



Wzorcowe zasady oceny skutków wykorzystania algorytmicznych systemów decyzyjnych w administracji publicznej

Sprawozdanie Europejskiego Instytutu Prawa



Translation into Polish of the official version of the ELI Model Rules on Impact Assessment of Algorithmic Decision-Making Systems Used by Public Administration published by the European Law Institute (ELI)* – The Office of the Prime Minister of the Republic of Poland gratefully acknowledges the permission to translate the text given by the ELI on 2 May 2022. Polish not being a working language of the ELI, the ELI has not reviewed this translation.

* ELI - Schottenring 16, Top 175, 1010 Vienna, Austria - <<https://www.europeanlawinstitute.eu/>> - secretariat@europeanlawinstitute.eu

Tłumaczenie na język polski oficjalnej wersji dokumentu „ELI Model Rules on Impact Assessment of Algorithmic Decision-Making Systems Used by Public Administration” opublikowanej przez Europejski Instytut Prawa (ELI)* zostało wykonane przez Kancelarię Prezesa Rady Ministrów Rzeczypospolitej Polskiej. KPRM z wdzięcznością przyjmuje do wiadomości zgodę na tłumaczenie tekstu udzieloną przez ELI w dniu 2 maja 2022 r. Język polski nie jest językiem roboczym ELI, ELI nie dokonała weryfikacji tego tłumaczenia.

* ELI – Schottenring 16, Top 175, 1010 Wiedeń, Austria - <https://www.europeanlawinstitute.eu/> - secretariat@europeanlawinstitute.eu



ELI

EUROPEAN
LAW
INSTITUTE

Wzorcowe zasady oceny skutków wykorzystania algorytmicznych systemów decyzyjnych w administracji publicznej

Sprawozdanie Europejskiego Instytutu Prawa

Europejski Instytut Prawa

Europejski Instytut Prawa jest niezależną organizacją typu non-profit, powołaną w celu inicjowania, prowadzenia i wspierania badań, a także wydawania zaleceń i zapewniania praktycznych wskazówek w dziedzinie rozwoju prawa europejskiego. Instytut opiera się na bogactwie różnorodnych tradycji prawnych, zaś jego misją jest dążenie do lepszego stanowienia prawa w Europie oraz wzmocnienia europejskiej integracji w zakresie samego prawa. Poprzez swoje działania EIP stara się przyczynić do powstania bardziej dynamicznej europejskiej wspólnoty prawnej, integrującej osiągnięcia różnych kultur prawnych oraz zwiększającej wartość wiedzy porównawczej i przyjmującej prawdziwie paneuropejską perspektywę. W związku z tym praca EIP obejmuje wszystkie gałęzie prawa: materialne i proceduralne, a także prywatne i publiczne.

EIP przestrzega zasad wszechstronności i współpracy, tym samym starając się zniwelować napotykaną często przepaść pomiędzy różnymi kulturami prawnymi, jak również pomiędzy prawem publicznym a prywatnym oraz między nauką a praktyką. W tym celu Instytut stara się angażować zróżnicowane kadry, odzwierciedlając bogactwo tradycji i dyscyplin prawnych oraz ram zawodowych występujących w całej Europie. Instytucja jest ponadto otwarta na stosowanie różnych podejść metodologicznych oraz na zbieranie opinii i perspektyw od jak najszerszego grona osób podzielających jej wizję.

Prezes: Pascal Pichonnaz

Pierwszy Wiceprezes: Lord John Thomas

Drugi Wiceprezes: Anne Birgitte Gammeljord

Skarbnik: Pietro Sirena

Marszałek Senatu: Reinhard Zimmermann

Sekretarz Generalny: Vanessa Wilcox

Dyrektor naukowy: Christiane Wendehorst

Sekretariat Europejskiego Instytutu Prawa

Schottenring 16/175

1010 Wiedeń

Austria

Tel.: + 43 1 4277 22101

E-mail: secretariat@europeanlawinstitute.eu

Witryna internetowa: www.europeanlawinstitute.eu

© Europejski Instytut Prawa 2022

Niniejsza publikacja otrzymała współfinansowanie w ramach europejskiego programu „Sprawiedliwość”. Składamy również serdeczne podziękowania Uniwersytetowi Wiedeńskiemu, który od 2011 r. gości Sekretariat EIP na mocy kolejnych ramowych umów o współpracy.

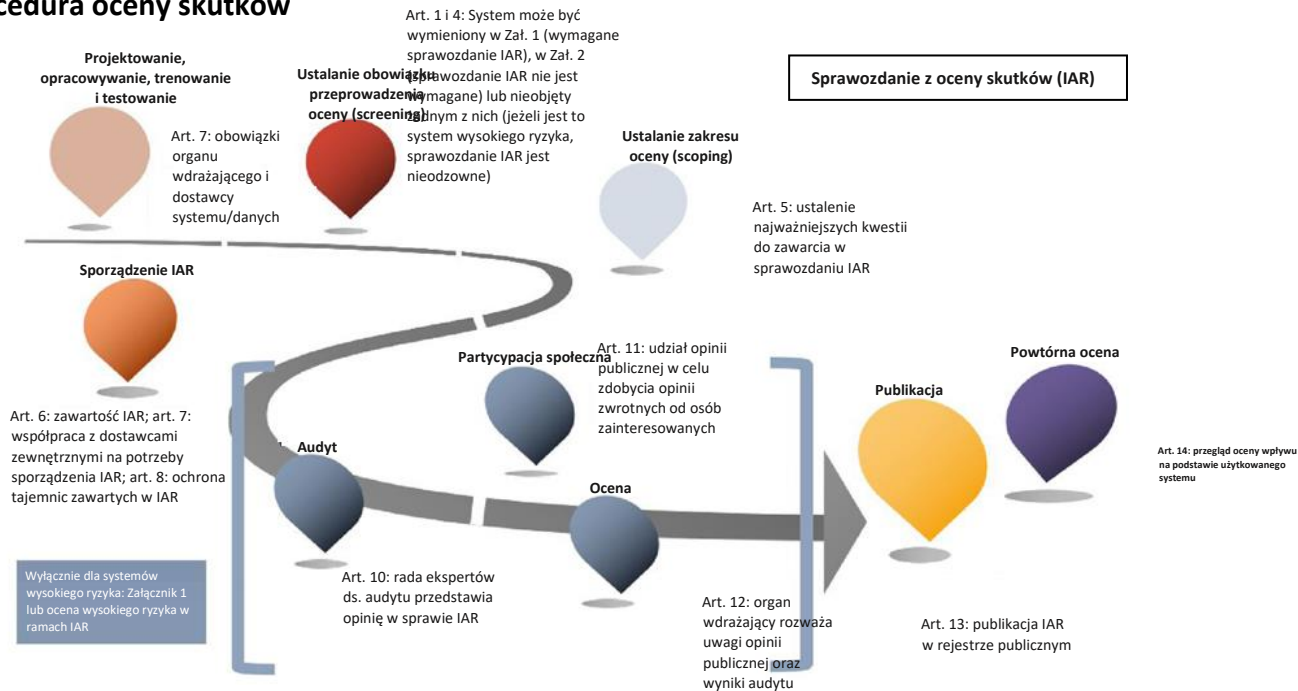


Spis treści

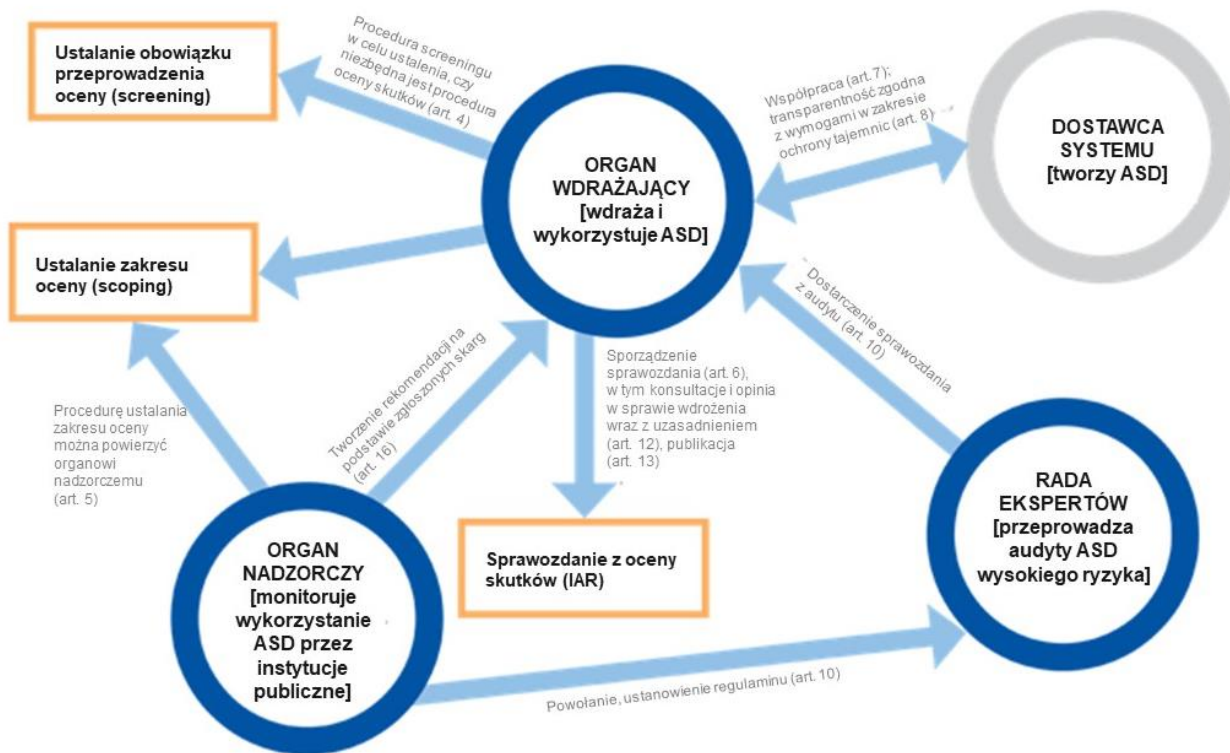
Podziękowania	8
Streszczenie	11
Przedmowa sprawozdawcy	13
Lista źródeł	15
Wzorcowe zasady EIP w zakresie oceny skutków wykorzystania algorytmicznych systemów decyzyjnych stosowanych w administracji publicznej — fundamentalne zasady.....	18
Rozdział 1: Postanowienia ogólne	18
Artykuł 1: Cel i zakres	18
Artykuł 2: Definicje.....	18
Artykuł 3: Koordynacja z innymi procedurami	19
Rozdział 2: Standardowa procedura oceny skutków	19
Artykuł 4: Ustalanie obowiązku przeprowadzenia oceny (screening)	19
Artykuł 5: Ustalanie zakresu oceny (scoping)	20
Artykuł 6: Sprawozdanie z oceny skutków	20
Artykuł 7: Współpraca i komunikacja z dostawcą systemu i dostawcą danych	21
Artykuł 8: Przejrzystość i ochrona tajemnic.....	22
Rozdział 3: Dodatkowe postanowienia dotyczące systemów wysokiego ryzyka	23
Artykuł 9: Zastosowanie niniejszego rozdziału	23
Artykuł 10: Audyt i Rada Ekspertów	23
Artykuł 11: Udział społeczeństwa	25
Artykuł 12: Ocena i sprawozdanie rozszerzone	26
Rozdział 4: Zakończenie oceny.....	26
Artykuł 13: Publikacja	26
Artykuł 14: Przegląd i powtórzenie oceny	27
Rozdział 5: Odpowiedzialność.....	28
Artykuł 15: Organ nadzorczy.....	28
Artykuł 16: Skargi i ochrona prawna.....	29
Załączniki	31
Załącznik 1: Systemy bezwzględnie podlegające ocenie skutków.....	31
Załącznik 2: Systemy niepodlegające ocenie skutków.....	31
Załącznik 3: Kwestionariusz dot. ustalania obowiązku przeprowadzenia oceny.....	32
Załącznik 4A: Kwestionariusz do sprawozdania z oceny skutków (wersja standardowa)	33
Uwagi ogólne	33
Załącznik 4B: Kwestionariusz do sprawozdania z oceny skutków (wersja rozszerzona)	37
Uwagi ogólne	37
Wzorcowe zasady EIP w zakresie oceny skutków wykorzystania algorytmicznych systemów decyzyjnych w administracji publicznej wraz z komentarzami i źródłami.....	45
Artykuł 1: Cel i zakres.....	45
Źródła	45
Uwagi	45
Artykuł 2: Definicje.....	46
Źródła	46
Uwagi	46
Artykuł 3: Koordynacja z innymi procedurami.....	48
Źródła	48
Uwagi	48
Artykuł 4: Ustalanie obowiązku przeprowadzenia oceny (screening)	48
Źródła	48
Uwagi	48
Artykuł 5: Ustalanie zakresu oceny (scoping)	49
Źródła	49

