…) 3. The basis for the processing referred to in points (c) and (e) of paragraph 1 must be provided for in: (a) Union law, or (b) national law of the Member State to which the controller is subject. The purpose of the processing shall be determined in this legal basis or as regards the processing referred to in point (e) of paragraph 1, be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.	(f) processing is necessary for the purposes of the legitimate interests pursued by ***the ~~a~~*** controller ***or in case of disclosure, by the third party to whom the data is disclosed, and which meet the reasonable expectations of the data subject based on his or her relationship with the controller***, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data***~~, in particular where the data subject is a child~~***. This shall not apply to processing carried out by public authorities in the performance of their tasks. 2. Processing of personal data which is necessary for the purposes of historical, statistical or scientific research shall be lawful subject to the conditions and safeguards referred to in Article 83. 3. The basis of the processing referred to in points (c) and (e) of paragraph 1 must be provided for in: (a) Union law, or

rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued. 4. Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract. 5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraph 1 for various sectors and data processing situations, including as regards the processing of personal data related to a child.	Within the limits of this Regulation, the controller, processing operations and processing procedures, including measures to ensure lawful and fair processing, may be specified in this legal basis. 3a. In order to ascertain whether a purpose of further processing is compatible with the one for which the data are initially collected, the controller shall take into account, inter alia: (a) any link between the purposes for which the data have been collected and the purposes of the intended further processing; (b) the context in which the data have been collected; (c) the nature of the personal data; (d) the possible consequences of the intended further processing for data subjects; (e) the existence of appropriate safeguards. 4. Where the purpose of further processing is incompatible with the one for which the personal data have been collected, the further processing must	(b) law of the Member State to which the controller is subject. The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued. ***Within the limits of this Regulation, the law of the Member State may provide details of the lawfulness of processing, particularly as regards data controllers, the purpose of processing and purpose limitation, the nature of the data and the data subjects, processing measures and procedures, recipients, and the duration of storage.*** ***~~4. Where the purpose of further processing is incompatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and~~***	

	have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1..	***~~general conditions of a contract.~~***
	5. (…).	***~~5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the conditions referred to in point (f) of paragraphs 1a to 1c for various sectors and data processing situations, including as regards the processing of personal data related to a child.~~***

Article 7 **Conditions for consent** **1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.** **2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.** **3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.** **4. Consent shall not provide a legal basis for the processing, where there is a significant imbalance**	*Article 7* *Conditions for consent* 1. Where Article 6(1)(a) applies the controller shall be able to demonstrate that unambiguous consent was given by the data subject. 1a. Where article 9(2)(a) applies, the controller shall be able to demonstrate that explicit consent was given by the data subject. 2. If the data subject's consent is to be given in the context of a written declaration which also concerns other matters, the request for consent must be presented in a manner which is clearly distinguishable (…) from the other matters. 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal (…). 4. (…).	Article 7 Conditions for Consent 1. *Where processing is based on consent,* the controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes. 2. If the data subject's consent is given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented *clearly* distinguishable in its appearance from this other matter. *Provisions on the data subject's consent which are partly in violation of this Regulation are fully void.* 3. *Notwithstanding other legal grounds for processing,* the data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. *It shall be as easy to withdraw consent as to give it. The data subject shall be informed by the controller if withdrawal of consent may result in the termination of the services provided or of the relationship with the controller.* ~~*4. Consent shall not provide a legal basis for the processing, where there is a significant, imbalance between the position of the data subject and the controller.*~~ *Consent shall be purpose-limited and shall lose its validity when the purpose ceases to exist or as soon as the processing of personal data is no longer necessary for carrying out the purpose for which they were originally collected. The execution of a contract or the provision of a service shall not be made*	PL zgłaszała wątpliwości do ust. 4 (zgoda jest nieważna w przypadku „poważnej nierówności między podmiotem danych a administratorem". PL wskazywała na zbyt niedookreślony i mogący prowadzić do niepewności prawnej charakter tego pojęcia. W efekcie przepis ten został usunięty w tekście Rady. Pozytywnie odnieśliśmy się do poprawek LIBE zmierzających do wzmocnienia wymogów i znaczenia zgody.

Article 8 **Processing of personal data of a child** **1. For the purposes of this Regulation, in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or custodian. The controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology.** **2. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.** **3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the methods to obtain verifiable consent referred to in paragraph 1. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.**	*Article 8* *Conditions applicable to child's consent in relation to information society services* 1. Where Article 6 (1)(a) applies, in relation to the offering of information society services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that such consent is given or authorised by the child's parent or guardian. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the child's parent or guardian , taking into consideration available technology. 2. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child. 3. [The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the methods to obtain verifiable consent referred to in paragraph 1(…). 4. The Commission may lay down standard forms for specific methods to obtain verifiable consent referred to in paragraph 1. Those implementing acts shall	Article 8 Processing of personal data of a child 1. For the purposes of this Regulation, in relation to the offering of ~~*information society*~~ *goods or* services directly to a child, the processing of personal data of a child below the age of 13 years shall only be lawful if and to the extent that consent is given or authorised by the child's parent or ~~*custodian*~~ *legal guardian*. The controller shall make reasonable efforts to *verify such* ~~*obtain verifiable*~~ consent, taking into consideration available technology *without causing otherwise unnecessary processing of personal data*. *1a. Information provided to children, parents and legal guardians in order to express consent, including about the controller's collection and use of personal data, should be given in a clear language appropriate to the intended audience.* 2. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child. 3. The *European Data Protection Board* ~~*Commission*~~ shall be *entrusted with the task* ~~*empowered to adopt delegated acts in accordance with Article 86 for the purpose*~~	PL zgłaszała wątpliwości, jak w środowisku cyfrowym administrator danych ma identyfikować, że odbiorcą jego usług jest osoba poniżej 13 roku życia, i w jaki sposób będzie uzyskiwał zgodę rodzica lub opiekuna. Jak w przypadku usług oferowanych na odległość dostawca usług może zweryfikować czy dana osoba jest rzeczywistym rodzicem lub opiekunem? W tym zakresie popieramy uzupełnienie LIBE w ust. 1: "*without causing otherwise unnecessary processing of personal data"*.

4. The Commission may lay down standard forms for specific methods to obtain verifiable consent referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	be adopted in accordance with the examination procedure referred to in Article 87(2)].	of *issuing guidelines, recommendations and best practices ~~further specifying the criteria and requirements~~* for the methods *of verifying ~~to obtain verifiable~~* consent referred to in paragraph 1, *in accordance with Article 66*. *~~4. The Commission may lay down standard forms for specific methods to obtain verifiable consent referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).~~*

Article 9 Processing of special categories of personal data 1. The processing of personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures shall be prohibited. 2. Paragraph 1 shall not apply where: (a) the data subject has given consent to the processing of those personal data, subject to the conditions laid down in Articles 7 and 8, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law in so far as it is authorised by Union law or Member State law providing for adequate safeguards; or (c) processing is necessary to protect the vital interests of the data subject or of another person where the	*Article 9* *Processing of special categories of personal data* 1. The processing of personal data, revealing racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life (…)shall be prohibited. 2. Paragraph 1 shall not apply if one of the following applies: (a) the data subject has given explicit consent to the processing of those personal data (…), except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law in so far as it is authorised by Union law or Member State law providing for adequate safeguards; or (c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent; or (d) processing is carried out in the	Article 9 Special categories of data 1. The processing of personal data, revealing race or ethnic origin, political opinions, religion or *philosophical* beliefs, *sexual orientation or gender identity,* trade-union membership *and activities*, and the processing of genetic *or biometric* data or data concerning health or sex life*, ~~or~~administrative sanctions, judgments,* criminal *or suspected offences,*convictions*,* or related security measures shall be prohibited. 2. Paragraph 1 shall not apply if one of the following applies: (a) the data subject has given consent to the processing of those personal data *for one or more specified purposes*, subject to the conditions laid down in Articles 7 and 8, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject, or *(aa) processing is necessary for the performance or execution of a contract to which the data subject is party or in order to take steps at the request of the data subject*	PL sugerowała rozszerzenie katalogu danych wrażliwych o dane nt. orzeczeń wydanych w postępowaniu sądowym lub administracyjnym (tak jak jest to w polskiej u.o.d.o).

data subject is physically or legally incapable of giving consent; or (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the data subjects; or (e) the processing relates to personal data which are manifestly made public by the data subject; or (f) processing is necessary for the establishment, exercise or defence of legal claims; or (g) processing is necessary for the performance of a task carried out in the public interest, on the basis of Union law, or Member State law which shall provide for suitable measures to safeguard the data subject's legitimate interests; or (h) processing of data concerning health is necessary for health purposes	course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed outside that body without the consent of the data subjects; or (e) the processing relates to personal data which are manifestly made public by the data subject; or (f) processing is necessary for the establishment, exercise or defence of legal claims; or (g) processing is necessary for the performance of a task carried out <u>for *important* reasons of</u> public interest, on the basis of Union law or Member State law which shall provide for suitable measures to safeguard the data subject's legitimate interests; or (h) processing of data concerning health is necessary for health purposes and subject to the conditions and safeguards referred to in Article 81; or (i) processing is necessary for historical, statistical or scientific (…)	*prior to entering into a contract;* (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller in the field of employment law in so far as it is authorised by Union law or Member State law *or collective agreements* providing for adequate safeguards *for the fundamental rights and the interests of the data subject such as right to non-discrimination, subject to the conditions and safeguards referred to in Article 82*; or (c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent; or (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the	lit. (aa) (poprawka LIBE) MAiC sugeruje uzupełnienie przepisu poprzez dodanie wymogu, "*given that the adequate safeguards for the rights and freedoms of data subjects are provided"*

and subject to the conditions and safeguards referred to in Article 81; or (i) processing is necessary for historical, statistical or scientific research purposes subject to the conditions and safeguards referred to in Article 83; or (j) processing of data relating to criminal convictions or related security measures is carried out either under the control of official authority or when the processing is necessary for compliance with a legal or regulatory obligation to which a controller is subject, or for the performance of a task carried out for important public interest reasons, and in so far as authorised by Union law or Member State law providing for adequate safeguards. A complete register of criminal convictions shall be kept only under the control of official authority. 3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria, conditions and appropriate safeguards for the processing of the special categories of personal data referred to in paragraph 1 and the exemptions laid down in paragraph 2.	purposes subject to the conditions and safeguards referred to in Article 83. (j) (…) 2a. Processing of data relating to criminal convictions and offences or related security measures may only be carried out either under the control of official authority or when the processing is necessary for compliance with an (…) obligation to which a controller is subject, or for the performance of a task carried out for important reasons of public interest (…), and in so far as authorised by Union law or Member State law providing for adequate safeguards for the rights and freedoms of data subjects. A complete register of criminal convictions may be kept only under the control of official authority. 3. (…)	data are not disclosed outside that body without the consent of the data subjects; (e) the processing relates to personal data which are manifestly made public by the data subject; or (f) processing is necessary for the establishment, exercise or defence of legal claims; or (g) processing is necessary for the performance of a task carried out ~~*in the*~~*for reasons of high* public interest, on the basis of Union law, or Member State law which shall *be proportionate to the aim pursued, respect the essence of the right to data protection and* provide for suitable measures to safeguard the *fundamental rights and the* ~~*data subject's legitimate*~~ interests *of the data subject*; or (h) processing of data concerning health is necessary for health purposes and subject to the conditions and safeguards referred to in Article 81; or (i) processing is necessary for historical, statistical or scientific research purposes subject to the conditions and safeguards referred to in Article 83; or

(i a) processing is necessary for archive services subject to the conditions and safeguards referred to in Article 83a; or

(j) processing of data relating to *administrative sanctions, judgments,*criminal *offences,* convictions or related security measures is carried out either under the control of official authority or when the processing is necessary for compliance with a legal or regulatory obligation to which a controller is subject, or for the performance of a task carried out for important public interest reasons, and in so far as authorised by Union law or Member State law providing for adequate safeguards *for the fundamental rights and the interests of the data subject*. ~~*A complete*~~ *Any* register of criminal convictions shall be kept only under the control of official authority.

3. The *European Data Protection Board* ~~*Commission*~~ shall be*en trusted with the task* ~~*empowered to adopt delegated acts in accordance with Article 86 for the purpose*~~ of *issuing guidelines, recommendations and best practices* ~~*further specifying the criteria and requirements*~~ for the processing of the special categories of personal data referred to in paragraph 1 and the exemptions laid down in paragraph 2*, in accordance with Article 66*.

Article 10 **Processing not allowing identification** **If the data processed by a controller do not permit the controller to identify a natural person, the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.**	*Article 10* *Processing not requiring identification* 1. If the purposes for which a controller processes personal data do not require the identification of a data subject by the controller, the controller shall not be obliged to acquire (…) additional information nor to engage in additional processing in order to identify the data subject for the sole purpose of complying with (…) this Regulation. 2. Where, in such cases the controller is not in a position to identify the data subject, articles 15, 16, 17, 17a, 17b and 18 (…) do not apply except where the data subject, for the purpose of exercising his or her rights under these articles, provides additional information enabling his or her identification.	Article 10 *Processing not allowing identification* *1.* If the data processed by a controller do not permit the controller *or processor* to *directly or indirectly* identify a natural person, *or consist only of pseudonymous data,* the controller shall not ~~*be obliged to*~~ *process or* acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation. *2. Where the data controller is unable to comply with a provision of this Regulation because of paragraph 1, the controller shall not be obliged to comply with that particular provision of this Regulation. Where as a consequence the data controller is unable to comply with a request of the data subject, it shall inform the data subject accordingly.*	PL uznała zaproponowane przez PREZ zmiany w dobrym kierunku. Chcielibyśmy jednak wyeliminować możliwość uchylania się przez administratorów danych od obowiązków przewidzianych rozporządzeniem w przypadku gdy podmiot danych poda dodatkowe informacje – doidentyfikuje się.
		Article 10a General principles for data subject rights *1. The basis of data protection is clear and unambiguous rights for the data subject which shall be respected by the data controller. The provisions of this Regulation aim to strengthen, clarify, guarantee and*	

		where appropriate, codify these rights. *2. Such rights include, inter alia, the provision of clear and easily understandable information regarding the processing of his or her personal data, the right of access, rectification and erasure of their data, the right to obtain data, the right to object to profiling, the right to lodge a complaint with the competent data protection authority and to bring legal proceedings as well as the right to compensation and damages resulting from an unlawful processing operation. Such rights shall in general be exercised free of charge. The data controller shall respond to requests from the data subject within a reasonable period of time.*

Article 11 **Transparent information and communication** **1. The controller shall have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights.** **2. The controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, adapted to the data subject, in particular for any information addressed specifically to a child.**	*Article 11* *Transparent information and communication* 1. (…) 2. (…)	Article 11 Transparent information and communication 1. The controller shall have *concise,* transparent*, clear* and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights. 2. The controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, ~~*adapted to the data subject,*~~ in particular for any information addressed specifically to a child.	PL nie zgłaszała zasadniczych uwag to tego przepisu.

Article 12 **Procedures and mechanisms for exercising the rights of the data subject** **1. The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19. Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically.** **2. The controller shall inform the data subject without delay and, at the latest within one month of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing. Where the data subject makes the request in electronic form, the information shall be provided**	*Article 12* *Transparent information, communication and modalities for exercising the rights of the data subject* 1. The controller shall take appropriate measures to provide any information referred to in Articles 14 and 14a and any communication under Articles 15 to 19 and 32 relating to the processing of personal data to the data subject in an intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or where appropriate, electronically or by other means. 1a. The controller shall facilitate the exercise of data subject rights under Articles 15 to 19. (…) 2. The controller shall provide the information referred to in Articles 14a and 15 and information on action taken on a request under Articles 16 to 19 to the data subject without undue delay and at the latest within one month of receipt of the request (…). This period may be extended for a further two months when necessary, taking into account the complexity of the request and the number of requests. Where the extended period applies, the data subject shall be informed within one month of receipt of the request of the reasons for the delay.	Article 12 Procedures and mechanisms for exercising the rights of the data subject 1.~~*The controller shall establish procedures for providing the information referred to in Article 14 and for the exercise of the rights of data subjects referred to in Article 13 and Articles 15 to 19. The controller shall provide in particular mechanisms for facilitating the request for the actions referred to in Article 13 and Articles 15 to 19.*~~ Where personal data are processed by automated means, the controller shall also provide means for requests to be made electronically *where possible*. 2. The controller shall inform the data subject without *undue* delay and, at the latest within ~~*one month*~~ *40 calendar days* of receipt of the request, whether or not any action has been taken pursuant to Article 13 and Articles 15 to 19 and shall provide the requested information. This period may be prolonged for a further month, if several data subjects exercise their rights and their cooperation is necessary to a reasonable extent to prevent an unnecessary and disproportionate effort on the part of the controller. The information shall be given in writing *and, where possible, the data controller may provide remote access to a secure system which would provide the data*	PL popierała zasadę bezpłatnego dostępu osoby, której dane są przetwarzane do jego/jej danych; sugerowaliśmy natomiast uszczegółowienie częstotliwości, z jaką podmiot danych może kierować wnioski np. poprzez wprowadzenie ograniczenia czasowego, że takie wnioski nie mogą być kierowane częściej niż raz na 6 miesięcy. Sformułowanie „*manifestly excessive*" może budzić wątpliwości interpretacyjne i dlatego w opinii PL wymaga doprecyzowania. ust. 1 – PL zaproponowała zrównanie formy pisemnej z elektroniczną poprzez dodanie zdania: „The information shall be provided in writing, electronically or where appropriate, by other means". Ta uwaga została uwzględniona przez PREZ.

in electronic form, unless otherwise requested by the data subject. **3. If the controller refuses to take action on the request of the data subject, the controller shall inform the data subject of the reasons for the refusal and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy.** **4. The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a fee for providing the information or taking the action requested, or the controller may not take the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request.** **5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the manifestly excessive requests and the fees referred to in paragraph 4.** **6. The Commission may lay down standard forms and specifying standard**	3. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint to a supervisory authority (…). 4. Information provided under Articles 14 and 14a (…) and any communication under Articles 16 to 19 and 32 shall be provided free of charge. Where requests from a data subject are (…)*manifestly* unfounded or excessive, in particular because of their repetitive character, the controller (…) may refuse to act on the request. In that case, the controller shall bear the burden of demonstrating the *manifestly* unfounded or excessive character of the request. 4a. Without prejudice to Article 10, where the controller has reasonable doubts concerning the identity of the individual making the request referred to in Articles 15 to 19, the controller may request the provision of additional information necessary to confirm the identity of the data subject. 5. (…) 6. (…)	*subject with direct access to their personal data*. Where the data subject makes the request in electronic form, the information shall be provided in electronic form *where possible*, unless otherwise requested by the data subject. 3. If the controller *does not ~~refuses to~~* take action on the request of the data subject, the controller shall inform the data subject of the reasons for the *inaction ~~refusal~~* and on the possibilities of lodging a complaint to the supervisory authority and seeking a judicial remedy. 4. The information and the actions taken on requests referred to in paragraph 1 shall be free of charge. Where requests are manifestly excessive, in particular because of their repetitive character, the controller may charge a *reasonable* fee *taking into account the administrative costs* for providing the information or *~~the controller may not take~~ taking* the action requested. In that case, the controller shall bear the burden of proving the manifestly excessive character of the request. *~~5. The Commission shall be empowered to adopt, delegated acts in accordance with~~*

procedures for the communication referred to in paragraph 2, including the electronic format. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized enterprises. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).		~~*Article 86 for the purpose of further specifying the criteria and conditions for the manifestly excessive requests and the fees referred to in paragraph 4.*~~ ~~*6. The Commission may lay down standard forms and specifying standard procedures for the communication referred to in paragraph 2, including the electronic format. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized enterprises. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).*~~	
Article 13 **Rights in relation to recipients** **The controller shall communicate any rectification or erasure carried out in accordance with Articles 16 and 17 to each recipient to whom the data have been disclosed, unless this proves impossible or involves a disproportionate effort.**	*Article 13* *Rights in relation to recipients* *(…)*	Article 13 ~~Rights in relation to recipients~~ *Notification requirement in the event of rectification and erasure* The controller shall communicate any rectification or erasure carried out in accordance with Articles 16 and 17 to each recipient to whom the data have been *transferred* ~~*disclosed*~~, unless this proves impossible or involves a disproportionate effort*. The controller shall inform the data subject about those recipients if the data subject requests this.*	PL nie zgłaszała zasadniczych uwag do tego przepisu. W tekście Rady został on przesunięty do art. 17b.

	Article 13a (new) *Standardized information policies* *1) Where personal data relating to a data subject are collected, the controller shall provide the data subject with the following particulars before providing information pursuant to Article 14:* *a) whether personal data are collected beyond the minimum necessary for each specific purpose of the processing;* *b) whether personal data are retained beyond the minimum necessary for each specific purpose of the processing;* *c) whether personal data are processed for purposes other than the purposes for which they were collected;* *d) whether personal data are disseminated to commercial third parties;* *e) whether personal data are sold or rented out;* *f) whether personal data are retained in encrypted form.* *2) The particulars referred to in paragraph 1 shall be presented pursuant to Annex X in an*	W ocenie MAiC koncepcja LIBE stworzenia zestandaryzowanej polityki informacyjnej w postaci symboli graficznych jest ciekawa i warta rozwinięcia.

	aligned tabular format, using text and symbols, in the following three columns: *a) the first column depicts graphical forms symbolising those particulars;* *b) the second column contains essential information describing those particulars;* *c) the third column depicts graphical forms indicating whether a specific particular is met.* *3) The information referred to in paragraphs 1 and 2 shall be presented in an easily visible and clearly legible way and shall appear in a language easily understood by the consumers of the Member States to whom the information is provided. Where the particulars are presented electronically, they shall be machine readable.* *4) Additional particulars shall not be provided. Detailed explanations or further remarks regarding the particulars referred to in paragraph 1 may be provided together with the other information requirements pursuant to Article 14.* *5) The Commission shall be empowered to adopt, after requesting an opinion of the European Data Protection Board, delegated acts in accordance with Article 86 for the purpose of further specifying the particulars referred to in paragraph 1 and their presentation as referred to in paragraph 2*

		and in Annex 1.	
Article 14 **Information to the data subject** **1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:** **(a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer;** **(b) the purposes of the processing for which the personal data are intended, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);** **(c) the period for which the personal data will be stored;** **(d) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject or to object to the processing of such personal data;**	*Article 14* *Information to be provided where the data are collected from the data subject* 1. Where personal data relating to a data subject are collected from the data subject, the controller shall (…), at the time when personal data are obtained, provide the data subject with the following information: (a) the identity and the contact details of the controller and, if any, of the controller's representative; the controller may also include the contact details of the data protection officer, if any; (b) the purposes of the processing for which the personal data are intended (…); 1a. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with such further information necessary to ensure fair and transparent processing in respect of the data subject, having regard to the specific circumstances and context in which the personal data are processed: (a) (…); (b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller;	Article 14 Information to the data subject 1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information, *after the particulars pursuant to Article 13a have been provided*: (a) the identity and the contact details of the controller and, if any, of the controller's representative, of the data protection officer; (b) the purposes of the processing for which the personal data are intended, *as well as information regarding the security of the processing of personal data*, including the contract terms and general conditions where the processing is based on point (b) of Article 6(1) and ~~*the legitimate interests pursued by the controller*~~*, where applicable, information on how they implement and meet the requirements of point f of Article 6(1)*; (c) the period for which the personal data will be stored*, or if this is not possible, the criteria used to determine this period*; (d) the existence of the right to request from the controller access to and rectification or erasure of the personal data	PL nie zgłaszała zasadniczych uwag to tego przepisu. W opinii MAiC zakres informacji przekazywanych podmiotowi danych powinien być dosyć szeroki, a informacje te powinny być przekazywane w przejrzystej formie. Obecne brzmienie tekstu Rady nie budzi naszych zasadniczych zastrzeżeń. PL nie zgłaszała również zastrzeżeń do rozbicia art. 14 na dwa artykuły: art. 14 - informacje przekazywane podmiotowi danych w przypadku gdy dane zebrane zostały od podmiotu danych oraz art. 14 a - informacje przekazywane podmiotowi danych w przypadku gdy dane nie zostały zebrane od podmiotu danych. Ust. 1a lit. h) - na wniosek PL usunięto słowo „logic" z informacji dotyczącej profilowania – tak aby administrator nie był obowiązany do przekazywania podmiotowi danych informacji dot. „logiki" profilowania. Była to uwaga zgłaszana przez uczestników warsztatów – słowo „logic of profiling" mogłoby wskazywać na wymóg ujawnienia całego algorytmu używanego do profilowania, który w wielu przypadkach jest ważną tajemnicą przedsiębiorstwa.

(e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority; **(f) the recipients or categories of recipients of the personal data;** **(g) where applicable, that the controller intends to transfer to a third country or international organisation and on the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission;** **(h) any further information necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected.** **2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is obligatory or voluntary, as well as the possible consequences of failure to provide such data.** **3. Where the personal data are not collected from the data subject, the controller shall inform the data subject,**	(c) the recipients or categories of recipients of the personal data; (d) where applicable, that the controller intends to transfer <u>personal data to a recipient</u> in <u>a</u> third country or international organisation; (e) the existence of the right to request from the controller access to and rectification or erasure of the personal data <u>or restriction of processing of personal data</u> concerning the data subject and to object to the processing of such personal data (…); (f) the right to lodge a complaint to <u>a</u> supervisory authority (…); (g) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as the possible consequences of failure to provide such data; and <u>(h)</u> the existence of profiling referred to in Article 20(1) and (3) and information concerning (…) the profiling, as well as the significance and the envisaged consequences of such profiling of the data subject. 2. (…) 3. (…)	concerning the data subject to object to the processing of such personal data, *or to obtain data*; (e) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority; (f) the recipients or categories of recipients of the personal data; (g) where applicable, that the controller intends to transfer *the data* to a third country or international organisation and on ~~*the level of protection afforded by that third country or international organisation by reference to*~~ *the existence or absence of* an adequacy decision by the Commission, *or in case of transfers referred to in Article 42, Article 43, or point (h) of Article 44(1), reference to the appropriate safeguards and the means to obtain a copy of them*; *(ga) where applicable, information about the existence of profiling, of measures based on profiling, and the envisaged effects of profiling on the data subject;* *(gb) meaningful information about the logic involved in any automated processing;* (h) any further information *which is* necessary to guarantee fair processing in respect of the data subject, having regard to the specific circumstances in which the personal data are collected *or processed, in*

in addition to the information referred to in paragraph 1, from which source the personal data originate. **4. The controller shall provide the information referred to in paragraphs 1, 2 and 3:** **(a) at the time when the personal data are obtained from the data subject; or** **(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a disclosure to another recipient is envisaged, and at the latest when the data are first disclosed.** **5. Paragraphs 1 to 4 shall not apply, where:** **(a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or** **(b) the data are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate**	4. (…) 5. Paragraphs 1 and <u>1a</u> shall not apply where <u>and insofar as</u> the data subject already has the information. 6. (…) 7. (…) 8. (…)	*particular the existence of certain processing activities and operations for which a personal data impact assessment has indicated that there may be a high risk.* *(ha) where applicable, information whether personal data was provided to public authorities during the last consecutive 12-month period.* 2. Where the personal data are collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, whether the provision of personal data is ~~*obligatory*~~ *mandatory* or ~~*voluntary*~~ *optional*, as well as the possible consequences of failure to provide such data. *2a. In deciding on further information which is necessary to make the processing fair under 1(h), controllers shall have regard to any relevant guidance under Article 38.* 3. Where the personal data are not collected from the data subject, the controller shall inform the data subject, in addition to the information referred to in paragraph 1, from which source the *specific* personal data originate. *If personal data originates from publicly available sources, a*

effort; or	*general indication may be given.*
(c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law; or	4. The controller shall provide the information referred to in paragraphs 1, 2 and 3:
(d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of others, as defined in Union law or Member State law in accordance with Article 21.	(a) at the time when the personal data are obtained from the data subject *or without undue delay where the above is not feasible*; or
6. In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's legitimate interests.	*(aa) on request by or a body, organization or association referred to in Article 73;*
7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria for categories of recipients referred to in point (f) of paragraph 1, the requirements for the notice of potential access referred to in point (g) of paragraph 1, the criteria for the further	(b) where the personal data are not collected from the data subject, at the time of the recording or within a reasonable period after the collection, having regard to the specific circumstances in which the data are collected or otherwise processed, or, if a ~~*disclosure*~~ *transfer* to another recipient is envisaged, and at the latest ~~*when the data are first disclosed*~~ *at the time of the first transfer, or, if the data are to be used for communication with the data subject concerned, at the latest at the time of the first communication to that data subject, or*
information necessary referred to in point (h) of paragraph 1 for specific sectors and situations, and the conditions and appropriate safeguards for the exceptions laid down in point	*(bb) only on request where the data are*

(b) of paragraph 5. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized-enterprises. **8. The Commission may lay down standard forms for providing the information referred to in paragraphs 1 to 3, taking into account the specific characteristics and needs of various sectors and data processing situations where necessary. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).**	*processed by a small or micro enterprise which processes personal data only as an ancillary activity* 5. Paragraphs 1 to 4 shall not apply, where: (a) the data subject has already the information referred to in paragraphs 1, 2 and 3; or (b) the data *are processed for historical, statistical or scientific research purposes subject to the conditions and safeguards referred to in Articles 81 and 83,* are not collected from the data subject and the provision of such information proves impossible or would involve a disproportionate effort *and the controller has published the information for anyone to retrieve*; or (c) the data are not collected from the data subject and recording or disclosure is expressly laid down by law *to which the controller is subject, which provides appropriate measures to protect the data subject's legitimate interests, considering the risks represented by the processing and the nature of the personal data*; or (d) the data are not collected from the data subject and the provision of such information will impair the rights and freedoms of other~~s~~ *natural persons*, as defined in Union law or Member State law

	in accordance with Article 21. *(da) the data are processed in the exercise of his profession by, or are entrusted or become known to, a person who is subject to an obligation of professional secrecy regulated by Union or Member State law or to a statutory obligation of secrecy, unless the data is collected directly from the data subject;* 6. In the case referred to in point (b) of paragraph 5, the controller shall provide appropriate measures to protect the data subject's *rights or* legitimate interests. ~~*7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria for categories of recipients referred to in point (f) of paragraph 1, the requirements for the notice of potential access referred to in point (g) of paragraph 1, the criteria for the further information necessary referred to in point (h) of paragraph 1 for specific sectors and situations, and the conditions and appropriate safeguards for the exceptions laid down in point (b) of paragraph 5. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized enterprises.*~~ ~~*8. The Commission shall lay down standard forms for providing the information referred to in paragraphs 1 to 3, taking into account*~~

		~~*the specific characteristics and needs of various sectors and data processing situations where necessary as well as the needs of the relevant stakeholders. Those implementing acts shall be adopted, after requesting an opinion of the European Protection Board, in accordance with the examination procedure referred to in Article 87(2).*~~	
	Article 14 a ***Information to be provided where the data have not been obtained from the data subject*** 1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: (a) the identity and the contact details of the controller and, if any, of the controller's representative; the controller may also include the contact details of the data protection officer, if any; (b) the purposes of the processing for which the personal data are intended. 2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with such further information necessary to ensure fair and transparent processing in respect of		Ust. 4 lit. b) – PL poparła uzupełnienie w lit. b: *(b) the data are not collected from the data subject and the provision of such information,* ***in particular when processing for historical, statistical, or scientific research purposes****, proves impossible or would involve a disproportionate effort* – tak, aby jasno wskazać, że kiedy dane są przetwarzane do celów satystycznych, historycznych I naukowych udzielenie informacji podmiotowi danych może wymagać nadmiernego wysiłku.

the data subject, having regard to the specific circumstances and context in which the personal data are processed (…):

(a) the categories of personal data concerned;

(b) (…)

(c) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller;

(d) the recipients or categories of recipients of the personal data;

(e) the existence of the right to request from the controller access to and rectification or erasure of the personal data concerning the data subject and to object to the processing of such personal data **(…)**;

(f) the right to lodge a complaint to a supervisory authority (…);

(g) the origin of the personal data, unless the data originate from publicly accessible sources;

(h) the existence of profiling referred to in Article 20(1) and (3) and information concerning (…) the profiling, as well as the significance and the envisaged consequences of such profiling of the data subject.

3. The controller shall provide the

information referred to in paragraphs 1 and 2:

(a) within a reasonable period after obtaining the data, having regard to the specific circumstances in which the data are processed, or

(b) if a disclosure to another recipient is envisaged, at the latest when the data are first disclosed.

4. Paragraphs 1 to 3 shall not apply where and insofar as:

(a) the data subject already has the information; or

(b) the provision of such information in particular when processing personal data for historical, statistical or scientific purposes proves impossible or would involve a disproportionate effort or is likely to render impossible or to seriously impair the achievement of such purposes; in such cases the controller shall take appropriate measures to protect the data subject's legitimate interests, for example by using pseudonymous data; or

(c) obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject, which provides appropriate measures to protect the data subject's legitimate interests; or

	(d) where the data originate from publicly available sources; or (e) where the data must remain confidential in accordance with a legal provision in Union or Member State law or because of the overriding legitimate interests of another person. 5. (…) 6. (…)	
Article 15 **Right of access for the data subject** **1. The data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed. Where such personal data are being processed, the controller shall provide the following information:** **(a) the purposes of the processing;** **(b) the categories of personal data concerned;** **(c) the recipients or categories of recipients to whom the personal data**	*Article 15* *Right of access for the data subject* 1. The data subject shall have the right to obtain from the controller at reasonable intervals and free of charge (…) confirmation as to whether or not personal data concerning him or her are being processed and where such personal data are being processed access to the data and the following information: (a) the purposes of the processing; (b) (…) (c) the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular to recipients in third countries; (d) where possible, the envisaged	Article 15 Right to access and to obtain data for the data subject 1. *Subject to Article 12(4),* the data subject shall have the right to obtain from the controller at any time, on request, confirmation as to whether or not personal data relating to the data subject are being processed, *and in clear and plain language,* the following information: (a) the purposes of the processing *for each category of personal data;* (b) the categories of personal data concerned; (c) the recipients ~~*or categories of recipients*~~ to whom the personal data are to be or have been disclosed, ~~*in particular*~~ *including*

are to be or have been disclosed, in particular to recipients in third countries; **(d) the period for which the personal data will be stored;** **(e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data;** **(f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority;** **(g) communication of the personal data undergoing processing and of any available information as to their source;** **(h) the significance and envisaged consequences of such processing, at least in the case of measures referred to in Article 20.2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing. Where the data subject makes the request in electronic form, the information shall be provided in electronic form, unless otherwise**	period for which the personal data will be stored; (e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data; (f) the right to lodge a complaint to a supervisory authority (…); (g) where the personal data are not collected from the data subject, any available information as to their source; (h) in the case of decisions referred to in Article 20, knowledge of the logic involved in any automated data processing as well as the significance and envisaged consequences of such processing. 1a. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 42 relating to the transfer. 1b. On request and without an excessive charge, the controller shall provide a copy of the personal data undergoing processing to the data subject. 2. Where personal data supplied by the data subject are processed by	to recipients in third countries; (d) the period for which the personal data will be stored*, or if this is not possible, the criteria used to determine this period*; (e) the existence of the right to request from the controller rectification or erasure of personal data concerning the data subject or to object to the processing of such personal data; (f) the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority; *~~(g) communication of the personal data undergoing processing and of any available information as to their source;~~* (h) the significance and envisaged consequences of such processing*~~, at least in the case of measures referred to in Article 20~~*. *(ha) intelligible information about the logic involved in any automated processing;* *(hb) without prejudice to Article 21, in the event of disclosure of personal data to a public authority as a result of a public authority request, confirmation of the fact that such a request has been made.* 2. The data subject shall have the right to obtain from the controller communication of the personal data undergoing processing.	li. h) - W ocenie MAiC użycie słowa „logic" może budzić wątpliwości czy konieczne jest ujawnienie całego algorytmu używanego do profilowania, który może być tajemnicą przedsiębiorstwa. Sugerowaliśmy zastąpienie tego sformułowaniem bardziej precyzyjnym jak np.: wiedza dotycząca kategorii przetwarzanych danych i celu ich przetwarzania" Ust. 1b, 2, 2a – PL zgłaszała wątpliwości, że ujawnienie kopii środków bezpieczeństwa może zwiększyć

requested by the data subject. **3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1.** **4. The Commission may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).**	automated means and in a structured and commonly used format, the controller shall, on request and without an excessive charge, provide a copy of the data concerning the data subject in that format to the data subject. 2a. The right to obtain a copy referred to in paragraphs 1b and 2 shall not apply where such copy cannot be provided without disclosing personal data of other data subjects 3. (…) 4. (…) 5. [The rights provided for in this Article do not apply when data are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1a) are met].	Where the data subject makes the request in electronic form, the information shall be provided in *an* electronic *and structured* format, unless otherwise requested by the data subject. *Without prejudice to Article 10, the controller shall take all reasonable steps to verify that the person requesting access to the data is the data subject.* *2a. Where the data subject has provided the personal data where the personal data are processed by electronic means, the data subject shall have the right to obtain from the controller a copy of the provided personal data in an electronic and interoperable format which is commonly used and allows for further use by the data subject without hindrance from the controller from whom the personal data are withdrawn. Where technically feasible and available, the data shall be transferred directly from controller to controller at the request of the data subject*. *2b. This Article shall be without prejudice to the obligation to delete data when no longer necessary under Article 5(1)(e).* *2c. There shall be no right of access in accordance with paragraphs 1 and 2 when data within the meaning of Article 14(5)(da) are concerned, except if the data subject is empowered to lift the secrecy in question and acts accordingly.* ~~*3. The Commission shall be empowered to*~~	zagrożenie związane z przekazywaniem danych osobowych i sugerowaliśmy zastąpienie słowa „copy” słowem „content”.

~~*adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the communication to the data subject of the content of the personal data referred to in point (g) of paragraph 1.*~~

~~*4. The Commission may specify standard forms and procedures for requesting and granting access to the information referred to in paragraph 1, including for verification of the identity of the data subject and communicating the personal data to the data subject, taking into account the specific features and necessities of various sectors and data processing situations. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2)*~~

Article 16 **Right to rectification** **The data subject shall have the right to obtain from the controller the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, including by way of supplementing a corrective statement.**	*Article 16* *Right to rectification* 1. (…) The data subject shall have the right to obtain from the controller the rectification of personal data concerning him or her which are inaccurate. Having regard to the purposes for which data were processed, the data subject shall have the right to obtain completion of incomplete personal data, including by means of providing a supplementary (…) statement. 2. [The rights provided for in this Article do not apply when data are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1a) are met.]	Article 16 Right to rectification The data subject shall have the right to obtain from the controller the rectification of personal data relating to them which are inaccurate. The data subject shall have the right to obtain completion of incomplete personal data, including by providing a supplementary statement.	PL nie zgłaszała zasadniczych uwag to tego przepisu.