Uwagi	49
Artykuł 6: Sprawozdanie z oceny skutków	49
Źródła	49
Uwagi	49
Artykuł 7: Współpraca i komunikacja z dostawcą systemu i dostawcą danych	52
Uwagi	52
Artykuł 8: Przejrzystość i ochrona tajemnic	52
Źródła	52
Uwagi	52
Artykuł 9: Zastosowanie niniejszego rozdziału	54
Artykuł 10: Audyt i Rada Ekspertów	54
Źródła	54
Uwagi	54
Artykuł 11: Udział społeczeństwa	54
Źródła	54
Uwagi	54
Artykuł 12: Ocena	55
Uwagi	55
Artykuł 13: Publikacja	55
Źródła	55
Uwagi	55
Artykuł 14: Przegląd i powtórzenie oceny	56
Źródła	56
Uwagi	56
Artykuł 15: Organ nadzorczy	56
Źródła	56
Uwagi	56
Artykuł 16: Skargi i ochrona prawna	57
Źródła	57
Uwagi	57

Procedura oceny skutków



Harmonogram opracowania procedury oceny skutków



Rola organów zaangażowanych w procedurę oceny skutków

Podziękowania

Zespół projektowy

Przewodniczący

Marek Wierzbowski (prawnik i profesor, Polska)

Sprawozdawcy projektu

Marc Clément (sędzia sądu administracyjnego; Francja)

Paul Craig (profesor, Wielka Brytania)

Jens-Peter Schneider (profesor, Niemcy)

Inni członkowie

Jonathan Dollinger (asystent naukowy i doktorant, Niemcy; „osoba odpowiedzialna za akta” (PWF))

Franz Merli (profesor, Austria)

Daniel Le Métayer (starszy pracownik naukowy, Francja)

Karolina Wojciechowska (pracownik naukowy i adiunkt, adwokat, Polska)

Katarzyna Ziółkowska (doktorant, Polska)

Komitet doradczy

Oceniający

Philip Moser QC (adwokat, Wielka Brytania)

Pascal Pichonnaz (profesor, Szwajcaria)

Ilaria Pretelli (radca prawny, Szwajcaria)

Fryderyk Zoll (profesor, Niemcy/Polska)

Inni członkowie

Fabrizio Cafaggi (członek włoskiej Rady Stanu, Włochy)

Raja Chatila (profesor, Francja)

Péter Darák (sędzia Sądu Najwyższego, Węgry)

Jonas Ebbesson (profesor, Szwecja)

Joanna Goodey (Kierownik Działu Badań i Danych w Agencji Praw Podstawowych Unii Europejskiej (FRA))

Michael Gøtze (profesor, Dania)

Alexia Maniaki-Griva (Kierownik Działu Oceny Ex-Ante Skutków, Dyrekcja Generalna ds. Analiz Parlamentarnych (DG EPRS))

William M. McKechnie (sędzia Sądu Najwyższego, Irlandia)

David Reichel (Kierownik Projektu, Dział Badań Społecznych, Badań i Danych, FRA)

Jane Reichel (profesor, Szwecja)

Jason M. Schultz (profesor, Stany Zjednoczone)

Yannick Meneceur (Doradca ds. polityki w zakresie transformacji cyfrowej i sztucznej inteligencji, Rada Europy)

Olivia Tambou (profesor nadzwyczajny, Francja)

Clara Velasco (profesor nadzwyczajny, Hiszpania)

Komitet Konsultacyjny Członków

Raquel Abajas (asystent prawny, Hiszpania)

Chiara Silvia Armida Angiolini (niezależny badacz, Włochy)

Francesco Avolio (prawnik, Włochy)

Arvind Babajee (konsultant, Mauritius)

Alexander Balthasar (profesor wizytujący, Austria) Robert

Bray (prawnik i językoznawca, Belgia)

Alessandro Cenerelli (Doktorant, Włochy)
Ignace Claeys (profesor, Belgia)
Rada Notariatów Unii Europejskiej (przedstawiciele: Tamás Parti, Raul Radoi i Tamás Sajben)
Edita Čulinović Herc (profesor, Chorwacja)
Alberto De Franceschi (profesor, Włochy)
Gudula Deipenbrock (profesor, Niemcy)
Darinka Dekleva Marguč (starszy sędzia sądu administracyjnego, Słowenia)
Mustafa Ebaid (badacz prawa, Turcja)
Wian Erlank (profesor, RPA)
Dessislava Fessenko (adwokat, Bułgaria)
Elena Mihaela Fodor (profesor nadzwyczajny, Rumunia)
Laurence Gormley (profesor, Holandia)
Patrícia Guimarães (profesor nadzwyczajny, Brazylia)
Sarah Houllier (sędzia sądu administracyjnego, Francja)
Dariusz Kloza (habilitant, Belgia)
Maria Lubomira Kubica (adiunkt, Hiszpania)
Stephanie Laulhe Shaelou (profesor, Cypr)
Dulce Lopes (adiunkt, Portugalia)
Elwira Macierzyńska-Franaszczyk (adiunkt, Polska)
Caroline Mantl (starszy ekspert prawny, Irlandia)
Carlos Marinho (sędzia sądu apelacyjnego, Portugalia)
Irena Nesterova (habilitant, Łotwa)
Elena Alina Ontanu (adiunkt, Holandia)
Manuel Peláez Muras (starszy ekspert ds. zamówień publicznych, Hiszpania)
Katarzyna Pokryszka (wykładowca, Polska)
Radim Polčák (profesor, Czechy)
Oreste Pollicino (profesor nadzwyczajny, Włochy)
Francesco Quarta (adiunkt, Włochy)
Teresa Rodriguez de las Heras Ballell (profesor nadzwyczajny, Hiszpania)
Leigh Sagar (Adwokat, Wielka Brytania)
David Michael Schneeberger (pracownik naukowo-dydaktyczny, Austria)
Anna Simonati (profesor, Włochy)
Guillem Soler Solé (sędzia, Hiszpania)
Henrique Sousa Antunes (profesor, Portugalia)
Sjef van Erp (profesor, Holandia)
Veronica Williams (specjalista ds. prawnych, Belgia)
Boštjan Zalar (sędzia Sądu Najwyższego, Słowenia)

Specjalista ds. projektów EIP

Katja Kolman (starszy specjalista ds. projektów, Austria)

W trakcie realizacji projektu pracę Zespołu Projektowego wspierały Organy EIP oraz Sekretariat EIP.

Uczestnicy spotkań Zespołów Projektowych

1. 15.04.2020 r.: Marc Clément, Paul Craig, Jonathan Dollinger, Franz Merli, Jens-Peter Schneider, Marek Wierzbowski, Karolina Wojciechowska, Katarzyna Ziółkowska.
2. 28.04.2020 r.: Marc Clément, Paul Craig, Jonathan Dollinger, Olivia Tambou, Franz Merli, Jens-Peter Schneider, Marek Wierzbowski, Karolina Wojciechowska, Katarzyna Ziółkowska.

3. 26.05.2020 r.: Marc Clément, Paul Craig, Jonathan Dollinger, Olivia Tambou, Franz Merli, Jens-Peter Schneider, Marek Wierzbowski, Karolina Wojciechowska, Katarzyna Ziótkowska.
4. 1.07.2020 r.: Marc Clément, Paul Craig, Jonathan Dollinger, Olivia Tambou, Franz Merli, Jens-Peter Schneider, Marek Wierzbowski, Karolina Wojciechowska, Katarzyna Ziótkowska.
5. 25.08.2020 r.: Marc Clément, Paul Craig, Jonathan Dollinger, Franz Merli, Jens-Peter Schneider, Marek Wierzbowski, Karolina Wojciechowska, Katarzyna Ziótkowska.
6. 8.10.2020 r.: Marc Clément, Paul Craig, Jonathan Dollinger, Olivia Tambou, Franz Merli, Jens-Peter Schneider, Marek Wierzbowski, Karolina Wojciechowska, Katarzyna Ziótkowska.
7. 16.11.2020 r.: Marc Clément, Paul Craig, Jonathan Dollinger, Olivia Tambou, Franz Merli, Jens-Peter Schneider, Marek Wierzbowski, Karolina Wojciechowska, Katarzyna Ziótkowska.
8. 9.12.2020 r.: Marc Clément, Paul Craig, Jonathan Dollinger, Olivia Tambou, Franz Merli, Jens-Peter Schneider, Marek Wierzbowski, Karolina Wojciechowska, Katarzyna Ziótkowska.
9. 26.01.2021 r.: Marc Clément, Paul Craig, Jonathan Dollinger, Olivia Tambou, Franz Merli, Jens-Peter Schneider, Marek Wierzbowski, Karolina Wojciechowska, Katarzyna Ziótkowska.
10. 25.02.2021 r.: Marc Clément, Paul Craig, Jonathan Dollinger, Franz Merli, Jens-Peter Schneider, Marek Wierzbowski, Karolina Wojciechowska, Katarzyna Ziótkowska.
11. 29.03.2021 r.: Marc Clément, Jonathan Dollinger, Franz Merli, Jens-Peter Schneider, Marek Wierzbowski, Karolina Wojciechowska, Katarzyna Ziótkowska.
12. 23.04.2021 r.: Marc Clément, Paul Craig, Jonathan Dollinger, Daniel Le Metayer, Franz Merli, Jens-Peter Schneider, Marek Wierzbowski, Karolina Wojciechowska, Katarzyna Ziótkowska.
13. 25.05.2021 r.: Marc Clément, Paul Craig, Jonathan Dollinger, Franz Merli, Jens-Peter Schneider, Marek Wierzbowski, Karolina Wojciechowska, Katarzyna Ziótkowska.
14. 21.07.2021 r.: Marc Clément, Paul Craig, Jonathan Dollinger, Franz Merli, Jens-Peter Schneider, Marek Wierzbowski, Karolina Wojciechowska, Katarzyna Ziótkowska.
15. 18.08.2021 r.: Marc Clément, Paul Craig, Franz Merli, Jens-Peter Schneider, Marek Wierzbowski, Karolina Wojciechowska, Katarzyna Ziótkowska.
16. 30.09.2021 r.: Marc Clément, Paul Craig, Jonathan Dollinger, Franz Merli, Jens-Peter Schneider, Marek Wierzbowski, Karolina Wojciechowska, Katarzyna Ziótkowska.
17. 24.11.2021 r.: Marc Clément, Paul Craig, Jonathan Dollinger, Franz Merli, Jens-Peter Schneider, Marek Wierzbowski, Karolina Wojciechowska, Katarzyna Ziótkowska.

27.10.2020 r.: Spotkanie z Komitetem Doradczym

29.06.2021 r.: Spotkanie z Komitetem Doradczym

27.10.2021 r.: Spotkanie z Komitetem Doradczym

24.11.2020 r.: Spotkanie z Komitetem Konsultacyjnym Członków

3.11.2021 r.: Spotkanie z Komitetem Konsultacyjnym Członków

Opinie przedstawione w niniejszym sprawozdaniu nie powinny być traktowane jako odzwierciedlające poglądy organów, w imieniu których działali poszczególni członkowie Zespołu Projektowego i Komitetu Doradczego.

Streszczenie

Institucje publiczne od niepamiętnych czasów podejmowały decyzje i tworzyły przepisy. Charakter poszczególnych organów publicznych jest z konieczności różny w poszczególnych systemach prawnych. Ponadto powszechnie przyjmuje się, że decyzje podejmowane przez podmioty prywatne mogą w pewnych przypadkach podlegać prawu publicznemu. U podstaw tej różnorodności leży jednak wspólna cecha. Polega ona na tym, że choć od zawsze istniały pewne różnice pomiędzy systemami prawnymi, to decyzje niezmiennie podejmowali ludzie. Każda poddawana w wątpliwość zasada lub decyzja była przygotowywana bądź wydawana przez określoną osobę lub instytucję. Przedmiot niniejszych Wzorcowych Zasad świadczy o istotnej zmianie w tym względzie, gdyż w rzeczywistości w wielu przypadkach nie jest już możliwe powiązanie decyzji z konkretną osobą. Decyzja operacyjna może zostać podjęta za pomocą algorytmu lub innego mechanizmu zautomatyzowanego podejmowania decyzji. Człowiek nadal może brać udział w takich procesach decyzyjnych poprzez zaprojektowanie samego algorytmu lub zaangażowanie w proces przed podjęciem decyzji operacyjnej. Po skonfigurowaniu system może być jednak w pełni zautomatyzowany, co oznacza, że dane wyjściowe mogą być wykorzystywane bez udziału człowieka — włącznie z podejmowaniem decyzji. Ponadto niektóre systemy umożliwiają także algorytmowi uczenie się i rozwój. Nic więc dziwnego, że istnienie takich zautomatyzowanych systemów w szerokim rozumieniu stwarza nowe problemy zarówno dla prawa publicznego, jak i prywatnego. Świadczy o tym mnogość inicjatyw dotyczących tej problematyki, podejmowanych przez instytucje takie jak Unia Europejska (UE) i Rada Europy, a także przez poszczególne państwa narodowe.

Należy podkreślić, że niniejsze Wzorcowe Zasady zostały opracowane w taki sposób, aby nie były zależne od prawa unijnego i mogły być stosowane w systemach prawnych państw niebędących członkami UE. Innymi słowy, musi istnieć możliwość dopasowania ich do różnych kontekstów prawnych niezawierających podstawowych elementów unijnego prawa ochrony danych, takich jak ogólne rozporządzenie o ochronie danych (RODO). Przedstawione zasady zostały jednak opracowane w taki sposób, aby zapewnić ich zgodność nie tylko z już obowiązującym, ale również z obecnie tworzonym prawem unijnym, w szczególności z projektem rozporządzenia w sprawie sztucznej inteligencji (SI). Wspomniany projekt dotyczy w dużej mierze projektów w zakresie SI opracowanych lub wykorzystywanych przez różne administracje. Niniejsze Wzorcowe Zasady uzupełniają podejście przyjęte w projekcie rozporządzenia, zapewniając konkretne mechanizmy zabezpieczające zasady demokracji i praworządności oraz prawo do dobrej administracji w przypadku stosowania przez administrację publiczną algorytmicznych systemów decyzyjnych. Przykładem tego są przepisy dotyczące oceny skutków w konkretnych przypadkach, w tym w zakresie udziału społeczeństwa i ekspertów.

Zastrzeżenia związane z podejmowaniem decyzji przy wsparciu algorytmów można rozwiązać na różne sposoby. Główną ideą leżącą u podstaw niniejszych Wzorcowych Zasad jest przeprowadzenie oceny skutków. Różnorodność sytuacji, w których stosuje się oparte na algorytmach procesy decyzyjne, uniemożliwia przyjęcie jednego uniwersalnego podejścia. Doprowadziłoby to do powstania zasad, które byłyby zbyt rygorystyczne dla jednych systemów, a jednocześnie zbyt łagodne dla innych. Podejście przyjęte w niniejszych Wzorcowych Zasadach jest zatem zróżnicowane. Przyjmując niniejsze Wzorcowe Zasady system prawny może określić, że niektóre z takich systemów objęte są postanowieniami Załącznika 1, tj., że są one obarczone wysokim ryzykiem, a zatem bezwzględnie podlegają ocenie skutków. W tym samym celu można zastrzec, że inne systemy powinny być objęte zapisami Załącznika 2, gdyż są uważane za obarczone niskim ryzykiem i tym samym nie wymagają takiej oceny. Mogą jednak istnieć inne systemy, których nie da się łatwo zaklasyfikować *ex ante* jako podlegających zapisom Załącznika 1 lub Załącznika 2. Systemy te objęte są wstępną oceną ryzyka zgodnie z procedurą ustalania obowiązku przeprowadzenia oceny. Ocena skutków wymagana jest w przypadku gdy system stanowi co najmniej istotne ryzyko zgodnie z rzeczoną procedurą.

Niniejsze Wzorcowe Zasady szczegółowo określają charakter oceny skutków, która jest ujęta w ramy wcześniejszej procedury ustalania zakresu oceny. Ustalenie zakresu oceny ma na celu określenie bardziej szczegółowych kwestii, na których powinna skupić się ocena skutków. Ocena skutków ma być zarówno miarodajna, tj. musi uwzględniać korzyści i zagrożenia wynikające ze stosowania algorytmicznego

podejmowania decyzji, jak również proporcjonalna, tj. nie może stanowić nadmiernego obciążenia dla przeprowadzających ją organów. Istnieją jednak dalsze wymagania dotyczące systemów uznawanych za rozwiązania wysokiego ryzyka, zarówno w przypadku gdy podlegają one pod Załącznik 1, jak i wówczas, gdy zostały uznane za cechujące się takim ryzykiem w wyniku oceny skutków. Wymagania te określono w rozdziale 3 niniejszych Wzorcowych Zasad. Obejmują one m.in. kontrolę oceny skutków przez radę ekspertów oraz możliwość partycypacji społecznej. Wzorcowe Zasady przewidują także powołanie Organu Nadzorczego, który będzie monitorował powyższe procesy, oraz określają okoliczności, w jakich mogą zostać wniesione zastrzeżenia prawne.

Przedmowa sprawozdawcy

Administracja publiczna, będąca emanacją funkcji publicznych państwa, wymaga przetwarzania znacznie większej ilości danych niż w przypadku większości podmiotów prywatnych. Nowe technologie, takie jak sztuczna inteligencja, mogą zatem odegrać istotną rolę w modernizacji i ogólnej poprawie jej funkcjonowania. Z drugiej strony, fundamentalne znaczenie ma tutaj także zagwarantowanie przejrzystości, poprawności i bezpieczeństwa przetwarzanych danych. Dlatego też możliwość wykorzystania SI w działalności administracji publicznej ograniczona jest zasadą legalności i koniecznością zapewnienia wysokiego stopnia niezawodności stosowanych technologii, a także koniecznością zapewnienia poszanowania praw obywateli.

W związku z tym administracja publiczna stoi przed szczególnymi wyzwaniami związanymi z wdrażaniem SI oraz, bardziej ogólnie, algorytmicznych systemów decyzyjnych (ASD) — nawet jeśli nie korzystają one z technologii SI, takich jak uczenie maszynowe. Stosowanie takich technik stwarza specyficzne problemy związane z zasadą dobrej administracji. W przypadku administracji publicznej szczególne znaczenie mają również kwestie takie jak przejrzystość, rozliczalność, przestrzeganie przepisów i niedyskryminacja. Niniejsze Wzorcowe Zasady mają na celu stworzenie podstaw do uzupełnienia europejskiego prawodawstwa dotyczącego SI w specyficznym kontekście administracji publicznej. Prawodawstwa, które nie będzie hamowało innowacji, a jednocześnie — poprzez promowanie znaczenia oceny skutków — zapewni solidne zabezpieczenia zwiększające zaufanie obywateli do stosowania technologii w tej dziedzinie.

Ocena skutków stanowi zatem narzędzie służące do analizowania rezultatów stosowania ASD przez władze publiczne. Ocena skutków powinna:

- podnosić świadomość zagrożeń związanych z wykorzystaniem ASD w administracji publicznej;
- umożliwić organom administracyjnym podejmowanie świadomych decyzji w zakresie wykorzystania ASD;
- umożliwić udział w procesie podejmowania decyzji ekspertom i społeczeństwu;
- sprawić, by proces podejmowania decyzji i jego skutki były bardziej przejrzyste dla społeczeństwa;
- oraz ułatwić rozliczanie administracji publicznej z wykorzystania ASD.

Ocena skutków nie stanowi procedury udzielania licencji. Jej wynikiem jest bowiem sprawozdanie, a nie licencja. Zgodność z wymaganiami prawnymi jest jednym z kryteriów oceny proponowanego zastosowania systemu ASD, jednak ocena ta nie prowadzi do podjęcia wiążącej decyzji co do jego legalności. W przypadku niektórych ASD przeprowadzenie oceny skutków jest obowiązkowe, a zatem zastosowanie ich bez uprzedniej oceny byłoby nielegalne. Niemniej z prawnego punktu widzenia ocena nie determinuje decyzji organu władzy publicznej o zastosowaniu określonego ASD, lecz pozostawia tę decyzję w gestii samego organu.

Mimo że przy tworzeniu niniejszych Wzorcowych Zasad w pewnym stopniu inspirowano się prawem UE, w założeniu reguły te mają mieć bardziej ogólny charakter i nadawać się do adaptacji w różnych kontekstach prawnych zarówno w UE, jak i poza nią.

Ważną kwestią jest to, które podmioty mogłyby przyjąć Wzorcowe Zasady. UE i jej państwa członkowskie mają do wyboru kilka opcji. UE posiada uprawnienia legislacyjne, by upoważnić swoje instytucje, organy i agencje do przeprowadzania ocen skutków zastosowania ASD zgodnie z Wzorcowymi Zasadami. Bardziej złożoną kwestią są kompetencje legislacyjne UE w zakresie obowiązku przeprowadzania oceny skutków wykorzystania ASD przez władze krajowe. To ważne zagadnienie prawne wymaga jednak dalszych rozważań i wykracza poza zakres niniejszego projektu EIP. Zgodnie z obecnym stanem prawnym państwa członkowskie UE są odpowiedzialne za zobowiązanie swoich władz publicznych do przeprowadzania oceny skutków zastosowania ASD oraz mają do tego kompetencje. Na szczeblu krajowym to, czy niniejsze Wzorcowe Zasady zostaną wdrożone do prawa krajowego, przepisów mniejszych jednostek administracyjnych, czy też na obu szczeblach, zależy od podziału kompetencji ustawodawczych i administracyjnych.

Zgodnie z art. 1 lit. a) obecnego projektu rozporządzenia w sprawie SI Komisja proponuje uregulowanie nie tylko rozwoju SI i wprowadzania jej do obrotu, ale także jej stosowania. W przypadku przyjęcia takiego podejścia przez UE Zespół Projektowy zaleca wdrożenie początkowych punktów, które pozwolą Państwom Członkowskim

na wprowadzenie zasad oceny skutków stosowania ASD zgodnie z niniejszymi Zasadami. Nie stanowiłoby to nadmiernego obciążenia dla wspólnego rynku: Ocena skutków nie dotyczy produkcji SI ani wprowadzania jej do obrotu. W przeciwieństwie do zapisów tytułu III, rozdziału 2 projektu rozporządzenia w sprawie SI, nie tworzy ona również przepisów materialnych.