Article 17 **Right to be forgotten and to erasure** **1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:** **(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;** **(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;** **(c) the data subject objects to the processing of personal data pursuant to Article 19;** **(d) the processing of the data does not comply with this Regulation for other reasons.** **2. Where the controller referred**	*Article 17* *Right to be forgotten and to erasure* 1. The (…) controller shall have the obligation to erase personal data without undue delay and the data subject shall have the right to obtain the erasure of personal data without undue delay where one of the following grounds applies: (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1) or point (a) of Article 9(2) and (…) there is no other legal ground for the processing of the data; (c) the data subject objects to the processing of personal data *pursuant to Article 19(1)* and there are no overriding legitimate grounds for the processing or the data subject objects to the processing of personal data pursuant to Article 19(2); (d) the data have been unlawfully processed; (e) the data have to be erased for compliance with a legal obligation to which the controller is subject. 2. (…). 2a. Where the controller (…) has made	**Article 17** **Right to ~~be forgotten and to~~ erasure** 1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, ***and to obtain from third parties the erasure of any links to, or copy or replication of that data, ~~especially in relation to personal data which are made available by the data subject while he or she was a child,~~*** where one of the following grounds applies: (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data; c) the data subject objects to the processing of personal data pursuant to Article 19; ***(ca) a court or regulatory authority based in the Union has ruled as final and absolute that the data concerned must be erased;*** (d) the ***~~processing of the~~*** data ***has been unlawfully processed ~~does not comply with~~***	Ust. 2a – PL sprzeciwiała się prawu do bycia zapomnianym jako rozwiązaniu trudnemu do realizacji w praktyce. PL wskazywała, że prawo to jest technicznie trudne do zastosowania (w szczególności w środowisku internetowym), i pociąga za sobą nadmierne i nieuzasadnione obciążenia dla administratorów danych, a także budzi wątpliwości w zakresie jego relacji do wolności wypowiedzi. Wskazywaliśmy również, że realizacja tego obowiązku mogłaby prowadzić do efektu odwrotnego niż zamierzony, w postaci zwrócenia powszechnej uwagi na dane, które podmiot danych próbuje usunąć. W tekście Rady to prawo jest już nieco ograniczone, PL popiera również LIBE mocno ograniczyło prawo do bycia zapomnianym (znajduje zastosowanie jedynie do przetwarzania danych bez podstawy prawnej), co sprawia, że praktycznie nie będzie miało zastosowania.

to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication. **3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:** **(a) for exercising the right of freedom of expression in accordance with Article 80;** **(b) for reasons of public interest in the area of public health in accordance with Article 81;** **(c) for historical, statistical and scientific research purposes in accordance with Article 83;** **(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject;**	the personal data public and is obliged pursuant to paragraph 1 to erase the data, the controller, taking account of available technology and the cost of implementation, shall take (…) reasonable steps, including technical measures, (…) to inform controllers which are processing the data, that a data subject requests them to erase any links to, or copy or replication of that personal data. 3. Paragraphs 1 and 2a shall not apply to the extent that (…) processing of the personal data is necessary: a. for exercising the right of freedom of for exercising the right of freedom of expression in accordance with Article 80; *b. for compliance with a legal obligation to process the personal data by Union or Member State law to which the controller is subject*or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; c. for reasons of public interest in the area of public health in accordance with Article 81; d. for historical, statistical and scientific (…) purposes in accordance with Article 83; e. (…) f. (…)	***~~this Regulation for other reasons~~***. ***1a. The application of paragraph 1 shall be dependent upon the ability of the data controller to verify that the person requesting the erasure is the data subject.*** 2. Where the controller referred to in paragraph 1 has made the personal data public ***without a justification based on Article 6(1), it shall take all reasonable steps to have the data erased, including by third parties, without prejudice to Article 77~~, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication~~. The controller shall inform the data subject, where possible, of the action taken by the relevant third parties. ~~Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication~~.***	Ust. 2a – PL sprzeciwiała się prawu do

Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued; **(e) in the cases referred to in paragraph 4.** **4. Instead of erasure, the controller shall restrict processing of personal data where:** **(a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;** **(b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof;** **(c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead;** **(d) the data subject requests to transmit the personal data into another automated processing system in accordance with Article 18(2).** **5. Personal data referred to in paragraph 4 may, with the exception of**	g. <u>for the establishment, exercise or defence of legal claims</u>. 4. (…) 5. (…)	(c) the data subject objects to the processing of personal data pursuant to Article 19; (c) the data subject objects to the processing of personal data pursuant to Article 19; ***(ca) a court or regulatory authority based in the Union has ruled as final and absolute that the data concerned must be erased;*** (d) the ~~***processing of the***~~ data ***has been unlawfully processed*** ~~***does not comply with this Regulation for other reasons***~~. ***1a. The application of paragraph 1 shall be dependent upon the ability of the data controller to verify that the person requesting the erasure is the data subject.*** 2. Where the controller referred to in paragraph 1 has made the personal data public ***without a justification based on Article 6(1), it shall take all reasonable steps to have the data erased, including by third parties, without prejudice to Article*** ~~***77, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of***~~	bycia zapomnianym jako rozwiązaniu trudnemu do realizacji w praktyce. PL wskazywała, że prawo to jest technicznie trudne do zastosowania (w szczególności w środowisku internetowym), i pociąga za sobą nadmierne i nieuzasadnione obciążenia dla administratorów danych, a także budzi wątpliwości w zakresie jego relacji do wolności wypowiedzi. Wskazywaliśmy również, że realizacja tego obowiązku mogłaby prowadzić do efektu odwrotnego niż zamierzony, w postaci zwrócenia powszechnej uwagi na dane, które podmiot danych próbuje usunąć. W tekście Rady to prawo jest już nieco ograniczone, PL popiera również LIBE mocno ograniczyło prawo do bycia zapomnianym (znajduje zastosowanie jedynie do przetwarzania danych bez podstawy prawnej), co sprawia, że praktycznie nie będzie miało zastosowania.

storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.	***~~personal data, the controller shall be considered responsible for that publication~~. The controller shall inform the data subject, where possible, of the action taken by the relevant third parties. ~~Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication~~.***
6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.	3. The controller ***and, where applicable, the third party*** shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:
7. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.	(a) for exercising the right of freedom of expression in accordance with Article 80;
8. Where the erasure is carried out, the controller shall not otherwise process such personal data.	(b) for reasons of public interest in the area of public health in accordance with Article 81;
9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:	(c) for historical, statistical and scientific research purposes in accordance with Article 83;
(a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;	(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect ***~~the essence of~~*** the right to the protection of personal data and be proportionate to the legitimate aim pursued;
(b) the conditions for deleting links, copies or replications of personal	

data from publicly available communication services as referred to in paragraph 2; **(c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.**	(e) in the cases referred to in paragraph 4. 4. Instead of erasure, the controller shall restrict processing of personal data ***in such a way that it is not subject to the normal data access and processing operations and can not be changed anymore,*** where: (a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data; (b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof; (c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead; ***(ca) a court or regulatory authority based in the Union has ruled as final and absolute that the data concerned must be restricted;*** (d) the data subject requests to transmit the personal data into another automated processing system in accordance with paragraphs ***2a of*** Article ~~***18(2)***~~ ***15;*** ***(da) the particular type of storage technology does not allow for erasure and has been installed before the entry into force of this Regulation.*** 5. Personal data referred to in paragraph 4 may, with the exception of storage, only be

processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.

6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.

~~***7. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.***~~

8. Where the erasure is carried out, the controller shall not otherwise process such personal data.

8a. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.

8b. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.

9. The Commission shall be empowered to

	adopt, ***after requesting an opinion of the European Data Protection Board,*** delegated acts in accordance with Article 86 for the purpose of further specifying: (a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations; (b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2; (c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.	Lit. (da) – trudno wyobrazić sobie system przetwarzania danych, z którego nie można danych usunąć z powodów technologicznych, dlatego postulujemy wykreślenie tego przepisu

Article 17*a*
Right to restriction of processing

1. The data subject shall have the right to obtain from the controller the restriction of the processing of personal data where:

(a) the accuracy of the data is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;

(b) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or

(c) he or she has objected to processing pursuant to Article 19(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

2. (…)

3. Where processing of personal data has been restricted under paragraph 1, such data may, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest.

4. A data subject who obtained the restriction of processing pursuant to paragraph 1 (…) shall be informed by the controller before the restriction of processing is lifted.

5. (…)

5a. [The rights provided for in this Article do not apply when data are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1a) are met.].

	Article 17b *Notification obligation regarding rectification, erasure or restriction* The controller shall communicate any rectification, erasure or restriction of processing carried out in accordance with Articles 16, 17(1) and 17a to each recipient to whom the data have been disclosed, unless this proves impossible or involves a disproportionate effort.	PL zgłaszała uwagę, że zakres art. 17b jest zbyt szeroki ze względu na zbyt szeroką definicję odbiorcy (recipient). Ta definicja została teraz jednak zawężona, a zatem uwaga PL nie jest już aktualna.

Article 18 **Right to data portability** **1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.** **2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.** **3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination**	*Article 18* *Right to data portability* 1. (…) 2. Where the data subject has provided personal data and the processing, (…) based on consent or on a contract, is carried on in an automated processing system provided by an information society service, the data subject shall have the right to withdraw these data in a form which permits the data subject to transmit them into another automated processing system without hindrance from the controller from whom the personal data are withdrawn . 2a. The right referred to in paragraph 2 shall be without prejudice to intellectual property rights. [3. The Commission may specify (…) the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).] 4. [The rights provided for in this Article do not apply when data are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1a) are met .]	Usunięto (zawarty w art. 15)	PL nie popierała szczególnie prawa do przenoszenia danych ale też mu się nie sprzeciwiała. W naszej ocenie jest to prawo w większym stopniu dotyczące prawa konkurencji niż ochrony danych osobowych. W ocenie PL dodanie ust. 2 a nie wydaje się właściwym rozwiązaniem, ze względu na niedookreślony charakter pojęcia „prawa własności intelektualnej”, który może wywoływać spory na tle czy dana forma danych może naruszać czyjeś prawa własności intelektualnej. Z tego względu właściwszym wydaje się uzupełnienie tego artykułu, że chodzi o dane w formie surowej, nieprzetworzonej. Z tego względu PL zaproponuje uzupełnienie w ust. 2 po słowie „data” określeniem „in non-aggregated and/or non-modified form”, co jest lepszym rozwiązaniem niż proponowany ustęp 2a. Należy jednocześnie rozważyć, czy w każdym przypadku będzie to możliwe i ewentualnie dopuścić przekazanie danych w stanie, w jakim się aktualnie znajdują, jeżeli będzie to wygodniejsze dla administratora – nie byłoby celowe ustanawianie obowiązku doprowadzania danych do stanu wyjściowego w każdym przypadku. Lub też można zaproponować dodanie zapisu jak np.: “These data shall be transmitted in non-modified form or in

procedure referred to in Article 87(2).			the form that is the most convenient to the controller".
Article 19 **Right to object** **1. The data subject shall have the right to object, on grounds relating to their particular situation, at any time to the processing of personal data which is based on points (d), (e) and (f) of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.** **2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object free of charge to the processing of their personal data for such marketing. This right shall be explicitly offered to the data subject in an intelligible manner and shall be clearly distinguishable from other information.** **3. Where an objection is upheld pursuant to paragraphs 1 and 2, the controller shall no longer use or otherwise process the personal data concerned.**	*Article 19* *Right to object* 1. The data subject shall have the right to object, on reasoned grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her which is based on point (…) (f) of Article 6(1); the personal data shall no longer be processed unless the controller demonstrates (…) legitimate grounds for the processing which override the interests or (…) rights and freedoms of the data subject. 1a. (…) Where an objection is upheld pursuant to paragraph 1 (…), the controller shall no longer (…)process the personal data concerned except for the establishment, exercise or defence of legal claims. 2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object (…)at any time to the processing of personal data concerning him or her for such marketing. This right shall be explicitly brought to the attention of the data subject (…) and shall be presented clearly and separately from any other information. 2a. Where the data subject objects to the processing for direct marketing	Article 19 Right to object 1. The data subject shall have the right to object~~, on grounds relating to their particular situation,~~ at any time to the processing of personal data which is based on points (d) *and* (e) ~~*and (f)*~~ of Article 6(1), unless the controller demonstrates compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject. 2. Where *the processing of* personal data ~~*is are processed for direct marketing purposes is based on points (d), (e) and (f) of Article 6(1)*~~, the data subject shall have *at any time and without any further justification,* the right to object free of charge *in general or for any particular purpose* to the processing of their personal data ~~*for such marketing. This right shall be explicitly offered to the data subject in an intelligible manner and shall be clearly distinguishable from other information*~~. *2a.* The ~~*This*~~ right *referred to in paragraph 2*	PL wnioskowała o doprecyzwanie terminu: *„compelling legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject.*". PL poparła poprawki LIBE wzmacniające prawo osoby do wniesienia sprzeciwu wobec przetwarzania jej danych osobowych (np. poprzez wykreślenie, że prawo to przysługuje jedynie „z przyczyn dotyczących jego/jej szczególnej sytuacji", czy poprzez wzmocnienie obowiązku informacyjnego o prawie do sprzeciwu przysługującego podmiotowi danych);

	purposes, the personal data shall no longer be processed for such purposes. 3. (...) 4. [The rights provided for in this Article do not apply to personal data which are processed only for historical, statistical, or scientific purposes and the conditions in Article 83(1A) are met].	shall be explicitly offered to the data subject in an intelligible manner *and form, using clear and plain language, in particular if addressed specifically to a child,* and shall be clearly distinguishable from other information. *2b. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the right to object may be exercised by automated means using a technical standard which allows the data subject to clearly express his or her wishes.* 3. Where an objection is upheld pursuant to paragraphs 1 and 2, the controller shall no longer use or otherwise process the personal data concerned *for the purposes determined in the objection*.	
Article 20 **Measures based on profiling** **1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to**	*Article 20* ***Profiling*** 1. Every data subject shall have the right not to be subject to a decision based solely on profiling *which produces legal effects* concerning him or her or severely affects him or her unless such processing:	Article 20 ~~*Measures based on*~~ Profiling 1. *Without prejudice to the provisions in Article 6 e*very natural person shall have the right ~~*not to be subject*~~ *to object* to ~~*a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural*~~	PL zgłaszała zastrzeżenie analityczne do art. 20 wskazując na trudne w interpretacji pojęcia „significantly/adversely/severely” przed „effect”. Ust. 3 – PL zgłaszała zastrzeżenia analityczne do ust. 3 propozycji KE i wnioskowała o wykreślenie słowa “solely”. Nowy zapis ust. 3 zaproponowany przez PREZ został przez PL poparty.

evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour. **2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing:** **(a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or** **(b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or** **(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.**	(a) is carried out in the course of the entering into, or performance of, a contract between the data subject and a data controller and suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the rights of the data subject to obtain human intervention on the part of the controller, to express his or her point of view, and to contest the decision; or (b) is (…) authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's legitimate interests; or (c) is based on the data subject's explicit consent (…). 2. (…) 3. Profiling shall not (…) be based on special categories of personal data referred to in Article 9(1), unless Article 9(2) applies and suitable measures to safeguard the data subject's legitimate interests are in place. (c) is based on the data subject's explicit consent (…). 2. (…) 3. Profiling shall not (…) be based on special categories of personal data referred	~~*person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.*~~ *profiling* ***in accordance with Article 19. The data subject shall be informed about the right to object to profiling in a highly visible manner.*** 2. Subject to the other provisions of this Regulation, a person may be subjected to ~~*a measure of the kind referred to in paragraph 1*~~ *profiling which leads to measures producing legal effects concerning the data subject or does similarly significantly affect the interests, rights or freedoms of the concerned data subject* only if the processing: *(a) is* ~~carried out in the course of~~ necessary for *the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied*, provided that ~~or where~~ *suitable measures to safeguard the data subject's legitimate interests have been adduced*~~, such as the right to obtain human intervention~~*;* or (b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; (c) is based on the data subject's consent,	Poza tym co do zasady w opinii PL przepis o profilowaniu w tekście Rady dobrze waży interesy przedsiębiorców wykorzystujących techniki profilowania z prawami podmiotów danych. PL popiera profilowanie niedyskryminujące, poinformowane, któremu można się sprzeciwić. MAiC popiera poprawki LIBE, które w opinii MAiC lepiej zabezpieczają interesy podmiotów danych, niż te dyskutowane w Radzie UE (np. zakazuje profilowania opartego na danych wrażliwych jak np. rasa czy wyznanie religijne, które ma skutek dyskryminujący, a informacja o możliwości sprzeciwienia się profilowaniu musi być widoczna). W wersji LIBE, w przypadku profilowania, które wywołuje skutek prawny albo znacząco wpływa na podmiot danych, LIBE wprowadziło gwarancję, iż nie będzie ono w pełni zautomatyzowane lecz będzie w nim występował czynnik ludzki, co MAiC zdecydowanie poparło.

3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9. **4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.** **5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.**	to in Article 9(1), unless Article 9(2) applies and suitable measures to safeguard the data subject's legitimate interests are in place. 4. (…) 5. (…)	subject to the conditions laid down in Article 7 and to suitable safeguards. 3. ***Profiling that has the effect of discriminating against individuals on the basis of race or ethnic origin, political opinions, religion or beliefs, trade union membership, sexual orientation or gender identity, or that results in measures which have such effect, shall be prohibited.*** *The controller shall implement effective protection against possible discrimination resulting from profiling. Profiling* shall not be based solely on the special categories of personal data referred to in Article 9. ~~*4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.*~~ 5. *Profiling which leads to measures producing legal effects concerning the data subject or does similarly significantly affect the interests, rights or freedoms of the concerned data subject shall not be based solely or predominantly on automated processing and shall include human assessment, including an explanation of the decision reached after such an assessment.* The ~~*Commission shall be empowered to adopt delegated acts in accordance with*~~

		~~*Article 86 for the purpose of further specifying the criteria and conditions for*~~ suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2 *shall include the right to obtain human assessment and an explanation of the decision reached after such assessment*. *5a. The European Data Protection Board shall be entrusted with the task of issuing guidelines, recommendations and best practices in accordance with Article 66 paragraph 1(b) for further specifying the criteria and conditions for profiling pursuant to paragraph 2.*

Article 21 **Restrictions** **1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in points (a) to (e) of Article 5 and Articles 11 to 20 and Article 32, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard:** **(a) public security;** **(b) the prevention, investigation, detection and prosecution of criminal offences;** **(c) other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters and the protection of market stability and integrity;** **(d) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;** **(e) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of**	Article 21 Restrictions 1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in points (a) to (e) of Article 5 and Articles 12 to 20 and Article 32, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard: (aa) national security; (ab) defence; (a) public security; (b) the prevention, investigation, detection and prosecution of criminal offences and, for these purposes, the maintenance of public order, or the execution of criminal penalties; (c) other important objectives of general public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including, monetary, budgetary and taxation matters and the protection of market stability and integrity; (d) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;	Article 21 Restrictions 1. Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights ~~*provided for*~~ in ~~*points (a) to (e) of Article 5 and*~~ Articles 11 to *19* ~~*20*~~ and Article 32, when such a restriction ~~*constitutes*~~ *meets a clearly defined objective of public interest, respects the essence of the right to protection of personal data, is proportionate to the legitimate aim pursued and respects the fundamental rights and interests of the data subject and is* a necessary and proportionate measure in a democratic society to safeguard: (a) public security; (b) the prevention, investigation, detection and prosecution of criminal offences; (c) ~~*other public interests of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and*~~ taxation matters ~~*and the protection of market stability and integrity*~~; (d) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; (e) a monitoring, inspection or regulatory	PL wnioskowała o wykreślenie z ust. 1 odniesienia do lit (a) – (e) art. 5., które są w naszej opinii prawami podstawowymi i nie powinny podlegać ograniczeniom.

official authority in cases referred to in (a), (b), (c) and (d); **(f) the protection of the data subject or the rights and freedoms of others.** **2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least as to the objectives to be pursued by the processing and the determination of the controller.**	(e) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (a), (b), (c) and (d); (f) the protection of the data subject or the rights and freedoms of others. 2. Any legislative measure referred to in paragraph 1 shall contain specific provisions at least as to the purposes of the processing or categories of processing, the categories of personal data, the scope of the restrictions introduced, the specification of the controller or categories of controllers and the applicable safeguards taking into account of the nature, scope and purposes of the processing and the risks for the rights and freedoms of data subjects.	function *in the framework of ~~connected, even occasionally, with~~* the exercise of a *competent public ~~official~~* authority in cases referred to in (a), (b), (c) and (d); (f) the protection of the data subject or the rights and freedoms of others. 2. In particular, any legislative measure referred to in paragraph 1 *must be necessary and proportionate in a democratic society and* shall contain specific provisions at least as to: *(a)* the objectives to be pursued by the processing *~~and~~*; *(b)* the determination of the controller; *(c) the specific purposes and means of processing;* *(d) the safeguards to prevent abuse or unlawful access or transfer;* *(e) the right of data subjects to be informed about the restriction.* *2a. Legislative measures referred to in paragraph 1 shall neither permit nor oblige private controllers to retain data additional to those strictly necessary for the original purpose.*

Article 22 **Responsibility of the controller** **1. The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.** **2. The measures provided for in paragraph 1 shall in particular include:** **(a) keeping the documentation pursuant to Article 28;** **(b) implementing the data security requirements laid down in Article 30;** **(c) performing a data protection impact assessment pursuant to Article 33;** **(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);** **(e) designating a data protection officer pursuant to Article 35(1).** **3. The controller shall implement mechanisms to ensure the verification of the effectiveness of the measures**	*Article 22* *Obligations of the controller* 1. Taking into account the nature, context, scope and purposes of the processing and the risks for the rights and freedoms of data subjects, the controller shall (…) implement appropriate measures and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation. 2. (…) 2a. Where proportionate in relation to the processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller. 2b. Compliance with the obligations of the controller may be demonstrated by means of adherence to codes of conduct pursuant to Article 38 or a certification mechanism pursuant to Article 39 (….). 3. (…) 4. (…)	Article 22 Responsibility *and accountability* of the controller 1. The controller shall adopt *appropriate* policies and implement appropriate *and demonstrable technical and organizational* measures to ensure and be able to demonstrate *in a transparent manner* that the processing of personal data is performed in compliance with this Regulation, *having regard to the state of the art, the nature of personal data processing, the context, scope and purposes of the processing, the risks for the rights and freedoms of the data subjects and the type of the organization, both at the time of the determination of the means for processing and at the time of the processing itself*. *1a. Having regard to the state of the art and the cost of implementation, the controller shall take all reasonable steps to implement compliance policies and procedures that persistently respect the autonomous choices of data subjects. These compliance policies shall be reviewed at least every two years and updated where necessary.* ~~*2. The measures provided for in paragraph 1 shall in particular include:*~~ ~~*(a) keeping the documentation pursuant to Article 28;*~~	Ust. 1 - pojęcie “rights and freedoms” jest zbyt szerokie, może dotyczyć sfer całkowicie niezwiązanych z danymi osobowymi, być może należy je zawęzić (np. do „privacy”), jest to uwaga także do innych odniesień do „rights and freedoms” w projekcie rozporządzenia. PL opowiedziała się za przywróceniem ustępu 2, jako pomocnego do wyjaśnienia co znaczą „appropriate measures”. Zmiana ta nie zmierza do poszerzenia zakresu obowiązków administratora danych, ponieważ odwołuje się do wymogów i procedur, które zostały przewidziane w innych przepisach projektowanego rozporządzenia. PL poparła wprowadzenie w art. 22 ustępu 2a, jako przykładu zastosowania zasady rozliczalności („accountability”). PL poparła wprowadzenie w art. 22 ustępu 2b i odniesienia do certyfikacji.

referred to in paragraphs 1 and 2. If proportionate, this verification shall be carried out by independent internal or external auditors.	~~*(b) implementing the data security requirements laid down in Article 30;*~~
	~~*(c) performing a data protection impact assessment pursuant to Article 33;*~~
	~~*(d) complying with the requirements for prior authorisation or prior consultation of the supervisory authority pursuant to Article 34(1) and (2);*~~
	~~*(e) designating a data protection officer pursuant to Article 35(1);*~~
4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized-enterprises.	3. The controller shall ~~*implement mechanisms to ensure the verification of*~~ *be able to demonstrate* the *adequacy and* effectiveness of the measures referred to in paragraphs 1 and 2. ~~*If proportionate, this verification shall be carried out by independent internal or external auditors.*~~ *Any regular general reports of the activities of the controller, such as the obligatory reports by publicly traded companies, shall contain a summary description of the policies and measures referred to in paragraph 1.*
	3a. The controller shall have the right to transmit personal data inside the Union within the group of undertakings the controller is part of, where such processing is necessary for legitimate internal administrative purposes between connected business areas of the group of undertakings and an adequate level of data protection as

well as the interests of the data subjects are safeguarded by internal data protection provisions or equivalent codes of conduct ass referred to in Article 38.

~~*4. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures referred to in paragraph 1 other than those already referred to in paragraph 2, the conditions for the verification and auditing mechanisms referred to in paragraph 3 and as regards the criteria for proportionality under paragraph 3, and considering specific measures for micro, small and medium-sized enterprises.*~~

Article 23 **Data protection by design and by default** **1. Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.** **2. The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.** **3. The Commission shall be empowered to adopt delegated acts in**	*Article 23* *Data protection by design and by default* 1. Having regard to available technology and the cost of implementation and taking account of the risks for rights and freedoms of individuals posed by the nature, scope and purpose of the processing, the controller shall (…), implement (…) technical and organisational measures appropriate to the processing activity being carried on and its objectives, including the use of pseudonymous data, in such a way that the processing will meet the requirements of this Regulation and (…) protect the rights of (…) data subjects. 2. The controller shall implement appropriate measures for ensuring that, by default, only (…) personal data (…) which are not excessive for each specific purpose of the processing are processed; this applies to the amount of (…) data collected, the period of their storage and their accessibility. Where the purpose of the processing is not intended to provide the public with information, those mechanisms shall ensure that by default personal data are not made accessible without human intervention to an indefinite number of individuals. 2a. The controller may demonstrate compliance with the requirements set out in paragraphs 1 and 2 by means of a certification mechanism pursuant to Article	Article 23 Data protection by design and by default 1. Having regard to the state of the art*, current technical knowledge, ~~and the cost of implementation~~, international best practices and the risks represented by the data processing*, the controller *and the processor, if any,* shall, both at the time of the determination of the *purposes and* means for processing and at the time of the processing itself, implement appropriate *and proportionate* technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject*, in particular with regard to the principles laid out in Article 5. Data protection by design shall have particular regard to the entire lifecycle management of personal data from collection to processing to deletion, systematically focusing on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data. Where the controller has carried out a data protection impact assessment pursuant to Article 33, the results shall be taken into account when developing those measures and procedures*. *1a. In order to foster its widespread implementation in different economic sectors, data protection by design shall be a*	Ust. 1 – PL wnioskowała o zamianę pojęcia „state of the art" na „aktualny poziom wiedzy technicznej". Wymóg stosowania najnowszych osiągnięć technicznych, wiązałby się z nadmiernymi kosztami dla administratorów danych. **Tą uwagę uwzględniono w tekście PREZ**. PL poparła wprowadzenie w art. 23 ustępu 2a - rozwiązanie to może zachęcić administratorów danych do certyfikacji i wzmocnić zasadę rozliczalności. PL zada pytanie jaka jest intencja umieszczenia w art. 23 ust. 2 „without human intervention". W naszej ocenie ustęp ten powinien zostać doprecyzowany, tak aby dotyczył podmiotu danych. W związku z tym jesteśmy za doprecyzowaniem tego zwrotu na „without data subject intervention".

accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services. **4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).**	39. 3. (…) 4. (…)	*prerequisite for public procurement tenders according to the Directive of the European Parliament and of the Council on public procurement as well as according to the Directive of the European Parliament and of the Council on procurement by entities operating in the water, energy, transport and postal services sector (Utilities Directive).* 2. The controller shall *ensure* ~~*implement mechanisms for ensuring*~~ that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected*,* ~~*or*~~ retained *or disseminated* beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals *and that data subjects are able to control the distribution of their personal data*. ~~*3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of specifying any further criteria and requirements for appropriate measures and mechanisms referred to in paragraph 1 and 2, in particular for data protection by design requirements applicable across sectors, products and services.*~~

		~~*4. The Commission may lay down technical standards for the requirements laid down in paragraph 1 and 2. Those implementing acts shall be adopted, after requesting an opinion by the European Data Protection Board, in accordance with the examination procedure referred to in Article 87(2).*~~	
Article 24 **Joint controllers** **Where a controller determines the purposes, conditions and means of the processing of personal data jointly with others, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them.**	Article 24 Joint controllers 1. (…) Joint controllers shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the (…) exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 14 and 14a, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. 2. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the (…) controllers unless the data subject has been informed in a transparent manner which of the joint controllers is responsible.	Article 24 Joint controllers Where ~~a~~ *several* controller*s jointly* determine~~s~~ the purpose~~s~~*~~, conditions~~* and means of the processing of personal data ~~*jointly with others*~~, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them. *The arrangement shall duly reflect the joint controllers' respective effective roles and relationships vis-à-vis data subjects, and the essence of the arrangement shall be made available for the data subject. In case of unclarity of the responsibility, the controllers shall be jointly and severally liable.*	ust. 2 - PL zaproponowała dodanie na końcu art. 24 ust. 2 zdania umożliwiającego umówienie się pomiędzy współadministratorami co do współadministratora odpowiedzialnego i poinformowanie o tym podmiotu danych. **Tą uwagę uwzględniono w tekście PREZ**.

Article 25 **Representatives of controllers not established in the Union** **1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union.** **2. This obligation shall not apply to:** **(a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or** **(b) an enterprise employing fewer than 250 persons; or** **(c) a public authority or body; or** **(d) a controller offering only occasionally goods or services to data subjects residing in the Union.** **3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside.**	Article 25 Representatives of controllers not established in the Union 1. Where Article 3(2) applies, the controller shall designate in writing a representative in the Union. 2. This obligation shall not apply to: (a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or (b) an enterprise employing fewer than 250 persons unless the processing it carries out involves specific risks for the rights and freedoms of data subjects, having regard to the nature, scope and purposes of the processing; or (c) a public authority or body. (d) (…) 3. The representative shall be established in one of those Member States where the data subjects whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, reside. 3a. The representative shall be mandated by the controller to be addressed in addition to or instead of the controller	Article 25 Representatives of controllers not established in the Union 1. In the situation referred to in Article 3(2), the controller shall designate a representative in the Union. 2. This obligation shall not apply to: (a) a controller established in a third country where the Commission has decided that the third country ensures an adequate level of protection in accordance with Article 41; or (b) ~~*an enterprise employing fewer than 250 persons*~~ *a controller processing personal data which relates to less than 5000 data subjects during any consecutive 12-month period and not processing special categories of personal data as referred to in Article 9(1), location data or data on children or employees in large-scale filing systems*; or (c) a public authority or body; or (d) a controller ~~*offering*~~ only occasionally *offering* goods or services to data subjects ~~*residing*~~ in the Union*, unless the processing of personal data concerns special categories of personal data as referred to in Article 9(1), location data or data on children or employees in large-scale filing systems*. 3. The representative shall be established in	Ust. 2 lit. (a) – to wyłaczenie dla administratorów z krajów trzecich o adekwatnym poziomie ODO z obowiązku posiadania przedstawiciela wydaje się nieuzasadnione. ust. 2 lit. b -sugerowaliśmy rozważenie czy kryterium 250 osób nie powinno zostać zastąpione kryterium liczby przetwarzanych rekordów. W naszej ocenie takie rozwiązanie odda ideę proporcjonalności i będzie się wpisywać w zasadę „risk based approach". Do art. 25 ust. 2 lit. b odnosi się także wcześniejsza uwaga PL, czy nie należy zamiast „rights and freedoms" użyć pojęcia „privacy". PL zgłosiła także propozycję, aby pojęcie „high risks" doprecyzować jako „high risks as specified in art. 33 point 2 of this Regulation". Tak, aby to pojęcie nie budziło wątpliwości wśród administratorów danych.

4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.	by, in particular, supervisory authorities and data subjects, on all issues related to the processing of personal data, for the purposes of ensuring compliance with this Regulation. 4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.	one of those Member States where ~~*the data subjects whose personal data are processed in relation to*~~ the offering of goods or services to *the data subjects* ~~*them*~~, or ~~*to*~~ *the monitoring of them*, *take place* ~~*reside*~~. 4. The designation of a representative by the controller shall be without prejudice to legal actions which could be initiated against the controller itself.

Article 26 **Processor** **1. Where a processing operation is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures.** **2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller and stipulating in particular that the processor shall:** **(a) act only on instructions from the controller, in particular, where the transfer of the personal data used is prohibited;** **(b) employ only staff who have committed themselves to confidentiality or are under a statutory**	Article 26 Processor 1. (…)The controller shall <u>use only</u> processor<u>s</u> providing sufficient guarantees to implement appropriate technical and organisational measures (…) in such a way that the processing will meet the requirements of this Regulation (…). 1a. The provision of sufficient guarantees referred to in paragraph 1 may be demonstrated by means of adherence to codes of conduct pursuant to Article 38 or a certification mechanism pursuant to Article 39. 2. The carrying out of processing by a processor shall be governed by a contract setting out the subject-matter and duration of the contract, the nature and purpose of the processing, the type of personal data and categories of data subjects or other legal act binding the processor to the controller and stipulating in particular that the processor shall: (a) process the personal data only on instructions from the controller (…), unless required to do so by Union or Member State law to which the processor is subject <u>and in such a case, the processor shall notify the controller unless the law prohibits such notification</u>;	Article 26 Processor 1. Where ~~*a*~~ processing ~~*operation*~~ is to be carried out on behalf of a controller, the controller shall choose a processor providing sufficient guarantees to implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject, in particular in respect of the technical security measures and organizational measures governing the processing to be carried out and shall ensure compliance with those measures. 2. The carrying out of processing by a processor shall be governed by a contract or other legal act binding the processor to the controller. ~~*and stipulating in particular that*~~ *The controller and the processor shall be free to determine respective roles and tasks with respect to the requirements of this Regulation, and shall provide that* the processor shall: (a) ~~*act*~~ *process personal data* only on instructions from the controller, ~~*in particular, where the transfer of the personal data used is prohibited*~~ *unless otherwise required by Union law or Member State law*;	ust. 1a - PL poparła dodanie odniesienia do certyfikacji. ust. 2 - PL opowiedziała się przeciwko zwolnieniu z obowiązku zawierania umów o powierzenie przetwarzania podmiotów z tej samej grupy kapitałowej czyli poparła usunięcie <u>Where the processor is not part of the same group of undertakings as the controller</u>. **Ta uwaga została uwzględniona.** Odnośnie ust. 3, PL zwróciła uwagę, iż zgodnie z polskim prawem formą ekwiwalentną do formy pisemnej jest forma elektroniczna z kwalifikowanym podpisem elektronicznym, która wciąż nie jest powszechna wśród przedsiębiorców. W związku z tym jesteśmy za tym, aby wyraźnie dopuścić do formy pisemnej, jako równoważną, formę elektroniczną. **Ta uwaga została uwzględniona.** PL prosiła o uzasadnienie użycia słowa „non-legible". PL opowiedziała się za usunięciem „or other non-legible form which is capable of being converted into a legible form" i pozostawieniem odniesienia tylko do formy pisemnej i elektronicznej.

obligation of confidentiality; **(c) take all required measures pursuant to Article 30;** **(d) enlist another processor only with the prior permission of the controller;** **(e) insofar as this is possible given the nature of the processing, create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;** **(f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34;** **(g) hand over all results to the controller after the end of the processing and not process the personal data otherwise;** **(h) make available to the controller and the supervisory authority all information necessary to control compliance with the obligations laid down in this Article.** **3. The controller and the processor shall document in writing the**	(b) (…) (c) take all (…) measures required pursuant to Article 30; (d) determine the conditions for enlisting another processor(…); (e) as far as (…) possible, taking into account the nature of the processing, assist the controller in responding to requests for exercising the data subject's rights laid down in Chapter III; (f) determine the extent to which the controller is to be assisted in ensuring compliance with the obligations pursuant to Articles 30 to 34; (g) return the personal data after the completion of the processing specified in the contract or other legal act, unless there is a requirement to store the data under Union or Member State law to which the processor is subject; (h) make available to the controller (…) all information necessary to demonstrate compliance with the obligations laid down in this Article. 3. The contract referred to in paragraph 2 shall be in writing or in an electronic or other non-legible form which is capable of being converted into a legible form.	(b) employ only staff who have committed themselves to confidentiality or are under a statutory obligation of confidentiality; (c) take all required measures pursuant to Article 30; (d) *determine the conditions for* enlist*ing* another processor only with the prior permission of the controller*, unless otherwise determined*. (e) insofar as this is possible given the nature of the processing, create in agreement with the controller the ~~*necessary*~~ *appropriate and relevant* technical and organisational requirements for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III; (f) assist the controller in ensuring compliance with the obligations pursuant to Articles 30 to 34*, taking into account the nature of processing and the information available to the processor*; (g) *return* ~~*hand over*~~ all results to the controller after the end of the processing*,* ~~*and*~~ not process the personal data otherwise *and delete existing copies unless Union or Member State law requires storage of the data*; (h) make available to the controller ~~*and the*~~

controller's instructions and the processor's obligations referred to in paragraph 2. **4. If a processor processes personal data other than as instructed by the controller, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24.** **5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular for the purposes of control and reporting.**	4. (…) 5. (…)	~~*supervisory authority*~~ all information necessary to *demonstrate* ~~*control*~~ compliance with the obligations laid down in this Article *and allow on-site inspections*; 3. The controller and the processor shall document in writing the controller's instructions and the processor's obligations referred to in paragraph 2. *3a. The sufficient guarantees referred to in paragraph 1 may be demonstrated by adherence to codes of conduct or certification mechanisms pursuant to Articles 38 or 39 of this Regulation.* 4. If a processor processes personal data other than as instructed by the controller *or becomes the determining party in relation to the purposes and means of data processing*, the processor shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers laid down in Article 24. ~~*5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the responsibilities, duties and tasks in relation to a processor in line with paragraph 1, and conditions which allow facilitating the processing of personal data within a group of undertakings, in particular*~~

~~*for the purposes of control and reporting.*~~

Article 27 **Processing under the authority of the controller and processor** **The processor and any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless required to do so by Union or Member State law.**	*Article 27* *Processing under the authority of the controller and processor* (…)	Article 27 Processing under the authority of the controller and processor The processor and any person acting under the authority of the controller or of the processor who has access to personal data shall not process them except on instructions from the controller, unless required to do so by Union or Member State law.	Usunięto przepis z uwagi na brak wartości dodanej w relacji do Art. 26 §2.
Article 28 **Documentation** **1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.** **2. The documentation shall contain at least the following information:** **(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;** **(b) the name and contact details of the data protection officer, if any;**	*Article 28* *Records of categories of personal data processing activities* 1. Each controller (…)and, if any, the controller's representative, shall maintain a record of all categories of personal data processing activities under its responsibility. This record shall contain (…) the following information: (a) the name and contact details of the controller and any joint controller (…), controller's representative and data protection officer, if any; (b) (…) (c) the purposes of the processing, including the legitimate interest when the processing is based on Article 6(1)(f);	Article 28 Documentation 1. Each controller and processor ~~*and, if any, the controller's representative,*~~ shall maintain *regularly updated* documentation necessary to fulfill the requirements laid down in this Regulation. 2. In addition, each controller and processor shall maintain documentation of the following information: (a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any; (b) the name and contact details of the data protection officer, if any; (c) the name and contact details of the	Ust. 1 – PL sugerowała wprowadzanie zapisu wskazującego, że dokumentacja może być prowadzona w formie elektronicznej. **Ta uwaga została uwzględniona w ust. 3a.** W ust. 2a PL proponowała dodanie, jako obowiązkowego, rekordu dotyczącego „the (…) regular categories of recipients of the personal data". Chodzi nam o to, aby procesor był zobowiązany prowadzić listę subprocesorów, taka informacja jest niezwykle istotna z punktu widzenia zapewnienia kontroli nad danymi osobowymi. W ust. 2a lit. d, PL wniesie o dodanie na końcu zdania "provided that the proccessor is transferring such data", taka by doprecyzować, że chodzi o dane,

(c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1); **(d) a description of categories of data subjects and of the categories of personal data relating to them;** **(e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;** **(f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;** **(g) a general indication of the time limits for erasure of the different categories of data;** **(h) the description of the mechanisms referred to in Article 22(3).** **3. The controller and the processor and, if any, the controller's representative, shall make the**	(d) a description of categories of data subjects and of the categories of personal data relating to them; (e) the (…) categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries; (f) where applicable, <u>the categories of</u> transfers of <u>personal</u> data to a third country or an international organisation (…); (g) <u>where possible, the envisaged</u> time limits for erasure of the different categories of data. (h) (…) <u>2a.</u> Each <u>processor shall maintain a record of all categories of personal data processing activities carried out on behalf of a controller, containing:</u> <u>(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and of the controller's representative, if any;</u> (b) the name and contact details of the data protection officer, if any; (c) the categories of processing carried out on behalf of each controller; (d) where applicable, the categories of	controllers to whom personal data are disclosed, if any;	które transferuje procesor. ust. 4 - kryterium to powinno zostać oparte na ilości rekordów a nie liczbie pracowników. Wyrażone w art. 28 przepisy nakładające na administratora i oraz ewentualnie przedstawicieli administratora obowiązek prowadzenia dokumentacji nie powinien skutkować w praktyce obowiązkiem prowadzenia podwójnej dokumentacji (w przypadku, gdy na podmocie ciąży obowiązek dokumentacyjny wynikający z innych przepisów prawa).

documentation available, on request, to the supervisory authority.	transfers of personal data to a third country or an international organisation .
4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors:	3a. The records referred to in paragraphs 1 and 2a shall be in writing or in an electronic or other non-legible form which is capable of being converted into a legible form.
(a) a natural person processing personal data without a commercial interest; or	3. On request, the controller and the processor and, if any, the controller's representative, shall make the record available (…) to the supervisory authority.
(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.	4. The obligations referred to in paragraphs 1 and 2a shall not apply to:
5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.	(a) (…) (b) an enterprise or a body employing fewer than 250 persons, unless the processing it carries out involves specific risks for the rights and freedoms of data subjects, having regard to the nature, scope and purposes of the processing; or (c) categories of processing activities which by virtue of the nature, scope or purposes of the processing are unlikely to represent specific risks for the rights and freedoms of data subjects.
6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	5. (…) 6. (…)

Article 29 **Co-operation with the supervisory authority** **1. The controller and the processor and, if any, the representative of the controller, shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph.** **2. In response to the supervisory authority's exercise of its powers under Article 53(2), the controller and the**	*Article 29* *Co-operation with the supervisory authority* (…)	Article 29 Co-operation with the supervisory authority 1. The controller and, *if any,* the processor and~~*, if any,*~~ the representative of the controller, shall co-operate, on request, with the supervisory authority in the performance of its duties, in particular by providing the information referred to in point (a) of Article 53(2) and by granting access as provided in point (b) of that paragraph. 2. In response to the supervisory authority's exercise of its powers under Article 53(2),	Deleted: this article was superfluous in that controllers and processors obviously had a legal obligation to comply with requests made by data protection authorities under this Regulation

processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.		the controller and the processor shall reply to the supervisory authority within a reasonable period to be specified by the supervisory authority. The reply shall include a description of the measures taken and the results achieved, in response to the remarks of the supervisory authority.	
Article 30 **Security of processing** **1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.** **2. The controller and the processor shall, following an evaluation of the risks, take the measures referred to in paragraph 1 to protect personal data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorised disclosure, dissemination or access, or alteration of personal data.** **3. The Commission shall be empowered to adopt delegated acts in**	SECTION 2 DATA SECURITY *Article 30* *Security of processing* 1. Having regard to available technology and the costs of implementation and taking into account the nature, context, scope and purposes of the processing and the risks for the rights and freedoms of data subjects, the controller and the processor shall implement appropriate technical and organisational measures, including the use of pseudonymous data to ensure a level of security appropriate to these risks. 2. (…) 2a. The controller and processor may demonstrate compliance with the requirements set out in paragraph 1 by means of adherence to codes of conduct pursuant to Article 38 or a certification mechanism pursuant to Article 39. 2b. The controller and processor shall take steps to ensure that any person acting	Article 30 Security of processing 1. The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing ~~*and the nature of the personal data to be protected*~~, *taking into account the results of a data protection impact assessment pursuant to Article 33,* having regard to the state of the art and the costs of their implementation. *1a. Having regard to the state of the art and the cost of implementation, such a security policy shall include:* *(a) the ability to ensure that the integrity of the personal data is validated;* *(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing*	PL poparła wprowadzenie w ust.1 odniesienia do „available technology" oraz wprowadzenie odniesienia do procesora w ust. 2a. PL poparła także zmiany wprowadzone w ust. 2b.

accordance with Article 86 for the purpose of further specifying the criteria and conditions for the technical and organisational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, unless paragraph 4 applies. **4. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1 and 2 to various situations, in particular to:** **(a) prevent any unauthorised access to personal data;** **(b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;** **(c) ensure the verification of the lawfulness of processing operations.** **Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).**	under the authority of the controller or the processor who has access to personal data shall not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law. 3. (…) 4. (…)	*personal data;* *(c) the ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident that impacts the availability, integrity and confidentiality of information systems and services;* *(d) in the case of sensitive personal data processing according to Articles 8 and 9, additional security measures to ensure situational awareness of risks and the ability to take preventive, corrective and mitigating action in near real time against vulnerabilities or incidents detected that could pose a risk to the data;* *(e) a process for regularly testing, assessing and evaluating the effectiveness of security policies, procedures and plans put in place to ensure ongoing effectiveness.* 2. The ~~*controller and the processor*~~ *measures referred to in paragraph 1* shall~~,~~ ~~*following an evaluation of the risks, take the measures referred to in paragraph 1 to*~~ *at least:* *(a) ensure that personal data can be accessed only by authorised personnel for legally authorised purposes;* *(b)* protect personal data *stored or*

	transmitted against accidental or unlawful destruction, ~~*or*~~ accidental loss *or alteration, and unauthorised or unlawful storage,* ~~*and to prevent any unlawful forms of, in particular any unauthorised*~~ processing, *access or* disclosure, ~~*dissemination, or access*~~; and *(c) ensure the implementation of a security policy with respect to the processing* of personal data. 3. The *European Data Protection Board* ~~*Commission*~~ shall be *entrusted with the task* ~~*empowered to adopt delegated acts in accordance with Article 86 for the purpose*~~ of *issuing guidlines, recommendations and best practices in accordance with Article 66 paragraph 1(b)* ~~*further specifying the criteria and conditions*~~ for the technical and organizational measures referred to in paragraphs 1 and 2, including the determinations of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default, ~~*unless paragraph 4 applies*~~. ~~*4. The Commission may adopt, where necessary, implementing acts for specifying the requirements laid down in paragraphs 1*~~

	~~*and 2 to various situations, in particular to:*~~ ~~*(a) prevent any unauthorised access to personal data;*~~ ~~*(b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;*~~ ~~*(c) ensure the verification of the lawfulness of processing operations.*~~ ~~*Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).*~~

Article 31 **Notification of a personal data breach to the supervisory authority** **1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within 24 hours.** **2. Pursuant to point (f) of Article 26(2), the processor shall alert and inform the controller immediately after the establishment of a personal data breach.** **3. The notification referred to in paragraph 1 must at least:** **(a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned;** **(b) communicate the identity and contact details of the data protection officer or other contact point where**	*Article 31* *Notification of a personal data breach to the supervisory authority* 1. In the case of a personal data breach <u>which is likely to severely affect the rights and freedoms of data subjects</u>, the controller shall without undue delay and, where feasible, not later than <u>72</u> hours after having become aware of it, notify the personal data breach to the supervisory authority <u>competent in accordance with Article 51</u>. The notification to the supervisory authority shall be accompanied by a reasoned justification in cases where it is not made within <u>72</u> hours. 1a. The notification referred to in paragraph 1 shall not be required if a communication of the data subject is not required under Article 32(3)(a) and (b). 2. (…) The processor shall alert and inform the controller <u>without undue delay after becoming aware</u> of a personal data breach. 3. The notification referred to in paragraph 1 must at least: (a) describe the nature of the personal data breach including, <u>where possible and appropriate</u>, the categories and number of data subjects concerned and the categories	Article 31 Notification of a personal data breach to the supervisory authority 1. In the case of a personal data breach, the controller shall without undue delay ~~*and, where feasible, not later than 24 hours after having become aware of it,*~~ notify the personal data breach to the supervisory authority. The notification to the supervisory authority shall be accompanied by a reasoned justification *in cases of any delay* ~~*where it is not made within 24 hours*~~. 2. ~~*Pursuant to point (f) of Article 26(2),*~~ the processor shall alert and inform the controller *without undue delay* ~~*immediately*~~ after the establishment of a personal data breach. 3. The notification referred to in paragraph 1 must at least: (a) describe the nature of the personal data breach including the categories and number of data subjects concerned and the categories and number of data records concerned; (b) communicate the identity and contact	W zakresie art. 31 ust. 1, PL zajmie stanowisko, iż każde naruszenie danych osobowych niesie ze sobą negatywny skutek dla podmiotu danych. W ocenie PL zamiast „adversely" powinno zostać użyte pojęcie „significantly", tak, aby ograniczyć zakres zgłaszanych naruszeń tylko do tych, które rzeczywiście wpływają na sytuację podmiotu danych (**uwaga częściowo uwzględniona – pozostało severely effect**) natomiast pojęcie praw i wolności (rights and freedoms) podmiotu danych powinno zostać zastąpione pojęciem „privacy" (prywatność). Obecne sformułowanie jest niezwykle szerokie, przez co może skutkować zalewem nieistotnych zgłoszeń. Odnośnie art. 31 ust. 1a, PL zajęła stanowisko, iż pomimo podjęcia działań przewidzianych w art. 32 ust. 3 lit. b, administrator powinien powiadomić organ nadzoru o naruszeniu, tak aby mógł on ocenić czy administrator podjął właściwe działanie. W związku z tym PL wypowiedziała się przeciwko dodaniu ust. 1a w zaproponowanym brzmieniu. PL opowiedziała się za usunięciem art. 31 pkt 5 i 6, przewidujących delegację dla Komisji Europejskiej, uznając, iż taka delegacja wprowadza element niepewności dla administratora danych.

more information can be obtained; **(c) recommend measures to mitigate the possible adverse effects of the personal data breach;** **(d) describe the consequences of the personal data breach;** **(e) describe the measures proposed or taken by the controller to address the personal data breach.** **4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with this Article. The documentation shall only include the information necessary for that purpose.** **5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for establishing the data breach referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach.** **6. The Commission may lay down**	and approximate number of data records concerned; (b) communicate the identity and contact details of the data protection officer or other contact point where more information can be obtained; (c) (…) (d) describe the likely consequences of the personal data breach identified by the controller; (e) describe the measures taken or proposed to be taken by the controller to address the personal data breach; and (f) where appropriate, indicate measures to mitigate the possible adverse effects of the personal data breach. 3a. Where, and in so far as, it is not possible to provide the information referred to in paragraph 3 (d), (e) and (f) at the same time as the information referred to in points (a) and (b) of paragraph 3, the controller shall provide this information without undue further delay. 4. The controller shall document any personal data breaches referred to in paragraphs 1 and 2, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to	details of the data protection officer or other contact point where more information can be obtained; (c) recommend measures to mitigate the possible adverse effects of the personal data breach; (d) describe the consequences of the personal data breach; (e) describe the measures proposed or taken by the controller to address the personal data breach *and mitigate its effects*. *The information may, if necessary be provided in phases.* 4. The controller shall document any personal data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken. This documentation must *be sufficient to* enable the supervisory authority to verify compliance with this Article *and with Article 30*. The documentation shall only include the information necessary for that purpose. *4a. The supervisory authority shall keep a public register of the types of breaches notified.*

the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).	verify compliance with this Article. (…). 5. (…) [6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).]	5. The *European Data Protection Board* ~~*Commission*~~ shall be *entrusted with the task* ~~*empowered to adopt delegated acts in accordance with Article 86 for the purpose*~~ of *issuing guidelines, recommendations and best practices in accordance with Article 66 paragraph 1(b)* ~~*further specifying the criteria and requirements*~~ for establishing the data breach *and determining the undue delay* referred to in paragraphs 1 and 2 and for the particular circumstances in which a controller and a processor is required to notify the personal data breach. ~~*6. The Commission may lay down the standard format of such notification to the supervisory authority, the procedures applicable to the notification requirement and the form and the modalities for the documentation referred to in paragraph 4, including the time limits for erasure of the information contained therein. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).*~~

Article 32 **Communication of a personal data breach to the data subject** **1. When the personal data breach is likely to adversely affect the protection of the personal data or privacy of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay.** **2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b) and (c) of Article 31(3).** **3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to**	Article 32 Communication of a personal data breach to the data subject 1. When the personal data breach is likely to <u>severely</u> affect the <u>rights and freedoms</u> of the data subject, the controller shall (…) communicate the personal data breach to the data subject without undue delay. 2. The communication to the data subject referred to in paragraph 1 shall describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b), (<u>e</u>) and (f) of Article 31(3). 3. The communication (…) to the data subject <u>referred to in paragraph 1</u> shall not be required if: a) the controller (…) has implemented appropriate technological protection measures and (…) those measures were applied to the data <u>affected by</u> the personal data breach, <u>in particular those that</u> render the data unintelligible to any person who is not authorised to access it<u>, such as encryption or the use of pseudonymous data</u>; or b) the controller has taken subsequent measures which ensure that the data subjects' rights and freedoms are no longer	Article 32 Communication of a personal data breach to the data subject 1. When the personal data breach is likely to adversely affect the protection of the personal data*, ~~or~~ the* privacy, *the rights or the legitimate interests* of the data subject, the controller shall, after the notification referred to in Article 31, communicate the personal data breach to the data subject without undue delay. 2. The communication to the data subject referred to in paragraph 1 shall *be comprehensive and use clear and plain language. It shall* describe the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b)*, ~~and~~* (c) and *(d)* of Article 31(3) *and information about the rights of the data subject, including redress*. 3. The communication of a personal data breach to the data subject shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.	Ust. 1 - PL wnioskowała o doprecyzowanie, że forma pisemna i elektroniczna są równoważne. PL opowiedziała się za usunięciem art. 32 ust. 5 i 6, przewidujących delegację dla Komisji Europejskiej, uznając iż taka delegacja wprowadza element niepewności dla administratora danych.

access it. **4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so.** **5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements as to the circumstances in which a personal data breach is likely to adversely affect the personal data referred to in paragraph 1.** **6. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).**	likely to be severely affected; or c) it would involve disproportionate effort, in particular owing to the number of cases involved. In such case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner; or d) it would adversely affect a substantial public interest. 4. (…) 5. (…) [6. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).]	4. Without prejudice to the controller's obligation to communicate the personal data breach to the data subject, if the controller has not already communicated the personal data breach to the data subject of the personal data breach, the supervisory authority, having considered the likely adverse effects of the breach, may require it to do so. 5. The *European Data Protection Board* ~~*Commission*~~ shall be *entrusted with the task* ~~*empowered to adopt delegated acts in accordance with Article 86 for the purpose*~~ of *issuing guidelines, recommendations and best practices in accordance with Article 66 paragraph 1(b)* ~~*further specifying the criteria and requirements*~~ as to the circumstances in which a personal data breach is likely to adversely affect the personal data *or the privacy, the rights or the legitimate interests of the data subject* referred to in paragraph 1. ~~*6. The Commission may lay down the format of the communication to the data subject referred to in paragraph 1 and the procedures applicable to that communication. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).*~~

Article 32a

Respect to Risk

1. The controller, or where applicable the processor, shall carry out a risk analysis of the potential impact of the intended data processing on the rights and freedoms of the data subjects, assessing whether its processing operations are likely to present specific risks.

2. The following processing operations are likely to present specific risks:

(a) processing of personal data relating to more than 5000 data subjects during any consecutive 12-month period;

(b) processing of special categories of personal data as referred to in Article 9(1), location data or data on children or employees in large scale filing systems;

(c) profiling on which measures are based that produce legal effects concerning the individual or similarly significantly affect the individual;

(d) processing of personal data for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;

(e) automated monitoring of publicly accessible areas on a large scale;

(f) other processing operations for which the consultation of the data protection officer or supervisory authority is required pursuant to point (b) of Article 34(2);

(g) where a personal data breach would likely adversely affect the protection of the personal data, the privacy, the rights or the legitimate interests of the data subject;

(h) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects;

(i) where personal data are made accessible to a number of persons which cannot reasonably be expected to be limited.

3. According to the result of the risk analysis:

(a) where any of the processing operations referred to in paragraph 2 (a) or (b) exist, controllers not established in the Union shall designate a representative in the Union in line with the requirements and exemptions laid down in Article 25;

(b) where any of the processing operations referred to in paragraph 2 (a), (b) or (h) exist, the controller shall designate a data

protection officer in line with the requirements and exemptions laid down in Article 35;

(c) where any of the processing operations referred to in paragraph 2 (a), (b), (c), (d), (e), (f), (g) or (h) exist, the controller or the processor acting on the controller's behalf shall carry out a data protection impact assessment pursuant to Article 33;

(d) where processing operations referred to in paragraph 2 (f) exist, the controller shall consult the data protection officer, or in case a data protection officer has not been appointed, the supervisory authority pursuant to Article 34.

4. The risk analysis shall be reviewed at the latest after one year, or immediately, if the nature, the scope or the purposes of the data processing operations change significantly. Where pursuant to paragraph 3 (c) the controller is not obliged to carry out a data protection impact assessment, the risk analysis shall be documented.

Article 33 **Data protection impact assessment** **1. Where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.** **2. The following processing operations in particular present specific risks referred to in paragraph 1:** **(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;** **(b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys**	*Article 33* *Data protection impact assessment* 1. Where the processing, taking into account the nature, scope or purposes of the processing, is likely to present specific risks for the rights and freedoms of data subjects, the controller (…)shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. (…). 2. The following processing operations (…) present specific risks referred to in paragraph 1: (a) a systematic and extensive evaluation (…) of personal aspects relating to (…) natural persons (…), which is based on profiling and on which decisions are based that produce legal effects concerning data subjects or severely affect data subjects; (b) data revealing racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions and offences or related security measures, where the data are processed for taking (…) decisions regarding specific individuals on a large scale; (c) monitoring publicly accessible	Article 33 Data protection impact assessment 1. *Where required pursuant to point c of Article 32a(3)* ~~*where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes,*~~ the controller or the processor acting on the controller's behalf shall carry out an assessment of the impact of the envisaged processing operations on the *rights and freedoms of the data subjects, especially their right to* protection of personal data. *A single assessment shall be sufficient to address a set of similar processing operations that present similar risks.* ~~*The following processing operations in particular present specific risks referred to in paragraph 1:*~~ ~~*(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;*~~ ~~*(b) information on sex life, health, race and ethnic origin or for the provision of health*~~	W ust. 1 – PL była przeciwko odniesieniu do procesora (**uwaga uwzględniona**) w art. 33 powinno być wyraźne odniesienie do art. 23 (privacy by design i by default), tak aby podkreślić związek między tymi dwoma rozwiązaniami, w szczególności, okoliczność, iż PIA powinno obejmować także analizę w zakresie privacy by design i privacy by default. Odnośnie art. 33 ust. 1 lit. e oraz ust. 2a oraz 2b, PL zajęła stanowisko, iż lepiej by kompetencja ta zamiast krajowym organom nadzoru, była przyznana Europejskiej Radzie Ochrony Danych. Przyznanie jej krajowym organom nadzoru kreuje element dużej niepewności dla administratorów danych. Uwaga ogólna: PL widzi wartość dodaną w przeprowadzaniu oceny wpływu w przypadku ryzykownego przetwarzania jako elementu dbałości o bezpieczeństwo przetwarzanych danych i tym samym budowania zaufania klienta do oferowanych usług. Przeprowadzanie oceny wpływu ochrony danych traktujemy jako element będący w interesie administratora i służący budowaniu jego przewagi konkurencyjnej.

of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale; **(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;** **(d) personal data in large scale filing systems on children, genetic data or biometric data;** **(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).** **3. The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned.** **4. The controller shall seek the views of data subjects or their representatives on the intended**	areas *on a large scale*, especially when using optic-electronic devices (…); (d) personal data in large scale processing systems containing genetic data or biometric data; (e) other operations where the competent supervisory authority considers that the processing is likely to present specific risks for the rights and freedoms of data subjects. 2a. The supervisory authority shall establish and make public a list of the kind of processing which are subject to the requirement for a data protection impact assessment pursuant to point (e) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board. 2b. Prior to the adoption of the list the supervisory authority shall apply the consistency mechanism referred to in Article 57 where the list provided for in paragraph 2a involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union. 3. The assessment shall contain at least a general description of the envisaged	~~*care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;*~~ ~~*(c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale;*~~ ~~*(d) personal data in large scale filing systems on children, genetic data or biometric data;*~~ ~~*(e) other processing operations for which the consultation of the supervisory authority is required pursuant to point (b) of Article 34(2).*~~ 3. The assessment shall *have regard to the entire lifecycle management of personal data from collection to processing to deletion. It shall* contain at least *(a)* a *systematic* description of the envisaged processing operations, *the purposes of the processing and, if applicable, the legitimate interests pursued by the controller,* *(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes*; *(c)* an assessment of the risks to the rights and freedoms of data subjects, *including the*

processing, without prejudice to the protection of commercial or public interests or the security of the processing operations. **5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.** **6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.** **7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3.**	processing operations, an assessment of the risks <u>for</u> rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned. 4. (…) 5. Where a controller is a public authority or body and where the processing pursuant to point (c) <u>or (e)</u> of Article 6(1) <u>has a legal basis in</u> Union law <u>or the law of the Member State to which the controller is subject</u>, paragraphs 1 to 3 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities. 6. (…) 7. (…)	*risk of discrimination being embedded in or reinforced by the operation,* *(d) a description of* the measures envisaged to address the risks *and minimise the volume of personal data which is processed*, *(e) a list of* safeguards, security measures and mechanisms to ensure the protection of personal data, *such as pseudonymisation,* and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned; *(f) a general indication of the time limits for erasure of the different categories of data;* *(h) an explanation which data protection by design and default practices pursuant to Article 23 have been implemented;* *(i) a list of the recipients or categories of recipients of the personal data;* *(j) where applicable, a list of the intended transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;* *(k) an assessment of the context of the data processing.*

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).		*3a. If the controller or the processor has designated a data protection officer, he or she shall be involved in the impact assessment proceeding.* *3b. The assessment shall be documented and lay down a schedule for regular periodic data protection compliance reviews pursuant to Article 33a(1). The assessment shall be updated without undue delay, if the results of the data protection compliance review referred to in Article 33a show compliance inconsistencies. The controller and the processor and, if any, the controller's representative, shall make the assessment available, on request, to the supervisory authority.* *~~4. The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.~~* *~~5. Where the controller is a public authority or body and where the processing results from a legal obligation pursuant to point (c) of Article 6(1) providing for rules and procedures pertaining to the processing operations and regulated by Union law, paragraphs 1 to 4 shall not apply, unless Member States deem it necessary to carry out such assessment prior to the processing activities.~~*

~~*6. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for the processing operations likely to present specific risks referred to in paragraphs 1 and 2 and the requirements for the assessment, referred to in paragraph 3, including conditions for scalability, verification and auditability. In doing so, the Commission shall consider specific measures for micro, small and medium-sized enterprises.*~~

~~*7. The Commission may specify standards and procedures for carrying out and verifying and auditing the assessment referred to in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).*~~

Article 33a

Data protection compliance review

1. At the latest two years after the carrying out of an impact assessment pursuant to Article 33(1), the controller or the processor acting on the controller's behalf shall carry out a compliance review. This compliance review shall demonstrate that the processing of personal data is performed in compliance with the data protection impact assessment.

2. The compliance review shall be carried out periodically at least once every two years, or immediately when there is a change in the specific risks presented by the processing operations.

3. Where the compliance review results show compliance inconsistencies, the compliance review shall include recommendations on how to achieve full compliance.

4. The compliance review and its recommendations shall be documented. The controller and the processor and, if any, the controller's representative, shall make the compliance review available, on request, to the supervisory authority.

5. If the controller or the processor has designated a data protection officer, he or she shall be involved in the compliance

review proceeding.

Article 34 **Prior authorisation and prior consultation** **1. The controller or the processor as the case may be shall obtain an authorisation from the supervisory authority prior to the processing of personal data, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data to a third country or an international organisation.** **2. The controller or processor acting on the controller's behalf shall consult the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:** **(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations**	*Article 34* *Prior (…) consultation* 1. (…) 2. The controller (…)shall consult the supervisory authority prior to the processing of personal data where a data protection impact assessment as provided for in Article 33 indicates that <u>the</u> processing <u>is</u> likely to present a high degree of specific risks. (…) 3. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 2 <u>would</u> not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall <u>within a maximum period of 6 weeks following the request for consultation</u> <u>give advice</u> to <u>the data controller</u> (…). <u>This period may be extended for a further month, taking into account the complexity of the intended processing. Where the extended period applies, the controller or processor shall be informed within one month of receipt of the request of the reasons for the delay.</u> 4. (…) 5. (…) 6. <u>When consulting the supervisory</u>	Article 34 ~~*Prior authorisation and p*~~Prior consultation ~~*1. The controller or the processor as the case may be shall obtain an authorisation from the supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where a controller or processor adopts contractual clauses as provided for in point (d) of Article 42(2) or does not provide for the appropriate safeguards in a legally binding instrument as referred to in Article 42(5) for the transfer of personal data personal data to a third country or an international organisation.*~~ 2. The controller or processor acting on the controller's behalf shall consult the *data protection officer, or in case a data protection officer has not been appointed, the* supervisory authority prior to the processing of personal data in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects where:	Odnośnie art. 34 ust. 2, PL opowie się za wykreśleniem podmiotu, któremu powierzono przetwarzanie jako zobowiązanego do konsultowania się z organem ochrony danych. (uwaga uwzględniona) PL zgłosi uwagę ogólną – zapyta o zastosowanie tego przepisu do sektora publicznego czy np. zakaz przetwarzania na podstawie art. 34 ust. 3 i 3a nie spowoduje paraliżu funkcjonowania organów publicznych PL opowie się za wykreśleniem delegacji dla KE z art. 34 ust. 8 jako zbędnej.

are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or **(b) the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4.** **3. Where the supervisory authority is of the opinion that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such incompliance.** **4. The supervisory authority shall establish and make public a list of the processing operations which are subject to prior consultation pursuant to point (b) of paragraph 2. The supervisory authority shall communicate those lists to the European Data Protection Board.** **5. Where the list provided for in paragraph 4 involves processing activities which are related to the**	<u>authority pursuant to paragraph 2,</u> the controller (…) shall provide the supervisory authority, on request, with the data protection impact assessment provided for in Article 33 and any (…) information <u>requested by</u> the supervisory authority (…). 7. Member States shall consult the supervisory authority during the preparation of proposals for legislative or regulatory measures which provide for the processing of personal data and which may severely affect categories of data subjects by virtue of the nature, scope or purposes of such processing. 7a. Notwithstanding paragraph 2, Member States' law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to the processing of personal data by a controller for the performance of a task carried out by the controller in the public interest, including the processing of such data in relation to social protection and public health. 8. (…) 9. (…)	(a) a data protection impact assessment as provided for in Article 33 indicates that processing operations are by virtue of their nature, their scope or their purposes, likely to present a high degree of specific risks; or (b) *the data protection officer or* the supervisory authority deems it necessary to carry out a prior consultation on processing operations that are likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope and/or their purposes, and specified according to paragraph 4. 3. Where the *competent* supervisory authority *determines in accordance with its power* ~~*is of the opinion*~~ that the intended processing does not comply with this Regulation, in particular where risks are insufficiently identified or mitigated, it shall prohibit the intended processing and make appropriate proposals to remedy such incompliance. 4. The *European Data Protection Board* ~~*supervisory authority*~~ shall establish and make public a list of the processing

offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.	operations which are subject to prior consultation pursuant to ~~*point (b) of*~~ paragraph 2. ~~*The supervisory authority shall communicate those lists to the European Data Protection Board.*~~
6. The controller or processor shall provide the supervisory authority with the data protection impact assessment provided for in Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.	~~*5. Where the list provided for in paragraph 4 involves processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57 prior to the adoption of the list.*~~ 6. The controller or processor shall provide the supervisory authority, *on request*, with the data protection impact assessment *pursuant to* ~~*provided for in*~~ Article 33 and, on request, with any other information to allow the supervisory authority to make an assessment of the compliance of the processing and in particular of the risks for the protection of personal data of the data subject and of the related safeguards.
7. Member States shall consult the supervisory authority in the preparation of a legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects.	7. Member States shall consult the supervisory authority in the preparation of a
8. The Commission shall be empowered to adopt delegated acts in	

accordance with Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2. **9. The Commission may set out standard forms and procedures for prior authorisations and consultations referred to in paragraphs 1 and 2, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).**	legislative measure to be adopted by the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing, in order to ensure the compliance of the intended processing with this Regulation and in particular to mitigate the risks involved for the data subjects. ~~*8. The Commission shall be empowered to adopt delegated acts in accordance with*~~ ~~*Article 86 for the purpose of further specifying the criteria and requirements for determining the high degree of specific risk referred to in point (a) of paragraph 2.*~~ ~~*9. The Commission may set out standard forms and procedures for prior authorizations and consultations referred to in paragraphs 1 and 2, and standard forms and procedures for informing the supervisory authorities pursuant to paragraph 6. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).*~~

Article 35 **Designation of the data protection officer** **1. The controller and the processor shall designate a data protection officer in any case where:** **(a) the processing is carried out by a public authority or body; or** **(b) the processing is carried out by an enterprise employing 250 persons or more; or** **(c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.** **2. In the case referred to in point (b) of paragraph 1, a group of undertakings may appoint a single data protection officer.** **3. Where the controller or the processor is a public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body.** **4. In cases other than those**	*Article 35* *Designation of the data protection officer* 1. The controller or the processor may, or where required by Union or Member State law shall, designate a data protection officer (…). 2. A group of undertakings may appoint a single data protection officer. 3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size. 4. (…). 5. The (…) data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37 (…). 6. (…) 7. (…). During their term of office, the data protection officer may, apart from serious grounds under the law of the Member State concerned which justify the dismissal of an employee or civil servant, be dismissed only if the data protection officer no longer fulfils the conditions required for	Article 35 Designation of the data protection officer 1. The controller and the processor shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body; or (b) the processing is carried out by *a legal person and relates to more than 5000 data subjects in any consecutive 12-month period* ~~*an enterprise employing 250 persons or more,*~~ or (c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects*; or*. *(d) the core activities of the controller or the processor consist of processing special categories of data pursuant to Article 9(1), location data or data on children or employees in large scale filing systems.* 2. ~~*In the case referred to in point (b) of paragraph 1,*~~ A group of undertakings may appoint a *main responsible* data protection officer, *provided it is ensured that a data protection officer is easily accessible from each establishment*. 3. Where the controller or the processor is a	Art. 35 – Rada JHA w marcu br. zadecydowała o fakultatywnym charakterze wyznaczania DPO. PL zgodziła się z tym podejściem. Powszechny obowiązek wyznaczenia inspektora ochrony danych osobowych byłby niezwykle uciążliwy zwłaszcza dla małych i średnich przedsiębiorców. Polska opowie się za dodaniem ustępu sankcjonującego powoływanie zastępców inspektora ochrony danych. W niektórych, zwłaszcza większych podmiotach, pojedynczy inspektor może nie wystarczyć, inspektor nie będzie też obecny w przedsiębiorstwie cały czas. Proponujemy w związku z tym dodanie w art. 35 ustępu 1a stanowiącego, iż „the controller or the processor may appoint one or more deputy data protection officers. Deputy data protection officer must fulfill conditions stipulated in art. 35 point 5 of this Regulation". W art. 35 ust. 5 sugerujemy wprowadzenie wymogu, aby inspektorem ochrony danych nie mogła być osoba prawomocnie skazana za przestępstwo z winy umyślnej. Inspektor ochrony danych musi mieć nieposzlakowaną opinię i gwarantować prawidłowe wykonywanie swojej funkcji. W związku z tym sugerujemy dodanie na końcu art. 35 ust. 5 zdania: „A person designated as a data protection officer

referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer. **5. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor.** **6. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests.** **7. The controller or the processor shall designate a data protection officer for a period of at least two years. The data protection officer may be reappointed for further terms. During their term of office, the data protection officer may only be**	the performance of <u>his or her tasks pursuant to Article 37</u>. 8. The data protection officer may be <u>a staff member of</u> the controller or processor, or fulfil <u>the</u> tasks on the basis of a service contract<u>.</u> 9. The controller or the processor shall <u>publish the</u> contact details of the data protection officer <u>and communicate these</u> to the supervisory authority (…). 10. Data subjects <u>may</u> contact the data protection officer on all issues related to the processing of the data subject's data and <u>the exercise of their</u> rights under this Regulation. 11. (…)	public authority or body, the data protection officer may be designated for several of its entities, taking account of the organisational structure of the public authority or body. 4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may designate a data protection officer. 5. The controller or processor shall designate the data protection officer on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and ability to fulfil the tasks referred to in Article 37. The necessary level of expert knowledge shall be determined in particular according to the data processing carried out and the protection required for the personal data processed by the controller or the processor. 6. The controller or the processor shall ensure that any other professional duties of the data protection officer are compatible with the person's tasks and duties as data protection officer and do not result in a conflict of interests. 7. The controller or the processor shall designate a data protection officer for a period of at least *four* ~~*two*~~ years *in case of an employee or two years in case of an*	cannot have a criminal record resulting from a criminal offence due to intentional guilt". Odnośnie art. 35 ust. 7, w związku z usunięciem z rozporządzenia postanowień dotyczących kadencji inspektora, sugerujemy usunięcie w tym ustępie "during their term of office" jako zbędnego. Odnośnie art. 35 ust. 10 to postanowienie jest niezwykle szerokie, być może wymaga doprecyzowania, Polska poprosi w szczególności o wyjaśnienie czy kontakt ze strony podmiotu danych kreuje po stronie administratora danych jakieś konkretne obowiązki, niezależne od wagi zapytania?

dismissed, if the data protection officer no longer fulfils the conditions required for the performance of their duties.	*external service contractor*. The data protection officer may be reappointed for further terms. During their term of office, the data protection officer may only be dismissed if the data protection officer no longer fulfils the conditions required for the performance of their duties.
8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.	8. The data protection officer may be employed by the controller or processor, or fulfil his or her tasks on the basis of a service contract.
9. The controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority and to the public.	9. The controller or the processor shall communicate the name and contact details of the data protection officer to the supervisory authority and to the public.
10. Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.	10. Data subjects shall have the right to contact the data protection officer on all issues related to the processing of the data subject's data and to request exercising the rights under this Regulation.
11. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core activities of the controller or the processor referred to in point (c) of paragraph 1 and the criteria for the professional qualities of the data protection officer referred to in paragraph 5.	~~*11. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the core activities of or the controller or the processor referred to in point (c) of paragraph 1 and the criteria for professional qualities of the data protection officer referred to in paragraph 5.*~~

Article 36 **Position of the data protection officer** **1. The controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data.** **2. The controller or processor shall ensure that the data protection officer performs the duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the management of the controller or the processor.** **3. The controller or the processor shall support the data protection officer in performing the tasks and shall provide staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37.**	*Article 36* *Position of the data protection officer* 1. The controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data. 2. The controller or the processor shall support the data protection officer in performing the tasks referred to in Article 37 by providing (…) resources necessary to carry out these tasks as well as access to personal data and processing operations. 3. The controller or processor shall ensure that the data protection officer can act in an independent manner with respect to the performance of his or her tasks and does not receive any instructions regarding the exercise of these tasks. The data protection officer shall directly report to the highest management level of the controller or the processor. 4. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.	Article 36 Position of the data protection officer 1. The controller or the processor shall ensure that the data protection officer is properly and in a timely manner involved in all issues which relate to the protection of personal data. 2. The controller or processor shall ensure that the data protection officer performs the duties and tasks independently and does not receive any instructions as regards the exercise of the function. The data protection officer shall directly report to the *executive* management of the controller or the processor. *The controller or processor shall for this purpose designate an executive management member who shall be responsible for the compliance with the provisions of this Regulation.* 3. The controller or the processor shall support the data protection officer in performing the tasks and shall provide *all means, including* staff, premises, equipment and any other resources necessary to carry out the duties and tasks referred to in Article 37*, and to maintain his or her professional knowledge*. *4. Data protection officers shall be bound by secrecy concerning the identity of data subjects and concerning circumstances enabling data subjects to be identified,*	Nie zgłaszaliśmy zasadniczych uwag.

unless they are released from that obligation by the data subject.