Jeśli jednak w wyniku dogłębnej analizy traktatów UE okaże się, że UE posiada kompetencje do zobowiązania państw członkowskich do przeprowadzania ocen skutków zastosowania ASD przez ich organy krajowe, Zespół Projektowy EIP opowiada się za wdrożeniem niniejszych Wzorcowych Zasady na poziomie całej UE. W takim przypadku projekt rozporządzenia w sprawie SI mógłby pozwolić państwom członkowskim na doprecyzowanie szczegółów, zwłaszcza dotyczących możliwości zastosowania i zakresu oceny skutków, poprzez wprowadzenie zmian do załączników I i II. To zaś umożliwiłoby im uwzględnienie kontekstu społecznego, kulturowego i technologicznego.

Lista źródeł

Prawodawstwo UE

Dyrektywa Rady z dnia 14 maja 1991 r. w sprawie ochrony prawnej programów komputerowych (91/250/EWG) [1991] Dz.U. L122/42

Dyrektywa 96/9/WE Parlamentu Europejskiego i Rady z dnia 11 marca 1996 r. w sprawie ochrony prawnej baz danych [1996] Dz.U. L77/20.

Dyrektywa 2007/2/WE Parlamentu Europejskiego i Rady z dnia 14 marca 2007 r. ustanawiająca infrastrukturę informacji przestrzennej we Wspólnocie Europejskiej (INSPIRE) [2007] Dz.U. L108/1.

Dyrektywa Parlamentu Europejskiego i Rady 2009/24/WE z dnia 23 kwietnia 2009 r. w sprawie ochrony prawnej programów komputerowych [2009] Dz.U. L 111/16

Dyrektywa Parlamentu Europejskiego i Rady 2011/92/UE z dnia 13 grudnia 2011 r. w sprawie oceny skutków wywieranych przez niektóre przedsięwzięcia publiczne i prywatne na środowisko [2011] Dz.U. L26/1.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję [2011] Dz.U. L55/13.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) [2016] Dz.U. L119/1.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu takich danych [2016] Dz.U. L119/89.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej [2018] Dz.U. L303/59.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych oraz ponownego wykorzystywania informacji sektora publicznego [2019] Dz.U. L172/56.

Wniosek Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii, COM (2021) 206 wersja ostateczna.

Inne przepisy

Konwencja o dostępie do informacji, udziale społeczeństwa w podejmowaniu decyzji oraz dostępie do sprawiedliwości w sprawach dotyczących środowiska, sporządzona w Aarhus dnia 25 czerwca 1998 r.

Directive on Automated Decision-Making [pol.: *Dyrektywa w sprawie zautomatyzowanego podejmowania decyzji*] (Kanada), <<https://tbs-sct.gc.ca/pol/doc-fra.aspx?id=32592>>, dostęp: 1.10.2021 r.

Bill Requiring Companies To Target Bias In Corporate Algorithms (USA, Senators Booker and Wyden) [pol.: *Ustawa zobowiązująca przedsiębiorstwa do zwalczania uprzedzeń w algorytmach firmowych (USA, senatorowie Booker i Wyden)*], <www.booker.senate.gov/?p=press_release&id=903> dostęp: 1.10.2021 r.

Senate Bill 5116 (Washington, Senators Hasegawa, Hunt, Kuderer and Wilson) [pol.: *Ustawa senacka nr 5116, (Waszyngton, senatorowie Hasegawa, Hunt, Kuderer i Wilson)*] <<https://lawfilesexternal.wa.gov/biennium/2021-22/Pdf/Bills/Senate%20Bills/5116.pdf>> dostęp: 1.10.2021 r.

Gesetz über die Umweltverträglichkeitsprüfung [pol.: *Ustawa o ocenie oddziaływania na środowisko*] (Niemcy).

Sprawozdania i dokumenty

KE, „Sztuczna inteligencja dla Europy” COM(2018) 237.

KE, „Dokument roboczy służb Komisji dotyczący odpowiedzialności za powstające technologie cyfrowe” SWD(2018) 137, wersja ostateczna

KE, „Budowanie zaufania do sztucznej inteligencji ukierunkowanej na człowieka” COM(2019) 168, wersja ostateczna.

KE, „Biała księga w sprawie sztucznej inteligencji – Europejskie podejście do doskonałości i zaufania”, Biała Księga COM(2020) 65, wersja ostateczna.

KE, „Sprawozdanie na temat wpływu sztucznej inteligencji, internetu rzeczy i robotyki na bezpieczeństwo i odpowiedzialność”, COM(2020) 64, wersja ostateczna.

Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji, „Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji”, <<https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai>> dostęp: 9.09.2021 r.

Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji, „Lista kontrolna oceny godnej zaufania sztucznej inteligencji (ALTAI)”, <<https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment>> dostęp: 9.09.2021 r.

Agencja Praw Podstawowych UE, Getting the future right [pol.: *Zapewnienie dobrej przyszłości*], <<https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights>>, dostęp: 14.12.2021 r.

Catelijne Muller, „The Impact of Artificial Intelligence on Human Rights, Democracy and the Rule of Law” [pol.: *Wpływ sztucznej inteligencji na prawa człowieka, demokrację i praworządność*] (CAHAI (2020) 06).

Rada Europy, Komitet ad hoc ds. sztucznej inteligencji, „Studium wykonalności” (CAHAI (2020) 23).

Rada Europy, Komitet ad hoc ds. sztucznej inteligencji, praw człowieka, demokracji i praworządności, „Impact Assessment of AI systems” [pol.: *Ocena wpływu systemów sztucznej inteligencji*] (CAHAI-PDG (2021) 05).

Komisja Etyki Danych (Niemcy), „Opinion of the Data Ethics Commission” [pol.: *Opinia Komisji Etyki Danych*], <www.bmjv.de/DE/Themen/FokusThemen/Datenethikkommission/Datenethikkommission_EN_node.html>, dostęp: 14.09.2021 r.

Biuro Komisarza ds. Informacji Publicznej, „AI Auditing Framework” [pol.: *Ramy audytu SI*], <<https://ico.org.uk/about-the-ico/news-and-events/ai-auditing-framework/>> dostęp: 14.12.2021 r.

KI Bundesverband, „Position Paper on EU-Regulation of Artificial Intelligence [pol.: *Stanowisko w sprawie unijnych regulacji w zakresie sztucznej inteligencji*], <https://ki-verband.de/wp-content/uploads/2021/02/Final_Regulierung-komprimiert-1.pdf> dostęp: 14.12.2021 r.

ReNEUAL, „Model Rules on EU Administrative Procedure Book II -Administrative Rulemaking” [pol.: *ReNEUAL: Model kodeksu postępowania administracyjnego, księga II — Wydawanie przepisów przez organy administracji*]

2014, <http://www.reneual.eu/images/Home/BookII-AdministrativeRulemaking_individualized_final_2014_09_03.pdf> dostęp: 9.09.2021 r.

Ponadto Zespół Projektowy zapoznał się z literaturą naukową. Chcąc jednak przedstawić niniejsze Wzorcowe Zasady w formie propozycji legislacyjnej, zespół redakcyjny postanowił zrezygnować z odniesień do niej.

Wzorcowe zasady EIP w zakresie oceny skutków wykorzystania algorytmicznych systemów decyzyjnych stosowanych w administracji publicznej — fundamentalne zasady

Rozdział 1: Postanowienia ogólne

1

Artykuł 1: Cel i zakres

1. Niniejsze Wzorcowe Zasady przewidują przeprowadzenie oceny skutków w zakresie wykorzystywanych przez władze publiczne algorytmicznych systemów decyzyjnych (zwanymi dalej „systemami” lub „ASD”), które mogą mieć znaczące skutki dla społeczeństwa.
2. Przed wdrożeniem systemu, który jest wymieniony w Załączniku 1 lub spełnia kryteria określone w art. 4 ust. 1, organ wdrażający przeprowadza ocenę skutków zgodnie z art. 5–13.
3. Niniejsze Wzorcowe Zasady nie mają zastosowania do systemów wyszczególnionych w Załączniku 2.
4. Organ wdrażający może dokonać implementacji systemów wymienionych w ust. 2 bez uprzedniej oceny skutków lub bez konsultacji, o których mowa w rozdziale 3, jeżeli:
 - a. system wdrażany jest w odpowiedzi na bezpośrednie zagrożenie publiczne, w szczególności związane ze zdrowiem lub bezpieczeństwem publicznym; oraz
 - b. opóźnienie spowodowane oceną skutków lub konsultacjami znacząco zaszkodziłoby celowi systemu; oraz
 - c. ryzyko związane z wdrożeniem systemu bez uprzedniej oceny skutków nie przewyższa ryzyka związanego z opóźnieniem wdrożenia systemu.

W takim przypadku organ wdrażający przeprowadza ocenę skutków natychmiast po rozpoczęciu korzystania z systemu.

2

Artykuł 2: Definicje

Na potrzeby niniejszych Wzorcowych Zasad:

1. „Algorytmiczny system decyzyjny” oznacza proces obliczeniowy, w tym powstały z wykorzystaniem uczenia maszynowego, statystyki lub innych technik przetwarzania danych lub sztucznej inteligencji, który podejmuje decyzję lub wspiera proces decyzyjny człowieka stosowany przez organ publiczny.
2. „Organ publiczny” oznacza:
 - a. każdy rząd lub inny organ administracji publicznej, w tym publiczne organy doradcze, na szczeblu Unii Europejskiej, jak również na poziomie krajowym, regionalnym lub lokalnym;
 - b. każdą osobę fizyczną lub prawną pełniącą publiczne funkcje administracyjne w ramach prawa Unii Europejskiej lub prawa krajowego; oraz
 - c. każdą osobę fizyczną lub prawną mającą obowiązki lub funkcje publiczne, lub

świadcząca usługi publiczne pod kontrolą organu lub osoby, o których mowa w lit. a) lub b).

3. „Decyzja” oznacza każde postanowienie organu władzy publicznej o podjęciu lub niepodjęciu działania.
4. „Społeczeństwo” oznacza jedną lub więcej osób fizycznych lub prawnych, posiadających osobowość prawną lub jej nieposiadających, oraz — zgodnie z ustawodawstwem lub praktyką krajową — ich stowarzyszenia, organizacje lub grupy.
5. „Dostawca systemu” oznacza podmiot, departament lub inną jednostkę organizacyjną w ramach podmiotu, która jest odpowiedzialna za: projektowanie, opracowywanie, konfigurowanie lub testowanie algorytmicznego systemu decyzyjnego.
6. „Dostawca danych” oznacza podmiot, departament lub inną jednostkę organizacyjną w ramach podmiotu, która dostarcza dostawcy systemu lub organowi wdrażającemu dane na potrzeby projektowania, opracowywania, konfigurowania, testowania i użytkowania algorytmicznego systemu decyzyjnego.
7. „Organ wdrażający” oznacza organ publiczny, który wykorzystuje lub zamierza wykorzystywać algorytmiczny system decyzyjny. Jeśli organ nadrzędny zdecyduje się polecić podległym organom stosowanie systemu, to organ nadrzędny jest uważany za organ wdrażający.
8. „Organ nadzoru” oznacza organ publiczny określony w art. 15.

3

Artykuł 3: Koordynacja z innymi procedurami

W przypadku konieczności przeprowadzenia oceny skutków zgodnie z niniejszymi Wzorcowymi Zasadami, organ wdrażający może odwołać się do ocen skutków lub równoważnych dokumentów wymaganych przez inne przepisy, np. przepisy dotyczące ochrony danych lub przepisy w zakresie bezpieczeństwa produktów. W takich przypadkach organ wdrażający wskazuje, którą część sprawozdania zgodnego z art. 6 należy zastąpić takimi dokumentami. Wspomniane dokumenty stanowią część sprawozdania przewidzianego w art. 6.

Rozdział 2: Standardowa procedura oceny skutków

4

Artykuł 4: Ustalanie obowiązku przeprowadzenia oceny (screening)

1. Systemy niewymienione w Załączniku 1 lub Załączniku 2 objęte są wstępną oceną ryzyka zgodnie z Załącznikiem 3 (procedura ustalania obowiązku przeprowadzenia oceny — *screening*). Organ wdrażający przeprowadza ocenę skutków zgodnie z art. 5–13, jeżeli system stanowi co najmniej istotne ryzyko zgodnie z procedurą ustalania obowiązku przeprowadzenia oceny.
2. Organ wdrażający ma obowiązek opublikować swoje odpowiedzi na kwestionariusz dot. ustalania obowiązku przeprowadzenia oceny (wyniki screeningu) przynajmniej w internecie, w ciągu dwóch tygodni od zakończenia procesu screeningu. Art. 13 ust. 3 stosuje się odpowiednio do wyników screeningu. Organ wdrażający przekazuje wyniki procesu screeningu organowi nadzorcemu.

5

Artykuł 5: Ustalanie zakresu oceny (scoping)

1. Przed sporządzeniem sprawozdania na podstawie art. 6 organ wdrażający może wstępnie określić niezbędny poziom szczegółowości oraz najważniejsze kwestie dotyczące zakresu oceny skutków (*scoping*). W tym celu organ wdrażający może konsultować się z organem nadzorczym określonym w art. 15, innymi odpowiednimi organami, radą niezależnych ekspertów ustanowioną na mocy art. 10, a także z przedstawicielami społeczeństwa.
2. Organ wdrażający może zwrócić się do organu nadzorczego określonego w art. 15 o ustalenie zakresu oceny. W takim przypadku organ wdrażający w jak największym stopniu uwzględnia wyniki ustalania zakresu. Jeśli organ wdrażający dokonuje odstępstwa od wyników tego procesu, to musi zawiadomić o tym fakcie organ nadzorczy oraz uzasadnić swoją decyzję. Wyniki ustalania zakresu nie są wiążące dla organu nadzorczego przy ocenie sprawozdania na podstawie art. 6 lub, w stosownych przypadkach, sprawozdania rozszerzonego.

6

Artykuł 6: Sprawozdanie z oceny skutków

1. Jeżeli zgodnie z art. 1 lub 4 konieczne jest przeprowadzenie oceny skutków, organ wdrażający sporządza sprawozdanie z oceny skutków (dalej: sprawozdanie).
2. Sprawozdanie zawiera:
 - a. opis przeznaczenia i działania systemu, w szczególności w zakresie:
 - i. rozwoju systemu, w szczególności jego algorytmów;
 - ii. charakteru i parametrów technicznych systemu;
 - iii. wyboru danych treningowych, walidacyjnych i testowych;
 - iv. kontekstu, w którym system jest wykorzystywany, w szczególności celów publicznych określonych w obowiązującym prawie;
 - v. wzajemnego powiązania systemu z innymi systemami cyfrowymi wdrożonymi przez organ wdrażający lub inne organy publiczne.
 - b. ocenę działania, skuteczności i wydajności systemu w odniesieniu do celów publicznych określonych w obowiązującym prawie, w szczególności w zakresie tego, czy działanie systemu może być zakłócone przez dostarczenie niskiej jakości danych podczas jego stosowania.
 - c. ocenę konkretnego i systemowego wpływu systemu na:
 - i. podstawowe lub inne indywidualne prawa lub interesy, w szczególności prawo do prywatności i ochrony danych, prawo do niedyskryminacji oraz prawo do dobrej administracji;
 - ii. demokrację, dobrobyt społeczny i środowiskowy;
 - iii. sam organ administracyjny, w szczególności szacowany odbiór systemu i jego decyzji przez pracowników, ryzyko nadmiernego lub niedostatecznego polegania przez pracowników na systemie, poziom umiejętności informatycznych oraz konkretnych umiejętności technicznych w ramach organu.
 - d. ocenę środków podjętych w celu zapewnienia:
 - i. maksymalizacji korzyści, jakie można osiągnąć dzięki wdrożeniu systemu, w odniesieniu do celów publicznych określonych w obowiązującym prawie;

- ii. minimalizacji zidentyfikowanego ryzyka i łagodzenia ewentualnych negatywnych skutków;
 - iii. sprawczości człowieka oraz jego nadzoru i kontroli nad systemem;
 - iv. wysokiej jakości danych;
 - v. dokładności we wszystkich grupach, a także precyzji i wrażliwości;
 - vi. solidności i bezpieczeństwa technicznego, odporności na ataki, bezpieczeństwa danych, planów awaryjnych, niezawodności, a także powtarzalności decyzji;
 - vii. przejrzystości systemu i możliwości wyjaśnienia jego decyzji;
 - viii. identyfikowalności umożliwiającej monitorowanie działania systemu;
 - ix. odpowiedzialności, w szczególności w zakresie nadzoru oraz możliwości audytu, jasnego podziału obowiązków, samokontroli, benchmarkingu oraz możliwości zadośćuczynienia za szkody lub krzywdy spowodowane przez system;
- e. o ile system nie jest określony jako „zawsze obciążony wysokim ryzykiem” w Załączniku 1 — końcowe określenie poziomu ryzyka;
- f. ogólną ocenę konieczności i proporcjonalności operacji przetwarzania w stosunku do celów, w szczególności kompromisów pomiędzy różnymi czynnikami określonymi w niniejszym artykule oraz tego, czy istnieją sensowne alternatywy dla przewidywanego systemu;
- g. oświadczenie o legalności korzystania z systemu w świetle obowiązującego prawa, w szczególności prawa o ochronie danych, prawa o postępowaniu administracyjnym i obowiązujących przepisów sektorowych, wraz z uzasadnieniem;
- h. wszelkie dodatkowe informacje wymagane przez inne artykuły niniejszych Wzorcowych Zasad.
3. Wytyczne dotyczące oceny zamieszczone w Załączniku 4 zawierają dalsze szczegóły dotyczące struktury i zawartości sprawozdania. Organ wdrażający może w razie potrzeby odstąpić od tych wytycznych lub zastosować inne, szczególnie w celu uwzględnienia specyfiki sektora, w którym system jest wykorzystywany. Organ wdrażający musi podać powody każdego istotnego odstępstwa.
4. W sprawozdaniu należy opisać system w taki sposób i z taką szczegółowością, jakie odpowiadają związanemu z nim poziomowi ryzyka oraz kontekstowi, w którym został on wdrożony. Sprawozdanie powinno zawierać dokładne informacje, a także być zrozumiałe dla społeczeństwa. W przypadku podania szczegółów, które nie są powszechnie zrozumiałe, organ wdrażający załącza streszczenie zrozumiałe dla przeciętnego odbiorcy.

7

Artykuł 7: Współpraca i komunikacja z dostawcą systemu i dostawcą danych

1. Organ wdrażający i dostawca systemu współpracują w procesie projektowania, opracowywania, trenowania oraz testowania systemu. Obie strony prowadzą stałą komunikację, zgodnie z odpowiednimi przepisami i umowami, w sposób umożliwiający odtworzenie prowadzonej wymiany informacji w późniejszym terminie.
2. Dostawca systemu dostarcza organowi wdrażającemu wszelkie informacje, dokumentację, dowody i prezentacje niezbędne do sporządzenia sprawozdania przewidzianego w art. 6.

3. Organ wdrażający i dostawca systemu wspólnie powołują zespół projektowy i wyznaczają swoich przedstawicieli w celu zapewnienia ogólnego, bieżącego nadzoru nad projektowaniem, rozwojem, trenowaniem oraz testowaniem systemu. Przedstawiciele wyznaczeni na członków zespołu projektowego powinni posiadać wystarczającą wiedzę specjalistyczną, aby być w stanie zrozumieć działanie systemu, jak również określić pożądane wyniki, rozpoznać potencjalne błędy, wady i usterki oraz zgłosić je organowi wdrażającemu. Zespół projektowy powinien mieć nieograniczony dostęp do informacji o postępie prac nad rozwojem systemu.
4. W celu zapewnienia, że system działa prawidłowo w warunkach ściśle odpowiadających rzeczywistym warunkom eksploatacji, jego badania końcowe przeprowadza się na sprzęcie organu wdrażającego lub innym wyposażeniu używanym przez rzeczony organ bądź eksploatowanym w jego imieniu. Badania przeprowadza personel organu wdrażającego po odpowiednim przeszkoleniu przez dostawcę systemu, obejmującym przekazanie wiedzy o systemie. Wyniki badań końcowych, wraz z ich parametrami i warunkami, zostaną włączone przez organ wdrażający do sprawozdania, o którym mowa w art. 6.
5. Organ wdrażający zamieszcza odpowiednie klauzule w umowie o udzielenie zamówienia lub podejmuje inne równoważne działania, aby zapewnić przestrzeganie przez dostawcę systemu obowiązków określonych w niniejszych Wzorcowych Zasadach.
6. Postanowienia ust. 1–5 stosuje się odpowiednio również do dostawcy danych.

8

Artykuł 8: Przejrzystość i ochrona tajemnic

1. Ocena skutków zastosowania systemu powinna być przeprowadzona z zachowaniem obowiązku poszanowania i ochrony poufności danych i informacji dotyczących lub należących do osób i podmiotów zaangażowanych w proces oceny, zgodnie z odpowiednimi przepisami i wymogami. Dotyczy to m.in. ochrony danych osobowych, prywatności, własności intelektualnej, tajemnic handlowych, bezpieczeństwa narodowego, a także obronności i bezpieczeństwa publicznego.
2. Organ wdrażający i dostawca systemu mogą zastrzec poufność danych i informacji udostępnianych, wykorzystywanych lub uzyskanych w trakcie oceny skutków, pod warunkiem że są to dane i informacje inne niż te o których mowa w ust. 1. Zastrzeżenie poufności takich danych i informacji powinno być odpowiednio uzasadnione i zbilansowane w stosunku do wymogów w zakresie przejrzystości oceny skutków, interesów organu wdrażającego i dostawcy systemu.
3. Organ wdrażający zamieszcza w sprawozdaniu, o którym mowa w art. 6, procedury dostępu do kodu źródłowego systemu i zbiorów danych wykorzystywanych do celów trenowania i testowania systemu. Dostęp do kodu źródłowego oraz zbiorów danych treningowych i testowych może zostać częściowo lub całkowicie ograniczony, jeżeli jest to niezbędne do ochrony uzasadnionych interesów i praw organu wdrażającego, dostawcy systemu lub osób trzecich.
4. Postanowienia ust. 1–3 stosuje się odpowiednio również do dostawcy danych.

Rozdział 3: Dodatkowe postanowienia dotyczące systemów wysokiego ryzyka

9

Artykuł 9: Zastosowanie niniejszego rozdziału

Postanowienia niniejszego rozdziału stosuje się w przypadku, gdy:

- a. system określony jest jako „zawsze obciążony wysokim ryzykiem” w Załączniku 1; lub
- b. organ wdrażający stwierdza w swoim sprawozdaniu, o którym mowa w art. 6, że system obciążony jest wysokim ryzykiem.