Article 37 **Tasks of the data protection officer** **1. The controller or the processor shall entrust the data protection officer at least with the following tasks:** **(a) to inform and advise the controller or the processor of their obligations pursuant to this Regulation and to document this activity and the responses received;** **(b) to monitor the implementation and application of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations, and the related audits;** **(c) to monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation;** **(d) to ensure that the documentation referred to in Article 28**	Article 37 Tasks of the data protection officer 1. The controller or the processor shall entrust the data protection officer (…) with the following tasks: (a) to inform and advise the controller or the processor and the employees who are processing personal data of their obligations pursuant to this Regulation (…); (b) to monitor compliance with this Regulation and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in the processing operations, and the related audits; (c) (…) (d) (…) (e) (…) (f) (…) (g) to monitor responses to requests from the supervisory authority and, within the sphere of the data protection officer's competence, to co-operate with the supervisory authority at the latter's request or on the data protection officer's own initiative;	Article 37 Tasks of the data protection officer 1. The controller or the processor shall entrust the data protection officer at least with the following tasks: (a) *to raise awareness,* to inform and advise the controller or the processor of their obligations pursuant to this Regulation*, in particular with regards to technical and organisational measures and procedures,* and to document this activity and the responses received; (b) to monitor the implementation and application of the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, the training of staff involved in the processing operations, and the related audits; (c) to monitor the implementation and application of this Regulation, in particular as to the requirements related to data protection by design, data protection by default and data security and to the information of data subjects and their requests in exercising their rights under this Regulation; (d) to ensure that the documentation referred to in Article 28 is maintained;	Odnośnie art. 37 Polska poprosi o doprecyzowanie czy obecne brzmienie art. 37 ust. 1 lit. b obejmuje także monitorowanie rekordów, o których mowa w art. 28 rozporządzenia. A także czy obejmuje monitorowanie notyfikacji naruszeń danych osobowych, o których mowa w art. 31 i 32 rozporządzenia.

is maintained; **(e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 31 and 32;** **(f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for prior authorisation or prior consultation, if required pursuant Articles 33 and 34;** **(g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, co-operating with the supervisory authority at the latter's request or on the data protection officer's own initiative;** **(h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on his/her own initiative.** **2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for tasks,**	(h) to act as the contact point for the supervisory authority on issues related to the processing of personal data, including the prior consultation referred to in Article 34, and consult, as appropriate, on any other matter. 2. (….)	(e) to monitor the documentation, notification and communication of personal data breaches pursuant to Articles 31 and 32; (f) to monitor the performance of the data protection impact assessment by the controller or processor and the application for prior ~~*authorisation or prior*~~ consultation, if required pursuant Articles 32a and 34; (g) to monitor the response to requests from the supervisory authority, and, within the sphere of the data protection officer's competence, co-operating with the supervisory authority at the latter's request or on the data protection officer's own initiative; (h) to act as the contact point for the supervisory authority on issues related to the processing and consult with the supervisory authority, if appropriate, on his/her own initiative~~.~~*;* *(i) to verify the compliance with this Regulation under the prior consultation mechanism laid out in Article 34;* *(j) to inform the employee representatives on data processing of the employees.* ~~*2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for*~~

certification, status, powers and resources of the data protection officer referred to in paragraph 1.	~~*tasks, certification, status, powers and resources of the data protection officer referred to in paragraph 1.*~~

Article 38 **Codes of conduct** **1. The Member States, the supervisory authorities and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors, in particular in relation to:** **(a) fair and transparent data processing;** **(b) the collection of data;** **(c) the information of the public and of data subjects;** **(d) requests of data subjects in exercise of their rights;** **(e) information and protection of children;** **(f) transfer of data to third countries or international organisations;** **(g) mechanisms for monitoring and ensuring compliance with the code by the controllers adherent to it;** **(h) out-of-court proceedings and**	*Article 38* *Codes of conduct* 1. The Member States, the supervisory authorities, the European Data Protection Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors and the specific needs of micro, small and medium-sized enterprises. 1a. Associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of provisions of this Regulation, such as: (a) fair and transparent data processing; (aa) the legitimate interests pursued by controllers in specific contexts; (b) the collection of data; (bb) the use of pseudonymous data; (c) the information of the public and of data subjects; (d) the exercise of the rights of data subjects;	Article 38 Codes of conduct 1. The Member States, the supervisory authorities and the Commission shall encourage the drawing up of codes of conduct *or the adoption of codes of conduct drawn up by a supervisory authority* intended to contribute to the proper application of this Regulation, taking account of the specific features of the various data processing sectors, in particular in relation to: (a) fair and transparent data processing; *(aa) respect for consumer rights;* (b) the collection of data; (c) the information of the public and of data subjects; (d) requests of data subjects in exercise of their rights; (e) information and protection of children; (f) transfer of data to third countries or international organisations; (g) mechanisms for monitoring and ensuring compliance with the code by the controllers	Artykuły 38-39 – PL poparła kierunek zmian, w szczególności rozwinięcie kodeksów postępowania, zgłosi jednak zastrzeżenia analityczne – potrzebujemy więcej czasu na analizy. PL popiera jednak narzędzia samoregulacji w rozporządzeniu.

other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data, without prejudice to the rights of the data subjects pursuant to Articles 73 and 75.	(e) information and protection of children and the way to collect the parent's and guardian's consent;	adherent to it;
	(ee) measures and procedures referred to in Articles 22 and 23 and measures to ensure security (…) of processing referred to in Article 30;	(h) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with respect to the processing of personal data, without prejudice to the rights of the data subjects pursuant to Articles 73 and 75.
2. Associations and other bodies representing categories of controllers or processors in one Member State which intend to draw up codes of conduct or to amend or extend existing codes of conduct may submit them to an opinion of the supervisory authority in that Member State. The supervisory authority may give an opinion whether the draft code of conduct or the amendment is in compliance with this Regulation. The supervisory authority shall seek the views of data subjects or their representatives on these drafts.	(ef) notification of personal data breaches to supervisory authorities and communication of such breaches to data subjects;	2. Associations and other bodies representing categories of controllers or processors in one Member State which intend to draw up codes of conduct or to amend or extend existing codes of conduct may submit them to an opinion of the supervisory authority in that Member State. The supervisory authority *shall without undue delay* ~~*may*~~ give an opinion in whether *the processing under* the draft code of conduct or the amendment is in compliance with this Regulation. The supervisory authority shall seek the views of data subjects or their representatives on these drafts.
	(f) transfer of data to third countries or international organisations.	
	1b. Such a code of conduct shall contain mechanisms for monitoring and ensuring compliance with it by the controllers or processors which undertake to apply it, without prejudice to the duties and powers of the supervisory authority which is competent pursuant to Article 51.	
3. Associations and other bodies representing categories of controllers in several Member States may submit draft codes of conduct and amendments or extensions to existing codes of conduct to the Commission.	2. Associations and other bodies referred to in paragraph 1a which intend to prepare a code of conduct, or to amend or extend an existing code, shall submit the draft code to the supervisory authority which is competent pursuant to Article 51. The supervisory authority shall give an opinion on whether the draft code, or amended or extended code, is in compliance with this Regulation.	3. Associations and other bodies representing categories of controllers *or processors* in several Member States may submit draft codes of conduct and amendments or extensions to existing
4. The Commission may adopt implementing acts for deciding that the codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union. Those implementing acts shall		

be adopted in accordance with the examination procedure set out in Article 87(2). **5. The Commission shall ensure appropriate publicity for the codes which have been decided as having general validity in accordance with paragraph 4.**	2a. Where the opinion referred to in paragraph 2 confirms that the code of conduct, or amended or extended code, is in compliance with this Regulation and the code of conduct does not relate to processing activities in several Member States, the supervisory authority shall register the code and publish the details thereof. 2b. Where the code of conduct relates to processing activities in several Member States, the supervisory authority shall submit it in the procedure referred to in Article 57 to the European Data Protection Board which may give an opinion on whether the draft code, or amended or extended code, is in compliance with this Regulation. 3. Where the opinion referred to in paragraph 2b confirms that the code of conduct, or amended or extended code, is in compliance with this Regulation, the European Data Protection Board shall submit its opinion to the Commission (…). 4. The Commission may adopt implementing acts for deciding that the codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to paragraph 3 have general validity within the Union. Those implementing acts shall be adopted in accordance with the examination	codes of conduct to the Commission. 4. The Commission *shall be empowered to adopt, after requesting an opinion of the European Data Protection Board, delegated acts in accordance with Article 86* ~~*may adopt implementing acts*~~ for deciding that the codes of conduct and amendments or extensions to existing codes of conduct submitted to it pursuant to paragraph 3 *are in line with this Regulation and* have general validity within the Union. *This delegated act shall confer enforceable rights on data subjects.* ~~*Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).*~~ 5. The Commission shall ensure appropriate publicity for the codes which have been decided as having general validity in accordance with paragraph 4.

procedure set out in Article 87(2).

5. The Commission shall ensure appropriate publicity for the codes which have been decided as having general validity in accordance with paragraph 4.

Article 38a
Monitoring (…) of codes of conduct

Without prejudice to the duties and powers of the competent supervisory authority under Articles 52 and 53, the monitoring of compliance with a code of conduct pursuant to Article 38 may be carried out by a (…) body which has an appropriate level of expertise in relation to the subject-matter of the code and is accredited for this purpose by the competent supervisory authority.

2. A body referred to in paragraph 1 may be accredited for this purpose if:

a) it has demonstrated its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority;

b) it has established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;

c) it has established procedures and structures to deal with complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make these procedures and structures transparent to data subjects and

the public;

d) it (…) demonstrates to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

3. The competent supervisory authority shall submit the draft criteria for accreditation of a body referred to in paragraph 1 to the European Data Protection Board pursuant to the consistency mechanism referred to in Article 57.

4. Without prejudice to the provisions of Chapter VIII, a body referred to in paragraph 1 may, subject to adequate safeguards, take appropriate action in cases of infringement of the code by a controller or processor, including suspension or exclusion of the controller or processor concerned from the code. It shall inform the competent supervisory authority of such actions and the reasons for taking them.

5. The competent supervisory authority shall revoke the accreditation of a body referred to in paragraph 1 if the conditions for accreditation are not, or no longer, met or actions taken by the body are not in compliance with this Regulation.

6. This article shall not apply to the processing of personal data carried out by

public authorities and bodies.

Article 39 **Certification** **1. The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.** **2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.** **3. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to**	*Article 39* *Certification* 1. The Member States, the European Data Protection Board and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks for the purpose of demonstrating compliance with this Regulation by controllers and processors. The specific needs of micro, small and medium-sized enterprises shall be taken into account. (…) 2. A certification pursuant to this Article does not reduce the responsibility of the controller or the processor for compliance with this Regulation and is without prejudice to the duties and powers of the supervisory authority which is competent pursuant to Article 51. 3. The controller or processor which submits its processing to the certification mechanism shall provide the body referred to in Article 39a (1) with all information and access to its processing activities which are necessary to conduct the certification procedure. (…) 4. The certification issued to a controller or processor shall be subject to a	Article 39 Certification 1. ~~*The Member States and the Commission shall encourage, in particular at European level, the establishment of data protection certification mechanisms and of data protection seals and marks, allowing data subjects to quickly assess the level of data protection provided by controllers and processors. The data protection certifications mechanisms shall contribute to the proper application of this Regulation, taking account of the specific features of the various sectors and different processing operations.*~~ *1a. Any controller or processor may request any supervisory authority in the Union, for a reasonable fee taking into account the administrative costs, to certify that the processing of personal data is performed in compliance with this Regulation, in particular with the principles set out in Article 5, 23 and 30, the obligations of the controller and the processor, and the data subject's rights.* *1b. The certification shall be voluntary, affordable, and available via a process that*	Artykuły 38-39 – PL poparła kierunek zmian, w szczególności rozwinięcie kodeksów postępowania, zgłosi jednak zastrzeżenia analityczne – potrzebujemy więcej czasu na analizy. PL popiera jednak narzędzia samoregulacji w rozporządzeniu.

promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).	periodic review by the body referred to in paragraph 1 of Article 39a or by the competent supervisory authority. It shall be withdrawn where the requirements for the certification are not or no longer met.	*is transparent and not unduly burdensome.* *1c. The supervisory authorities and the European Data Protection Board shall cooperate under the consistency mechanism pursuant to Article 57 to guarantee a harmonised data protection certification mechanism including harmonised fees within the Union.* *1d. During the certification procedure, the supervisory authority may accredit specialised third party auditors to carry out the auditing of the controller or the processor on their behalf. Third party auditors shall have sufficiently qualified staff, be impartial and free from any conflict of interests regarding their duties. Supervisory authorities shall revoke accreditation, if there are reasons to believe that the auditor does not fulfil its duties correctly. The final certification shall be provided by the supervisory authority.* *1e. Supervisory authorities shall grant controllers and processors, who pursuant to the auditing have been certified that they process personal data in compliance with this Regulation, the standardised data protection mark named "European Data*

Protection Seal".

1f. The "European Data Protection Seal" shall be valid for as long as the data processing operations of the certified controller or processor continue to fully comply with this Regulation.

1g. Notwithstanding paragraph 1f, the certification shall be valid for maximum five years.

1h. The European Data Protection Board shall establish a public electronic register in which all valid and invalid certificates which have been issued in the Member States can be viewed by the public.

~~*2. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1, including conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries.*~~

		2a. The European Data Protection Board may on its own initiative certify that a data protection-enhancing technical standard is compliant with this Regulation.
		3. The Commission shall be empowered to adopt*, after requesting an opinion of the European Data Protection Board and consulting with stakeholders, in particular industry and non-governmental organisations,* delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the data protection certification mechanisms referred to in paragraph 1-*1h*, including *requirements for accreditation of auditors,* conditions for granting and withdrawal, and requirements for recognition within the Union and in third countries. *These delegated acts shall confer enforceable rights on data subjects.*

Article 39a
Certification body and procedure

1. Without prejudice to the duties and powers of the competent supervisory authority under Articles 52 and 53, the certification and its periodic review may be carried out by a certification body which has an appropriate level of expertise in relation to data protection and is accredited by the supervisory authority which is competent according to Article 51.

2. The body referred to in paragraph 1 may be accredited for this purpose if:

a) it has demonstrated its independence and expertise in relation to the subject-matter of the certification to the satisfaction of the competent supervisory authority;

b) it has established procedures for the issue, periodic review and withdrawal of data protection seals and marks;

c) it has established procedures and structures to deal with complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make these procedures and structures transparent to data subjects and the public;

(d) it (…) demonstrates to the satisfaction

of the competent supervisory authority that its tasks and duties do not result in a conflict of interests.

3. The supervisory authorities shall submit the draft criteria for the accreditation of the body referred to in paragraph 1 to the European Data Protection Board pursuant to the consistency mechanism referred to in Article 57.

4. The body referred to in paragraph 1 shall be responsible for the proper assessment leading to the certification, without prejudice to the responsibility of the controller or processor for compliance with this Regulation.

4a. Without prejudice to the provisions of Chapter VIII, the body referred to in paragraph 1 shall, subject to adequate safeguards, in cases of inappropriate use of the certification or where the requirements of the certification are not, or no longer, met by the controller or processor, withdraw the certification.

5. The body referred to in paragraph 1 shall provide the competent supervisory authority with the details of certifications issued and withdrawn and the reasons for withdrawing the certification.

6. The criteria for certification and the certification details shall be made public by

the supervisory authority in an easily accessible form.

6a. The competent supervisory authority shall revoke the accreditation of a body referred to in paragraph 1 if the conditions for accreditation are not, or no longer, met or actions taken by the body are not in compliance with this Regulation.

7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of (…) specifying the criteria and requirements to be taken into account for the data protection certification mechanisms referred to in paragraph 1, [including conditions for granting and revocation, and requirements for recognition of the certification and the requirements for a standardised 'European Data Protection Seal' within the Union and in third countries].

8. The Commission may lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and recognize certification mechanisms and data protection seals and marks. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).

Article 40 **General principle for transfers** **Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation may only take place if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation.**	*Article 40* *General principle for transfers* (…).	Article 40 General principle for transfers Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation may only take place if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation.	PL nie zgłaszała sprzeciwu wobec usunięcia treści tego artykułu. W naszej ocenie zawiera on postanowienia, które wynikają z przepisów rozporządzenia i znajdą zastosowanie bez względu na to, czy zostaną expressis verbis wskazane w tym artykule.
Article 41 **Transfers with an adequacy decision** **1. A transfer may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any further authorisation.** **2. When assessing the adequacy of the level of protection, the**	Article 41 Transfers with an adequacy decision 1. A transfer <u>of personal data to a recipient or recipients in a third country or an international organisation</u> may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any <u>specific</u> authorisation. 2. When assessing the adequacy of	Article 41 Transfers with an adequacy decision 1. A transfer may take place where the Commission has decided that the third country, or a territory or a processing sector within that third country, or the international organisation in question ensures an adequate level of protection. Such transfer shall not require any *specific ~~further~~* authorisation. 2. When assessing the adequacy of the level of protection, the Commission shall give consideration to the following elements:	Ad. 41.1 - PL poprosiła o doprecyzowanie czy dobrze rozumiemy, że w przypadku pojęcia „processing sector" chodzi o sektor w sensie terytorialnym a nie o sektor gospodarki. Jesteśmy przeciwko wprowadzeniu możliwości uznania adekwatności sektorów w państwie trzecim. Będzie to prowadzić do wzrostu niepewności prawnej w zakresie adekwatności, w szczególności w zakresie oceny czy na danym obszarze obowiązuje adekwatność. Ust. 2 – PL wnioskowała aby lista w ust.

Commission shall give consideration to the following elements: **(a) the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law, the professional rules and security measures which are complied with in that country or by that international organisation, as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;** **(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organisation in question responsible for ensuring compliance with the data protection rules, for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and** **(c) the international commitments the third country or international organisation in question has entered into.** **3. The Commission may decide**	the level of protection, the Commission shall, <u>in particular, take account of</u> the following elements: (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation (…), data protection rules and security measures, including rules for onward transfer of personal data to another third country or international organisation, which are complied with in that country or by that international organisation, as well as the existence of effective and enforceable data subject rights and effective administrative and judicial redress for data subjects whose personal data are being transferred(…),; (b) the existence and effective functioning of one or more independent supervisory authorities in the third country, or <u>to which an</u> international organisation <u>is subject, with responsibility</u> for ensuring compliance with the data protection rules, for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and (c) the international commitments the third country or international organisation <u>concerned</u> has entered into <u>in relation to the protection of personal data,</u> 3. The Commission, <u>after assessing the adequacy of the level of protection,</u> may	(a) the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law *as well as the implementation of this legislation*, the professional rules and security measures which are complied with in that country or by that international organisation, *jurisprudential precedents,* as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred; (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organisation in question responsible for ensuring compliance with the data protection rules, *including sufficient sanctioning powers*, for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and (c) the international commitments the third country or international organisation in question has entered into*, in particular any legally binding conventions or instruments with respect to the protection of personal data.*	2 była otwarta. Ad. 41.4a – Przedstawiciel PL poprze wprowadzenie 41.4a. Państwa trzecie, których adekwatność została uznana muszą być monitorowane, konieczne jest zagwarantowanie Komisji Europejskiej możliwości zmiany decyzji dotyczącej adekwatności. Ad. 41.5 – Uważamy, że decyzja Komisji Europejskiej dotycząca wygaśnięcia adekwatności powinna zostać poprzedzona wydaniem opinii przez European Data Protection Board. Ponadto, jesteśmy za możliwością przyjmowania przez Komisję Europejską negatywnych decyzji dotyczących adekwatności. W naszej ocenie będzie to czynnik motywujący państwa trzecie do wprowadzania u siebie wysokich standardów ochrony danych a także informacja dla podmiotów w UE, na które kraje szczególnie należy zwracać uwagę. W związku z powyższym, prosimy o dodania Polski do przypisu 22. Jesteśmy także za przywróceniem poprzedniego brzmienia pierwszego zdania motywu 82. Ad. 41.6 –PL opowiedziała się za pozostawieniem 41.6. Niemniej prosilibyśmy o wyjaśnienie od Komisji Europejskiej, czym miałaby skutkować konsultacja przeprowadzana przez

that a third country, or a territory or a processing sector within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2). **4. The implementing act shall specify its geographical and sectoral application, and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2.** **5. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. Those implementing acts shall be adopted in accordance with the examination procedure referred to**	decide that a third country, or a territory or a processing sector within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. <u>The implementing act shall specify its territorial and sectoral application and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2. The</u> implementing act shall be adopted in accordance with the examination procedure referred to in Article 87(2). <u>3a</u> Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force until amended, replaced or repealed by the Commission. 4. (…) 4a. The Commission shall monitor the functioning of decisions adopted pursuant to paragraph 3 and decisions adopted on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC. 5. The Commission may decide that a third country, or a territory or a processing sector within that third country, or an international organisation <u>no longer</u> ensures an adequate level of protection within the meaning of paragraph 2 <u>and may, where necessary, repeal, amend or suspend such decision without retro-active effect.</u>	3. The Commission *shall be empowered to adopt delegated acts in accordance with Article 86 to* ~~*may*~~ decide that a third country, or a territory or a processing sector within that third country, or an international organisation ensures an adequate level of protection within the meaning of paragraph 2. ~~*Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).*~~ *Such delegated acts shall provide for a sunset clause if they concern a processing sector and shall be revoked according to paragraph 5 as soon as an adequate level of protection according to this Regulation is no longer ensured.* 4. The *delegated* ~~*implementing*~~ act shall specify its *territorial* ~~*geographical*~~ and sectoral application, and, where applicable, identify the supervisory authority mentioned in point (b) of paragraph 2. *4a. The Commission shall, on an on-going basis, monitor developments in third countries and international organisations that could affect the elements listed in paragraph 2 where a delegated act pursuant to paragraph 3 has been adopted.* 5. The Commission *shall be empowered to adopt delegated acts in accordance with*	Komisję.

in Article 87(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 87(3). **6. Where the Commission decides pursuant to paragraph 5, any transfer of personal data to the third country, or a territory or a processing sector within that third country, or the international organisation in question shall be prohibited, without prejudice to Articles 42 to 44. At the appropriate time, the Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation resulting from the Decision made pursuant to paragraph 5 of this Article.** **7. The Commission shall publish in the Official Journal of the European Union a list of those third countries, territories and processing sectors within a third country and international organisations where it has decided that an adequate level of protection is or is not ensured.** **8. Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force, until amended, replaced or repealed by the**	The implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2) or, in cases of extreme urgency (…), in accordance with the procedure referred to in Article 87(3). 6. (…) A decision (…) pursuant to paragraph 5 (…) is without prejudice to transfers of personal data to the third country, or the territory or (…) processing sector within that third country, or the international organisation in question pursuant to Articles 42 to 44 (…). At the appropriate time, the Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the Decision made pursuant to paragraph 5. 7. The Commission shall publish in the *Official Journal of the European Union* a list of those third countries, territories and processing sectors within a third country and international organisations in respect of which decisions have been taken pursuant to paragraphs 3 and 5. 8. (…)	*Article 86 to ~~may~~* decide that a third country, or a territory or a processing sector within that third country, or an international organisation does not ensure *or no longer ensures* an adequate level of protection within the meaning of paragraph 2 of this Article, in particular in cases where the relevant legislation, both general and sectoral, in force in the third country or international organisation, does not guarantee effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred. ~~*Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2), or, in cases of extreme urgency for individuals with respect to their right to personal data protection, in accordance with the procedure referred to in Article 87(3).*~~ 6. Where the Commission decides pursuant to paragraph 5, any transfer of personal data to the third country, or a territory or a processing sector within that third country, or the international organisation in question shall be prohibited, without prejudice to Articles 42 to 44. At the appropriate time, the Commission shall enter into consultations with the third country or international organisation with a view to remedying the situation resulting from the	Odnośnie art. 41 ust. 5 (poprawka LIBE), popieramy możliwość wydawania negatywnych decyzji o adekwatności przez KE, zmiany pod koniec tego ustępu wymagają dalszej analizy.

Commission.	Decision made pursuant to paragraph 5 of this Article. *6a. Prior to adopting a delegated act pursuant to paragraphs 3 and 5, the Commission shall request the European Data Protection Board to provide an opinion on the adequacy of the level of protection. To that end, the Commission shall provide the European Data Protection Board with all necessary documentation, including correspondence with the government of the third country, territory or processing sector within that third country or the international organisation.* 7. The Commission shall publish in the *Official Journal of the European Union and on its website* a list of those third countries, territories and processing sectors within a third country and international organisations where it has decided that an adequate level of protection is or is not ensured. 8. Decisions adopted by the Commission on the basis of Article 25(6) or Article 26(4) of Directive 95/46/EC shall remain in force until *five years after the entry into force of this Regulation unless amended, replaced or repealed by the Commission before the end of this period*.

Article 42 **Transfers by way of appropriate safeguards** **1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument.** **2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by:** **(a) binding corporate rules in accordance with Article 43; or** **(b) standard data protection clauses adopted by the Commission. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2); or** **(c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 when declared generally valid by the Commission pursuant to**	*Article 42* *Transfers by way of appropriate safeguards* 1. Where the Commission has taken no decision pursuant to Article 41, a controller or processor may transfer personal data to a recipient or recipients in a third country or an international organisation only if the controller or processor has adduced appropriate safeguards *in a legally binding instrument* with respect to the protection of personal data (…). 2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by: (a) binding corporate rules pursuant to Article 43; or (b) standard data protection clauses adopted by the Commission (…) in accordance with the examination procedure referred to in Article 87(2); or (c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 and adopted by the Commission pursuant to the examination procedure referred to in Article 87(2); or (d) contractual clauses between the controller or processor and the recipient of	Article 42 Transfers by way of appropriate safeguards 1. Where the Commission has taken no decision pursuant to Article 41, *or decides that a third country, or a territory or processing sector within that third country, or an international organisation does not ensure an adequate level of protection in accordance with Article 41(5),* a controller or processor may *not* transfer personal data to a third country, territory or an international organisation ~~*only if*~~ *unless* the controller or processor has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument. 2. The appropriate safeguards referred to in paragraph 1 shall be provided for, in particular, by: (a) binding corporate rules in accordance with Article 43; or *(aa) a valid "European Data Protection Seal" for the controller and the recipient in accordance with paragraph 1e of Article 39;* ~~*(b) standard data protection clauses adopted by the Commission after consulting the European Data Protection. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2); or*~~	Ad. 42.2.f – PL opowie się przeciwko odniesieniu w tym miejscu do certyfikacji. Mocno popieramy ideę certyfikacji, niemniej w tym miejscu odwołanie do certyfikacji mogłoby się przełożyć, w naszej ocenie, na obniżenie poziomu ochrony danych osobowych przy transferach danych. Ponadto, mechanizmy certyfikacji nie mają mocy prawnej i nie przewidują możliwości egzekwowania praw podmiotów danych, dlatego nie powinny stanowić podstawy przekazania danych do państwa trzeciego. Ad. 42.5 – odstępstwo to powinno znajdować zastosowanie tylko do organów publicznych. Ponadto, zwracamy uwagę, iż porozumienie administracyjne („administrative arrangement"), ma w niektórych systemach prawnych, w tym polskim, określone znaczenie prawne i jest jednym ze zdefiniowanych instrumentów prawnych. Chcielibyśmy wyjaśnienia co oznacza to pojęcie w tym przepisie. Ponadto zwracamy uwagę, iż usunęliśmy w toku prac grupy DAPIX art. 34.1, w którym były wyraźne odniesienia do uprzedniej autoryzacji („prior authorisation") z art. 42.2.d oraz 42.5. Pojęcie uprzedniej autoryzacji wydaje się dostatecznie jasne, niemniej chcielibyśmy upewnić się, iż usunięcie art. 34.1 pozostaje bez wpływu na 42.5.

point (b) of Article 62(1); or **(d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4.** **3. A transfer based on standard data protection clauses or binding corporate rules as referred to in points (a), (b) or (c) of paragraph 2 shall not require any further authorisation.** **4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses according to point (a) of Article 34(1) from the supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.** **5. Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor shall obtain prior authorisation for the**	the data authorised by a supervisory authority pursuant to paragraph 4; or (e) an approved code of conduct pursuant to Article 38; or (f) a certification mechanism pursuant to Article 39., 3. A transfer based on *binding corporate rules or standard data protection clauses* as referred to in points (a), (b) or (c) of paragraph 2 shall not require any specific authorisation. 4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 (…), the controller or processor shall obtain prior authorisation of the contractual clauses (…) from the competent supervisory authority (…). 5. Where, nothwithstanding the requirement for a legally binding instrument in paragraph 1, appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor, being a public authority or body, shall obtain prior authorisation from the competent supervisory authority for any transfer, or category of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such a transfer (…).	(c) standard data protection clauses adopted by a supervisory authority in accordance with the consistency mechanism referred to in Article 57 when declared generally valid by the Commission pursuant to point (b) of Article 62(1); or (d) contractual clauses between the controller or processor and the recipient of the data authorised by a supervisory authority in accordance with paragraph 4. 3. A transfer based on standard data protection clauses*, a "European Data Protection Seal"* or binding corporate rules as referred to in points (a), *(aa)* ~~*(b)*~~ or (c) of paragraph 2 shall not require any ~~further~~ *specific* authorisation. 4. Where a transfer is based on contractual clauses as referred to in point (d) of paragraph 2 of this Article the controller or processor shall obtain prior authorisation of the contractual clauses from the supervisory authority. If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or

transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer. Such authorisation by the supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57. Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid, until amended, replaced or repealed by that supervisory authority.	5a. If the transfer referred to in paragraph 4 (…)is related to processing activities which concern data subjects in several Member States, or may substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57. 5b. Authorisations by a Member State or supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid until amended, replaced or repealed by that supervisory authority 6. (…)	substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57. 5. ~~Where the appropriate safeguards with respect to the protection of personal data are not provided for in a legally binding instrument, the controller or processor shall obtain prior authorisation for the transfer, or a set of transfers, or for provisions to be inserted into administrative arrangements providing the basis for such transfer. Such authorisation by the supervisory authority shall be in accordance with point (a) of Article 34(1). If the transfer is related to processing activities which concern data subjects in another Member State or other Member States, or substantially affect the free movement of personal data within the Union, the supervisory authority shall apply the consistency mechanism referred to in Article 57.~~ Authorisations by a supervisory authority on the basis of Article 26(2) of Directive 95/46/EC shall remain valid~~,~~ until *two years after the entry into force of this Regulation* ~~*amended, replaced or repealed by that supervisory authority*~~.	Ust. 5 (poprawka LIBE) - jesteśmy za pozostawieniem możliwości uzyskania uprzedniej zgody organu nadzorczego na transfer.

Article 43 **Transfers by way of binding corporate rules** **1. A supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they:** **(a) are legally binding and apply to and are enforced by every member within the controller's or processor's group of undertakings, and include their employees;** **(b) expressly confer enforceable rights on data subjects;** **(c) fulfil the requirements laid down in paragraph 2.** **2. The binding corporate rules shall at least specify:** **(a) the structure and contact details of the group of undertakings and its members;** **(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in**	*Article 43* *Transfers by way of binding corporate rules* 1. The competent supervisory authority shall *approve binding corporate rules* in accordance with the consistency mechanism set out in Article 58 (…) provided that they: (a) are legally binding and apply to, and are enforced by, every member concerned of the group of undertakings or group of enterprises engaged in a joint economic activity; (b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; (c) fulfil the requirements laid down in paragraph 2. 2. The binding corporate rules referred to in paragraph 1 shall at least specify the following elements: (a) the structure and contact details of the group concerned and of each of its members; (b) the data transfers or categories of transfers, including the types of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;	Article 43 Transfers by way of binding corporate rules 1. ~~*A*~~ *The* supervisory authority shall in accordance with the consistency mechanism set out in Article 58 approve binding corporate rules, provided that they: (a) are legally binding and apply to and are enforced by every member within the controller's ~~*or processor's*~~ group of undertakings *and those external subcontractors that are covered by the scope of the binding corporate rules*, and include their employees; (b) expressly confer enforceable rights on data subjects; (c) fulfil the requirements laid down in paragraph 2. *1a. With regard to employment data, the representatives of the employees shall be informed about and, in accordance with Union or Member State law and practice, be involved in the drawing-up of binding*	Ad. 43.3 - PL opowiedziała się za utrzymaniem 43.3, Komisja Europejska ma już doświadczenie w zakresie wiążących reguł korporacyjnych, z którego powinniśmy korzystać.

question; **(c) their legally binding nature, both internally and externally;** **(d) the general data protection principles, in particular purpose limitation, data quality, legal basis for the processing, processing of sensitive personal data; measures to ensure data security; and the requirements for onward transfers to organisations which are not bound by the policies;** **(e) the rights of data subjects and the means to exercise these rights, including the right not to be subject to a measure based on profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;** **(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the group of undertakings not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, if he**	(c) their legally binding nature, both internally and externally; (d) application of the general data protection principles, in particular purpose limitation, including the purposes which govern further processing, data quality, legal basis for the processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies (…) not bound by the binding corporate rules; (e) the rights of data subjects in regard to the processing of their personal data and the means to exercise these rights, including the right not to be subject to (…) profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules; (f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, on proving that that member is not responsible for the event	*corporate rules pursuant to Article 43.* 2. The binding corporate rules shall at least specify: (a) the structure and contact details of the group of undertakings and its members *and those external subcontractors that are covered by the scope of the binding corporate rules*; (b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question; (c) their legally binding nature, both internally and externally; (d) the general data protection principles, in particular purpose limitation, *data minimisation, limited retention periods,* data quality, *data protection by design and by default,* legal basis for the processing, processing of sensitive personal data;

proves that that member is not responsible for the event giving rise to the damage; **(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Article 11;** **(h) the tasks of the data protection officer designated in accordance with Article 35, including monitoring within the group of undertakings the compliance with the binding corporate rules, as well as monitoring the training and complaint handling;** **(i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules;** **(j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority;** **(k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, in particular by making available to the supervisory authority the results of the**	giving rise to the damage; (g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Articles 14 and 14a; (h) the tasks of any data protection officer designated in accordance with Article 35, including monitoring (…) compliance with the binding corporate rules within the group, as well as monitoring the training and complaint handling; (hh) the complaint procedures; (i) the mechanisms within the group (…) for ensuring the verification of compliance with the binding corporate rules; (j) the mechanisms for reporting and recording changes to the rules and reporting these changes to the supervisory authority; (k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group (…), in particular by making available to the supervisory authority the results of (…) verifications of the measures referred to in point (i) of this paragraph.	measures to ensure data security; and the requirements for onward transfers to organisations which are not bound by the policies; (e) the rights of data subjects and the means to exercise these rights, including the right not to be subject to a measure based on profiling in accordance with Article 20, the right to lodge a complaint before the competent supervisory authority and before the competent courts of the Member States in accordance with Article 75, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules; (f) the acceptance by the controller ~~*or processor*~~ established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member of the group of undertakings not established in the Union; the controller or the processor may only be exempted from this liability, in whole or in part, if he proves that that member is not responsible for the event giving rise to the damage; (g) how the information on the binding corporate rules, in particular on the

verifications of the measures referred to in point (i) of this paragraph. **3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.** **4. The Commission may specify the format and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).**	[3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.] 4. The Commission may specify the format and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 87(2).	provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in accordance with Article 11; (h) the tasks of the data protection officer designated in accordance with Article 35, including monitoring within the group of undertakings the compliance with the binding corporate rules, as well as monitoring the training and complaint handling; (i) the mechanisms within the group of undertakings aiming at ensuring the verification of compliance with the binding corporate rules; (j) the mechanisms for reporting and recording changes to the policies and reporting these changes to the supervisory authority; (k) the co-operation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, in particular by making available to the supervisory authority the results of the verifications of the measures

referred to in point (i) of this paragraph.

3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the *format, procedures,* criteria and requirements for binding corporate rules within the meaning of this Article, in particular as regards the criteria for their approval, *including transparency for data subjects,* the application of points (b), (d), (e) and (f) of paragraph 2 to binding corporate rules adhered to by processors and on further necessary requirements to ensure the protection of personal data of the data subjects concerned.

~~*4. The Commission may specify the format and procedures for the exchange of information by electronic means between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted, after requesting an opinion of the European Data Protection Board, in accordance with the examination procedure set out in Article 87(2).*~~

	Article 42a (propozycja DE) *Disclosures not authorised by Union law* *1. No judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a non-public controller or processor to disclose personal data shall be recognised or be enforceable in any manner, unless this is provided for by a mutual assistance treaty or an international agreement between the requesting third country and the Union or a Member State or other legal provisions at national or Union level.* *2. Where a judgment of a court or tribunal or a decision of an administrative authority of a third country requests a non-public controller or processor to disclose personal data, the controller or processor and, if any, the controller's representative, shall notify the supervisory authority of the request without undue delay and must obtain prior authorisation for the transfer by the supervisory authority in accordance with point (i) of Article 44 (1).* *3. The supervisory authority shall inform the competent national authority of the request. The controller or processor shall also inform the data subject of the request and of the authorisation by the supervisory authority.* *4. Paragraphs (2) and (3) shall not apply to the disclosure of personal data for the*	*Article 43a* *Transfers or disclosures not authorised by Union law* *1. No judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognized or be enforceable in any manner, without prejudice to a mutual legal assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State.* *2. Where a judgment of a court or tribunal or a decision of an administrative authority of a third country requests a controller or processor to disclose personal data, the controller or processor and, if any, the controller's representative, shall notify the supervisory authority of the request without undue delay and must obtain prior authorisation for the transfer or disclosure by the supervisory authority.* *3. The supervisory authority shall assess the compliance of the requested disclosure with the Regulation and in particular whether the disclosure is necessary and legally required in accordance with Article 44(1)(d) and (e)*	PL poparła wprowadzenie tego artykułu który lepiej będzie zabezpieczać dane osobowe obywateli UE przed transferami do państw trzecich, w przypadku gdy w prawie Unii lub państw członkowskich nie ma do takiego transferu odpowiedniej podstawy prawnej, a administrator danych jest zobowiązany do tego na podstawie prawa obcego.

	purpose of investigation, detection or prosecution of criminal offences or the execution of criminal penalties.	*and (5). Where data subjects from other Member States are affected, the supervisory authority shall apply the consistency mechanism referred to in Article 57.* *4. The supervisory authority shall inform the competent national authority of the request. Without prejudice to Article 21, the controller or processor shall also inform the data subject of the request and of the authorisation by the supervisory authority and where applicable inform the data subject whether personal data was provided to public authorities during the last consecutive 12-month period, pursuant to point (ha) of Article 14(1).* ~~*5. The Commission may lay down the standard format of the notifications to the supervisory authority referred to in paragraph 2 and the information of the data subject referred to in paragraph 4 as well as the procedures applicable to the notification and information. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).*~~

Article 44 **Derogations** **1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:** **(a) the data subject has consented to the proposed transfer, after having been informed of the risks of such transfers due to the absence of an adequacy decision and appropriate safeguards; or** **(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or** **(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or** **(d) the transfer is necessary for important grounds of public interest;**	*Article 44* ***Derogations for specific situations*** 1. In the absence of an adequacy decision pursuant to Article 41, or of appropriate safeguards pursuant to Article 42, a transfer or a category of transfers of personal data to a third country or an international organisation may take place only on condition that: (a) the data subject has consented to the proposed transfer, after having been informed of the risks of such transfers due to the absence of an adequacy decision and appropriate safeguards; or (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; or (d) the transfer is necessary for *important* reasons of (…) public interest; *this must be a public interest recognised in Union law or in the national law of the Member State to which the controller is*	Article 44 Derogations 1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that: (a) the data subject has consented to the proposed transfer, after having been informed of the risks of such transfers due to the absence of an adequacy decision and appropriate safeguards; or (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural	Ad. 44.1.d – Przedstawiciel PL poprze zmianę wprowadzoną w 44.1.d Jest to niezwykle istotne doprecyzowanie. W ocenie PL zdecydowanie nie powinno się zezwalać na przekazywanie danych do kraju trzeciego ze względu na interes państwa trzeciego. Ad. 44.1.h – Przedstawiciel PL opowie się za usunięciem tego ustępu, w naszej ocenie obniża on poziom ochrony danych osobowych w porównaniu do poziomu ochrony z dyrektywy 95/46. W razie pozostawienia 44.1.h, Przedstawiciel PL w toku dyskusji popierze stanowisko IT z przypisu 65 i opowie się za usunięciem ”where necessary” z 44.1.h. Ad. 44.2 – PL poprze pozostawienie 44.2. Ad. 44.6a – PL opowie się za utrzymaniem 44.6a, zwracamy uwagę na liczbę umów międzynarodowych, które być może trzeba by renegocjować w przypadku wejścia rozporządzenia w życie. W naszej ocenie powinny tu przeważyć względy zachowania pewności prawa. Ad. 44.7 – PL poprze usunięcie delegacji dla Komisji Europejskiej z 44.7.

or	*subject* ; or	or legal person; or	
(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or	(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or	(d) the transfer is necessary for important grounds of public interest; or	
(f) the transfer is necessary in order to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent; or	(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or	(e) the transfer is necessary for the establishment, exercise or defence of legal claims; or	
(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or	[(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case;] or	(f) the transfer is necessary in order to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent; or	
(h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where	(h) the transfer *which* is not large scale or *frequent*, is necessary for the purposes of legitimate interests pursued by the controller or the processor and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and*, where necessary*, based on this assessment adduced suitable safeguards with respect to the protection of personal data;. 2. [A transfer pursuant to point (g) of	(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case; or ~~*(h) the transfer is necessary for the purposes*~~	Ust. 1 lit. h) (poprawka LIBE) - Popieramy usunięcie art. 44 ust. 1 lit. h.

necessary. **2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.** **3. Where the processing is based on point (h) of paragraph 1, the controller or processor shall give particular consideration to the nature of the data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and adduced appropriate safeguards with respect to the protection of personal data, where necessary.** **4. Points (b), (c) and (h) of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers.** **5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the law of the Member State to which the**	paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.] 3. (…) 4. Points <u>(a),</u> (b) <u>and</u> (c) of paragraph 1 shall not apply to activities carried out by public authorities in the exercise of their public powers. 5. (…). 6. The controller or processor shall document the assessment as well as the <u>suitable</u> safeguards <u>(…)</u> referred to in point (h) of paragraph 1 in the <u>records</u> referred to in Article 28 (…). <u>[6a International agreements involving the transfer of personal data to third countries or international organisations which were concluded by Member States prior to the entry into force of this Regulation, and which are in compliance with Directive 95/46/EC, shall remain in force until amended, replaced or revoked.]</u> 7. (…)	~~*of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.*~~ 2. A transfer pursuant to point (g) of paragraph 1 shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients. ~~*3. Where the processing is based on point (h) of paragraph 1, the controller or processor shall give particular consideration to the nature of the data, the purpose and duration of the proposed processing operation or operations, as well as the situation in the country of origin, the third country and the country of final destination, and adduced appropriate safeguards with respect to the protection of personal data, where necessary.*~~ 4. Points (b)~~*,*~~ *and* (c) ~~*and (h)*~~ of paragraph 1

controller is subject.	shall not apply to activities carried out by public authorities in the exercise of their public powers.
6. The controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in point (h) of paragraph 1 of this Article in the documentation referred to in Article 28 and shall inform the supervisory authority of the transfer.	5. The public interest referred to in point (d) of paragraph 1 must be recognised in Union law or in the law of the Member State to which the controller is subject. ~~*6. The controller or processor shall document the assessment as well as the appropriate safeguards adduced referred to in point (h) of paragraph 1 of this Article in the documentation referred to in Article 28 and shall inform the supervisory authority of the transfer.*~~
7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying 'important grounds of public interest' within the meaning of point (d) of paragraph 1 as well as the criteria and requirements for appropriate safeguards referred to in point (h) of paragraph 1.	7. The ~~*Commission*~~ *European Data Protection Board* shall be *entrusted with the task of issuing guidelines, recommendations and best practices in accordance with Article 66 paragraph 1(b)* ~~*empowered to adopt delegated acts in accordance with Article 86*~~ for the purpose of further specifying ~~*'important grounds of public interest' within the meaning of point (d) of paragraph 1 as well as*~~ the criteria and requirements for ~~*appropriate safeguards referred to in point (h)*~~ *data transfers on the basis* of paragraph 1.