10

Artykuł 10: Audyt i Rada Ekspertów

1. Sprawozdanie, o którym mowa w art. 6, weryfikowane jest przez niezależną radę ekspertów.
2. Podczas audytu rada ekspertów ocenia ogólną jakość sprawozdania sporządzanego zgodnie z art. 6. Kryteria oceny obejmują dokładność, adekwatność i kompletność oceny skutków oraz jej zgodność z niniejszymi Wzorcowymi Zasadami. Organ wdrażający zapewnia ekspertom dostęp do systemu — włącznie z możliwością przeglądania jego kodu źródłowego i zbiorów danych wykorzystywanych do celów treningowych i testowych — a także możliwość wykorzystania go i przetestowania jego działania w praktyce.
3. Wyniki audytu dokumentowane są w sprawozdaniu z audytu. W sprawozdaniu z audytu rada ekspertów może zawrzeć uwagi i zastrzeżenia dotyczące w szczególności brakujących etapów procesu oceny skutków, braków w zakresie projektowania, rozwijania, trenowania lub testowania systemu, jak również dodatkowych, nieprzewidzianych zagrożeń, niewystarczających środków ochrony członków społeczeństwa, lub dodatkowych zastrzeżeń bądź zaleceń dla organu wdrażającego.
4. Niezależnie od obowiązków wynikających z art. 12 organ wdrażający może odpowiedzieć na uwagi i zastrzeżenia zgłoszone przez radę ekspertów zgodnie z ust. 3 i odpowiednio uzupełnić lub zmienić sprawozdanie, o którym mowa w art. 6. Organ wdrażający może poprosić radę ekspertów o złożenie oświadczenia w sprawie wystosowanej przez niego odpowiedzi na sprawozdanie z audytu.
5. Kandydaci do rady ekspertów mogą zgłaszać się w odpowiedzi na publiczne zaproszenie do wyrażenia zainteresowania wystosowane przez organ nadzorczy lub mogą być proponowani przez organy publiczne bądź społeczeństwo. Listę zgłoszonych kandydatów przechowuje organ nadzorczy.
6. Kandydaci do rady ekspertów powoływani są przez organ nadzorczy z listy, o której mowa w ust. 5, na podstawie otwartej, konkurencyjnej, niedyskryminacyjnej i przejrzystej procedury, pod warunkiem że spełniają obiektywne kryteria określone z wyprzedzeniem.
7. Członkowie rady ekspertów powoływani są spośród osób posiadających odpowiednią wiedzę i doświadczenie przy uwzględnieniu różnorodności pod względem geograficznym, narodowościowym i zawodowym, jak również w zakresie płci i wieku. Powinni oni posiadać niezbędne kompetencje i doświadczenie związane z wykorzystaniem algorytmicznych systemów decyzyjnych w administracji publicznej, w tym umiejętności technologiczne, handlowe, biznesowe, polityczne i prawne.

8. W celu uniknięcia potencjalnego konfliktu interesów oraz zapewnienia bezstronności audytu, członkowie rady ekspertów oraz podmioty, z którymi są powiązani, nie mogą uczestniczyć w konsultacjach społecznych i nie mogą być powiązani, bezpośrednio lub pośrednio, z dostawcą systemu, dostawcą danych, lub organem wdrażającym. Jeżeli uznaje się, że w przypadku danego członka rady ekspertów występuje konflikt interesów lub gdy można się spodziewać, że taki konflikt wystąpi, taki członek rady ekspertów powinien wstrzymać się od udziału w kontroli eksperckiej odpowiedniego sprawozdania sporządzanego zgodnie z art. 6.
9. Organ nadzorczy odwołuje członka rady ekspertów w przypadku niewykonania lub nienależytego wykonania obowiązków określonych w niniejszym artykule lub w regulaminie, o którym mowa w kolejnym ustępie.
10. Organ nadzorczy przyjmuje regulamin postępowania dla rady ekspertów.

11

Artykuł 11: Udział społeczeństwa

1. Po zakończeniu audytu organ wdrażający przeprowadza konsultacje społeczne, zapewniając możliwość udziału w tym procesie osobom, na które system ma szczególny wpływ.
2. Społeczeństwo oraz organ nadzorczy niezwłocznie, a najpóźniej wówczas, gdy jest to możliwe, informowani są przez organ wdrażający — przynajmniej przez internet — o następujących kwestiach:
 - a. fakt podlegania przez system procedurze oceny skutków, wraz z przekazaniem krótkiego opisu systemu;
 - b. dane identyfikacyjne i kontaktowe organu wdrażającego oraz szczegółowe informacje na temat harmonogramu przekazywania uwag lub pytań; oraz
 - c. czas i miejsce udostępnienia informacji określonych w ust. 3 oraz środki, które zostaną wykorzystane w tym celu.
3. Sprawozdanie zgodne z art. 6 i sprawozdanie z audytu (oraz, w stosownych przypadkach, odpowiedź instytucji wdrażającej i dodatkowe oświadczenie eksperta zgodnie z art. 10 ust. 4 podawane są do wiadomości publicznej przynajmniej w internecie w czasie, gdy społeczeństwo otrzymuje informację zgodnie z ust. 2 lit. c) niniejszego artykułu. Jeśli dokumenty wymienione w zdaniu pierwszym zawierają informacje niejawne w rozumieniu art. 8, organ wdrażający udostępnia zredagowaną i pozbawioną informacji niejawnych wersję takich dokumentów.
4. Społeczeństwo powinno z wyprzedzeniem otrzymać skuteczne możliwości udziału w ocenie systemu. W tym celu powinno być uprawnione do przekazywania uwag organowi wdrażającemu co najmniej w drodze konsultacji on-line.
5. Proces informowania społeczeństwa i konsultacji z nim może obejmować wysłuchanie publiczne. Informację o nim należy podać do wiadomości publicznej — przynajmniej na oficjalnej stronie internetowej.
6. Termin konsultacji społecznych nie może być krótszy niż 30 dni od daty publikacji, o której mowa w ust. 3.
7. Inne organy publiczne, których system może dotyczyć ze względu na ich szczególne obowiązki, w tym, w stosownych przypadkach, właściwy organ ochrony danych, również mają możliwość wyrażenia swojej opinii. Informacje zebrane zgodnie z art. 6 przekazywane są takim organom przez organ wdrażający. Do tego rodzaju konsultacji stosuje się odpowiednio postanowienia ust. 1–6.

12

Artykuł 12: Ocena i sprawozdanie rozszerzone

Organ wdrażający uwzględnia informacje, uwagi i opinie wyrażone w sprawozdaniu z audytu i w procesie włączenia społeczeństwa, o którym mowa w art. 11, oraz wydaje uzasadnioną opinię końcową na temat wdrożenia proponowanego systemu. Ocena ta, wraz z opinią końcową, powinna być zawarta w rozszerzonym sprawozdaniu, które powinno zawierać także wstępne sprawozdanie zgodne z art. 6, sprawozdanie z audytu, a także przynajmniej podsumowanie wyników udziału społeczeństwa.

Rozdział 4: Zakończenie oceny

13

Artykuł 13: Publikacja

1. Organ wdrażający publikuje sprawozdanie, o którym mowa w art. 6, lub, w stosownych przypadkach, rozszerzone sprawozdanie zgodnie z art. 12. Sprawozdanie zamieszcza się przynajmniej w internecie. Musi ono pozostać dostępne przez cały okres użytkowania systemu. Po zaprzestaniu korzystania z systemu organ wdrażający przechowuje wspomniane dokumenty zgodnie z ogólnymi zasadami dotyczącymi akt publicznych, przy czym muszą one pozostać dostępne w internecie przynajmniej przez rok.
2. Organ wdrażający powiadamia o publikacji ekspertów i członków społeczeństwa, którzy uczestniczyli w konsultacjach zgodnie z art. 10 i 11. Dostarcza także organowi nadzorcemu sprawozdanie, o którym mowa w art. 6, lub, w stosownych przypadkach, sprawozdanie rozszerzone.
3. Jeśli dokumenty wymienione w ust. 1 zawierają informacje niejawne w rozumieniu art. 8, organ wdrażający publikuje zredagowaną i pozbawioną informacji niejawnych wersję tych dokumentów. Organ wdrażający zapewnia dostęp do ich niezredagowanej wersji zgodnie z ogólnymi zasadami dotyczącymi wolności informacji. Organ nadzorczy każdorazowo otrzymuje zarówno wersję zredagowaną, jak i niezredagowaną.
4. Dokumenty wymienione w ust. 1 włączane są do rejestru publicznego na mocy art. 15 ust. 4.

14

Artykuł 14: Przegląd i powtórzenie oceny

1. Organ wdrażający monitoruje wykorzystanie systemu i dokonuje jego przeglądu w każdym przypadku, gdy istnieją faktyczne przesłanki co do istotnego negatywnego wpływu na aspekty objęte zapisami art. 6 ust. 2 lit. a)–d), które nie zostały przewidziane w sprawozdaniu, o którym mowa w art. 6, lub, w stosownych przypadkach, w sprawozdaniu rozszerzonym. W szczególności, organ ten dokonuje przeglądu systemu w przypadku gdy nastąpią zmiany w systemie lub w kontekście, w którym jest on używany, lub też w personelu wykorzystującym system, które to zmiany mogą mieć przynieść wspomniany wyżej skutek. Jeżeli organ wdrażający stwierdzi, że zmiany przyniosły taki skutek, to wówczas odpowiednio aktualizuje sprawozdanie, o którym mowa w art. 6 lub, w stosownych przypadkach, sprawozdanie rozszerzone.
2. Niezależnie od postanowień ust. 1, organ wdrażający dokonuje przeglądu systemu i jego oddziaływania:
 - a. po sześciu miesiącach użytkowania systemu, jeżeli w ciągu ostatnich trzech miesięcy nie został on poddany przeglądowi zgodnie z ust. 1; oraz
 - b. co dwa lata przekazuje organowi nadzorczemu sprawozdanie, o którym mowa w art. 6, lub, w stosownych przypadkach, sprawozdanie rozszerzone. W szczególności zmiany te powinny odzwierciedlać wszelką dodatkową wiedzę zdobytą podczas praktycznego użytkowania systemu.
3. Do takich powtórnych ocen skutków mają zastosowanie artykuły 5, 7 i 8, z uwzględnieniem niezbędnych zmian. Jeśli podczas wstępnej oceny skutków organ wdrażający konsultował się z ekspertami zgodnie z art. 10, to wówczas przekazuje on zmienione sprawozdanie również takim ekspertom, którzy mogą ponadto zgłaszać dodatkowe uwagi. Jeżeli organ wdrażający nie przeprowadził wcześniej konsultacji zgodnie z art. 10 i 11, lecz po dokonaniu przeglądu dojdzie do wniosku, że system spełnia już warunki określone w art. 9, to wówczas przeprowadza takie konsultacje.
4. Zmienione sprawozdanie oraz, w stosownych przypadkach, wszelkie uwagi zgłoszone zgodnie z ust. 3, publikowane są zgodnie z art. 13.

Rozdział 5: Odpowiedzialność

15

Artykuł 15: Organ nadzorczy

1. W celu nadzorowania korzystania z systemów przez władze publiczne ustanawia się organ nadzorczy.
2. Organ nadzorczy jest niezależnym podmiotem dysponującym odpowiednimi zasobami finansowymi i ludzkimi do tego, aby wykonywać swoje zadania zgodnie z niniejszymi przepisami. W szczególności na potrzeby organu nadzorczego należy zapewnić odpowiednią liczbę stale dostępnego personelu, którego kompetencje i wiedza fachowa obejmowały będą dogłębne zrozumienie sztucznej inteligencji i innych technologii algorytmicznych, jak również danych i ich przetwarzania, praw podstawowych, zagrożeń dla zdrowia i bezpieczeństwa, a także znajomość obowiązujących norm i wymogów prawnych. Organ nadzorczy powinien posiadać radę doradczą, w skład której powinni wejść m.in. przedstawiciele społeczeństwa obywatelskiego.
3. Do obowiązków organu nadzorczego należy:
 - a. nadzorowanie stosowania niniejszych zasad, a także przepisów przyjętych na ich podstawie;
 - b. monitorowanie istotnych zmian dotyczących wykorzystania systemu przez władze publiczne;
 - c. promowanie wśród społeczeństwa wiedzy na temat ryzyka, zasad, zabezpieczeń i praw związanych z korzystaniem z systemu przez władze publiczne;
 - d. na wniosek osoby dotkniętej skutkami stosowania systemu — udzielanie takiej osobie informacji o zasadach przeprowadzania oceny skutków oraz korzystania z systemu przez władze publiczne;
 - e. doradzanie władzom publicznym w zakresie oceny skutków oraz użytkowania systemu, w szczególności w kwestii ustalania zakresu, zgodnie z art. 5 ust. 2;
 - f. zapewnienie dostępności wystarczającej liczby ekspertów na potrzeby audytów przeprowadzanych zgodnie z art. 10;
 - g. prowadzenie rejestru publicznego zgodnie z ust. 4;
 - i. rozpatrywanie, w odpowiednim zakresie, skarg wniesionych zgodnie z art. 16 ust. 1;

- j. współpraca z innymi organami nadzorczymi;
 - k. wydawanie rocznego sprawozdania dla parlamentu i społeczeństwa na temat swojej działalności i istotnych wydarzeń dotyczących korzystania z systemu przez władze publiczne;
 - l. bez uszczerbku dla ust. 5 lit. e), przestrzeganie zasad poufności określonych w art. 8 w swojej komunikacji z innymi stronami.
4. Organ nadzorczy zapewnia internetowy rejestr publiczny zawierający:
- a. wyniki procesu ustalania obowiązku przeprowadzenia oceny (screening), zgodnie z art. 4 ust. 2;
 - b. bieżące konsultacje społeczne na podstawie art. 11;
 - c. sprawozdania opublikowane na podstawie art. 13. Art. 13 ust. 3 stosuje się odpowiednio do dokumentów w rejestrze publicznym.
5. Niezależnie od uprawnień przyznanych na mocy innych artykułów niniejszych Zasad, organ nadzorczy ma prawo:
- a. badać stosowanie niniejszych Wzorcowych Zasad przez organy wdrażające, wyznaczonych ekspertów oraz dostawców systemów lub danych z własnej inicjatywy lub na podstawie skargi złożonej na podstawie art. 16 ust. 1;
 - b. bez ograniczeń wynikających z art. 8, uzyskiwać wszelkie informacje niezbędne do wykonywania swoich zadań od organów wdrażających, wyznaczonych ekspertów oraz dostawców systemów lub danych;
 - c. formułować zalecenia dla organów wdrażających;
 - d. po bezskutecznym wydaniu zalecenia, wszcząć postępowanie sądowe lub wydać wiążący nakaz w celu powstrzymania organu wdrażającego przed korzystaniem z systemu, który — z naruszeniem niniejszych zasad — nie został poddany odpowiedniej ocenie skutków lub odpowiedniej powtórnej ocenie skutków;
 - e. wydać, z własnej inicjatywy lub na wniosek, opinię dla parlamentu i rządu lub innych instytucji i organów, a także dla społeczeństwa, dotyczącą wszelkich kwestii związanych z użytkowaniem systemu przez władze publiczne.

16

Artykuł 16: Skargi i ochrona prawna

1. Bez uszczerbku dla bardziej korzystnych warunków zapewnia się, że zgodnie z obowiązującym prawem zainteresowani członkowie społeczeństwa, którzy mają w tym zakresie wystarczający interes lub utrzymują, że doszło do naruszenia prawa, jeśli administracyjne prawo proceduralne wymaga tego jako nieodzownego warunku, mogą wnieść do organu nadzorczego skargę na wykorzystanie przez organ wdrażający systemu, który — z naruszeniem niniejszych zasad — nie został poddany odpowiedniej ocenie skutków lub odpowiedniej powtórnej ocenie skutków.
2. Jeśli organ nadzorczy uzna, że skarga jest zasadna, może skorzystać z uprawnień wymienionych w art. 15 ust. 5 lit. c) i d). Organ nadzorczy przekazuje skarżącemu i organowi wdrażającemu uzasadnioną decyzję w ciągu trzech miesięcy od otrzymania skargi, chyba że wystąpią wyjątkowe okoliczności. Ponadto informuje on skarżącego o odpowiedzi organu wdrażającego.
3. Bez uszczerbku dla bardziej korzystnych warunków zapewnia się, że zgodnie z obowiązującym prawem zainteresowani członkowie społeczeństwa, którzy mają w tym zakresie wystarczający interes lub utrzymują, że doszło do naruszenia prawa, jeśli

administracyjne prawo proceduralne wymaga tego jako warunku koniecznego, będą mieli:

- a. dostęp do procedury odwoławczej przed sądem w następstwie skargi złożonej na podstawie ust. 1. W ramach procedury odwoławczej możliwe będzie zakwestionowanie:
 - i. odrzucenia i oddalenia skargi przez organ nadzorczy;
 - ii. braku decyzji organu nadzorczego w ciągu trzech miesięcy, z wyjątkiem przypadków wystąpienia wyjątkowych okoliczności;
 - iii. dalszego stosowania systemu przez organ wdrażający po wydaniu przez organ nadzorczy zalecenia zaprzestania jego użytkowania.
 - b. dostęp do procedury odwoławczej przed sądem w celu zakwestionowania legalności orzeczeń podlegających kontroli zgodnie z obowiązującym prawem ze względu na fakt, że zostały wydane przez system, który nie został poddany właściwej ocenie skutków lub powtórnej ocenie skutków, bądź też przy wsparciu takiego systemu.
4. To, co stanowi wystarczający interes lub naruszenie prawa, określa się w sposób spójny z celem, jakim jest zapewnienie zainteresowanej społeczności szerokiego dostępu do wymiaru sprawiedliwości. W tym celu uznaje się, że każda organizacja pozarządowa, która spełnia wymogi określone przepisami prawa, spełnia również wymogi określone w ust. 1 lub 3.
5. Każda tego typu procedura musi charakteryzować się uczciwością, sprawiedliwością i terminowością, a ponadto nie może być nadmiernie kosztowna.

Załączniki

Załącznik 1: Systemy bezwzględnie podlegające ocenie skutków

Komentarz:

Załącznik 1 nie został sporządzony ze względu na fakt, że jego treść powinna być przedmiotem decyzji politycznych właściwych organów ustawodawczych. Dobrym punktem wyjścia do przygotowania jego treści byłby Załącznik III do unijnego projektu rozporządzenia w sprawie SI (COM (2021) 206, wersja ostateczna). Typowymi kandydatami do uwzględnienia w Załączniku 1 byłyby zatem wszelkiego rodzaju systemy rozpoznawania twarzy, systemy określające uprawnienia do otrzymywania świadczeń socjalnych lub niektóre systemy prognozowania zdarzeń przestępczych. Niemniej w Załączniku III do projektu rozporządzenia w sprawie SI nadal występują pewne luki. Dotyczy to przede wszystkim infrastruktury krytycznej, w której nie uwzględniono ruchu kolejowego i lotniczego, a także sieci telekomunikacyjnych i innej infrastruktury cyfrowej. Ponadto należy uwzględnić systemy wykorzystywane np. przez organy podatkowe lub organy zajmujące się prawem ochrony środowiska bądź prawem gospodarczym. Inne obszary administracji publicznej mogą budzić podobne obawy, wobec czego je również można zakwalifikować do kategorii wysokiego ryzyka.

W związku z tym Zespół Projektowy zachęca wszystkie organy ustawodawcze do wyjścia poza definicję SI wysokiego ryzyka zawartą w unijnym projekcie rozporządzenia w sprawie SI przy opracowywaniu treści Załącznika 1. Kryteria wymienione w art. 6 oraz w Załącznikach 3 i 4 do niniejszych Wzorcowych Zasad mogą być pomocne przy określaniu tego, jakie systemy powinny być uwzględnione w Załączniku 1. Treść załącznika powinna być również inspirowana debatą publiczną.

Wśród możliwych opcji legislacyjnych jest zapewnienie regularnych przeglądów załączników 1 i 2. Jeżeli Załącznik 1 obejmuje dodatkowe ASD, prawodawca powinien również zdecydować, czy już wdrożone systemy także wymagają oceny skutków.

Załącznik 1 powinien składać się z dwóch części:

- systemy bezwzględnie podlegające ocenie skutków, przy czym organ wdrażający nadal musi określić, czy system jest obciążony wysokim

ryzykiem;

- systemy, które zawsze są obciążone wysokim ryzykiem.

Załącznik 2: Systemy niepodlegające ocenie skutków

Komentarz:

Załącznik 2 nie został sporządzony ze względu na fakt, że jego treść powinna być przedmiotem decyzji politycznych.

W zamierzeniu Załącznik 2 zawierałby różne rodzaje systemów, które są już tak powszechnie stosowane, że związane z nimi ryzyko jest dobrze znane i łatwe do opanowania, jak również systemy, w przypadku których nie można zastosować wysokiego stopnia kontroli publicznej, jaki zapewnia ocena skutków (głównie systemy stosowane w dziedzinie bezpieczeństwa narodowego).

Załącznik 3: Kwestionariusz dot. ustalania obowiązku przeprowadzenia oceny

Komentarz:

Pytania w kwestionariuszu dot. ustalania obowiązku przeprowadzenia oceny powinny być wzorowane na tych zawartych w Załączniku 4. Jest jednak zasadnicza różnica: Podczas gdy Załącznik 4 wymaga sformułowania odpowiedzi od organu wdrażającego, Załącznik 3 będzie w większości testem wielokrotnego wyboru wzorowanym na kanadyjskiej ocenie wpływu algorytmów. Wyniki tego testu pozwolą określić, czy system stwarza małe ryzyko (tzn. nie jest konieczna ocena skutków), istotne ryzyko (ocena skutków jest konieczna) bądź też duże ryzyko (konieczna jest ocena skutków z udziałem społeczeństwa/ekspertów). Niektóre pytania będą wymagały krótkich wyjaśnień w celu zwiększenia przejrzystości.

Zespół Projektowy zrezygnował z opracowania kompletnego kwestionariusza dot. ustalania obowiązku przeprowadzenia oceny. Nie posiada on bowiem niezbędnej wiedzy technicznej oraz legitymacji politycznej do tego, aby przypisać odpowiednią wagę poszczególnym pytaniom, co do pewnego stopnia jest również zadaniem politycznym.

Wartość ryzyka przypisana do każdej odpowiedzi będzie zależała od wagi problemu. Przykładowo pytaniom dotyczącym obaw związanych z dyskryminacją należy przypisać wyższe wartości ryzyka. Pytania dotyczące niektórych środków w zakresie przejrzystości, które wspomagają ekspertów w lepszym zrozumieniu systemu, ale nie są zbyt istotne dla społeczeństwa, powinny mieć niższą wartość ryzyka.

Poniżej podano przykłady pytań, które powinny znaleźć się w Załączniku 3:

Pytanie typu 1: Odpowiedzi tak/nie w zakresie poziomu ryzyka Czy stosowany algorytm będzie stanowił tajemnicę (handlową)?

- Tak [wartość ryzyka 1 lub wyższa]
- Nie [wartość ryzyka 0]

Pytanie typu 2: Kilka odpowiedzi na skali ruchomej

- Czy skutki decyzji są odwracalne?
-
-
-

Tak, są łatwo odwracalne. [wartość ryzyka równa 0].