Article 45 **International co-operation for the protection of personal data** **1. In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to:** **(a) develop effective international co-operation mechanisms to facilitate the enforcement of legislation for the protection of personal data;** **(b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms;** **(c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data;** **(d) promote the exchange and documentation of personal data**	Article 45 International co-operation for the protection of personal data 1. In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to: (a) develop international co-operation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data; (b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through (…) , complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms; (c) engage relevant stakeholders in discussion and activities aimed at promoting international co-operation in the enforcement of legislation for the protection of personal data; (d) promote the exchange and documentation of personal data protection legislation and practice. 2. For the purposes of paragraph 1, the Commission shall take appropriate steps to advance the relationship with third	Article 45 International co-operation for the protection of personal data 1. In relation to third countries and international organisations, the Commission and supervisory authorities shall take appropriate steps to: (a) develop effective international co-operation mechanisms to *ensure ~~facilitate~~* the enforcement of legislation for the protection of personal data; (b) provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other fundamental rights and freedoms; (c) engage relevant stakeholders in discussion and activities aimed at furthering international co-operation in the enforcement of legislation for the protection of personal data; (d) promote the exchange and documentation of personal data protection legislation and practice*~~;~~* *(da) clarify and consult on jurisdictional conflicts with third countries.*	Dostrzegamy wartość dodatnią utrzymania tego artykułu dla międzynarodowej współpracy w zakresie ochrony danych osobowych.

protection legislation and practice. **2. For the purposes of paragraph 1, the Commission shall take appropriate steps to advance the relationship with third countries or international organisations, and in particular their supervisory authorities, where the Commission has decided that they ensure an adequate level of protection within the meaning of Article 41(3).**	countries and international organisations, including their supervisory authorities, <u>in particular</u> where the Commission has decided that they ensure an adequate level of protection within the meaning of Article 41(3)	2. For the purposes of paragraph 1, the Commission shall take appropriate steps to advance the relationship with third countries or international organisations, and in particular their supervisory authorities, where the Commission has decided that they ensure an adequate level of protection within the meaning of Article 41(3).	
		Article 45a *Report by the Commission* *The Commission shall submit to the European Parliament and the Council at regular intervals, starting not later than four years after the date referred to in Article 91(1), a report on the application of Articles 40 to 45. For that purpose, the Commission may request information from the Member States and supervisory authorities, which shall be supplied without undue delay. The report shall be made public.*	Popieramy ten ustęp, przekazywanie informacji dotyczących transferów danych jest niezwykle istotne.

Article 46 **Supervisory authority** **1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application of this Regulation and for contributing to its consistent application throughout the Union, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the Union. For these purposes, the supervisory authorities shall co-operate with each other and the Commission.** **2. Where in a Member State more than one supervisory authority are established, that Member State shall designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the European Data Protection Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 57.** **3. Each Member State shall notify to the Commission those**	*Article 46* ***Supervisory authority*** 1. Each Member State shall provide that one or more independent public authorities are responsible for monitoring the application of this Regulation. 1a Each supervisory authority shall contribute to the consistent application of this Regulation throughout the Union (…). For this purpose, the supervisory authorities shall co-operate with each other and the Commission **in accordance with Chapter VII**. 2. Where in a Member State more than one supervisory authority are established, that Member State shall designate the supervisory authority which shall represent those authorities in the European Data Protection Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 57. [3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to this Chapter, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them	Article 46 Supervisory authority 1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application of this Regulation and for contributing to its consistent application throughout the Union, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of their personal data and to facilitate the free flow of personal data within the Union. For these purposes, the supervisory authorities shall co-operate with each other and the Commission. 2. Where in a Member State more than one supervisory authority are established, that Member State shall designate the supervisory authority which functions as a single contact point for the effective participation of those authorities in the European Data Protection Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 57. 3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to this Chapter, by the date specified in Article 91(2) at the latest and, without delay, any subsequent	Brak uwag

provisions of its law which it adopts pursuant to this Chapter, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.	amendment affecting them.

Article 47 **Independence** **1. The supervisory authority shall act with complete independence in exercising the duties and powers entrusted to it.** **2. The members of the supervisory authority shall, in the performance of their duties, neither seek nor take instructions from anybody.** **3. Members of the supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.** **4. Members of the supervisory authority shall behave, after their term of office, with integrity and discretion as regards the acceptance of appointments and benefits.** **5. Each Member State shall ensure that the supervisory authority is provided with the adequate human, technical and financial resources, premises and infrastructure necessary for the effective performance of its duties and powers, including those to be carried out in the context of mutual**	*Article 47* ***Independence*** 1. Each supervisory authority shall act with complete independence in performing the duties and *exercising* the powers entrusted to it (…). 2. The member or members of each supervisory authority shall, in the performance of their duties and exercise of their powers, remain free from external influence, whether direct or indirect and neither seek nor take instructions from anybody. 3. (…) 4. (…) 5. Each Member State shall ensure that each supervisory authority is provided with the (…) human, technical and financial resources, premises and infrastructure necessary for the effective performance of its duties and exercise of its powers, including those to be carried out in the context of mutual assistance, co-operation and participation in the European Data Protection Board. 6. Each Member State shall ensure that each supervisory authority has its own staff which shall (…) be subject to the direction of the member or members of the	Article 47 Independence 1. The supervisory authority shall act with complete independence in exercising the duties and powers entrusted to it*, notwithstanding co-operation and consistency arrangements pursuant to Chapter VII of this Regulation*. 2. The members of the supervisory authority shall, in the performance of their duties, neither seek nor take instructions from anybody*, and maintain complete independence and impartiality*. 3. Members of the supervisory authority shall refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not. 4. Members of the supervisory authority shall behave, after their term of office, with integrity and discretion as regards the acceptance of appointments and benefits. 5. Each Member State shall ensure that the	PL podkreślała znaczenie zapewnienia gwarancji niezależności organu ochrony danych dla prawidłowego funkcjonowania nowych ram prawnych w zakresie ochrony danych osobowych.

assistance, co-operation and participation in the European Data Protection Board. **6. Each Member State shall ensure that the supervisory authority has its own staff which shall be appointed by and be subject to the direction of the head of the supervisory authority.** **7. Member States shall ensure that the supervisory authority is subject to financial control which shall not affect its independence. Member States shall ensure that the supervisory authority has separate annual budgets. The budgets shall be made public.**	supervisory authority. 7. Member States shall ensure that each supervisory authority is subject to financial control which shall not affect its independence. Member States shall ensure that each supervisory authority has separate **public** annual budgets, which **may be part of the overall state or national budget**.	supervisory authority is provided with the adequate human, technical and financial resources, premises and infrastructure necessary for the effective performance of its duties and powers, including those to be carried out in the context of mutual assistance, co-operation and participation in the European Data Protection Board. 6. Each Member State shall ensure that the supervisory authority has its own staff which shall be appointed by and be subject to the direction of the head of the supervisory authority. 7. Member States shall ensure that the supervisory authority is subject to financial control which shall not affect its independence. Member States shall ensure that the supervisory authority has separate annual budgets. The budgets shall be made public. *7a. Each Member State shall ensure that the supervisory authority shall be accountable to the national parliament for reasons of budgetary control.*

Article 48 **General conditions for the members of the supervisory authority** **1. Member States shall provide that the members of the supervisory authority must be appointed either by the parliament or the government of the Member State concerned.** **2. The members shall be chosen from persons whose independence is beyond doubt and whose experience and skills required to perform their duties notably in the area of protection of personal data are demonstrated.** **3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement in accordance with paragraph 5.** **4. A member may be dismissed or deprived of the right to a pension or other benefits in its stead by the competent national court, if the member no longer fulfils the conditions required for the performance of the duties or is guilty of serious misconduct.** **5. Where the term of office expires or the member resigns, the member shall continue to exercise the**	*Article 48* ***General conditions for the members of the supervisory authority*** 1. Member States shall provide that the member or members of each supervisory authority must be appointed (…) by the parliament **and/**or the government or the head of State of the Member State concerned **or by an independent body entrusted by Member State law with the appointment by means of a transparent procedure**. 2. The member or members shall have the qualifications, experience and skills required to perform their duties and exercise their powers (…). 3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement **in accordance with the law of the Member State concerned.** 4. (…). 5. (…)	Article 48 General conditions for the members of the supervisory authority 1. Member States shall provide that the members of the supervisory authority must be appointed either by the parliament or the government of the Member State concerned. 2. The members shall be chosen from persons whose independence is beyond doubt and whose experience and skills required to perform their duties notably in the area of protection of personal data are demonstrated. 3. The duties of a member shall end in the event of the expiry of the term of office, resignation or compulsory retirement in accordance with paragraph 5. 4. A member may be dismissed or deprived of the right to a pension or other benefits in its stead by the competent national court, if the member no longer fulfills the conditions required for the performance of the duties or is guilty of serious misconduct. 5. Where the term of office expires or the member resigns, the member shall continue to exercise the duties until a new member is appointed.	**Art. 48.1** – W opinii PL kwestia trybu wyboru członków organu nadzorczego nie powinna być regulowana rozporządzeniem. Przepis w obecnej formule nie ma istotnej treści normatywnej, ponieważ de facto dopuszcza powoływanie organu nadzorczego przez jakikolwiek podmiot wyznaczony przez prawo wewnętrzne państwa członkowskiego. Nie powinniśmy ponadto wywodzić ze spełnienia przesłanek z zapisu określającego sposób powoływania organu nadzorczego gwarancji jego niezależności – widzimy takie niebezpieczeństwo. Zwracamy również uwagę na przepis art. 49 ust. 1 lit. c, zgodnie z którym procedury powoływania członków organu nadzorczego będą określone w prawie krajowym. Ten przepis jest w opinii PL wystarczającym do określenia zasad i procedur wyboru organu nadzorczego.

duties until a new member is appointed.			
Article 49 **Rules on the establishment of the supervisory authority** **Each Member State shall provide by law within the limits of this Regulation:** **(a) the establishment and status of the supervisory authority;** **(b) the qualifications, experience and skills required to perform the duties of the members of the supervisory authority;** **I the rules and procedures for the appointment of the members of the supervisory authority, as well the rules on actions or occupations incompatible with the duties of the**	*Article 49* ***Rules on the establishment of the supervisory authority*** 1. Each Member State shall provide by law for: (a) the establishment (…) of each supervisory authority; (b) the qualifications (…) required to perform the duties of the members of the supervisory authority; (c) the rules and procedures for the appointment of the member or members of each supervisory authority (…); (d) the duration of the term of the member or members of each supervisory authority which shall not be (…) less than four years, except for the first appointment after entry into force of this Regulation, part	Article 49 Rules on the establishment of the supervisory authority Each Member State shall provide by law within the limits of this Regulation: (a) the establishment and status of the supervisory authority; (b) the qualifications, experience and skills required to perform the duties of the members of the supervisory authority;	**Art. 49.1.f -** Przepis nie jest do końca jasny co do tego, co PCz powinno określić w swoim prawie krajowym, i czy sformułowanie *including* oznacza obligatoryjność czy fakultatywność PCz do określania zasad dot. niepodejmowania przez członków i personel organu nadzorczego czynności niezgodnych z pełnionym stanowiskiem. Poza tym zastrzeżenia budzi sformułowanie „*members and staff*". O ile obostrzenia dot. pełnienia innych funkcji są uzasadnione w stosunku do członków organu nadzorczego (rozumianych jako sami rzecznicy ochrony danych osobowych i ich zastępcy), o tyle takie szerokie regulowanie zakresu obowiązków i możliwości pełnienia innych zadań w przypadku personelu budzi już

office; **(d) the duration of the term of the members of the supervisory authority which shall be no less than four years, except for the first appointment after entry into force of this Regulation, part of which may take place for a shorter period where this is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure;** **(e) whether the members of the supervisory authority shall be eligible for reappointment;** **(f) the regulations and common conditions governing the duties of the members and staff of the supervisory authority;** **(g) the rules and procedures on the termination of the duties of the members of the supervisory authority, including in case that they no longer fulfil the conditions required for the performance of their duties or if they are guilty of serious misconduct.**	of which may take place for a shorter period where this is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure; (e) whether and, if so, for how many terms the member or members of each supervisory authority shall be eligible for reappointment; (f) the (…) conditions governing the **duties** of the member or members and staff of each supervisory authority**, including prohibitions on actions and occupations incompatible therewith during and after the term of office** and rules governing the cessation of employment; (g) (…) 2. The member or members and the staff of each supervisory authority shall, in accordance with Union or Member State law, be subject to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their (…) duties or exercise of their powers, *both during and after their term of office*.	(c) the rules and procedures for the appointment of the members of the supervisory authority, as well the rules on actions or occupations incompatible with the duties of the office; (d) the duration of the term of the members of the supervisory authority which shall be no less than four years, except for the first appointment after entry into force of this Regulation, part of which may take place for a shorter period where this is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure; (e) whether the members of the supervisory authority shall be eligible for reappointment; (f) the regulations and common conditions governing the duties of the members and staff of the supervisory authority; (g) the rules and procedures on the termination of the duties of the members of the supervisory authority, including in case that they no longer fulfil the conditions required for the performance of their duties	wątpliwości, w szczególności co do tego, czy cały personel musi być objęty tego typu regulacją. PL chce uzyskać jasność co do zakresu swobody uregulowania tych kwestii w prawie krajowym.

		or if they are guilty of serious misconduct.	
Article 50 **Professional secrecy** **The members and the staff of the supervisory authority shall be subject, both during and after their term of office, to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their official duties.**	*Article 50* ***Professional secrecy*** (…)	Article 50 Professional secrecy The members and the staff of the supervisory authority shall be subject, both during and after their term of office *and in conformity with national legislation and practice*, to a duty of professional secrecy with regard to any confidential information which has come to their knowledge in the course of the performance of their official duties, *whilst conducting their duties with independence and transparency as set out in the Regulation*.	PL nie zgłosiła zastrzeżeń do przeniesienia art. 50 do art. 49.2.

Article 51 **Competence** **1. Each supervisory authority shall exercise, on the territory of its own Member State, the powers conferred on it in accordance with this Regulation.** **2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.** **3. The supervisory authority shall not be competent to supervise processing operations of courts acting in their judicial capacity.**	*Article 51* ***Competence*** 1. Each supervisory authority shall be competent to perform the duties and to exercise the powers conferred on it in accordance with this Regulation on the territory of its own Member State. 1a. **OPTION 1:** Where pursuant to Article 54a a supervisory authority **acts** as lead authority, *this authority shall be the sole supervisory authority competent for (…) exercising the powers pursuant to paragraph 1c of Article 53 as regards the processing activities of the controller or the processor in all Member States concerned*. 1a. **OPTION 2:** Where pursuant to Article 54a a supervisory authority **acts** as lead authority, *this authority shall be the sole supervisory authority competent for (…) exercising the powers pursuant to point (c) of paragraph 1, points (e) and (f) of paragraph 1b and paragraph 1c of Article 53 as regards the processing activities of the controller or the processor in all Member States concerned*. 1a. **OPTION 3:** Where pursuant to Article 54a a supervisory authority **acts** as lead authority, *this authority shall be the sole supervisory authority competent for (…) exercising the powers pursuant to point (c) of paragraph 1, points (e) to (g) of paragraph*	Article 51 Competence 1. Each supervisory authority shall be *competent to perform the duties and to* exercise~~*, on the territory of its own Member State,*~~ the powers conferred on it in accordance with this Regulation *on the territory of its own Member State, without prejudice to Articles 73 and 74. Data processing by a public authority shall be supervised only by the supervisory authority of that Member State.* ~~*2. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State, the supervisory authority of the main establishment of the controller or processor shall be competent for the supervision of the processing activities of the controller or the processor in all Member States, without prejudice to the provisions of Chapter VII of this Regulation.*~~ 3. The supervisory authority shall not be competent to supervise processing	Poland supports option 3, in our opinion the lead authority should have a strong position and broadest possible competences. We would like to give lead authority not only authorisation powers and exclusive power to issue orders but as well to impose limitations on processing, order suspension of data flows and to impose administrative fines pursuant to Article 79 and 79a.

	1b and paragraph 1c of Article 53 as regards the processing activities of the controller or the processor in all Member States concerned. 1b. **Paragraph 1a shall not apply where the processing concerned only relates to one Member State.** 1c. *Paragraph 1a shall not apply to public authorities and bodies.* 2. (…) 2a. (…) 2b. (…) 3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.	operations of courts acting in their judicial capacity.

Article 52 **Duties** **1. The supervisory authority shall:** **(a) monitor and ensure the application of this Regulation;** **(b) hear complaints lodged by any data subject, or by an association representing that data subject in accordance with Article 73, investigate, to the extent appropriate, the matter and inform the data subject or the association of the progress and the outcome of the complaint within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary;** **I share information with and provide mutual assistance to other supervisory authorities and ensure the consistency of application and enforcement of this Regulation;** **(d) conduct investigations either on its own initiative or on the basis of a complaint or on request of another supervisory authority, and inform the data subject concerned, if the data subject has addressed a complaint to this supervisory authority, of the**	*Article 52* ***Duties*** 1. **Without prejudice to other duties set out under this Regulation, e**ach supervisory authority shall: (a) monitor and enforce the application of this Regulation; (aa) *promote (…) public awareness of the risks, rules, safeguards and rights in relation to the processing of personal data. Activities addressed specifically to children shall receive specific attention*; (ab) *inform the national parliament, the government or other political institution as well as the public on any issue related to the protection of personal data* (ac) *promote the awareness of controllers* (…) *and processors of their obligations under this Regulation;* (ad) *upon request, provide information to any data subject concerning the exercise of their rights under this Regulation and, if appropriate, co-operate with the supervisory authorities in other Member States to this end;*. (b) deal with complaints lodged by a data subject, or body, organisation or association representing a data subject in	Article 52 Duties 1. The supervisory authority shall: (a) monitor and ensure the application of this Regulation; (b) hear complaints lodged by any data subject, or by an association ~~*representing that data subject*~~ in accordance with Article 73, investigate, to the extent appropriate, the matter and inform the data subject or the association of the progress and the outcome of the complaint within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary; (c) share information with and provide mutual assistance to other supervisory authorities and ensure the consistency of application and enforcement of this Regulation; (d) conduct investigations, either on its own initiative or on the basis of a complaint or *of specific and documented information received alleging unlawful processing or* on request of another supervisory authority, and inform the data subject concerned, if the data subject has addressed a complaint to this supervisory authority, of the outcome of the investigations within a	**Art. 52.1.k** - PL zwróci uwagę, że zapis ten ma charakter bardzo ogólny – nie wiadomo, jaki jest charakter wydawanych na tej podstawie opinii (wiążący czy niewiążący) ani czy te opinie mają być wydawane na wniosek czy też z inicjatywy samego organu nadzorczego, kto ewentualnie mógłby się zwracać do organu nadzorczego o przedstawienie tych opinii (administrator?). W związku z tym wnioskujemy o usunięcie tego przepisu bądź jego doprecyzowanie, w szczególności poprzez zaznaczenie, że opinie te nie mają charakteru wiążącego.

outcome of the investigations within a reasonable period; **(e) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;** **(f) be consulted by Member State institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data;** **(g) uthorize and be consulted on the processing operations referred to in Article 34;** **(h) issue an opinion on the draft codes of conduct pursuant to Article 38(2);** **(i) approve binding corporate rules pursuant to Article 43;** **(j) participate in the activities of the European Data Protection Board.** **2. Each supervisory authority shall promote the awareness of the public on risks, rules, safeguards and rights in relation to the processing of personal data. Activities addressed**	accordance with Article 73, and investigate, to the extent appropriate, the subject matter of the complaint and inform the data subject or the body, organisation or association of the progress and the outcome of the investigation within a reasonable period, in particular if further investigation or coordination with another supervisory authority is necessary; (c) share information with and provide mutual assistance to other supervisory authorities with a view to ensuring the consistency of application and enforcement of this Regulation; (d) conduct investigations on the application of this Regulation either on its own initiative or on the basis of a information received from another supervisory or other public authority (…); (e) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices; (f) (…); (fa) (…); (g) (…); (ga) (…);	reasonable period; (e) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices; (f) be consulted by Member State institutions and bodies on legislative and administrative measures relating to the protection of individuals' rights and freedoms with regard to the processing of personal data; (g) authorise and be consulted on the processing operations referred to in Article 34; (h) issue an opinion on the draft codes of conduct pursuant to Article 38(2); (i) approve binding corporate rules pursuant to Article 43;

specifically to children shall receive specific attention. **3. The supervisory authority shall, upon request, advise any data subject in exercising the rights under this Regulation and, if appropriate, co-operate with the supervisory authorities in other Member States to this end.** **4. For complaints referred to in point (b) of paragraph 1, the supervisory authority shall provide a complaint submission form, which can be completed electronically, without excluding other means of communication.** **5. The performance of the duties of the supervisory authority shall be free of charge for the data subject.** **6. Where requests are manifestly excessive, in particular due to their repetitive character, the supervisory authority may charge a fee or not take the action requested by the data subject. The supervisory authority shall bear the burden of proving the manifestly excessive character of the request.**	(gb) (…); (gc) (…); (gd) (…); (h) (…); (ha) (…); (hb) (…); (i) (…); (j) contribute to the activities of the European Data Protection Board; *(k) issue opinions as well as fulfill any other duties related to the protection of personal data.* 2. (…). 3. (…). 4. Each supervisory authority shall **enable** the submission of complaints referred to in point (b) of paragraph 1, by measures which can be completed electronically, *such as providing a complaint submission form,* without excluding other means of communication. 5. The performance of the duties of each supervisory authority shall be free of charge for the data subject and for the data protection officer.	(j) participate in the activities of the European Data Protection Board*;* *(ja) certify controllers and processors pursuant to Article 39.* 2. Each supervisory authority shall promote the awareness of the public on risks, rules, safeguards and rights in relation to the processing of personal data *and on appropriate measures for personal data protection*. Activities addressed specifically to children shall receive specific attention. *2a. Each supervisory authority shall together with the European Data Protection Board promote the awareness of controllers and processors on risks, rules, safeguards and rights in relation to the processing of personal data. This includes keeping a register of sanctions and breaches. The register should enroll both all warnings and sanctions as detailed as possible, and the resolving of breaches. Each supervisory authority shall provide micro, small and medium sized enterprise controllers and processors on request with general information on their responsibilities and*	PL poparła dodanie art. 52 ust. 2a (LIBE)

	6. Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may refuse to act on the request (…). The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.	*obligations in accordance with this Regulation.* 3. The supervisory authority shall, upon request, advise any data subject in exercising the rights under this Regulation and, if appropriate, co-operate with the supervisory authorities in other Member States to this end. 4. For complaints referred to in point (b) of paragraph 1, the supervisory authority shall provide a complaint submission form, which can be completed electronically, without excluding other means of communication. 5. The performance of the duties of the supervisory authority shall be free of charge for the data subject. 6. Where requests are manifestly excessive, in particular due to their repetitive character, the supervisory authority may charge a *reasonable* fee or not take the action requested by the data subject. *Such a fee shall not exceed the costs of taking the action requested.* The supervisory authority shall bear the burden of proving the manifestly excessive character of the request.

Article 53 **Powers** **1. Each supervisory authority shall have the power:** **(a) to notify the controller or the processor of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, order the controller or the processor to remedy that breach, in a specific manner, in order to improve the protection of the data subject;** **(b) to order the controller or the processor to comply with the data subject's requests to exercise the rights provided by this Regulation;** **(c) to order the controller and the processor, and, where applicable, the representative to provide any information relevant for the performance of its duties;** **(d) to ensure the compliance with prior authorisations and prior consultations referred to in Article 34;** **(e) to warn or admonish the controller or the processor;** **(f) to order the rectification, erasure or destruction of all data when they have been processed in breach of**	***Art. 53*** ***Powers*** 1. Each Member State shall provide by law that its supervisory authority shall have at least the following monitoring powers: *(a) to order the controller and the processor, and, where applicable, the representative to provide any information it requires for the performance of its duties;* *(aa) to carry out data protection audits ;* (b) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights provided by this Regulation; *(c) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;* *(d) to notify the controller or the processor of an alleged infringement of this Regulation, and where appropriate, order the controller or the processor to remedy that infringement;* 1a. Each Member State shall provide by law that its supervisory authority shall	Article 53 Powers 1. Each supervisory authority shall*, in line with this regulation,* have the power: (a) to notify the controller or the processor of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, order the controller or the processor to remedy that breach, in a specific manner, in order to improve the protection of the data subject, *or to order the controller to communicate a personal data breach to the data subject*; (b) to order the controller or the processor to comply with the data subject's requests to exercise the rights provided by this Regulation; (c) to order the controller and the processor, and, where applicable, the representative to provide any information relevant for the performance of its duties; (d) to ensure the compliance with prior authorisations and prior consultations referred to in Article 34; (e) to warn or admonish the controller or the processor;	**Art. 53.1.(aa)** – należy dokładnie wyjaśnić co należy rozumieć przez audyt. Jak rozumiemy, chodzi tu o inspekcję przeprowadzaną przez organ nadzorczy, czyli kontrolę przestrzegania przepisów. Być może należałoby w tym miejscu użyć pojęcia „*inspection*" jako bardziej jednoznacznego. **Art. 53.1b lit (a) i (b)** – zastrzeżenie analityczne. Przedstawiciel PL zaznaczy, iż należy dokładniej wyjaśnić, czym są upomnienia („*reprimands*") a czym są ostrzeżenia („*warnings*"). Rozumiemy, że upomnienia znajdują zastosowanie, gdy doszło już do naruszenia przepisów, a ostrzeżenia w przypadku, gdy takie ryzyko dopiero potencjalnie istnieje. Nie jest jednak znany skutek prawny wydania przez organ nadzorczy wobec administratora bądź procesora upomnienia/ostrzeżenia jak i nie są do końca znane relacje uprawnień do wydawania upomnień i ostrzeżeń do uprawnień związanych z nakładaniem przez DPA sankcji administracyjnych i kar. Czy w przypadku wydania przez organ nadzorczy upomnienia/ostrzeżenia administrator/procesor będzie miał możliwość ich zaskarżenia? Czy administrator/procesor będzie musiał wskutek otrzymania upomnienia/ostrzeżenia podjąć czynności naprawcze i wg jakiej

the provisions of this Regulation and the notification of such actions to third parties to whom the data have been disclosed; **(g) to impose a temporary or definitive ban on processing;** **(h) to suspend data flows to a recipient in a third country or to an international organisation;** **(i) to issue opinions on any issue related to the protection of personal data;** **(j) to inform the national parliament, the government or other political institutions as well as the public on any issue related to the protection of personal data.** **2. Each supervisory authority shall have the investigative power to obtain from the controller or the processor:** **(a) access to all personal data and to all information necessary for the performance of its duties;** **(b) access to any of its premises, including to any data processing equipment and means, where there are reasonable grounds for presuming that an activity in violation of this**	have at least the folllowing investigatatory powers: (a) *to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its duties*; (b) *to obtain access to any premises of the controller and the processor , including to any data processing equipment and means* (…). 1b. Each Member State shall provide by law that its supervisory authority shall have the folllowing corrective powers: (a) *to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;* *(b) to issue reprimands to a controller or processor where processing operations have infringed provisions of this Regulation;* (c) (…) *(*d) to order the rectification, restriction or erasure (…) of (…) data pursuant to Articles 16, 17a and 17 (…) and the notification of such actions to recipients to whom the data have been disclosed pursuant to Articles 17(2a) and 17b; (e) to impose a temporary or definitive	(f) to order the rectification, erasure or destruction of all data when they have been processed in breach of the provisions of this Regulation and the notification of such actions to third parties to whom the data have been disclosed; (g) to impose a temporary or definitive ban on processing; (h) to suspend data flows to a recipient in a third country or to an international organisation; (i) to issue opinions on any issue related to the protection of personal data; *(ia) to certify controllers and processors pursuant to Article 39;* (j) to inform the national parliament, the government or other political institutions as well as the public on any issue related to the protection of personal data.	procedury? Czy PCz będą miały możliwość dookreślenia charakteru prawnego tych instrumentów w prawie wewnętrznym? **Art. 53.5** – PL poparł wprowadzenie tego ustępu – każdy przeciwko komu DPA podejmuje kroki prawne powinien mieć prawo do obrony, w szczególności rzetelnego procesu **(teraz usunięty)**

Regulation is being carried out there. **The powers referred to in point (b) shall be exercised in conformity with Union law and Member State law.** **3. Each supervisory authority shall have the power to bring violations of this Regulation to the attention of the judicial authorities and to engage in legal proceedings, in particular pursuant to Article 74(4) and Article 75(2).** **4. Each supervisory authority shall have the power to sanction administrative offences, in particular those referred to in Article 79(4), (5) and (6).**	**limitation** on processing; (f) to order the suspension of data flows to a recipient in a third country or to an international organisation; g) *to impose an administrative fine pursuant to Articles 79 and 79a*. .c. Each Member State shall provide by law that its supervisory authority shall have the folllowing authorisation powers: *a) authorise contractual clauses referred to in* ***Article 34, or in points (c) and (d) of*** *Article 42(2);* *(b) approve binding corporate rules pursuant to Article 43.* 2. (…) The powers referred to in paragraphs 1, 1a, 1b and 1c shall be exercised in conformity with **and** *subject to appropriate procedural safeguards, including effective judicial remedy and due process*, **set out in** Union law or Member State law. 3. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities **or** to commence or engage otherwise in legal proceedings in order to enforce the provisions of this Regulation.	*(ja) to put in place effective mechanisms to encourage confidential reporting of breaches of this Regulation, taking into account guidance issued by the European Data Protection Board pursuant to Article 66(4b).* 2. Each supervisory authority shall have the investigative power to obtain from the controller or the processor *without prior notice*: (a) access to all personal data and to all *documents and* information necessary for the performance of its duties; (b) access to any of its premises, including to any data processing equipment and means, ~~*where there are reasonable grounds for presuming that an activity in violation of this Regulation is being carried out there*~~. The powers referred to in point (b) shall be exercised in conformity with Union law and Member State law. 3. Each supervisory authority shall have the power to bring violations of this Regulation to the attention of the judicial authorities

4.	(…)	and to engage in legal proceedings, in particular pursuant to Article 74(4) and Article 75(2).
4a.	(…).	
5.	(…)	4. Each supervisory authority shall have the power to sanction administrative offences, in *accordance with* ~~*particular those referred to in*~~ Article 79~~*(4), (5) and (6)*~~. *This power shall be exercised in an effective, proportionate and dissuasive manner.*

	Article 54 Activity report Each supervisory authority <u>shall</u> draw up an annual report on its activities. The report shall be presented to the national parliament <u>or the government</u> and shall be made available to the public, the Commission and the European Data Protection Board.	Article 54 Activity report Each supervisory authority must draw up *a ~~an annual~~* report on its activities *at least every two years*. The report shall be presented to the *respective ~~national~~* parliament and shall be made be available to the public, the Commission and the European Data Protection Board.	
Article 54 **Activity report** **Each supervisory authority must draw up an annual report on its activities. The report shall be presented to the national parliament and shall be made be available to the public, the Commission and the European Data Protection Board.**	*<u>Article 54a</u>* ***<u>(…) Lead authority</u>*** 1. <u>Where the processing of personal data takes place in the context of the activities of **an** establishment of a controller or processor in **the Union and where the controller or processor is established in several Member States, the authority of the main establishment of a controller or processor shall act as lead authority as regards the processing activities of the controller or the processor in all Member States concerned by the processing activities.**</u> **1a. <u>Where the processing of personal data takes place in the context of the activities of a single establishment of a</u>**	*Article 54a* *Lead Authority* 1. Where the processing of personal data takes place in the context of the activities of an establishment of a controller or a processor in the Union, and the controller or processor is established in more than one Member State*, or where personal data of the residents of several Member States are processed,* the supervisory authority of the main establishment of the controller or processor shall *act as the lead authority responsible ~~be competent~~* for the supervision of the processing activities of the controller or the processor in all Member States, *in accordance with ~~without prejudice to~~* the provisions of Chapter VII of	we support the changes made by the Presidency in Article 54a, we agree with the concept and functions of the lead authority. We are glad to see conflict rules in paragraph 6 and very useful right to ask a supervisory authority whether it is the lead authority

	controller or processor in the Union but the processing affects substantially data subjects in several Member States or the free movement of data within the Union, the supervisory authority of that Member State shall act as lead authority as regards all Member States concerned by the processing activities.	this Regulation.
	2. **The lead authority shall be the sole contact point for the controller or processor**.	*2. The lead supervisory authority shall take appropriate measures for the supervision of the processing activities of the controller or processor for which it is responsible only after consulting all other competent supervisory authorities within the meaning of paragraph 1 of Article 51 in an endeavour to reach a consensus. For that purpose it shall in particular submit any relevant information and consult the other authorities before it adopts a measure intended to produce legal effects vis-à-vis a controller or a processor within the meaning of paragraph 1 of Article 51. The lead authority shall take the utmost account of the opinions of the authorities involved. The lead authority shall be the sole authority empowered to decide on measures intended to produce legal effects as regards the processing activities of the controller or processor for which it is responsible.*
	3. Where the controller exercises also activities as a processor, the supervisory authority of the main establishment of the controller shall act as lead authority (…).	
	4. (…)	
	5. (…)	
	6. Where there are conflicting views between the supervisory authorities involved on which supervisory authority shall be competent to act as lead authority, **any of the supervisory authorities involved may communicate the matter to the European Data Protection Board.** The European Data Protection Board shall issue an opinion on the identification of the lead authority.	*3. The European Data Protection Board shall, at the request of a competent supervisory authority, issue an opinion on the identification of the lead authority responsible for a controller or processor, in cases where:*
	7. **Any controller or processor may ask the supervisory authority of the**	*(a) it is unclear from the facts of the case*

	Member State in which it considers that its main establishment is located for confirmation that it is the lead authority. The lead authority shall communicate its reply to the other supervisory authorities concerned.	*where the main establishment of the controller or processor is located; or* *(b) the competent authorities do not agree on which supervisory authority shall act as lead authority;* *(c) the controller is not established in the Union, and residents of different Member States are affected by processing operations within the scope of this Regulation.* *3a. Where the controller exercises also activities as a processor, the supervisory authority of the main establishment of the controller shall act as lead authority for the supervision of processing activities.* *4. The European Data Protection Board may request the Commission to decide on the identification of the lead authority.*

Article 54b
Cooperation between the lead authority and other supervisory authorities

1. The lead authority referred to in Article 54a shall cooperate with the supervisory authorities of the Member States concerned (…) in an endeavour to reach consensus **on the cases set out hereafter**.

2. When preparing and deciding on a measure (…) **referred to in […]**, the lead authority shall:

a) share all relevant information with the supervisory authorities of the Member States concerned;

b) submit the draft measure to all **supervisory** authorities **of the Member States concerned**;

c) take utmost account of the views of the supervisory authorities **of the Member States concerned**.

3. **Where, in accordance with Article 73, a complaint has been lodged with a supervisory authority other than the lead authority referred to in Article 54a, this supervisory authority may prepare a draft a measure (…) referred to […] and submit it to the lead authority, which shall act in accordance with paragraph 2.**

Przedstawiciel PL opowie się za silną pozycją *lead authority* i wyrazi poparcie dla nowego brzmienia art. 54b

We support "in endeavour to reach consensus" in paragraph 1, we support the current wording of paragraph 2, we think that it gives local authorities a possibility to actively participate in the proceeding. We have doubts concerning paragraph 3 (and, accordingly, paragraph 5) – we think that, for the sake of speed and concentration of proceedings, the preparation of a draft measure should be generally entrusted to the lead authority. Paragraph 3 is not necessary also because every draft measure may be submitted to the consistency mechanism in accordance with paragraph 4.

4. Where **any of the** supervisory authorit**ies** has **objected**, within a period of two weeks after having been consulted **under paragraphs 2 or 3**, to the draft measure, **this** authority **may** submit the matter to the consistency mechanism referred to in Article 57.

5. **Where the lead authority does not act on a draft measure referred to in paragraph 3, within a period of two weeks after having received the draft measure, the supervisory authority to which a complaint has been lodged may submit the matter to the consistency mechanism referred to in Article 57.**

6. **By way of derogation to paragraph 1a of Article 51, each supervisory authority may, where there is an urgent need to act in order to protect the rights of data subjects, adopt a provisional measure on the territory of its Member State with a maximum validity of one month. The supervisory authority shall, without delay, communicate such a measure with full reasons to the European Data Protection Board in accordance with the consistency mechanism referred to in Article 57.**

7. **The lead authority and the other supervisory authorities concerned shall supply the information required under this Article to each other by electronic means, using a standardised format.**

	Article 54c ***Notification and enforcement of the measures adopted by the lead authority*** 1. **The lead authority shall notify the measure it adopts to the controller or processor concerned.** 2. **The supervisory authority to which a complaint has been lodged shall notify the measure which the lead authority has adopted to the data subject.** 3. **The measures adopted by the lead authority pursuant to this article shall be enforced by each supervisory authority concerned in accordance with Article 63.** **4. The controller or processor which is concerned by a measure referred to in paragraph 1 shall have the right to an effective judicial remedy against the lead**	Ad. Article 54c – Poland has serious doubts regarding paragraph 4 and 5, which in our opinion create too much confusion. It is difficult to imagine that data controller/processor has the right to judicial remedy in one Member State, and data subject, with respect to the same measure has the right to judicial remedy in another Member State. We suggest that both controller/processor and data subject should have the right to an effective judicial remedy against the lead authority. This situation does not differs from the one we have under the directive 95/46. We see the intention lying at the root of this proposal, but we feel that this is a complex issue of interplay between Member States' legal systems and cannot be resolved with one short

	authority in accordance with Article 74(1) and (3). 5. **The data subject which is concerned by a measure notified to him or her pursuant to paragraph 2 shall have the right to an effective judicial remedy against the supervisory authority to which the complaint has been lodged in accordance with Article 74.**		sentence.
Article 56 **Joint operations of supervisory authorities** **1. In order to step up co-operation and mutual assistance, the supervisory authorities shall carry out joint investigative tasks, joint enforcement measures and other joint operations, in which designated members or staff from other Member States' supervisory authorities are involved.** **2. In cases where data subjects in several Member States are likely to be affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in the joint investigative tasks or joint operations, as appropriate. The competent**	Article 56 Joint operations of supervisory authorities 1. (…) The supervisory authorities may, where appropriate, conduct *joint operations,* including joint investigatons and joint enforcement measures (…) in which (…) members or staff from other Member States' supervisory authorities are involved. 2. In cases where **the controller or processor has establishments in several Member States or where [**a significant number of] data subjects in several Member States are likely to be adversely affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in the (…) joint operations, as appropriate. The competent supervisory authority shall invite the supervisory authority of each of those Member States to take part in the (…) joint operations concerned and respond to the	Article 56 Joint operations of supervisory authorities 1. In order to step up co-operation and mutual assistance, the supervisory authorities shall carry out joint investigative tasks, joint enforcement measures and other joint operations, in which designated members or staff from other Member States' supervisory authorities are involved. 2. In cases *where the controller or processor has establishments in several Member States or* where data subjects in several Member States are likely to be affected by processing operations, a supervisory authority of each of those Member States shall have the right to participate in the joint investigative tasks or joint operations,	Art. 56.2 – W ostatnim zdaniu sugerujemy zamianę "the competent supervisory authority" na „the lead supervisory authority as defined in Article 54a" oraz zamianę "shall invite" na "shall involve". Art. 56.3a-3c – PL zgłosi zastrzeżenie analityczne. W toku przeprowadzanych konsultacji część ich uczestników wyrażała obawy, że ten przepis może stać się narzędziem zniechęcającym organy nadzorcze do udziału we wspólnych operacjach. Art. 56.2 - PL wnioskuje o dodanie na początku akapitu „In cases where the controller or processor has establishments in several Member States or" i dalej: "where a singificant number of data subjects" **(uwaga uwzględniona)**

supervisory authority shall invite the supervisory authority of each of those Member States to take part in the respective joint investigative tasks or joint operations and respond to the request of a supervisory authority to participate in the operations without delay. **3. Each supervisory authority may, as a host supervisory authority, in compliance with its own national law, and with the seconding supervisory authority's authorisation, confer executive powers, including investigative tasks on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the host supervisory authority's law permits, allow the seconding supervisory authority's members or staff to exercise their executive powers in accordance with the seconding supervisory authority's law. Such executive powers may be exercised only under the guidance and, as a rule, in the presence of members or staff from the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the host supervisory authority's national law. The host supervisory authority shall assume responsibility for their actions.** **4. Supervisory authorities shall**	request of a supervisory authority to participate (…) without delay. 3. A supervisory authority may, (…) in compliance with its own Member State law, and with the seconding supervisory authority's authorisation, confer (…) powers, including investigative powers on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the host supervisory authority's law permits, allow the seconding supervisory authority's members or staff to exercise their investigative powers in accordance with the seconding supervisory authority's law. Such investigative powers may be exercised only under the guidance and (…) in the presence of members or staff from the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the host supervisory authority's national law. (…) 3a. Where, in accordance with paragraph 1, officials of a Member State are operating in another Member State, the first Member State shall be liable for any damage caused by them during their operations, in accordance with the law of the Member State in whose territory they are operating.	as appropriate. The *lead authority as defined in Article 54a* ~~*competent authority*~~ shall *involve* ~~*invite*~~ the supervisory authority of each of those Member States ~~*to take part*~~ in the respective joint investigative tasks or joint operations and respond to the request of a supervisory authority to participate in the operations without delay. *The lead authority shall act as the single contact point for the controller or processor.* 3. Each supervisory authority may, as a host supervisory authority, in compliance with its own national law, and with the seconding supervisory authority's authorisation, confer executive powers, including investigative tasks on the seconding supervisory authority's members or staff involved in joint operations or, in so far as the host supervisory authority's law permits, allow the seconding supervisory authority's members or staff to exercise their executive powers in accordance with the seconding supervisory authority's law. Such executive powers may be exercised only under the guidance and, as a rule, in the presence of members or staff from the host supervisory authority. The seconding supervisory authority's members or staff shall be subject to the host supervisory authority's national law. The host supervisory authority shall assume responsibility for their actions.

lay down the practical aspects of specific co-operation actions. **5. Where a supervisory authority does not comply within one month with the obligation laid down in paragraph 2, the other supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 51(1).** **6. The supervisory authority shall specify the period of validity of a provisional measure referred to in paragraph 5. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission and shall submit the matter in the mechanism referred to in Article 57.**	3b. The Member State in whose territory the damage was caused shall make good such damage under the conditions applicable to damage caused by its own officials. The Member State whose officials have caused damage to any person in the territory of another Member State shall reimburse the latter in full any sums it has paid to the victims or persons entitled on their behalf. 3c. Without prejudice to the exercise of its rights vis-à-vis third parties and with the exception of paragraph 3b, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement of damages it has sustained from another Member State. 4. (…) 5. Where a joint operation is intended and a supervisory authority does not comply within one month with the obligation laid down in the second sentence of paragraph 2, the other supervisory authorities may adopt a provisional measure on the territory of its Member State in accordance with Article 51(1). 6. The supervisory authority shall specify the period of validity of a provisional measure referred to in paragraph 5, which	4. Supervisory authorities shall lay down the practical aspects of specific co-operation actions. 5. Where a supervisory authority does not comply within one month with the obligation laid down in paragraph 2, the other supervisory authorities shall be competent to take a provisional measure on the territory of its Member State in accordance with Article 51(1). 6. The supervisory authority shall specify the period of validity of a provisional measure referred to in paragraph 5. This period shall not exceed three months. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission and shall submit the matter in the mechanism referred to in Article 57.

	shall not exceed three months. The supervisory authority shall, without delay, communicate <u>such a</u> measure, <u>together with its</u> reasons <u>for adopting it</u>, to the European Data Protection Board and to the Commission (…) in <u>accordance with</u> the <u>consistency</u> mechanism referred to in Article 57.		
Article 57 **Consistency mechanism** **For the purposes set out in Article 46(1), the supervisory authorities shall co-operate with each other and the Commission through the consistency mechanism as set out in this section.**	**SECTION 2** **CONSISTENCY** Article 57 ***Consistency mechanism*** 1. For the purpose set out in Article 46(1<u>a</u>), the supervisory authorities shall co-operate with each other through the consistency mechanism as set out in this section. *2.* **<u>Without prejudice to the cases referred to in paragraph 4 of Article 54b,</u>** ***<u>a</u>*** *<u>competent</u> supervisory authority* **<u>which intends to</u>** *adopt a measure* **<u>aimed at</u>** <u>producing legal effects,</u> *shall communicate the draft measure to the European Data Protection Board and the Commission,* <u>when the measure:</u> *(a)* (…); *(b)* (…);	Article 57 Consistency mechanism For the purposes set out in Article 46(1), the supervisory authorities shall co-operate with each other and the Commission through the consistency mechanism *both on matters of general scope and in individual cases in accordance with the provisions of* ~~*as set out*~~ this section.	**Art. 57.2.c** – przedstawiciel PL podkreśli, iż Polska konsekwentnie opowiada się za powierzeniem zadania opracowania wymogów PIA EDPB, a nie organom krajowym. Takie rozwiązanie zapewni jednolite stosowanie rozporządzenia w całej UE i zmniejszy ryzyko forum shopping w tym zakresie. Jesteśmy za wykluczeniem Komisji z uczestnictwa w mechanizmie zgodności, wystarczy, że będzie o jego wynikach informowana. Uczestnictwo Komisji może mieć negatywny wpływ na niezależność procesujących organów nadzorczych.

(c) aims at adopting a list of the processing operations subject to the requirement for a data protection impact assesment pursuant to Article 33(2b); or

(ca) concerns a matter pursuant to Article 38(2b) whether a draft code of conduct or an amendment or extension to a code of conduct is in compliance with this Regulation; or

(cb) aims to approve the criteria for accereditation of a body pursuant to paragraph 3 of Article 38a or a certification body pursuant to paragraph 3 of Article 39a;

(d) aims to determine standard data protection clauses referred to in point (c) of Article 42(2); or

(e) aims to authorise contractual clauses referred to in point (d) of Article 42(2); or

(f) aims to approve binding corporate rules within the meaning of Article 43.

3. Where the competent supervisory authority does not submit a draft measure referred to in paragraph 2 to the Board or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56, *any supervisory authority concerned ,the European Data Protection*

Board or the Commission may request that such matter shall be communicated to the European Data Protection Board.

4. (…).

5. Supervisory authorities and the Commission shall electronically communicate to the European Data Protection Board, using a standardised format any relevant information, including as the case may be a summary of the facts, the draft measure, (…) the grounds which make the enactment of such measure necessary, and the views of other supervisory authorities concerned.

6. The chair of the European Data Protection Board shall without undue delay electronically inform the members of the European Data Protection Board and the Commission of any relevant information which has been communicated to it using a standardised format. The secretariat *of the European Data Protection Board shall, where necessary, provide translations of relevant information*.

Article 58 **Opinion by the European Data Protection Board** **1. Before a supervisory authority adopts a measure referred to in paragraph 2, this supervisory authority shall communicate the draft measure to the European Data Protection Board and the Commission.** **2. The obligation set out in paragraph 1 shall apply to a measure intended to produce legal effects and which:** **(a) relates to processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour; or** **(b) may substantially affect the free movement of personal data within the Union; or** **(c) aims at adopting a list of the processing operations subject to prior consultation pursuant to Article 34(5); or** **(d) aims to determine standard data protection clauses referred to in point (c) of Article 42(2); or** **(e) aims to authorise contractual**	*Article 58* ***Opinion by the European Data Protection Board*** 1. (…) 2. (…) 3. (…) 4. (…) 5. (…) 6. (…) 6a. **7.** In the cases referred to in **paragraph 4 of Article 54b, paragraph 6 of Article 54a and paragraph 2** of Article 57**, the** European Data Protection Board shall issue an opinion on **the subject**- matter submitted to it in the consistency mechanism provided it has not already issued an opinion on the same matter. **This** opinion (…) shall be adopted within one month by simple majority of the members of the European Data Protection Board (…) 7b. Where within the period referred to in paragraph 7a the European Data Protection Board does not adopt an opinion, the supervisory authority referred to in paragraph 2 of Article 57 may adopt its draft measure. 7c. The chair of the European Data	Article 58 *Consistency on matters of general application ~~Opinion by the European Data Protection Board~~* 1. Before a supervisory authority adopts a measure referred to in paragraph 2, this supervisory authority shall communicate the draft measure to the European Data Protection Board and the Commission. 2. The obligation set out in paragraph 1 shall apply to a measure intended to produce legal effects and which: *~~(a) relates to processing activities which are related to the offering of goods or services to data subjects in several Member States, or to the monitoring of their behaviour; or~~* *~~(b) may substantially affect the free movement of personal data within the Union; or~~* *~~(c) aims at adopting a list of the processing operations subject to prior consultation~~*	we are curious what lies behind limitation of the scope of EDPB opinions as set out in paragraph 7. Poland prefers to have the widest possible scope (at least as in the doc. 12929 from August 2013) so these opinions should include the measures that are intended to produce legal effects and that are intended to exercise the monitoring and corrective powers (including imposition of fines) and relate to processing activities which substantially affect a significant number of data subjects in several Member States. Proponujemy **usunięcie ust. 6a i 7** i przywrócenie poprzedniego brzmienia: *6a. The European Data Protection Board shall issue an opinion on the matters submitted to it in the consistency mechanism referred to in art. 57* Ponadto, w opinii PL EDPB powinna mieć prawo odmowy zajęcia się daną sprawą (podejmując taka decyzję zwykłą większością głosów) bez względu na jej charakter i biorąc pod uwagę, czy sprawa zawiera element nowości ze względu na okoliczności faktyczne lub prawne dotyczące rozwoju technologii oraz czy EDPB wcześniej wydawała opinię w podobnej sprawie. PL jest za **usunięciem ust. 10 i 11** i

clauses referred to in point (d) of Article 42(2); or **(f) aims to approve binding corporate rules within the meaning of Article 43.** **3. Any supervisory authority or the European Data Protection Board may request that any matter shall be dealt with in the consistency mechanism, in particular where a supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56.** **4. In order to ensure correct and consistent application of this Regulation, the Commission may request that any matter shall be dealt with in the consistency mechanism.** **5. Supervisory authorities and the Commission shall electronically communicate any relevant information, including as the case may be a summary of the facts, the draft measure, and the grounds which make the enactment of such measure necessary, using a standardised format.** **6. The chair of the European Data**	Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 2 and 4 of Article 57 and the Commission (…) of the opinion and make it public. 8. The supervisory authority referred to in paragraph 2 of Article 57 (…) shall take utmost account of the opinion of the European Data Protection Board and shall within two weeks after receiving the opinion , electronically communicate to the chair of the European Data Protection Board (…) whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format. 9. Where the supervisory authority concerned does not intend to follow the opinion, it shall inform the chair of the European Data Protection Board and the Commission within the period referred to in paragraph 8 and shall explain its refusal to follow the opinion. 10. Within one month after receiving the information referred to in paragraph 9, the European Data Protection Board may by a two-third majority of its members, adopt a further opinion on the subject-matter. 11. Where the supervisory authority concerned does not intend to follow such opinion, it shall inform the chair of the European Data Protection Board and the	~~*pursuant to Article 34(5); or*~~ (d) aims to determine standard data protection clauses referred to in point (c) of Article 42(2); or (e) aims to authorise contractual clauses referred to in point (d) of Article 42(2); or (f) aims to approve binding corporate rules within the meaning of Article 43. 3. Any supervisory authority or the European Data Protection Board may request that any matter *of general application* shall be dealt with in the consistency mechanism, in particular where a supervisory authority does not submit a draft measure referred to in paragraph 2 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56. 4. In order to ensure correct and consistent application of this Regulation, the Commission may request that any matter *of*	popiera **wprowadzenie w ich miejsce ust. 10 w wersji zaproponowanej przez IT:** *10. (new)The European Data Protection Board may request the Commission to decide that an opinion rendered by the Board shall be binding on the authority referred to in paragraph 2 of Article 57 or on any of the supervisory authorities concerned, as the case may be.* W opinii PL jest to dobre rozwiązanie, które pozwoli zapewnić stosowanie się krajowych DPA do opinii wydanych przez EDPB.

Protection Board shall immediately electronically inform the members of the European Data Protection Board and the Commission of any relevant information which has been communicated to it, using a standardised format. The chair of the European Data Protection Board shall provide translations of relevant information, where necessary.	Commission within 10 working days of the receipt of that opinion and shall explain its refusal to follow the opinion.	*general application* shall be dealt with in the consistency mechanism.
		5. Supervisory authorities and the Commission shall *without undue delay* ~~*immediately*~~ electronically communicate any relevant information, including as the case may be a summary of the facts, the draft measure, and the grounds which make the enactment of such measure necessary, using a standardised format.
		6. The chair of the European Data Protection Board shall *without undue delay* ~~*immediately*~~ electronically inform the members of the European Data Protection Board and the Commission of any relevant information which has been communicated to it, using a standardised format. The secretariat of the European Data Protection Board shall provide translations of relevant information, where necessary.
		6a. The European Data Protection Board shall adopt an opinion on matters referred to it under paragraph 2.
7. The European Data Protection Board shall issue an opinion on the matter, if the European Data Protection Board so decides by simple majority of its members or any supervisory authority or the Commission so requests within one week after the relevant information has been provided according to paragraph 5. The opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 1 and 3, the Commission and the supervisory authority competent under Article 51 of the opinion and make it public.		
8. The supervisory authority referred to in paragraph 1 and the supervisory authority competent under		7. The European Data Protection Board ~~*shall*~~ *may decide by simple majority whether to*

Article 51 shall take account of the opinion of the European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format.	adopt an opinion on *any ~~the~~ matter submitted under paragraphs 3 and 4 taking into account ~~if the European Data Protection Board so decides by simple majority of its members or any supervisory authority or the Commission so requests within one week after the relevant information has been provided according to paragraph 5. The opinion shall be adopted within one month by simple majority of the members of the European Data Protection Board. The chair of the European Data Protection Board shall inform, without undue delay, the supervisory authority referred to, as the case may be, in paragraphs 1 and 3, the Commission and the supervisory authority competent under Article 51 of the opinion and make it public.~~:* *(a) whether the matter presents elements of novelty, taking account of legal or factual developments, in particular in information technology and in the light of the state of progress in the information society; and* *(b) whether the European Data Protection Board has already issued an opinion on the same matter.* 8. *The European Data Protection Board shall*

		adopt opinions pursuant to paragraphs 6a and 7 by a simple majority of its members. These opinions shall be made public. ~~*The supervisory authority referred to in paragraph 1 and the supervisory authority competent under Article 51 shall take account of the opinion of the European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains or amends its draft measure and, if any, the amended draft measure, using a standardised format.*~~

	Article 58a *Consistency in individual cases* *1. Before taking a measure intended to produce legal effects within the meaning of Article 54a, the lead authority shall share all relevant information and submit the draft measure to all other competent authorities. The lead authority shall not adopt the measure if a competent authority has, within a period of three weeks, indicated it has serious objections to the measure.* *2. Where a competent authority has indicated that it has serious objections to a draft measure of the lead authority, or where the lead authority does not submit a draft measure referred to in paragraph 1 or does not comply with the obligations for mutual assistance in accordance with Article 55 or for joint operations in accordance with Article 56, the issue shall be considered by the European Data Protection Board.* *3. The lead authority and/or other competent authorities involved and the Commission shall without undue delay electronically communicate to the European Data Protection Board using a standardised format any relevant information, including*

		as the case may be a summary of the facts, the draft measure, the grounds which make the enactment of such measure necessary, the objections raised against it and the views of other supervisory authorities concerned. *4. The European Data Protection Board shall consider the issue, taking into account the impact of the draft measure of the lead authority on the fundamental rights and freedoms of data subjects, and shall decide by simple majority of its members whether to issue an opinion on the matter within two weeks after the relevant information has been provided pursuant to paragraph 3.* *5. In case the European Data Protection Board decides to issue an opinion, it shall do so within six weeks and make the opinion public.* *6. The lead authority shall take utmost account of the opinion of the European Data Protection Board and shall within two weeks after the information on the opinion by the chair of the European Data Protection Board, electronically communicate to the chair of the European Data Protection Board and to the Commission whether it maintains*

		or amends its draft measure and, if any, the amended draft measure, using a standardised format. Where the lead authority intends not to follow the opinion of the European Data Protection Board, it shall provide a reasoned justification. *7. In case the European Data Protection Board still objects to the measure of the supervisory authority as referred to in paragraph 5, it may within one month adopt by a two thirds majority a measure which shall be binding upon the supervisory authority.*	
Article 59 **Opinion by the Commission** **1. Within ten weeks after a matter has been raised under Article 58, or at the latest within six weeks in the case of Article 61, the Commission may adopt, in order to ensure correct and consistent application of this Regulation, an opinion in relation to matters raised pursuant to Articles 58 or 61.** **2. Where the Commission has adopted an opinion in accordance with paragraph 1, the supervisory authority**	Article 59 Opinion by the Commission (…)	~~*Article 59*~~ ~~*Opinion by the Commission*~~ ~~*1. Within ten weeks after a matter has been raised under Article 58, or at the latest within six weeks in the case of Article 61, the Commission may adopt, in order to ensure correct and consistent application of this Regulation, an opinion in relation to matters raised pursuant to Articles 58 or 61.*~~ ~~*2. Where the Commission has adopted an opinion in accordance with paragraph 1, the*~~	Jesteśmy za usunięciem uczestnictwa Komisji w mechanizmie zgodności, w związku z czym, konsekwentnie, za usunięciem tego artykułu.

concerned shall take utmost account of the Commission's opinion and inform the Commission and the European Data Protection Board whether it intends to maintain or amend its draft measure. **3. During the period referred to in paragraph 1, the draft measure shall not be adopted by the supervisory authority.** **4. Where the supervisory authority concerned intends not to follow the opinion of the Commission, it shall inform the Commission and the European Data Protection Board thereof within the period referred to in paragraph 1 and provide a justification. In this case the draft measure shall not be adopted for one further month.**		*~~supervisory authority concerned shall take utmost account of the Commission's opinion and inform the Commission and the European Data Protection Board whether it intends to maintain or amend its draft measure.~~* *~~3. During the period referred to in paragraph 1, the draft measure shall not be adopted by the supervisory authority.~~* *~~4. Where the supervisory authority concerned intends not to follow the opinion of the Commission, it shall inform the Commission and the European Data Protection Board thereof within the period referred to in paragraph 1 and provide a justification. In this case the draft measure shall not be adopted for one further month.~~*	
Article 60 **Suspension of a draft measure** **1. Within one month after the communication referred to in Article 59(4), and where the Commission has serious doubts as to whether the draft measure would ensure the correct application of this Regulation or would otherwise result in its inconsistent**	Article 60 Suspension of a draft measure (…)	*~~Article 60~~* *~~Suspension of a draft measure~~* *~~1. Within one month after the communication referred to in Article 59(4), and where the Commission has serious doubts as to whether the draft measure would ensure the correct application of this~~*	Jesteśmy za usunięciem uczestnictwa Komisji w mechanizmie zgodności, w związku z czym, konsekwentnie, za usunięciem tego artykułu.

application, the Commission may adopt a reasoned decision requiring the supervisory authority to suspend the adoption of the draft measure, taking into account the opinion issued by the European Data Protection Board pursuant to Article 58(7) or Article 61(2), where it appears necessary in order to:	~~*Regulation or would otherwise result in its inconsistent application, the Commission may adopt a reasoned decision requiring the supervisory authority to suspend the adoption of the draft measure, taking into account the opinion issued by the European Data Protection Board pursuant to Article 58(7) or Article 61(2), where it appears necessary in order to:*~~
(a) reconcile the diverging positions of the supervisory authority and the European Data Protection Board, if this still appears to be possible; or	~~*(a) reconcile the diverging positions of the supervisory authority and the European Data Protection Board, if this still appears to be possible; or*~~
(b) adopt a measure pursuant to point (a) of Article 62(1).	~~*(b) adopt a measure pursuant to point (a) of Article 62(1).*~~
2. The Commission shall specify the duration of the suspension which shall not exceed 12 months.	~~*2. The Commission shall specify the duration of the suspension which shall not exceed 12 months.*~~
3. During the period referred to in paragraph 2, the supervisory authority may not adopt the draft measure.	~~*3. During the period referred to in paragraph 2, the supervisory authority may not adopt the draft measure.*~~

		Article 60a *Notification of Parliament and Council* *The Commission shall notify the Council and the European Parliament at regular intervals, at least every two years, on the basis of a report from the Chair of the European Data Protection Board, of the matters dealt with under the consistency procedure, setting out the conclusions drawn by the Commission and the European Data Protection Board with a view to ensuring the consistent implementation and application of this regulation.*	Jesteśmy za usunięciem uczestnictwa Komisji w mechanizmie zgodności, w związku z czym, konsekwentnie, za usunięciem tego artykułu.
Article 61 **Urgency procedure** **1. In exceptional circumstances, where a supervisory authority considers that there is an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded by means of an alteration of the existing state or for averting major disadvantages or for other reasons, by way of derogation from the procedure referred to in**	*Article 61* ***Urgency procedure*** 1. In exceptional circumstances, where <u>the competent</u> supervisory authority considers that there is an urgent need to act in order to protect <u>rights and freedoms</u> of data subjects, (…) *it may*, by way of derogation from the <u>consistency mechanism</u> referred to in Article <u>57</u>, immediately adopt provisional measures <u>pursuant to</u> points **<u>(a), (b) and (c) of paragraph 1 of Article 53 and points (d), (e) and (f) of paragraph 1b of Article 53</u>**,with a specified period of validity. The supervisory authority shall, without delay, communicate	Article 61 Urgency procedure 1. In exceptional circumstances, where a supervisory authority considers that there is an urgent need to act in order to protect the interests of data subjects, in particular when the danger exists that the enforcement of a right of a data subject could be considerably impeded by means of an alteration of the existing state or for averting major disadvantages or for other reasons, by way of derogation from the procedure referred to in Article *58a* ~~*57*~~, it may immediately adopt provisional measures with a specified period of validity.	Wciąż zastanawiamy się nad procedurą z art. 61, w szczególności czy nie będzie ona wyłomem w ogólnych zasadach i czy nie będzie nadużywana przez organy ochrony danych.

Article 58, it may immediately adopt provisional measures with a specified period of validity. The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission.	those measures and the reasons for adopting them, to the European Data Protection Board and to the Commission.	The supervisory authority shall, without delay, communicate those measures, with full reasons, to the European Data Protection Board and to the Commission.
2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion of the European Data Protection Board, giving reasons for requesting such opinion, including for the urgency of final measures.	2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion of the European Data Protection Board, giving reasons for requesting such opinion (…).	2. Where a supervisory authority has taken a measure pursuant to paragraph 1 and considers that final measures need urgently be adopted, it may request an urgent opinion of the European Data Protection Board, giving reasons for requesting such opinion, including for the urgency of final measures.
3. Any supervisory authority may request an urgent opinion where the competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the interests of data subjects, giving reasons for requesting such opinion, including for the urgent need to act.	3. Any supervisory authority may request an urgent opinion where the competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the rights and freedoms of data subjects, giving reasons for requesting such opinion, including for the urgent need to act.	3. Any supervisory authority may request an urgent opinion where the competent supervisory authority has not taken an appropriate measure in a situation where there is an urgent need to act, in order to protect the interests of data subjects, giving reasons for requesting such opinion, including for the urgent need to act.
4. By derogation from Article 58(7), an urgent opinion referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the European Data Protection Board.	4. By derogation from paragraph 7a of Article 58, an urgent opinion referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the European Data Protection Board.	4. ~~*By derogation from Article 58(7), an*~~ *An* urgent opinion referred to in paragraphs 2 and 3 of this Article shall be adopted within two weeks by simple majority of the members of the European Data Protection Board.

Article 62 **Implementing acts** **1. The Commission may adopt implementing acts for:** **(a) deciding on the correct application of this Regulation in accordance with its objectives and requirements in relation to matters communicated by supervisory authorities pursuant to Article 58 or 61, concerning a matter in relation to which a reasoned decision has been adopted pursuant to Article 60(1), or concerning a matter in relation to which a supervisory authority does not submit a draft measure and that supervisory authority has indicated that it does not intend to follow the opinion of the Commission adopted pursuant to Article 59;** **(b) deciding, within the period referred to in Article 59(1), whether it declares draft standard data protection clauses referred to in point (d) of Article 58(2), as having general validity;** **(c) specifying the format and procedures for the application of the consistency mechanism referred to in this section;** **(d) specifying the arrangements**	*Article 62* ***Implementing acts*** 1. The Commission may adopt implementing acts of general **scope** for: (a) ensuring the correct and uniform application of this Regulation (…) in relation to matters communicated by supervisory authorities pursuant to Article 57(**2**)(b) (…). (b) (…); (c) (…) (d) specifying the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in Article 57(6) and (7) and in Article 58(5). Those implementing acts shall be adopted in accordance with the examination precedure referred to in Article 87(2). 2. On duly justified imperative grounds of urgency relating to the interests of data subjects in the cases referred to in point (a) of paragraph 1, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 87(3). Those acts shall remain in force for a period not	Article 62 Implementing Acts 1. The Commission may adopt implementing acts *of general application*, *after requesting an opinion of the European Data Protection Board,* for: ~~*(a) deciding on the correct application of this Regulation in accordance with its objectives and requirements in relation to matters communicated by supervisory authorities pursuant to Article 58 or 61, concerning a matter in relation to which a reasoned decision has been adopted pursuant to Article 60(1), or concerning a matter in relation to which a supervisory authority does not submit a draft measure and that supervisory authority has indicated that it does not intend to follow the opinion of the Commission adopted pursuant to Article 59;*~~ (b) deciding~~, within the period referred to in Article 59(1),~~ whether it declares draft standard data protection clauses referred to in point (d) of Article *42* ~~58~~(2), as having general validity; ~~*(c) specifying the format and procedures for the application of the consistency mechanism referred to in this section;*~~ (d) specifying the arrangements for the exchange of information by electronic

for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in Article 58(5), (6) and (8). **Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).** **2. On duly justified imperative grounds of urgency relating to the interests of data subjects in the cases referred to in point (a) of paragraph 1, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 87(3). Those acts shall remain in force for a period not exceeding 12 months.** **3. The absence or adoption of a measure under this Section does not prejudice any other measure by the Commission under the Treaties.**	exceeding 12 months. 3. The absence or adoption of a measure under this Section does not prejudice any other measure by the Commission under the Treaties.	means between supervisory authorities, and between supervisory authorities and the European Data Protection Board, in particular the standardised format referred to in Article 58(5), (6) and (8). ~~*Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).*~~ ~~*2. On duly justified imperative grounds of urgency relating to the interests of data subjects in the cases referred to in point (a) of paragraph 1, the Commission shall adopt immediately applicable implementing acts in accordance with the procedure referred to in Article 87(3). Those acts shall remain in force for a period not exceeding 12 months.*~~ 3. The absence or adoption of a measure under this Section does not prejudice any other measure by the Commission under the Treaties.

Article 63 **Enforcement** **1. For the purposes of this Regulation, an enforceable measure of the supervisory authority of one Member State shall be enforced in all Member States concerned.** **2. Where a supervisory authority does not submit a draft measure to the consistency mechanism in breach of Article 58(1) to (5), the measure of the supervisory authority shall not be legally valid and enforceable.**	*Article 63* ***Enforcement*** 1. For the purposes of this Regulation, a (…)**legally binding** measure of a supervisory authority of one Member State which is compliant with the requirements of this **Chapter** shall be enforceable in all Member States concerned **in accordance with their national law**. 2. (…)	Article 63 Enforcement 1. For the purposes of this Regulation, an enforceable measure of the supervisory authority of one Member State shall be enforced in all Member States concerned. 2. Where a supervisory authority does not submit a draft measure to the consistency mechanism in breach of Article 58(1) *and (2) ~~to (5)~~ or adopts a measure despite an indication of serious objection pursuant to Article 58a(1)*, the measure of the supervisory authority shall not be legally valid and enforceable.

Article 64 **European Data Protection Board** **1. A European Data Protection Board is hereby set up.** **2. The European Data Protection Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor.** **3. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, they shall nominate the head of one of those supervisory authorities as joint representative.** **4. The Commission shall have the right to participate in the activities and meetings of the European Data Protection Board and shall designate a representative. The chair of the European Data Protection Board shall, without delay, inform the Commission on all activities of the European Data Protection Board.**	**SECTION 3** **EUROPEAN DATA PROTECTION BOARD** *Article 64* ***European Data Protection Board*** 1. A European Data Protection Board is hereby set up. 2. The European Data Protection Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor. 3. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, they shall nominate the head of one of those supervisory authorities as joint representative. 4. The Commission shall have the right to participate in the activities and meetings of the European Data Protection Board and shall designate a representative without voting rights. The chair of the European Data Protection Board shall, **communicate** the Commission **the** activities of the European Data Protection Board.	Article 64 European Data Protection Board 1. A European Data Protection Board is hereby set up. 2. The European Data Protection Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor. 3. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, they shall nominate the head of one of those supervisory authorities as joint representative. 4. The Commission shall have the right to participate in the activities and meetings of the European Data Protection Board and shall designate a representative. The chair of the European Data Protection Board shall, without delay, inform the Commission on all activities of the European Data Protection Board.

Article 65 **Independence** **1. The European Data Protection Board shall act independently when exercising its tasks pursuant to Articles 66 and 67.** **2. Without prejudice to requests by the Commission referred to in point (b) of paragraph 1 and in paragraph 2 of Article 66, the European Data Protection Board shall, in the performance of its tasks, neither seek nor take instructions from anybody.**	*Article 65* ***Independence*** 1. The European Data Protection Board shall act independently when performing its tasks pursuant to Articles 66 and 67. 2. Without prejudice to requests by the Commission referred to in point (b) of paragraph 1 and in paragraph 2 of Article 66, the European Data Protection Board shall, in the performance of its tasks, neither seek nor take instructions from anybody.	Article 65 Independence 1. The European Data Protection Board shall act independently when exercising its tasks pursuant to Articles 66 and 67. 2. Without prejudice to requests by the Commission referred to in point (b) of paragraph 1 and in paragraph 2 of Article 66, the European Data Protection Board shall, in the performance of its tasks, neither seek nor take instructions from anybody.

Article 66 **Tasks of the European Data Protection Board** **1. The European Data Protection Board shall ensure the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative or at the request of the Commission, in particular:** **(a) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation;** **(b) examine, on its own initiative or on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices addressed to the supervisory authorities in order to encourage consistent application of this Regulation;** **(c) review the practical application of the guidelines, recommendations and best practices referred to in point (b) and report regularly to the Commission on these;**	*Article 66* ***Tasks of the European Data Protection Board*** 1. The European Data Protection Board shall promote the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative or at the request of the Commission, in particular: (a) advise the Commission on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation; (b) examine, on its own initiative or on request of one of its members or on request of the Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices (…) in order to encourage consistent application of this Regulation; (ba) draw up guidelines for supervisory authorities concering the application of measures referred to in point **(c) of paragraph 1 of Article 53 and in paragraph 1b of Article 53** and the fixing of administrative fines pursuant to Articles 79 and 79a (c) review the practical application of the guidelines, recommendations and best practices referred to in points (b) and (ba); (ca) encourage the drawing-up of codes	Article 66 Tasks of the European Data Protection Board 1. The European Data Protection Board shall ensure the consistent application of this Regulation. To this effect, the European Data Protection Board shall, on its own initiative or at the request of the *European Parliament, Council or* Commission, in particular: (a) advise the *European Institutions ~~Commission~~* on any issue related to the protection of personal data in the Union, including on any proposed amendment of this Regulation; (b) examine, on its own initiative or on request of one of its members or on request of the *European Parliament, Council or* Commission, any question covering the application of this Regulation and issue guidelines, recommendations and best practices addressed to the supervisory authorities in order to encourage consistent application of this Regulation*, including on the use of enforcement powers*;

(d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 57; **(e) promote the co-operation and the effective bilateral and multilateral exchange of information and practices between the supervisory authorities;** **(f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations;** **(g) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide.** **2. Where the Commission requests advice from the European Data Protection Board, it may lay out a time limit within which the European Data Protection Board shall provide such advice, taking into account the urgency of the matter.** **3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the**	of conduct and the establishment of data protection certification mechanisms and data protection seals and marks pursuant to Articles 38 and 39; (cb) give the Commission an opinion on the level of protection in third countries or international organisations; (d) issue opinions on draft <u>measures</u> of supervisory <u>authorities</u> pursuant to the consistency mechanism referred to in Article 57 (…); (e) promote the co-operation and the effective bilateral and multilateral exchange of information and practices between the supervisory authorities; (f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory authorities of third countries or of international organisations; (g) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide; 2. Where the Commission requests advice from the European Data Protection Board, it may **<u>indicate</u>** a time limit <u>(…)</u> taking	(c) review the practical application of the guidelines, recommendations and best practices referred to in point (b) and report regularly to the Commission on these; (d) issue opinions on draft decisions of supervisory authorities pursuant to the consistency mechanism referred to in Article 57; *(da) provide an opinion on which authority should be the lead authority pursuant to Article 54a(3);* (e) promote the co-operation and the effective bilateral and multilateral exchange of information and practices between the supervisory authorities*, including the coordination of joint operations and other joint activities, where it so decides at the request of one or several supervisory authorities*; (f) promote common training programmes and facilitate personnel exchanges between the supervisory authorities, as well as, where appropriate, with the supervisory

committee referred to in Article 87 and make them public. **4. The Commission shall inform the European Data Protection Board of the action it has taken following the opinions, guidelines, recommendations and best practices issued by the European Data Protection Board.**	into account the urgency of the matter. 3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the Commission and to the committee referred to in Article 87 and make them public. 4. The Commission shall inform the European Data Protection Board of the action it has taken following the opinions, guidelines, recommendations and best practices issued by the European Data Protection Board.	authorities of third countries or of international organisations; (g) promote the exchange of knowledge and documentation on data protection legislation and practice with data protection supervisory authorities worldwide. *(ga) give its opinion to the Commission in the preparation of delegated and implementing acts based on this Regulation;* *(gb) give its opinion on codes of conduct drawn up at Union level pursuant to Article 38(4);* *(gc) give its opinion on criteria and requirements for the data protection certification mechanisms pursuant to Article 39(9).* *(gd) maintain a public electronic register on valid and invalid certificates pursuant to Article 39(8);*

(ge) provide assistance to a national supervisory authorities, at their request;

(gf) establish and make public a list of the processing operations which are subject to prior consultation pursuant to Article 34;

(gg) maintain a registry of sanctions imposed on controllers or processors by the competent supervisory authorities.

2. Where the *European Parliament, Council or* Commission requests advice from the European Data Protection Board, it may lay out a time limit within which the European Data Protection Board shall provide such advice, taking into account the urgency of the matter.

3. The European Data Protection Board shall forward its opinions, guidelines, recommendations, and best practices to the *European Parliament, Council and* Commission and to the committee referred to in Article 87 and make them public.

4. The Commission shall inform the

European Data Protection Board of the action it has taken following the opinions, guidelines, recommendations and best practices issued by the European Data Protection Board.

4a. The European Data Protection Board shall, where appropriate, consult interested parties and give them the opportunity to comment within a reasonable period. The European Data Protection Board shall, without prejudice to Article 72, make the results of the consultation procedure publicly available.

4b. The European Data Protection Board shall be entrusted with the task of issuing guidelines, recommendations and best practices in accordance with paragraph 1 (b) for establishing common procedures for receiving and investigating information concerning allegations of unlawful processing and for safeguarding confidentiality and sources of information received.

Article 67 **Reports** **1. The European Data Protection Board shall regularly and timely inform the Commission about the outcome of its activities. It shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Union and in third countries.** **The report shall include the review of the practical application of the guidelines, recommendations and best practices referred to in point (c) of Article 66(1).** **2. The report shall be made public and transmitted to the European Parliament, the Council and the Commission.**	*Article 67* ***Reports*** 1. (…) 2. **The European Data Protection Board** shall draw up an annual report (…) regarding the protection of natural persons with regard to the processing of personal data in the Union and, where relevant, in third countries and international organisations. The report shall be made public and be transmitted to the European Parliament, the Council and the Commission. 3. The annual report shall include a review of the practical application of the guidelines, recommendations and best practices referred to in point (c) of Article 66(1).	Article 67 Reports 1. The European Data Protection Board shall regularly and timely inform the *European Parliament, Council and* Commission about the outcome of its activities. It shall draw up ~~*an annual*~~ *a* report *at least every two years* on the situation regarding the protection of natural persons with regard to the processing of personal data in the Union and in third countries. The report shall include the review of the practical application of the guidelines, recommendations and best practices referred to in point (c) of Article 66(1). 2. The report shall be made public and transmitted to the European Parliament, the Council and the Commission.

Article 68 **Procedure** **1. The European Data Protection Board shall take decisions by a simple majority of its members.** **2. The European Data Protection Board shall adopt its own rules of procedure and organise its own operational arrangements. In particular, it shall provide for the continuation of exercising duties when a member's term of office expires or a member resigns, for the establishment of subgroups for specific issues or sectors and for its procedures in relation to the consistency mechanism referred to in Article 57.**	Article 68 Procedure 1. The European Data Protection Board shall take decisions by a simple majority of its members <u>unless a two-third majority is required pursuant to Article 58(**10**).</u> 2. The European Data Protection Board shall adopt its own rules of procedure and organise its own operational arrangements. (…).	Article 68 Procedure 1. The European Data Protection Board shall take decisions by a simple majority of its members*, unless otherwise provided in its rules of procedure*. 2. The European Data Protection Board shall adopt its own rules of procedure and organise its own operational arrangements. In particular, it shall provide for the continuation of exercising duties when a member's term of office expires or a member resigns, for the establishment of subgroups for specific issues or sectors and for its procedures in relation to the consistency mechanism referred to in Article 57.

Article 69 **Chair** **1. The European Data Protection Board shall elect a chair and two deputy chairpersons from amongst its members. One deputy chairperson shall be the European Data Protection Supervisor, unless he or she has been elected chair.** **2. The term of office of the chair and of the deputy chairpersons shall be five years and be renewable.**	Article 69 **Chair** 1. The European Data Protection Board shall elect a chair and two deputy chairpersons from amongst its members (…). 2. The term of office of the chair and of the deputy chairpersons shall be five years and be renewable once.	Article 69 Chair 1. The European Data Protection Board shall elect a chair and *at least* two deputy chairpersons from amongst its members. ~~*One deputy chairperson shall be the European Data Protection Supervisor, unless he or she has been elected chair.*~~ 2. The term of office of the chair and of the deputy chairpersons shall be five years and be renewable. *2a. The position of the chair shall be a full-time position.*	PL wnioskuje o przywrócenie zapisu, zgodnie z którym EDPS pełni funkcję jednego z 2 wiceprzewodniczących EDPB. Takie rozwiązanie jest uzasadnione z uwagi na potrzebę zapewnienia większej spójności stosowania rozporządzenia i rolę jaką powinien w tym kontekście mieć EDPS, jak też z uwagi na fakt, że to EDPS zapewnia administracyjną obsługę sekretariatu EDPB.

Article 70 **Tasks of the chair** **1. The chair shall have the following tasks:** **(a) to convene the meetings of the European Data Protection Board and prepare its agenda;** **(b) to ensure the timely fulfilment of the tasks of the European Data Protection Board, in particular in relation to the consistency mechanism referred to in Article 57.** **2. The European Data Protection Board shall lay down the attribution of tasks between the chair and the deputy chairpersons in its rules of procedure.**	Article 70 Tasks of the chair 1. The chair shall have the following tasks: (a) to convene the meetings of the European Data Protection Board and prepare its agenda; (b) to ensure the timely performance of the tasks of the European Data Protection Board, in particular in relation to the consistency mechanism referred to in Article 57. 2. The European Data Protection Board shall lay down the attribution of tasks between the chair and the deputy chairpersons in its rules of procedure.	Article 70 Tasks of the chair 1. The chair shall have the following tasks: (a) to convene the meetings of the European Data Protection Board and prepare its agenda; (b) to ensure the timely fulfilment of the tasks of the European Data Protection Board, in particular in relation to the consistency mechanism referred to in Article 57. 2. The European Data Protection Board shall lay down the attribution of tasks between the chair and the deputy chairpersons in its rules of procedure.

Article 71 **Secretariat** **1. The European Data Protection Board shall have a secretariat. The European Data Protection Supervisor shall provide that secretariat.** **2. The secretariat shall provide analytical, administrative and logistical support to the European Data Protection Board under the direction of the chair.** **3. The secretariat shall be responsible in particular for:** **(a) the day-to-day business of the European Data Protection Board;** **(b) the communication between the members of the European Data Protection Board, its chair and the Commission and for communication with other institutions and the public;** **(c) the use of electronic means for the internal and external communication;** **(d) the translation of relevant information;** **(e) the preparation and follow-up of the meetings of the European Data**	Article 71 Secretariat 1. The European Data Protection Board shall have a secretariat. The European Data Protection Supervisor shall provide that secretariat. 2. The secretariat shall provide analytical, administrative and logistical support to the European Data Protection Board under the direction of the chair. 3. The secretariat shall be responsible in particular for: (a) the day-to-day business of the European Data Protection Board; (b) the communication between the members of the European Data Protection Board, its chair, and the Commission and for communication with other institutions and the public; (c) the use of electronic means for the internal and external communication; (d) the translation of relevant information; (e) the preparation and follow-up of the meetings of the European Data Protection Board; (f) the preparation, drafting and	Article 71 Secretariat 1. The European Data Protection Board shall have a secretariat. The European Data Protection Supervisor shall provide that secretariat. 2. The secretariat shall provide analytical, *legal,* administrative and logistical support to the European Data Protection Board under the direction of the chair. 3. The secretariat shall be responsible in particular for: (a) the day-to-day business of the European Data Protection Board; (b) the communication between the members of the European Data Protection Board, its chair and the Commission and for communication with other institutions and the public; (c) the use of electronic means for the internal and external communication; (d) the translation of relevant information;

Protection Board; **(f) the preparation, drafting and publication of opinions and other texts adopted by the European Data Protection Board.**	publication of opinions and other texts adopted by the European Data Protection Board.	(e) the preparation and follow-up of the meetings of the European Data Protection Board; (f) the preparation, drafting and publication of opinions and other texts adopted by the European Data Protection Board.
Article 72 **Confidentiality** **1. The discussions of the European Data Protection Board shall be confidential.** **2. Documents submitted to members of the European Data Protection Board, experts and representatives of third parties shall be confidential, unless access is granted to those documents in accordance with Regulation (EC) No 1049/2001 or the European Data Protection Board otherwise makes them public.** **3. The members of the European Data Protection Board, as well as experts and representatives of third parties, shall be required to respect the**	Article 72 Confidentiality 1. The discussions of the European Data Protection Board shall be confidential. 2. Access to documents submitted to members of the European Data Protection Board, experts and representatives of third parties shall be governed by Regulation (EC) No 1049/2001.	Article 72 Confidentiality 1. The discussions of the European Data Protection Board *may ~~shall~~* be confidential *where necessary, unless otherwise provided in the rules of procedure*. *The agendas of the meetings of the Board shall be made public.* 2. Documents submitted to members of the European Data Protection Board, experts and representatives of third parties shall be confidential, unless access is granted to those documents in accordance with Regulation (EC) No 1049/2001 or the European Data Protection Board otherwise

confidentiality obligations set out in this Article. The chair shall ensure that experts and representatives of third parties are made aware of the confidentiality requirements imposed upon them.		makes them public. 3. The members of the European Data Protection Board, as well as experts and representatives of third parties, shall be required to respect the confidentiality obligations set out in this Article. The chair shall ensure that experts and representatives of third parties are made aware of the confidentiality requirements imposed upon them.	
Article 73 **Right to lodge a complaint with a supervisory authority** **1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority in any Member State if they consider that the processing of personal data relating to them does not comply with this Regulation.** **2. Any body, organisation or association which aims to protect data subjects' rights and interests concerning the protection of their personal data and has been properly constituted according to the law of a**	*Article 73* ***Right to lodge a complaint with a supervisory authority*** 1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority [**competent in accordance with Article 51 or to a supervisory authority** in the Member State of his or her habitual residence,] if the data subject considers that the processing of personal data relating to him or her does not comply with this Regulation. 1a. **The supervisory authority to which a complaint has been lodged shall not take any measure [referred to in paragraph 1b of Article 53] if a possible violation of the**	Article 73 Right to lodge a complaint with a supervisory authority 1. Without prejudice to any other administrative or judicial remedy *and the consistency mechanism*, every data subject shall have the right to lodge a complaint with a supervisory authority in any Member State if they consider that the processing of personal data relating to them does not comply with this Regulation. 2. Any body, organisation or association which ~~*aims to protect data subjects' rights and interests concerning the protection of*~~	***Ad. 73 ust. 1*** –uważamy, że jako niezbędne minimum powinna być możliwość złożenia skargi w organie właściwym ze względu na główną siedzibę lub miejsce zamieszkania. Wydaje nam się jednak, że optymalnie powinna istnieć możliwość złożenia skargi w dowolnie wybranym przez podmiot danych organie krajowym. Przy silnej pozycji organu wiodącego (*lead authority*), nie wystąpi tu ryzyko *forum shopping*. Stąd Polska popiera poprzednie brzmienie tego ustępu. ***Ad. 73 ust. 1a*** – przepis ten wymaga dalszych analiz, zastanawiamy się na przykład w jaki sposób organ nadzoru będzie uzyskiwał informację o toczących się postępowaniach sądowych w innych Państwach Członkowskich. Czy nie

Member State shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data. **3. Independently of a data subject's complaint, any body, organisation or association referred to in paragraph 2 shall have the right to lodge a complaint with a supervisory authority in any Member State, if it considers that a personal data breach has occurred.**	**same rights related to the same processing activities is already being examined by a court in accordance with Article 74, provided the data subject is party to these proceedings.** 2. (…) 3. (…) **4. When the supervisory authority to which a complaint has been lodged is not competent for the supervision of the controller or the processor, it shall ex officio transmit the complaint to the supervisory authority which is competent under Article 51.** **5. The supervisory authority to which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint. Where the supervisory authority competent [in accordance with Article 51] finds the complaint unfounded, the supervisory authority to which the complaint has been lodged shall notify the complainant thereof and inform him of the reasons for the rejection and of the possibility of an judicial remedy pursuant Article 74.**	~~*their personal data*~~ *acts in the public interest* and has been properly constituted according to the law of a Member State shall have the right to lodge a complaint with a supervisory authority in any Member State on behalf of one or more data subjects if it considers that a data subject's rights under this Regulation have been infringed as a result of the processing of personal data. 3. Independently of a data subject's complaint, any body, organisation or association referred to in paragraph 2 shall have the right to lodge a complaint with a supervisory authority in any Member State, if it considers that ~~*a personal data*~~ breach *of this regulation* has occurred.	należałoby tej kwestii doprecyzować w rozporządzeniu? Jesteśmy za zapewnieniem pewności prawa, stąd pozytywnie oceniamy ideę stojącą za tym przepisem. ***Ad. 73 ust. 4*** – popieramy brzmienie tego ustępu. W naszej ocenie musi być jasne, który organ jest właściwy i podejmuje decyzje w danej sprawie. Inne organy powinny we wszelki możliwy sposób współpracować z organem wiodącym (*lead authority*). ***Ad. 73 ust. 5*** – popieramy brzmienie tego ustępu. W naszej ocenie podmiot danych powinien mieć bieżącą i jak najszerszą informację o stanie toczącego się postępowania, którą powinien móc uzyskać od najbliższego organu nadzorczego, czyli w zdecydowanej większości przypadków, tego do którego złożył skargę. Ustęp ten wydaje się dobrze realizować zasadę bliskości (*proximity*)

Article 74 **Right to a judicial remedy against a supervisory authority** **1. Each natural or legal person shall have the right to a judicial remedy against decisions of a supervisory authority concerning them.** **2. Each data subject shall have the right to a judicial remedy obliging the supervisory authority to act on a complaint in the absence of a decision necessary to protect their rights, or where the supervisory authority does not inform the data subject within three months on the progress or outcome of the complaint pursuant to point (b) of Article 52(1).** **3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established.** **4. A data subject which is concerned by a decision of a supervisory authority in another Member State than where the data subject has its habitual residence, may request the supervisory authority of the Member State where it has its habitual residence to bring proceedings on its behalf against the competent**	*Article 74* ***Right to a judicial remedy against a supervisory authority*** 1. Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a decision of a supervisory authority. 2. Without prejudice to any other administrative or non-judicial remedy, **each** data subject shall have the right to a judicial remedy where the supervisory authority [**competent in accordance with Article 51]** does not deal with a complaint**, has rejected the complaint , in part or wholly,** or does not inform the data subject within three months **or any shorter period provided under Union or Member State law** on the progress or outcome of the complaint lodged under Article 73. 3. Proceedings against **a decision of** a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established **according to the laws of that Member State**. 4. (…) 5. (…)	Article 74 Right to a judicial remedy against a supervisory authority 1. *Without prejudice to any other administrative or non-judicial remedy,* each natural or legal person shall have the right to a judicial remedy against decisions of a supervisory authority concerning them. 2. *Without prejudice to any other administrative or non-judicial remedy,* each data subject shall have the right to a judicial remedy obliging the supervisory authority to act on a complaint in the absence of a decision necessary to protect their rights, or where the supervisory authority does not inform the data subject within three months on the progress or outcome of the complaint pursuant to point (b) of Article 52(1). 3. Proceedings against a supervisory authority shall be brought before the courts of the Member State where the supervisory authority is established. 4. *Without prejudice to the consistency*	***Ad. 74 ust. 1*** –zastrzeżenia do zastosowania przymiotnika “effective”, w naszej ocenie jest on niejasny, co do zasady każdy środek prawny powinien być efektywny. Analogiczną uwagę zgłaszamy do użycia tego słowa w art. 75 ***Ad. 74 ust. 2 i 74 ust. 3*** – popieramy zmiany wprowadzone przez Prezydencję, w naszej opinii czynią one ten artykuł bardziej precyzyjnym. w art. 74 ust. 3 doprecyzować, iż chodzi o „*competent supervisory authority*”, tak aby uniknąć możliwych niejasności.

supervisory authority in the other Member State. **5. The Member States shall enforce final decisions by the courts referred to in this Article.**		*mechanism a* ~~A~~ data subject which is concerned by a decision of a supervisory authority in another Member State than where the data subject has its habitual residence, may request the supervisory authority of the Member State where it has its habitual residence to bring proceedings on its behalf against the competent supervisory authority in the other Member State. 5. The Member States shall enforce final decisions by the courts referred to in this Article.	
Article 75 **Right to a judicial remedy against a controller or processor** **1. Without prejudice to any available administrative remedy, including the right to lodge a complaint with a supervisory authority as referred to in Article 73, every natural person shall have the right to a judicial remedy if they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in non-compliance with this Regulation.**	*Article 75* ***Right to a judicial remedy against a controller or processor*** 1. Without prejudice to any available administrative <u>or non-judicial</u> remedy, including the right to lodge a complaint with a supervisory authority <u>under</u> Article 73, <u>a data subject shall</u> have the right to <u>an effective</u> judicial remedy if they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in non-compliance with this Regulation. 2. Proceedings against a controller or a processor shall be brought before the	Article 75 Right to a judicial remedy against a controller or processor 1. Without prejudice to any available administrative remedy, including the right to lodge a complaint with a supervisory authority as referred to in Article 73, every natural person shall have the right to a judicial remedy if they consider that their rights under this Regulation have been infringed as a result of the processing of their personal data in non-compliance with this Regulation.	PL zgłosiła zastrzeżenia analityczne. W szczególności prosimy o wyjaśnienie o jakiego rodzaju środki chodzi w przypadku „*effective judical remedy*". Czy chodzi o wspólny środek dostępny dla każdego obywatela Unii, przyznany na mocy rozporządzenia, czy też każde Państwo Członkowskie będzie mogło przyjąć własne regulacje w tym zakresie? Widzimy tutaj potencjalny problem pojawienia się spraw cywilnych dotyczących kwestii mających charakter czysto administracyjny. W naszej ocenie kwestie z art. 75 można uregulować w całości na poziomie prawa krajowego państw członkowskich.

2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has its habitual residence, unless the controller is a public authority acting in the exercise of its public powers. **3. Where proceedings are pending in the consistency mechanism referred to in Article 58, which concern the same measure, decision or practice, a court may suspend the proceedings brought before it, except where the urgency of the matter for the protection of the data subject's rights does not allow to wait for the outcome of the procedure in the consistency mechanism.** **4. The Member States shall enforce final decisions by the courts referred to in this Article.**	courts of the Member State where the controller or processor has an establishment **according to the laws of that Member State**. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller is a public authority acting in the exercise of its public powers. 3. (…) 4. (…)	2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has its habitual residence, unless the controller is a public authority *of the Union or a Member State* acting in the exercise of its public powers. 3. Where proceedings are pending in the consistency mechanism referred to in Article 58, which concern the same measure, decision or practice, a court may suspend the proceedings brought before it, except where the urgency of the matter for the protection of the data subject's rights does not allow to wait for the outcome of the procedure in the consistency mechanism. 4. The Member States shall enforce final decisions by the courts referred to in this Article.	Ponadto zwracamy uwagę w odniesieniu do art. 75 ust. 2 na obowiązujące już rozporządzenia UE (przede wszystkim 44/2000 Bruksela I) dotyczące jurysdykcji sądów w sprawach cywilnych. Regulowanie tych spraw ponownie nie wydaje się potrzebne i może prowadzić do niepewności prawnej. Proponujemy wykreślenie tego przepisu.

Article 76 **Common rules for court proceedings** **1. Any body, organisation or association referred to in Article 73(2) shall have the right to exercise the rights referred to in Articles 74 and 75 on behalf of one or more data subjects.** **2. Each supervisory authority shall have the right to engage in legal proceedings and bring an action to court, in order to enforce the provisions of this Regulation or to ensure consistency of the protection of personal data within the Union.** **3. Where a competent court of a Member State has reasonable grounds to believe that parallel proceedings are being conducted in another Member State, it shall contact the competent court in the other Member State to confirm the existence of such parallel proceedings.** **4. Where such parallel proceedings in another Member State concern the same measure, decision or practice, the court may suspend the proceedings.** **5. Member States shall ensure that court actions available under national law allow for the rapid**	*Article 76* ***Representation of of data subjects*** 1. The data subject shall have the right to mandate a body, organisation or association*, which has been properly constituted according to the law of a Member State and whose* ***statutory*** *objectives include the protection of data subjects' rights and freedoms with regard to the protection of their personal data, to lodge the complaint on his or her behalf (…)* and to exercise the rights referred to in Articles **73**, 74 and 75 on his or her behalf]. 1a. [Independently of a data subject's mandate or complaint, any body, organisation or association referred to in **paragraph 1** shall have the right to lodge a complaint with the supervisory authority competent **in accordance with Article 51** (…) if it has reasons to consider that a personal data breach referred to in Article 32(1) has occurred and Article 32(3) does not apply.]. 2. (…) 3. (…) 4. (…) 5. (…)	Article 76 Common rules for court proceedings 1. Any body, organisation or association referred to in Article 73(2) shall have the right to exercise the rights referred to in Articles 74*, ~~and~~* 75 *and 77 ~~on behalf of~~ if mandated by* one or more data subjects. 2. Each supervisory authority shall have the right to engage in legal proceedings and bring an action to court, in order to enforce the provisions of this Regulation or to ensure consistency of the protection of personal data within the Union. 3. Where a competent court of a Member State has reasonable grounds to believe that parallel proceedings are being conducted in another Member State, it shall contact the competent court in the other Member State to confirm the existence of such parallel proceedings. 4. Where such parallel proceedings in another Member State concern the same measure, decision or practice, the court	Dziękujemy Prezydencji za uwzględnienie naszej uwagi z przypisu 21. ***Ad. 76 ust. 1a*** – zastanawiamy się skąd organizacje będą uzyskiwać informacje o naruszeniach ochrony danych. W Polsce jest wiele organizacji, które wyszukują, np. w regulaminach sklepów internetowych, klauzule niezgodne z prawem i pozywają przedsiębiorców z nich korzystających, często nadużywając prawa. Boimy się analogicznych sytuacji tutaj, np. celowego włamywania się do systemów, po to żeby móc zgłosić naruszenie. Odnośnie tego ustępu uważamy, iż organizacje, o których mowa w ustępie 1 powinny, gdy powezmą informację odnośnie naruszenia, poinformować o tym organ ochrony danych, aby to on podjął odpowiednie działania z urzędu. Dlatego opowiadamy się za usunięciem tego ustępu. Możliwość udzielenia pełnomocnictwa takiej organizacji przez podmiot danych wydaje nam się całkowicie wystarczająca.

adoption of measures including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved.		may suspend the proceedings. 5. Member States shall ensure that court actions available under national law allow for the rapid adoption of measures including interim measures, designed to terminate any alleged infringement and to prevent any further impairment of the interests involved.	
	Article 76a ***Suspension of proceedings*** **1. Where a competent court of a Member State has reasonable grounds to believe that proceedings concerning the same processing activities are being conducted in another Member State, it shall contact the competent court in the other Member State to confirm the existence of such proceedings.** **2. Where a possible violation of the same rights related to the same processing activities is already being examined by a court in another Member State, the competent court may suspend its proceedings concerning a natural and/or legal person provided these persons are also party to the proceedings in the other**		Wydaje nam się, że idea stojąca za propozycją Prezydencji jest słuszna, natomiast zaproponowany mechanizm wymaga dopracowania. W szczególności trudna może być wymiana informacji pomiędzy sądami z różnych Państw Członkowskich i koordynowanie przez nie swoich działań. Niestety często mamy do czynienia z sytuacją, gdy sąd nie chce się zająć daną sprawą. Co więc stanie się w sytuacji, gdy dwa sądy z dwóch różnych Państw Członkowskich jednocześnie uznają, że w danej sprawie toczy się już postępowanie przed tym drugim sądem?

	Member State.		
Article 77 **Right to compensation and liability** **1. Any person who has suffered damage as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to receive compensation from the controller or the processor for the damage suffered.** **2. Where more than one controller or processor is involved in the processing, each controller or processor shall be jointly and severally liable for the entire amount of the damage.** **3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage.**	*Article 77* ***Right to compensation and liability*** 1. Any person who has suffered damage as a result of a processing operation which is non compliant with this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered. 2. Where more than one controller or processor **or a controller and processor** are involved in the processing **which gives rise to the damage**, each controller or processor shall be jointly and severally liable for the entire amount of the damage. **This is without prejudice to recourse claims between controllers and/or processors.** 3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage.	Article 77 Right to compensation and liability 1. Any person who has suffered damage*, including non-pecuniary damage,* as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to ~~*receive*~~ *claim* compensation from the controller or the processor for the damage suffered. 2. Where more than one controller or processor is involved in the processing, each *of those* controller*s* or processor*s* shall be jointly and severally liable for the entire amount of the damage*, unless they have an appropriate written agreement* ~~*establishing liability in the determination of*~~ *determining the responsibilities pursuant to Article 24*. 3. The controller or the processor may be exempted from this liability, in whole or in part, if the controller or the processor proves that they are not responsible for the event giving rise to the damage.	Uważamy, *że* zmiany wprowadzone przez Prezydencję czynią ten artykuł bardziej precyzyjnym. Jednocześnie podtrzymujemy przypis 34, uważamy, że zamiana „may" na „shall" w art. 77 ust. 3 zwiększy pewność prawną w zakresie wyłączenia odpowiedzialności administratorów danych i podmiotów przetwarzających dane.

Article 78 **Penalties** **1. Member States shall lay down the rules on penalties, applicable to infringements of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented, including where the controller did not comply with the obligation to designate a representative. The penalties provided for must be effective, proportionate and dissuasive.** **2. Where the controller has established a representative, any penalties shall be applied to the representative, without prejudice to any penalties which could be initiated against the controller.** **3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent**	(…)	*Article 78* ***Penalties*** (…) 1. Member States shall lay down the rules on penalties, applicable to infringements of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented, including where the controller did not comply with the obligation to designate a representative. The penalties provided for must be effective, proportionate and dissuasive. ~~*The rules on penalties adopted in accordance with this Article shall be subject to appropriate procedural safeguards in conformity with the general principles of Union law and the Charter of Fundamental Rights, including those concerning the right to an effective judicial remedy, due process and the principle of ne bis in idem.*~~ 2. Where the controller has established a representative, any penalties shall be applied to the representative, without	Article 78 Penalties 1. Member States shall lay down the rules on penalties, applicable to infringements of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented, including where the controller did not comply with the obligation to designate a representative. The penalties provided for must be effective, proportionate and dissuasive. ~~*The rules on penalties adopted in accordance with this Article shall be subject to appropriate procedural safeguards in conformity with the general principles of Union law and the Charter of Fundamental Rights, including those concerning the right to an effective judicial remedy, due process and the principle of ne bis in idem.*~~ 2. Where the controller has established a representative, any penalties shall be applied to the representative, without	Przeniesiony do art. 79 b

amendment affecting them.		prejudice to any penalties which could be initiated against the controller. 3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.	
Article 79 **Administrative sanctions** **1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article.** **2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and**	*Article 79* ***General conditions for imposing administrative fines*** 1. Each supervisory authority [**competent in accordance with Article 51]** shall be empowered to impose administrative fines pursuant to this Article in respect of infringements of this Regulation. **Administrative** fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in Article 53. 2. Administrative fines imposed pursuant to Article 79a shall in each individual case be effective, proportionate and dissuasive. 2a. **When deciding whether to impose**	Article 79 Administrative sanctions 1. Each supervisory authority shall be empowered to impose administrative sanctions in accordance with this Article. *The supervisory authorities shall co-operate with each other in accordance with Articles 46 and 57 to guarantee a harmonized level of sanctions within the Union.* 2. The administrative sanction shall be in each individual case effective, proportionate and dissuasive. ~~*The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the*~~	***Art. 79 ust. 2a*** – dostrzegamy, że Prezydencja usunęła część czynników, które wzbudzały kontrowersje podczas ostatnich dyskusji. W każdym przypadku widzimy potrzebę doprecyzowania zasad z art. 79 ust. 2a w wytycznych Europejskiej Rady Ochrony Danych. W innym przypadku może zaistnieć ryzyko różnej interpretacji jego postanowień przez krajowe organy, a przez to – *forum shopping*. Ponadto, jesteśmy za tym, aby chociaż w podstawowym zakresie rozróżnić czynniki, które zaostrzają odpowiedzialność, od tych, które ją łagodzą. W szczególności trzeba dokonać takiego rozróżnienia w odniesieniu do stosowania kodeksów postępowania i mechanizmów certyfikacji, faktu bycia podmiotem publicznym czy prywatnych oraz powołania lub nie DPO.

procedures implemented pursuant to Article 23 and the degree of co-operation with the supervisory authority in order to remedy the breach. **3. In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, where:** **(a) a natural person is processing personal data without a commercial interest; or** **(b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity ancillary to its main activities.** **4. The supervisory authority shall impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently:** **(a) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2);** **(b) charges a fee for the**	**an administrative fine and deciding on** the amount of the administrative fine in each individual case (…) due regard **shall be had** to the following: (a) the nature, gravity and duration of the infringment having regard to the nature scope or purpose of the processing concerned; (b) the intentional or negligent character of the infringement, (c) the number of data subjects affected by the infringement and the level of damage suffered by them; (d) action taken by the controller or processor to mitigate the damage suffered by data subjects; (e) the degree of responsibility of the controller or processor having regard to technical and organisational measures implemented by them pursuant to Articles 23 and 30; (f) any previous infringements by the controller or processor; (g) (…) any financial benefits gained, or losses avoided, directly or indirectly from the infringement; (h) the maner in which the infringement became known to the supervisory authority, in particular whether,	~~*degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of co-operation with the supervisory authority in order to remedy the breach.*~~ *2a. To anyone who does not comply with the obligations laid down in this Regulation, the supervisory authority shall impose at least one of the following sanctions:* *a) a warning in writing in cases of first and non-intentional non-compliance;* *b) regular periodic data protection audits;* *c) a fine up to 100 000 000 EUR or up to 5% of the annual worldwide turnover in case of an enterprise, whichever is greater.* *2b. If the controller or the processor is in possession of a valid "European Data Protection Seal" pursuant to Article 39, a fine pursuant to paragraph 2c) shall only be imposed in cases of intentional or negligent incompliance.* *2c. The administrative sanction shall take*	***Art. 79 ust. 2b*** – opowiadamy się za jak najszerszym wachlarzem możliwych sankcji, które może nakładać organ krajowy, tak aby jak najlepiej odpowiadały potrzebom konkretnej sprawy. Niemniej, widzimy tutaj ryzyko *forum shopping*, w związku z czym także w tym zakresie konieczne będą silne wytyczne Europejskiej Rady Ochrony Danych. PL opowiadała się za utrzymaniem ust. 3a; w kwestii ustanowienia przedstawiciela, DPA powinien móc wybrać czy chce nałożyć karę administracyjną na administratora czy na jego przedstawiciela, przedstawiciel musi się liczyć z tym, że może zostać pociągnięty do odpowiedzialności. ust. 4 - wątpliwości co do wartości dodanej tego przepisu - wydaje się, że w każdym państwie członkowskim istnieją środki prawne zapewniające kontrolę sądową decyzji DPA. Aby nadać ustępowi faktyczną treść, należałoby dodać (na przykład), że decyzja powinna być poddana kontroli merytorycznej (czyli w Polsce w trybie postępowania cywilnego), a nie tylko formalnej (przed sądami administracyjnymi). Wtedy przepis faktycznie niósłby istotna treść normatywną.

information or for responses to the requests of data subjects in violation of Article 12(4). **5. The supervisory authority shall impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or negligently:** **(a) does not provide the information, or does provide incomplete information, or does not provide the information in a sufficiently transparent manner, to the data subject pursuant to Article 11, Article 12(3) and Article 14;** **(b) does not provide access for the data subject or does not rectify personal data pursuant to Articles 15 and 16 or does not communicate the relevant information to a recipient pursuant to Article 13;** **(c) does not comply with the right to be forgotten or to erasure, or fails to put mechanisms in place to ensure that the time limits are observed or does not take all necessary steps to inform third parties that a data subjects requests to erase any links to, or copy or replication of the personal data pursuant Article 17;** **(d) does not provide a copy of the**	and if so to what extent, the controller or processor notified the infringement; (i) **compliance with measures referred to in point (b) and (c) of paragraph 1 and points (a), (d), (e) and (f) of paragraph 1b of Article 53, ordered against the controller or processor concerned with regard to the same subject-matter;** (j) adherence to approved codes of conduct pursuant to Article 38 or approved certification mechanisms pursuant to Article 39 ; (k) (…); (l) (…); (m) any other aggravating or mitigating factor applicable to the circumstances of the case. **2b. When the consideration of the factors set out in paragraph 2 leads to the conclusion that it concerns a less grave violation, it may be decided to impose measures referred to in points (b) of paragraph 1b of Article 53 instead of the imposing an administrative fine.** 3. (…) 3a. (…) 3b. Each Member State may lay down the rules on whether and to what extent	*into account the following factors:* *a) the nature, gravity and duration of the incompliance,* *b) the intentional or negligent character of the infringement,* *c) the degree of responsibility of the natural or legal person and of previous breaches by this person,* *d) the repetitive nature of the infringement,* *e) the degree of co-operation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement,* *f) the specific categories of personal data affected by the infringement,* *(fa) the level of damage, including non-pecuniary damage, suffered by the data subjects,* *(fb) the action taken by the controller or processor to mitigate the damage suffered by data subjects,* *(fc) any financial benefits intended or gained, or losses avoided, directly or indirectly from the infringement,* *g) the degree of technical and organisational measures and procedures*

personal data in electronic format or hinders the data subject to transmit the personal data to another application in violation of Article 18; **(e) does not or not sufficiently determine the respective responsibilities with co-controllers pursuant to Article 24;** **(f) does not or not sufficiently maintain the documentation pursuant to Article 28, Article 31(4), and Article 44(3);** **(g) does not comply, in cases where special categories of data are not involved, pursuant to Articles 80, 82 and 83 with rules in relation to freedom of expression or with rules on the processing in the employment context or with the conditions for processing for historical, statistical and scientific research purposes.** **6. The supervisory authority shall impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently:** **(a) processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent pursuant to**	administrative fines may be imposed on public authorities and bodies established in that Member State. 4. The *exercise by the supervisory authority* [**competent in accordance with Article 51]** of its powers under this Article shall be subject to appropriate procedural safeguards in conformity with Union law and Member State law, including effective judicial remedy and due process.	*implemented pursuant to:* *i) Article 23 - Data protection by design and by default* *ii) Article 30 - Security of processing* *iii) Article 33 - Data protection impact assessment* *iv) Article 33 a (new) - Data protection compliance review* *v) Article 35 - Designation of the data protection officer* *(ga) the refusal to cooperate with or obstruction of inspections, audits and controls carried out by the supervisory authority pursuant to Article 53,* *(gb) other aggravating or mitigating factors applicable to the circumstance of the case.* ~~*3. In case of a first and non-intentional non-compliance with this Regulation, a warning in writing may be given and no sanction imposed, where:*~~ ~~*(a) a natural person is processing personal data without a commercial interest; or*~~ ~~*(b) an enterprise or an organisation employing fewer than 250 persons is processing personal data only as an activity*~~

Articles 6, 7 and 8; **(b) processes special categories of data in violation of Articles 9 and 81;** **(c) does not comply with an objection or the requirement pursuant to Article 19;** **(d) does not comply with the conditions in relation to measures based on profiling pursuant to Article 20;** **(e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, 23 and 30;** **(f) does not designate a representative pursuant to Article 25;** **(g) processes or instructs the processing of personal data in violation of the obligations in relation to processing on behalf of a controller pursuant to Articles 26 and 27;** **(h) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject pursuant to Articles 31 and 32;** **(i) does not carry out a data**	~~*ancillary to its main activities.*~~ ~~*4. The supervisory authority shall impose a fine up to 250 000 EUR, or in case of an enterprise up to 0,5 % of its annual worldwide turnover, to anyone who, intentionally or negligently:*~~ ~~*(a) does not provide the mechanisms for requests by data subjects or does not respond promptly or not in the required format to data subjects pursuant to Articles 12(1) and (2);*~~ ~~*(a) charges a fee for the information or for responses to the requests of data subjects in violation of Article 12(4).*~~ ~~*5. The supervisory authority shall impose a fine up to 500 000 EUR, or in case of an enterprise up to 1 % of its annual worldwide turnover, to anyone who, intentionally or negligently:*~~ ~~*(a) does not provide the information, or does provide incomplete information, or does not provide the information in a sufficiently transparent manner, to the data subject pursuant to Article 11, Article 12(3) and Article 14;*~~ ~~*(b) does not provide access for the data subject or does not rectify personal data*~~

protection impact assessment pursuant or processes personal data without prior authorisation or prior consultation of the supervisory authority pursuant to Articles 33 and 34; **(j) does not designate a data protection officer or does not ensure the conditions for fulfilling the tasks pursuant to Articles 35, 36 and 37;** **(k) misuses a data protection seal or mark in the meaning of Article 39;** **(l) carries out or instructs a data transfer to a third country or an international organisation that is not allowed by an adequacy decision or by appropriate safeguards or by a derogation pursuant to Articles 40 to 44;** **(m) does not comply with an order or a temporary or definite ban on processing or the suspension of data flows by the supervisory authority pursuant to Article 53(1);** **(n) does not comply with the obligations to assist or respond or provide relevant information to, or access to premises by, the supervisory authority pursuant to Article 28(3), Article 29, Article 34(6) and Article**	~~*pursuant to Articles 15 and 16 or does not communicate the relevant information to a recipient pursuant to Article 13;*~~ ~~*(c) does not comply with the right to be forgotten or to erasure, or fails to put mechanisms in place to ensure that the time limits are observed or does not take all necessary steps to inform third parties that a data subjects requests to erase any links to, or copy or replication of the personal data pursuant Article 17;*~~ ~~*(d) does not provide a copy of the personal data in electronic format or hinders the data subject to transmit the personal data to another application in violation of Article 18;*~~ ~~*(e) does not or not sufficiently determine the respective responsibilities with co-controllers pursuant to Article 24;*~~ ~~*(f) does not or not sufficiently maintain the documentation pursuant to Article 28, Article 31(4), and Article 44(3);*~~ ~~*(g) does not comply, in cases where special categories of data are not involved, pursuant to Articles 80, 82 and 83 with rules in relation to freedom of expression or with rules on the processing in the employment context or with the conditions for processing for historical, statistical and scientific research purposes.*~~

53(2); **(o) does not comply with the rules for safeguarding professional secrecy pursuant to Article 84.** **7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of updating the amounts of the administrative fines referred to in paragraphs 4, 5 and 6, taking into account the criteria referred to in paragraph 2.**	*~~6. The supervisory authority shall impose a fine up to 1 000 000 EUR or, in case of an enterprise up to 2 % of its annual worldwide turnover, to anyone who, intentionally or negligently:~~* *~~(a) processes personal data without any or sufficient legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7 and 8;~~* *~~(b) processes special categories of data in violation of Articles 9 and 81;~~* *~~(c) does not comply with an objection or the requirement pursuant to Article 19;~~* *~~(d) does not comply with the conditions in relation to measures based on profiling pursuant to Article 20;~~* *~~(e) does not adopt internal policies or does not implement appropriate measures for ensuring and demonstrating compliance pursuant to Articles 22, 23 and 30;~~* *~~(f) does not designate a representative pursuant to Article 25;~~* *~~(g) processes or instructs the processing of personal data in violation of the obligations in relation to processing on behalf of a controller pursuant to Articles 26 and 27;~~* *~~(h) does not alert on or notify a personal~~*

~~*data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject pursuant to Articles 31 and 32;*~~

~~*(i) does not carry out a data protection impact assessment pursuant or processes personal data without prior authorisation or prior consultation of the supervisory authority pursuant to Articles 33 and 34;*~~

~~*(j) does not designate a data protection officer or does not ensure the conditions for fulfilling the tasks pursuant to Articles 35, 36 and 37;*~~

~~*(k) misuses a data protection seal or mark in the meaning of Article 39;*~~

~~*(l) carries out or instructs a data transfer to a third country or an international organisation that is not allowed by an adequacy decision or by appropriate safeguards or by a derogation pursuant to Articles 40 to 44;*~~

~~*(m) does not comply with an order or a temporary or definite ban on processing or the suspension of data flows by the supervisory authority pursuant to Article 53(1);*~~

~~*(n) does not comply with the obligations to assist or respond or provide relevant information to, or access to premises by, the supervisory authority pursuant to Article*~~

		~~*28(3), Article 29, Article 34(6) and Article 53(2);*~~ ~~*(o) does not comply with the rules for safeguarding professional secrecy pursuant to Article 84.*~~ 7. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of updating the *absolute* amounts of the administrative fines referred to in paragraph~~s~~ *2a* ~~*4, 5 and 6*~~, taking into account the criteria *and factors* referred to in paragraph*s* 2 *and 2c*.	
	Article 79a ***Administrative fines*** 1. The supervisory authority **[competent in accordance with Article 51]** may impose a fine that shall not exceed […] EUR, or in case of an undertaking […] % of its total worldwide annual turnover **of the preceding financial year**, on a controller who, intentionally or negligently: (a) does not respond within the period referred to in Article 12(2) to requests of the data subject; (b) charges a fee in violation of **the first sentence of** paragraph 4 of		Chcielibyśmy, żeby ten artykuł był jak najbardziej czytelny i prosty. Potrzebujemy jednolitej aplikacji sankcji administracyjnych w całej Unii Europejskiej. Dziękujemy za dodanie zaproponowanego przez nas ustępu 3a – rozjaśnia on wątpliwości, które mogli mieć administratorzy danych lub podmioty przetwarzające dane w przypadku kumulacji podstaw odpowiedzialności. Popieramy całe nowe brzmienie ust. 3a – to dobre rozwiązanie. Musimy pamiętać, że są podmioty, zwłaszcza duże, międzynarodowe korporacje, dla których sankcje przewidziane w rozporządzeniu mogą nie być

	Article 12. 2. The supervisory authority **[competent in accordance with Article 51]** may impose a fine that shall not exceed […] EUR, or in case of an undertaking […]% of its total worldwide annual (…) turnover **of the preceding financial year**, on a controller or processor who, intentionally or negligently: (a) does not provide the information, or (…) provides incomplete information, or does not provide the information **timely or** in a sufficiently transparent manner, to the data subject pursuant to Articles **12(3),**14 and 14a; (b) does not provide access for the data subject or does not rectify personal data pursuant to Articles 15 and 16 or does not comply with the rights and obligations pursuant to Articles 17, 17a, 17b, 18 or 19; (c) (…); (d) (…); (e) does not or not sufficiently determine the respective responsibilities with joint controllers pursuant to Article 24; (f) does not or not sufficiently maintain the documentation pursuant to Article 28 and Article 31(4). (g) (…) 3. The supervisory authority	wystarczająco dotkliwe. To o nich myślimy czytając ten ustęp. Odnośnie pojęcia poprzedni rok obrotowy (*proceding financial year*) uważamy to za dobrą zmianę, doprecyzowującą podstawę do wyliczania sankcji. ***Art. 79a ust. 4*** – w naszej ocenie może pozostać w tekście, pozwoli on dostosować wysokość sankcji do zmieniających się uwarunkowań ekonomicznych. Kary administracyjne nakładane przez organy nadzoru powinny być z jednej strony elastyczne, ale z drugiej powinny mieć taką wysokość, aby stanowiły skuteczny środek prewencyjny. Należy to także prawidłowo osadzić w kontekście międzynarodowym – obowiązku stosowania reguł UE przez zagraniczne podmioty, w tym potężne korporacje posiadające wielomiliardowe przychody. Aby zapewnić stosowanie przez nie rozporządzenia kary muszą być odpowiednio dotkliwe i mieć na względzie rozwiązania obowiązujące w państwach trzecich. Przedstawiciel PL zada pytanie, czy mając na uwadze wytyczne w art. 79 i określenie jedynie górnego pułapu kar, faktycznie niezbędne jest rozdzielenia

	[competent in accordance with Article 51] may impose a fine that shall not exceed […] EUR or, in case of an undertaking, […] % of its total worldwide annual turnover **of the preceding financial year**, on a controller or processor who, intentionally or negligently: (a) processes personal data without **a** (…) legal basis for the processing or does not comply with the conditions for consent pursuant to Articles 6, 7, 8 and 9; (b) (…); (c) (…); (d) does not comply with the conditions in relation to (…) profiling pursuant to Article 20; (e) does not (…) implement appropriate measures or is not able to demonstrate compliance pursuant to Articles 22 (…) and 30; (f) does not designate a representative in violation of Article 25; (g) processes or instructs the processing of personal data in violation of (…) Articles 26; (h) does not alert on or notify a personal data breach or does not timely or completely notify the data breach to the supervisory authority or to the data subject	poszczególnych kategorii naruszeń i osobne określenie kar dla każdej z nich. Czy nie prostszym i klarowniejszym rozwiązaniem byłoby ogólnie uprawnienie DPA do nałożenia kary za naruszenie któregokolwiek przepisu rozporządzenia?

in violation of Articles 31 and 32;

(i) does not carry out a data protection impact assessment in violation of Article 33 or processes personal data without prior consultation of the supervisory authority in violation of Article 34(1);

(j) (…);

(k) misuses a data protection seal or mark in the meaning of Article 39 or does not comply with the conditions and procedures laid down in Articles 38a and 39a;

(l) carries out or instructs a data transfer to a recipient in a third country or an international organisation in violation of Articles 40 to 44;

(m) does not comply with an order or a temporary or definite ban on processing or the suspension of data flows by the supervisory authority pursuant to Article 53(1) or does not provide access in violation of Article 53(2).

(n) (…)

(o) (…).

[3a. If a controller or processor intentionally or negligently violates several provisions of this Regulation listed in paragraphs 1, 2 or 3, the total amount of

the fine may not excceed the amount specified for the gravest violation.

The administrative fines shall be higher than the economic advantage obtained by comitting the violation concerned. Should the maximum amounts referred to in paragraphs 1 to 3 not allow for the deprivation of this economic adavantage, the supervisory authority competent in accordance with Article 51 shall be authorised to impose a higer amount.]

4. [The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of adjusting the maximum amounts of the administrative fines referred to in paragraphs 1, 2 and 3 to monetary developments, taking into account the criteria referred to in paragraph 2a of Article 79.]

Article 79b
Penalties

1. For infringments of the provisions of this Regulation not listed in Article 79a Member States shall lay down the rules on penalties applicable to such infringements and shall take all measures necessary to ensure that they are implemented (…). Such penalties shall be effective, proportionate

Art. 79b ust. 1 – Popieramy poprzednie brzmienie tego artykułu – bez „for infringments of the provisions of this Regulation not listed in Article 79a", który naszym zdaniem nie pomaga w zrozumieniu tego artykułu – artykuł ten jest obecnie niejasny i nie widzimy żadnego uzasadnienia dla tego rozwiązania. Chcielibyśmy, aby

	and dissuasive. *2. (…).* *3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them*.	Prezydencja jeszcze raz wyjaśniła czemu służą wprowadzone przez nią zmiany w ustępie 1. PL opowiadała się za powrotem do pierwotnego brzmienia przepisu, w którym kary mogą być przewidziane w prawie krajowym za naruszenie wszystkich przepisów rozporządzenia. Zaproponowane rozwiązanie, ograniczające tą możliwość jedynie do naruszeń nieopisanych w art. 79a, nie znajduje w ocenie Polski żadnego uzasadnienia. **Pytanie do Prezydencji:** czy przy obecnym brzmieniu art. 79b ust. 1 Państwa Członkowskie wciąż mogą nakładać kary za naruszenia wymienione w art. 79a projektu rozporządzenia? W naszej ocenie odpowiedzialność karna, a o taką głównie chodzi w tym ustępie, nie może być zharmonizowana w prawie Unii Europejskiej, więc rozporządzenie nie może w tym zakresie wprowadzać żadnych ograniczeń. W związku z czym w naszej ocenie zmiany wprowadzone przez Prezydencję w ustępie 1 w praktyce nic nie zmieniają. Prosimy o wyjaśnienie naszych wątpliwości. Ten artykuł jest bardzo różnie rozumiany, także w toku naszych konsultacji interpretacje są całkowicie rozbieżne. Być może należy go lepiej wyjaśnić na przykład w motywach do

			rozporządzenia. Przedstawiciel zada także pytanie, czy, mając na uwadze bardzo lakoniczne brzmienie przepisu, możliwe będzie zakwestionowanie efektywności, proporcjonalności i odpowiednio odstraszającego wymiaru kar ustanowionych przez państwo członkowskie w postępowaniu przed Trybunałem Sprawiedliwości UE i czy będzie to jedyny przysługujący środek? Ponownie widzimy tu możliwość wtórnej fragmentaryzacji reżimu prawnego pomiędzy Państwami Członkowskimi i potencjalnie źródło *forum shopping*.
Article 80 **Processing of personal data and freedom of expression** **1. Member States shall provide for exemptions or derogations from the provisions on the general principles in Chapter II, the rights of the data subject in Chapter III, on controller and processor in Chapter IV, on the transfer of personal data to third countries and international organisations in Chapter V, the independent supervisory authorities in Chapter VI and on co-**	***Processing of personal data and freedom of expression*** 1. Member State law shall (…) reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression, including the processing of personal data for journalistic purposes and the purposes of artistic or literary expression.	Article 80 Processing of personal data and freedom of expression 1. Member States shall provide for exemptions or derogations from the provisions on the general principles in Chapter II, the rights of the data subject in Chapter III, on controller and processor in Chapter IV, on the transfer of personal data to third countries and international organisations in Chapter V, the independent	

operation and consistency in Chapter VII for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression in order to reconcile the right to the protection of personal data with the rules governing freedom of expression. **2. Each Member State shall notify to the Commission those provisions of its law which it has adopted pursuant to paragraph 1 by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment law or amendment affecting them.**	2.	(…)	supervisory authorities in Chapter VI, ~~*and*~~ on co-operation and consistency in Chapter VII *and specific data processing situations in Chapter IX whenever this is necessary* ~~*for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression*~~ in order to reconcile the right to the protection of personal data with the rules governing freedom of expression *in accordance with the Charter of Fundamental Rights of the European Union*. 2. Each Member State shall notify to the Commission those provisions of its law which it has adopted pursuant to paragraph 1 by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment law or amendment affecting them.

	Article 80a ***Processing of personal data and public access to official documents***	*Article 80a* *Access to documents*
	Personal data in official documents held by a public authority <u>or a public body</u> may be disclosed by the authority <u>or body</u> in accordance with Union law or Member State law to which the public authority <u>or body</u> is subject in order to reconcile public access to such official documents with the right to the protection of personal data pursuant to this Regulation.	*1. Personal data in documents held by a public authority or a public body may be disclosed by this authority or body in accordance with Union or Member State legislation regarding public access to official documents, which reconciles the right to the protection of personal data with the principle of public access to official documents.*
		2. Each Member State shall notify to the Commission provisions of its law which it adopts pursuant to paragraph 1 by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.

	Article 80b ***Processing of national identification number*** Member States may determine the conditions for the processing of a national identification number or any other identifier of general application	
Article 81 **Processing of personal data concerning health** **1. Within the limits of this Regulation and in accordance with point (h) of Article 9(2), processing of personal data concerning health must be on the basis of Union law or Member State law which shall provide for suitable and specific measures to safeguard the data subject's legitimate interests, and be necessary for:** **(a) the purposes of preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation**	Article 81 Processing of personal data concerning health 1. Within the limits of this Regulation and in accordance with point (h) of Article 9(2), processing of personal data concerning health must be on the basis of Union law or Member State law which shall provide for suitable and specific measures to safeguard the data subject's legitimate interests, and be necessary for: (a) the purposes of preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a	Article 81 Processing of personal data concerning health 1. ~~*Within the limits of*~~ *In accordance with the rules set out in* this Regulation, ~~*and in accordance*~~ *in particular* with point (h) of Article 9(2), processing of personal data concerning health must be on the basis of Union law or Member State law which shall provide for suitable, *consistent,* and specific measures to safeguard the data subject's ~~*legitimate*~~ interests *and fundamental rights,* to the extent that these are necessary *and proportionate*, *and of which the effects shall be foreseeable by the data subject,* for:

of professional secrecy or another person also subject to an equivalent obligation of confidentiality under Member State law or rules established by national competent bodies; or		health professional subject to the obligation of professional secrecy or another person also subject to an equivalent obligation of confidentiality under Member State law or rules established by national competent bodies; or	(a) the purposes of preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or another person also subject to an equivalent obligation of confidentiality under Member State law or rules established by national competent bodies; or
(b) reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety, inter alia for medicinal products or medical devices; or	(b)	reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety, inter alia for medicinal products or medical devices; or	(b) reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety, inter alia for medicinal products or medical devices, *and if the processing is carried out by a person bound by a confidentiality obligation;* or
(c) other reasons of public interest in areas such as social protection, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system.	(c)	other reasons of public interest in areas such as social protection, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system.	(c) other reasons of public interest in areas such as social protection, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system *and the provision of health services. Such processing of personal data concerning health for reasons of public interest shall not result in data being processed for other purposes, unless with the consent of the data subject or on the*
2. Processing of personal data concerning health which is necessary for historical, statistical or scientific research purposes, such as patient registries set up for improving diagnoses and differentiating between similar types of diseases and preparing studies for therapies, is subject to the conditions and safeguards referred to in Article 83.	2.	Processing of personal data concerning health which is necessary for historical, statistical or scientific research purposes, such as patient registries set up for improving diagnoses and differentiating between similar types of diseases and preparing studies for therapies, is subject to the conditions and safeguards referred to in Article 83.	
3. The Commission shall be empowered to adopt delegated acts in			

accordance with Article 86 for the purpose of further specifying other reasons of public interest in the area of public health as referred to in point (b) of paragraph 1, as well as criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.	3.	The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying other reasons of public interest in the area of public health as referred to in point (b) of paragraph 1, as well as criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.	*basis of Union or Member State law.* *1a. When the purposes referred to in points (a) to (c) of paragraph 1 can be achieved without the use of personal data, such data shall not be used for those purposes, unless based on the consent of the data subject or Member State law.* *1b. Where the data subject's consent is required for the processing of medical data exclusively for public health purposes of scientific research, the consent may be given for one or more specific and similar researches. However, the data subject may withdraw the consent at any time.* *1c. For the purpose of consenting to the participation in scientific research activities in clinical trials, the relevant provisions of Directive 2001/20/EC shall apply.* 2. Processing of personal data concerning health which is necessary for historical, statistical or scientific research purposes~~, such as patient registries set up for improving diagnoses and differentiating between similar types of diseases and preparing studies for therapies, is~~ *shall be*

permitted only with the consent of the data subject, and shall be subject to the conditions and safeguards referred to in Article 83.

2a. Member States law may provide for exceptions to the requirement of consent for research, as referred to in paragraph 2, with regard to research that serves a high public interests, if that research cannot possibly be carried out otherwise. The data in question shall be anonymised, or if that is not possible for the research purposes, pseudonymised under the highest technical standards, and all necessary measures shall be taken to prevent unwarranted re-identification of the data subjects. However, the data subject shall have the right to object at any time in accordance with Article 19.

3. The Commission shall be empowered to adopt, *after requesting an opinion of the European Data Protection Board,* delegated acts in accordance with Article 86 for the purpose of further specifying ~~*other reasons of*~~ public interest in the area of public health as referred to in point (b) of paragraph 1 *and high public interest in the area of research as referred to in paragraph 2a~~, as well as criteria and requirements for the safeguards for the processing of personal~~*

		~~*data for the purposes referred to in paragraph 1*~~. *3a. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.*
Article 82 **Processing in the employment context** **1. Within the limits of this Regulation, Member States may adopt by law specific rules regulating the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination**	*Article 82* ***Processing in the employment context*** 1. Within the limits of this Regulation, Member States may adopt by law specific rules regulating the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment	Article 82 Minimum standards for processing data in the employment context 1. Member States may, *in accordance with the rules set out in this Regulation, and taking into account the principle of proportionality,* adopt by ~~*law*~~ *legal provisions* specific rules regulating the processing of employees' personal data in the employment context, in particular ~~*for*~~ *but not limited to* the purposes of the recruitment *and job applications within the group of undertakings,* the performance of the contract of employment, including discharge of obligations, laid down by law *and* by collective agreements, *in accordance with national law and practice,* management, planning and organisation of

of the employment relationship. **2. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.** **3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.**	relationship. 2. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them. 3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.	work, health and safety at work, and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship. *Member States may allow for collective agreements to further specify the provisions set out in this Article.* *1a. The purpose of processing such data must be linked to the reason it was collected for and stay within the context of employment. Profiling or use for secondary purposes shall not be allowed.* *1b. Consent of an employee shall not provide a legal basis for the processing of data by the employer when the consent has not been given freely.* *1c. Notwithstanding the other provisions of this Regulation, the legal provisions of Member States referred to in paragraph 1 shall include at least the following minimum standards:* *(a) the processing of employee data without the employees' knowledge shall not be permitted. Notwithstanding sentence 1,*

Member States may, by law, provide for the admissibility of this practice, by setting appropriate deadlines for the deletion of data, providing there exists a suspicion based on factual indications that must be documented that the employee has committed a crime or serious dereliction of duty in the employment context, providing also the collection of data is necessary to clarify the matter and providing finally the nature and extent of this data collection are necessary and proportionate to the purpose for which it is intended. The privacy and private lives of employees shall be protected at all times. The investigation shall be carried out by the competent authority;

(b) the open optical-electronic and/or open acoustic-electronic monitoring of parts of an undertaking which are not accessible to the public and are used primarily by employees for private activities, especially in bathrooms, changing rooms, rest areas, and bedrooms, shall be prohibited. Clandestine surveillance shall be inadmissible under all circumstances;

(c) where undertakings or authorities collect and process personal data in the context of medical examinations and/or aptitude tests, they must explain to the applicant or employee beforehand the purpose for which these data are being used, and ensure that afterwards they are provided with these data together with the results, and that they receive an explanation of their significance

on request. Data collection for the purpose of genetic testing and analyses shall be prohibited as a matter of principle;

(d) whether and to what extent the use of telephone, e-mail, internet and other telecommunications services shall also be permitted for private use may be regulated by collective agreement. Where there is no regulation by collective agreement, the employer shall reach an agreement on this matter directly with the employee. In so far as private use is permitted, the processing of accumulated traffic data shall be permitted in particular to ensure data security, to ensure the proper operation of telecommunications networks and telecommunications services and for billing purposes.

Notwithstanding sentence 3, Member States may, by law, provide for the admissibility of this practice, by setting appropriate deadlines for the deletion of data, providing there exists a suspicion based on factual indications that must be documented that the employee has committed a crime or serious dereliction of duty in the employment context, providing also the collection of data is necessary to clarify the matter and providing finally the nature and extent of this data collection are necessary and proportionate to the purpose for which it is intended. The privacy and private lives of employees shall be protected at all times. The investigation shall be carried out by the

competent authority;

(e) workers' personal data, especially sensitive data such as political orientation and membership of and activities in trade unions, may under no circumstances be used to put workers on so-called 'blacklists', and to vet or bar them from future employment. The processing, the use in the employment context, the drawing-up and passing-on of blacklists of employees or other forms of discrimination shall be prohibited. Member States shall conduct checks and adopt adequate sanctions in accordance with Article 79(6) to ensure effective implementation of this point.

1d. Transmission and processing of personal employee data between legally independent undertakings within a group of undertakings and with professionals providing legal and tax advice shall be permitted, providing it is relevant to the operation of the business and is used for the conduct of specific operations or administrative procedures and is not contrary to the interests and fundamental rights of the person concerned which are worthy of protection. Where employee data are transmitted to a third country and/or to an international organization, Chapter V shall apply.

	2. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to *paragraphs 1 and 1b*, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them. 3. The Commission shall be empowered, *after requesting an opinion from the European Data Protection Board,* to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the safeguards for the processing of personal data for the purposes referred to in paragraph 1.
	Article 82a *Processing in the social security context* *1. Member States may, in accordance with the rules set out in this Regulation, adopt specific legislative rules particularising the conditions for the processing of personal data by their public and private institutions and departments in the social security context if carried out in the public interest.* *2. Each Member State shall notify to the*

		Commission those provisions which it adopts pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and any subsequent amendment affecting them.	
Article 83 **Processing for historical, statistical and scientific research purposes** **1. Within the limits of this Regulation, personal data may be processed for historical, statistical or scientific research purposes only if:** **(a) these purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject;** **(b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information as long as these purposes can be**	***Article 83a*** ***Processing of personal data for historical purposes*** 1. Processing of personal data for historical purposes in archives carried out by public authorities or public bodies pursuant to Union or Member State law, shall not be considered incompatible with the purpose for which the data are initially collected, provided that the controller provides appropriate safeguards for the rights and freedoms of data subjects, in particular to ensure that the data are not processed for any other purposes or used in support of measures or decisions regarding any particular individual, and specifications on the conditions for	Article 83 Processing for historical, statistical and scientific research purposes 1. *In accordance with the rules set out in this Regulation*, personal data may be processed for historical, statistical or scientific research purposes only if: (a) these purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject; (b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information ~~*as long as these purposes can be fulfilled in this manner*~~ *under the highest technical standards, and all necessary measures are taken to prevent*	<u>PL poparła rozbicie art. 83 na trzy artykuły – wg celu przetwarzania</u> Ponadto zasugerowaliśmy aby jeden artykuł traktował cele historyczne i archiwalne <u>Ad. Par. 1</u> – The term "*used in support of measures or decisions regarding any particular individual*" should be deleted in order to allow the citizens to exercise their administrative rights by using the documentation stored in archives. <u>Ad. Par. 4</u> - In PL's opinion the right of access (in art. 15) is one of the basic rights of the data subjects enabling them to better control the processing of their personal data. This law should not be denied to the data subject, especially since in this case the data will be

fulfilled in this manner. **2. Bodies conducting historical, statistical or scientific research may publish or otherwise publicly disclose personal data only if:** **(a) the data subject has given consent, subject to the conditions laid down in Article 7;** **(b) the publication of personal data is necessary to present research findings or to facilitate research insofar as the interests or the fundamental rights or freedoms of the data subject do not override these interests; or** **(c) the data subject has made the data public.** **3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the processing of personal data for the purposes referred to in paragraph 1 and 2 as well as any necessary limitations on the rights of information to and access by the data subject and detailing the conditions and safeguards for the rights of the data subject under these circumstances.**	access to the data. 2. The controller shall ensure that personal data which are processed for the purposes referred to in paragraph 1 may be made accessible only to recipients after having demonstrated that the data will be used only for historical purposes. 3. Article 14a shall not apply where and insofar as, for processing for historical purposes, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by Union law or Member State law. In these cases, the controller shall provide for appropriate safeguards. 4. Articles 15, 17, 17a, and 18 shall not apply when personal data are kept for a period which does not exceed the period necessary for the sole purpose of processing for historical purposes, provided that the controller provides appropriate safeguards, taking into account the risks for the rights and freedoms of data subjects, in particular to ensure that the data are not used for taking measures or decisions regarding particular individual.	*unwarranted re-identification of the data subjects;* ~~*2. Bodies conducting historical, statistical or scientific research may publish or otherwise publicly disclose personal data only if:*~~ ~~*(a) the data subject has given consent, subject to the conditions laid down in Article 7;*~~ ~~*(b) the publication of personal data is necessary to present research findings or to facilitate research insofar as the interests or the fundamental rights or freedoms of the data subject do not override these interests; or*~~ ~~*(c) the data subject has made the data public.*~~ ~~*3. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the processing of personal data for the purposes referred to in paragraph 1 and 2 as well as any necessary limitations on the rights of information to and access by the data subject and detailing the conditions and safeguards for the rights of the data subject under these circumstances.*~~	processed for the purpose incompatible with the purpose for which the data were initially collected. We are aware of the potential burden that may arise in this respect for public institutions that process the data for these purposes on a large scale, it should be noted however that the possibility of exercising this right is already limited (data subject can exercise this right "*at reasonable intervals*"). PL is ready to further limit this right in the case of processing the data for statistical and archive purposes statistics (due to the effect of scale) by adding: "when it proves impossible or involves disproportionate effort". However, we are against the general exclusion from the right of access for data processed for statistical, scientific and historical purposes as it would deprive the data subject of control over their data. - The term "*the period necessary for the sole purpose of processing for historical purposes*" seems to be problematic and vague. It can be difficult for the controller to assess when the period necessary for the purpose of processing for historical purposes expired as it can be difficult to define "*sole*" historical purpose. PL suggests the need to exclude or limit the use of art. 16 (*right to rectification*) in relation to the data processed by the

archiving institutions for historical purposes, what is related to the function of the archives as a reliable repository safeguarding historical memory. This derogation seems to be essential in order to guarantee the historical reliability and authenticity of the data collected in archives.

Zaproponowaliśmy nastepujące brzmienie przepisu:

Article 83a
Processing of personal data for historical and archiving purposes

1. Processing of personal data for historical **and archiving** purposes ~~in archives~~ carried out by public authorities or public bodies pursuant to Union or Member State law, shall not be considered incompatible with the purpose for which the data are initially collected, provided that the controller provides appropriate safeguards for the rights and freedoms of data subjects, in particular to ensure that the data are not processed for any other purposes ~~or used in support of measures or decisions regarding any particular individual,~~ and specifications on the conditions for access to the data.

2. The controller shall ensure that personal data which are processed for the purposes referred to

in paragraph 1 may be made accessible only to recipients after having demonstrated that the data will be used only for historical purposes.

3. Article 14a shall not apply where and insofar as, for processing for historical purposes, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by Union law or Member State law. In these cases, the controller shall provide for appropriate safeguards.

4. Articles ~~15,~~ 17, 17a, and 18 shall not apply when personal data are kept for a period which does not exceed the period necessary for the ~~sole~~ purpose of processing for historical **and archiving** purposes, provided that the controller provides appropriate safeguards, taking into account the risks for the rights and freedoms of data subjects, in particular to ensure that the data are not used for taking measures or decisions regarding particular individual.

5. Article 16 shall not apply when processing for historical and archiving purposes, provided that the controller provides appropriate safeguards, taking into account the risks for the rights and freedoms of data subjects, in particular to ensure that the data are not used for taking measures or decisions regarding

particular individual.

Article 83b
Processing of personal data for statistical purposes

1. Processing of personal data for statistical purposes shall not be considered incompatible with the purpose for which the data are initially collected, provided that the controller provides appropriate safeguards for the rights and freedoms of data subjects, in particular to ensure that the data are not processed for any other purposes or used in support of measures or decisions regarding any particular individual or by the

<u>PL poparła rozbicie art. 83 na trzy artykuły – wg celu przetwarzania</u>

Poland sees the need to clearly define the "statistical purpose", which should be understood only as official statistics' purpose pursued in the public interest in order to exclude from the scope of this provision cases of application of the methods and statistical techniques for the commercial purposes.

Zaproponowaliśmy nastepujące brzmienie przepisu: Article 83b Processing of personal data for official statistics' purposes

1a. Personal data may be processed for official statistics' purposes only if:

	use of pseudonymous data. 2. Article 14a shall not apply where and insofar as, for processing for statistical purposes, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by Union law or Member State law. In these cases, the controller shall provide for appropriate safeguards. 3. Articles 15, 17, 17a, and 18 shall not apply when personal data are kept for a period which does not exceed the period necessary for the sole purpose of compiling statistics, provided that that the controller provides appropriate safeguards, taking into account the risks for the rights and freedoms of data subjects, in particular to ensure that the data are not used for taking measures or decisions regarding particular individuals.	(a) these purposes cannot be otherwise fulfilled by processing data which does not permit or no longer permits the identification of the data subject; (b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information, as long as these purposes can be fulfilled in this manner (c) data are not processed for any other purposes or used in support of measures or decisions regarding any particular individual (d) the data are not processed for any other purposes ~~1.~~ Processing of personal data for statistical purposes shall not be considered incompatible with the purpose for which the data are initially collected, provided that the controller provides ~~appropriate safeguards for the rights and freedoms of data subjects, in particular to ensure that the data are not processed for any other purposes or used in support of measures or decisions regarding any particular individual or by the use of pseudonymous data.~~ 2. Article 14a shall not apply where and insofar as, for

		processing for statistical purposes, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by Union law or Member State law. In these cases, the controller shall provide for appropriate safeguards. 3. Articles ~~15,~~ 17, 17a, and 18 shall not apply when personal data are kept for a period which does not exceed the period necessary for the ~~sole~~ **official statistics'** purpose ~~of compiling statistics~~, provided that that the controller provides appropriate safeguards, taking into account the risks for the rights and freedoms of data subjects, in particular to ensure that the data are not used for taking measures or decisions regarding particular individuals.
	Article 83c ***Processing for scientific purposes*** 1. Within the limits of this Regulation, personal data may be processed for scientific purposes only if: (a) these purposes cannot be otherwise fulfilled by processing	Propozycja PL: **Article 83c** **Processing for scientific purposes** 1. Within the limits of this Regulation, personal data may be processed for scientific purposes only if: (a) these purposes cannot be

		data which does not permit or no longer permits the identification of the data subject; (b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information, as long as these purposes can be fulfilled in this manner.			otherwise fulfilled by processing data which does not permit or no longer permits the identification of the data subject; (b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information, as long as these purposes can be fulfilled in this manner.
	2.	Personal data processed for scientific purposes may be published or otherwise publicly disclosed by the controller only if the publication of personal data is necessary to present scientific findings or to facilitate scientific purposes insofar as the interests or the rights or freedoms of the data subject do not override these interests and: (a) the data subject has given explicit consent; or (b) the data were made public by the data subject.		2.	Personal data processed for scientific purposes may be published or otherwise publicly disclosed by the controller only if ~~the publication of personal data is necessary to present scientific findings or to facilitate scientific purposes insofar as the interests or the rights or freedoms of the data subject do not override these interests and:~~ (a) the data subject has given explicit consent **or** **(ab) the publication of personal data is necessary to present scientific findings or to facilitate scientific purposes insofar as the interests or the rights or freedoms of the data**
	3.	Processing of personal data for scientific purposes shall not be considered incompatible with the purpose for which the data are initially collected, provided that the controller implements appropriate			

	safeguards for the rights and freedoms of data subjects, in particular to ensure that the data are not processed for any other purposes or used in support of measures or decisions regarding any particular individual or by the use of pseudonymous data.		**subject do not override these interests or** (b) the data were made public by the data subject.
	4. Article 14a shall not apply where and insofar as, for processing for scientific purposes, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by Union law or Member State law. In these cases, the controller referred to in paragraph 1 shall provide for appropriate safeguards.	3.	Processing of personal data for scientific purposes shall not be considered incompatible with the purpose for which the data are initially collected, provided that the controller implements appropriate safeguards for the rights and freedoms of data subjects, in particular to ensure that the data are not processed for any other purposes or used in support of measures or decisions regarding any particular individual or by the use of pseudonymous data.
	5. Articles 15, 17, 17a, and 18 shall not apply when personal data are kept for a period which does not exceed the period necessary for solely for scientific purposes, provided that that the controller implements appropriate safeguards, taking into account the risks for the rights and freedoms of data subjects, in particular to ensure that the data are not used for taking measures or decisions regarding particular individuals.	4.	Article 14a shall not apply where and insofar as, for processing for scientific purposes, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by Union law or Member State law. In these cases, the controller referred to in paragraph 1 shall provide for appropriate

			safeguards. 5. Articles ~~15~~, 17, 17a, and 18 shall not apply when personal data are kept for a period which does not exceed the period necessary for solely for scientific purposes, provided that that the controller implements appropriate safeguards, taking into account the risks for the rights and freedoms of data subjects, in particular to ensure that the data are not used for taking measures or decisions regarding particular individuals.
		Article 83a *Processing of personal data by archive services* *1. Once the initial processing for which they were collected has been completed, personal data may be processed by archive services whose main or mandatory task is to collect, conserve, provide information about, exploit and disseminate archives in the public interest, in particular in order to substantiate individuals' rights or for historical, statistical or scientific research*	

		purposes. These tasks shall be carried out in accordance with the rules laid down by Member States concerning access to and the release and dissemination of administrative or archive documents and in accordance with the rules set out in this Regulation, specifically with regard to consent and the right to object. *2. Each Member State shall notify to the Commission provisions of its law which it adopts pursuant to paragraph 1 by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.*
Article 84 **Obligations of secrecy** **1. Within the limits of this Regulation, Member States may adopt specific rules to set out the investigative powers by the supervisory authorities laid down in Article 53(2) in relation to controllers or processors that are subjects under national law or rules established by national competent bodies to an obligation of professional secrecy or**	*Article 84* ***Obligations of secrecy*** 1. Within the limits of this Regulation, Member States may adopt specific rules to set out the investigative powers by the supervisory authorities laid down in Article 53(2) in relation to controllers or processors that are subjects under national law or rules established by national competent bodies to an obligation of professional secrecy or other equivalent obligations of secrecy, where this is necessary and proportionate	Article 84 Obligations of secrecy 1. *In accordance with the rules set out in* this Regulation, Member States ~~*may adopt*~~ *shall ensure* specific rules *are in place setting* ~~*set*~~ out the ~~*investigative*~~ powers by the supervisory authorities laid down in Article 53~~*(2)*~~ in relation to controllers or processors that are subjects under national law or rules established by national competent bodies to an obligation of professional secrecy or other equivalent

other equivalent obligations of secrecy, where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. These rules shall only apply with regard to personal data which the controller or processor has received from or has obtained in an activity covered by this obligation of secrecy. **2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.**	to reconcile the right of the protection of personal data with the obligation of secrecy. These rules shall only apply with regard to personal data which the controller or processor has received from or has obtained in an activity covered by this obligation of secrecy. 2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.	obligations of secrecy, where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy. These rules shall only apply with regard to personal data which the controller or processor has received from or has obtained in an activity covered by this obligation of secrecy. 2. Each Member State shall notify to the Commission the rules adopted pursuant to paragraph 1, by the date specified in Article 91(2) at the latest and, without delay, any subsequent amendment affecting them.
Article 85 **Existing data protection rules of churches and religious associations** **1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of individuals with regard to the processing of personal data, such rules may continue to apply, provided that they are brought in line with the provisions of this Regulation.** **2. Churches and religious**	Article 85 **Existing data protection rules of** churches and religious associations 1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, comprehensive rules relating to the protection of individuals with regard to the processing of personal data, such rules may continue to apply, provided that they are brought in line with the provisions of this Regulation. 2. Churches and religious associations which apply comprehensive rules in accordance with paragraph 1 shall provide	Article 85 Existing data protection rules of churches and religious associations 1. Where in a Member State, churches and religious associations or communities apply, at the time of entry into force of this Regulation, ~~*comprehensive*~~ *adequate* rules relating to the protection of individuals with regard to the processing of personal data, such rules may continue to apply, provided that they are brought in line with the provisions of this Regulation. 2. Churches and religious associations which apply ~~*comprehensive*~~ *adequate* rules in

associations which apply comprehensive rules in accordance with paragraph 1 shall provide for the establishment of an independent supervisory authority in accordance with Chapter VI of this Regulation.	for the establishment of an independent supervisory authority in accordance with Chapter VI of this Regulation.	accordance with paragraph 1 shall ~~*provide for the establishment of an independent supervisory authority in accordance with Chapter VI of this Regulation*~~ *obtain a compliance opinion pursuant to Article 38*.
		Article 85a *Respect of fundamental rights* *This Regulation shall not have the effect of modifying the obligation to respect fundamental rights and fundamental legal principles as enshrined in Article 6 of the TEU.*
		Article 85b Standard Forms *The Commission may, taking into account the specific features and necessities of various sectors and data processing situations, lay down standard forms for* *a) specific methods to obtain verifiable*

consent referred to in Article 8(1),

b) the communication referred to in Article 12(2), including the electronic format,

c) providing the information referred to in paragraphs 1 to 3 of Article 14,

d) requesting and granting access to the information referred to in Article 15(1), including for communicating the personal data to the data subject,

e) documentation referred to in paragraph 1 of Article 28,

f) breach notifications pursuant to Article 31 to the supervisory authority and the documentation referred to in Article 31(4),

g) prior consultations referred to in Article 34, and for informing the supervisory authorities pursuant to Article 34(6).

2. In doing so, the Commission shall take the appropriate measures for micro, small and medium-sized enterprises.

3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 86 **Exercise of the delegation** **1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.** **2. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 336), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation.** **3. The delegation of power referred to in Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and**	*Article 86* ***Exercise of the delegation*** 1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article. 2. The delegation of power referred to in (…) Article 8(3), Article 9, (…) , Article 39a(7), [Article 43(3)], (…), Article 79a(4), Article 81(3), Article 82(3) and Article 83(3) shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation. 3. The delegation of power referred to in (…) Article 8(3), (…) Article 39a(7), [Article 43(3)], (…) Article 79a(4), Article 81(3), Article 82(3) and Article 83(3) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force. 4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.	Article 86 Exercise of the delegation 1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article. 2. The delegation of power referred to in *[Articles XXX]* shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation. 3. The delegation of power referred to in *[Articles XXX]* may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force. 4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the

Article 83(3) may be revoked at any time by the European Parliament or by the Council. A decision of revocation shall put an end to the delegation of power specified in that decision. It shall take effect the day following the publication of the decision in the Official Journal of the European Union or at a later date specified therein. It shall not affect the validity of any delegated acts already in force. **4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.** **5. A delegated act adopted pursuant to Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3), Article 17(9), Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 33(6), Article 34(8), Article 35(11), Article 37(2), Article 39(2), Article 43(3), Article 44(7), Article 79(6), Article 81(3), Article 82(3) and Article 83(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that**	5. A delegated act adopted pursuant to (…) Article 8(3), Article 9(3), (…) Article 39a(7), [Article 43(3)], (…), Article 79a(4), Article 81(3), Article 82(3) and Article 83(3) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.	Council. 5. A delegated act adopted pursuant to *[Articles XXX]* shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of *six ~~two~~* months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by *six ~~two~~* months at the initiative of the European Parliament or the Council.

period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or the Council.		
Article 87 **Committee procedure** **1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.** **2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.** **3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.**	*Article 87* ***Committee procedure*** 1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011. 2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply. 3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.	Article 87 Committee procedure 1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011. 2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply. ~~*3. Where reference is made to this paragraph, Article 8 of Regulation (EU) No 182/2011, in conjunction with Article 5 thereof, shall apply.*~~

Article 88 **Repeal of Directive 95/46/EC** **1. Directive 95/46/EC is repealed.** **2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.**	*Article 88* ***Repeal of Directive 95/46/EC*** 1. Directive 95/46/EC is repealed. 2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.	Article 88 Repeal of Directive 95/46/EC Directive 95/46/EC is repealed. 2. References to the repealed Directive shall be construed as references to this Regulation. References to the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC shall be construed as references to the European Data Protection Board established by this Regulation.
Article 89 **Relationship to and amendment of Directive 2002/58/EC** **1. This Regulation shall not impose additional obligations on natural or legal persons in relation to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with**	Article 89 Relationship to and amendment of Directive 2002/58/EC 1. This Regulation shall not impose additional obligations on natural or legal persons in relation to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same	Article 89 Relationship to and amendment of Directive 2002/58/EC 1. This Regulation shall not impose additional obligations on natural or legal persons in relation to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same

the same objective set out in Directive 2002/58/EC. **2 Article 1(2) of Directive 2002/58/EC shall be deleted.**	objective set out in Directive 2002/58/EC. 2 Article 1(2) of Directive 2002/58/EC shall be deleted.	objective set out in Directive 2002/58/EC. 2. Article*s* 1(2)*, 4 and 15* of Directive 2002/58/EC shall be deleted. *2a. The Commission shall present, without delay and by the date referred to in Article 91(2) at the latest, a proposal for the revision of the legal framework for the processing of personal data and the protection of privacy in electronic communications, in order to align the law with this regulation and ensure consistent and uniform legal provisions on the fundamental right to protection of personal data in the European Union*.
		Article 89a *Relationship to and amendment of Regulation (EC) 2001/45* *1. The rules set out in this Regulation shall be applied to the processing of personal data by Union institutions, bodies, offices and agencies in relation to matters for which they are not subject to additional rules set out in Regulation (EC) 2001/45.* *2. The Commission shall present, without delay and by the date specified in Article 91(2) at the latest, a proposal for the revision of the legal framework applicable to the processing of personal data by the*

		Union institutions, bodies, offices and agencies.
Article 90 **Evaluation** **The Commission shall submit reports on the evaluation and review of this Regulation to the European Parliament and the Council at regular intervals. The first report shall be submitted no later than four years after the entry into force of this Regulation. Subsequent reports shall be submitted every four years thereafter. The Commission shall, if necessary, submit appropriate proposals with a view to amending this Regulation, and aligning other legal instruments, in particular taking account of developments in information technology and in the light of the state of progress in the information society. The reports shall be made public.**	Article 90 Evaluation The Commission shall submit reports on the evaluation and review of this Regulation to the European Parliament and the Council at regular intervals. The first report shall be submitted no later than four years after the entry into force of this Regulation. Subsequent reports shall be submitted every four years thereafter. The Commission shall, if necessary, submit appropriate proposals with a view to amending this Regulation, and aligning other legal instruments, in particular taking account of developments in information technology and in the light of the state of progress in the information society. The reports shall be made public.	Article 90 Evaluation The Commission shall submit reports on the evaluation and review of this Regulation to the European Parliament and the Council at regular intervals. The first report shall be submitted no later than four years after the entry into force of this Regulation. Subsequent reports shall be submitted every four years thereafter. The Commission shall, if necessary, submit appropriate proposals with a view to amending this Regulation, and aligning other legal instruments, in particular taking account of developments in information technology and in the light of the state of progress in the information society. The reports shall be made public.

Article 91 **Entry into force and application** **1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.** **2. It shall apply from [two years from the date referred to in paragraph 1].** **This Regulation shall be binding in its entirety and directly applicable in all Member States.**		*Article 91* ***Entry into force and application*** 1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*. 2. It shall apply from [*two years from the date referred to in paragraph 1*].	Article 91 Entry into force and application 1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*. 2. It shall apply from [*two years from the date referred to in paragraph 1*]. This Regulation shall be binding in its entirety and directly applicable in all Member States.