Prawdopodobnie są odwracalne. [wartość ryzyka równa 1]

Są trudne do odwrócenia. [wartość ryzyka 2].

Są nieodwracalne. [wartość ryzyka równa 3 lub wyższa].

Poszczególne odpowiedzi mogą również nie być dokładnie zdefiniowane, aby podkreślić, że nie istnieją tutaj wyraźne linie podziału, zaś same odpowiedzi zasadniczo dotyczą stopnia trudności:

W skali od 1 do 5, jak łatwo można odwrócić skutki decyzji?

(0 = bardzo łatwo, 5 = wcale)

Pytanie typu 3: Środki ograniczające ryzyko

W przypadku obu typów pytań do niektórych odpowiedzi można również przypisać wartość negatywną. Jest to możliwe wówczas, gdy odpowiedź wskazuje, że organ wdrażający dokonał wdrożenia środków zarządzania ryzykiem wykraczających poza to, czego można by w uzasadniony sposób oczekiwać.

Czy konsultowali Państwo swoją definicję sprawiedliwości z zainteresowanymi społecznościami?

- Tak [wartość ryzyka -1]
- Nie [wartość ryzyka 0]

Pytanie typu 4: Odniesienie do istniejących ocen skutków

Ryzyko stwarzane przez system maleje, jeśli jest on już powszechnie stosowany. Dlatego też wynik oceny ryzyka powinien zostać istotnie zredukowany, jeśli inne organy przeprowadziły już ocenę wpływu. Taka redukcja zależy od maksymalnej liczby punktów przyznanych w ramach oceny ryzyka. Powinna ona mieć większą wagę niż poszczególne pytania.

Czy inne organy przeprowadziły już ocenę skutków w odniesieniu do tego samego lub podobnego systemu na podstawie niniejszych Wzorcowych Zasad i w porównywalnym kontekście?

- Tak, w odniesieniu do tego samego systemu.
- [redukcja oceny ryzyka o 10 pkt]
- Tak, w odniesieniu do bardzo podobnego systemu. [redukcja oceny ryzyka o 8 pkt]
- Tak, w odniesieniu do podobnego systemu. [redukcja oceny ryzyka o 4 pkt]
- Tak, w tym samym kontekście. [redukcja oceny ryzyka o 10 pkt]

Tak, w bardzo podobnym kontekście. [redukcja oceny ryzyka o 8 pkt]

Tak, w podobnym kontekście. [redukcja oceny ryzyka o 4 pkt]

Nie, [brak redukcji wyniku ryzyka]

Załącznik 4A: Kwestionariusz do sprawozdania z oceny skutków (wersja standardowa)

Komentarz:

Zawarte poniżej pytania, a także spora część sformułowań, opierają się na Liście kontrolnej oceny godnej zaufania sztucznej inteligencji (ALTAI) opracowanej przez Grupę Ekspertów Wysokiego Szczebla.¹ Zespół projektowy EIP dodał lub zmodyfikował kilka pytań. Niektóre z tych zmian inspirowane są projektem rozporządzenia Komisji Europejskiej w sprawie sztucznej inteligencji,² stanowiskiem niemieckiego stowarzyszenia „KI Bundesverband” w sprawie rzeczonego rozporządzenia UE,³ Studium Wykonalności Komitetu ad hoc ds. sztucznej inteligencji Rady Europy (CAHAI),⁴ jak również przez sprawozdanie Europejskiej Agencji Praw Podstawowych pt. „Getting the Future Right”.⁵ W poniższych przypisach podano źródła wykorzystane do stworzenia kwestionariusza. Zakres projektu nie obejmował uzasadnionej oceny kwestionariuszy.

Uwagi ogólne

Udzielając odpowiedzi należy podawać merytoryczne wyjaśnienia i unikać podsumowań zdawkowych, jednowyrazowych. Jeśli pytanie nie wydaje się

odpowiednie dla danego systemu, należy wyjaśnić przyczynę.

We wszystkich poniższych sekcjach należy rozważyć:

- Czynności szkoleniowe mające na celu zaznajomienie pracowników korzystających z systemu z istotnymi kwestiami technicznymi, etycznymi i prawnymi;
- Bieżące monitorowanie podczas użytkowania systemu;
- Odpowiednie informowanie/komunikowanie się z zainteresowanymi osobami, zwłaszcza gdy wymagana jest ich współpraca;
- Mechanizmy zgłaszania przez zainteresowane osoby wszelkich napotkanych problemów;
- Mechanizmy rozwiązywania problemów, które mogą pojawić się podczas korzystania z systemu.

Struktura kwestionariusza opiera się na art. 6.

a) opis przeznaczenia i działania systemu, w szczególności w zakresie:

i. rozwoju systemu, w szczególności jego algorytmów;

1. Kto zaprojektował system i w jaki sposób został on opracowany?⁶ Od kogo zakupiono system?
2. Czy istnieją normy zharmonizowane opublikowane w Dzienniku Urzędowym UE lub specyfikacje techniczne, które mają (częściowo lub w całości) zastosowanie do posiadanego systemu?

ii. charakter i parametry techniczne systemu;

3. Proszę opisać, w miarę możliwości w sposób nietechniczny, technologię lub technologie, których zamierzają Państwo użyć.
4. W stosownych przypadkach należy także podać opis przewidywanych lub planowanych zmian w systemie i jego działaniu.

¹ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji, „Lista kontrolna oceny godnej zaufania sztucznej inteligencji (ALTAI)”, <<https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment>> dostęp: 14.12.2021 r.

² KE, projekt rozporządzenia w sprawie sztucznej inteligencji (COM (2021) 206 wersja ostateczna).

KI Bundesverband, „Position Paper on EU-Regulation of Artificial Intelligence [pol.: Stanowisko w sprawie unijnych regulacji w zakresie sztucznej inteligencji]”, <[\[content/uploads/2021/02/Final_Regulierung-komprimiert-1.pdf\]\(content/uploads/2021/02/Final_Regulierung-komprimiert-1.pdf\)> dostęp: 14.12.2021 r.](https://ki-verband.de/wp-</p>
</div>
<div data-bbox=)

⁴ Rada Europy, Komitet ad hoc ds. sztucznej inteligencji, „Studium wykonalności” (CAHAI (2020) 23).

⁵ Agencja Praw Podstawowych UE, Getting the future right [pol.: Zapewnienie dobrej przyszłości], <<https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights>>, dostęp: 14.12.2021 r.

⁶ Zob. KE (nr 2), Załącznik 4 do projektu rozporządzenia w sprawie sztucznej inteligencji, 2.

iii. wybór danych treningowych, walidacyjnych i testowych;

5. Proszę opisać stosowane metodologie i techniki szkoleniowe. Opis powinien obejmować informacje o pochodzeniu takich zbiorów danych, jak również ich zakresie i głównych cechach, sposobie pozyskania i selekcji danych, a także o procedurach etykietowania i metodologiach czyszczenia danych.⁷

iv. kontekst, w którym system jest wykorzystywany, w szczególności cele publiczne określone w obowiązującym prawie;

6. Jakie zadanie lub zadania administracyjne wykonuje system? Jaki jest cel jego funkcjonowania? Kto odpowiada za jego wdrożenie, a także nadzór nad nim oraz rozpatrywanie reklamacji?

v. wzajemne powiązania systemu z innymi systemami cyfrowymi wdrożonymi przez organ wdrażający lub inne organy publiczne;

7. Czy system współdziała z innymi systemami sprzętowymi bądź systemami oprogramowania? Jeśli tak, to w jaki sposób?

b) ocena działania, skuteczności i wydajności systemu w odniesieniu do celów publicznych określonych w obowiązującym prawie, w szczególności w zakresie tego, czy działanie systemu może być zakłócone przez dostarczenie niskiej jakości danych podczas jego stosowania.

8. W jaki sposób system pozwoli skuteczniej wykonać odpowiednie zadania administracyjne w porównaniu ze stanem aktualnym (np. zapewni szybsze przetwarzanie, zwiększoną dokładność, niższe koszty)?

9. Czy system oraz podejmowane przez niego decyzje będą możliwe do zaakceptowania przez społeczeństwo i osoby zainteresowane?

10. Czy wzięto pod uwagę ryzyko celowego lub innego niewłaściwego wykorzystania systemu? Czy

wprowadzono środki mające na celu złagodzenie lub uniknięcie skutków takiego działania?

c) ocena konkretnych i systemowego skutków zastosowania systemu;

Przy rozpatrywaniu poniższych pytań należy wziąć pod uwagę oddziaływanie bezpośrednie i pośrednie, jak również ich dotkliwość, czas trwania i odwracalność.⁸ Należy rozważyć wpływ systemu na:

i. podstawowe lub inne indywidualne prawa lub interesy, w szczególności prawo do prywatności i ochrony danych, prawo do niedyskryminacji oraz prawo do dobrej administracji;

11. Czy Państwa system został opracowany lub jest obsługiwany przy użyciu danych osobowych bądź jest trenowany z ich wykorzystaniem (w tym szczególnych kategorii danych osobowych)? Jeśli tak, to jakie wprowadzono zabezpieczenia gwarantujące przestrzeganie obowiązków w zakresie ochrony danych?⁹

12. Czy system może dyskryminować osoby ze względu na (lista niewyczerpująca): płeć biologiczną, tożsamość płciową, rasę, kolor skóry, pochodzenie etniczne lub społeczne, cechy genetyczne, język, religię lub przekonania, poglądy polityczne lub inne, przynależność do mniejszości narodowej, status materialny, miejsce urodzenia, niepełnosprawność, wiek lub orientację seksualną?¹⁰

13. Jeżeli system posiada ogólnodostępny interfejs — czy dokonano oceny tego, czy wspomniany interfejs uwzględnia zróżnicowane umiejętności informatyczne społeczeństwa i czy mogą z niego korzystać osoby o szczególnych potrzebach, a także niepełnosprawne lub zagrożone wykluczeniem?¹¹

14. Czy system zapewnia ochronę prawa do bycia wysłuchanym, a także zgodność z obowiązkiem uzasadnienia, prawem dostępu do akt i innymi elementami prawa do dobrej administracji, zgodnie z obowiązującymi przepisami?

⁷ KE (nr 2), Załącznik 4 do projektu rozporządzenia w sprawie sztucznej inteligencji, 2 (d).

⁸ Kryteria częściowo zaczerpnięte z Canadian Algorithmic Impact Assessment [pol.: *Kanadyjska Ocena Skutków Stosowania Algorytmów*].

⁹ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 6; Rada Europy, Komitet ad hoc ds. sztucznej inteligencji (nr 4), 35–37.

¹⁰ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 5; Rada Europy, Komitet ad hoc ds. sztucznej inteligencji (nr 4), 31–33.

¹¹ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 17.

15. Czy istnieje inne prawo podstawowe o szczególnym znaczeniu dla Państwa systemu?

ii. demokracja, dobrobyt społeczny i środowiskowy;

16. Czy system może mieć negatywny wpływ na procesy wyborcze, dyskurs publiczny i inne równie ważne aspekty demokracji i czy podjęto kroki w celu zminimalizowania go?¹²

17. Czy system kontroluje lub wpływa na krytyczną infrastrukturę publiczną (np. transport, komunikację lub sektor energetyczny)?¹³

18. Czy występują dowolne inne skutki w zakresie dobrobytu społecznego i środowiskowego (np. edukacja, umiejętności informatyczne, dysproporcje regionalne, zużycie energii lub emisja gazów cieplarnianych), które są szczególnie istotne w odniesieniu do Państwa systemu?

iii. sam organ administracyjny, w szczególności szacowany odbiór systemu i jego decyzji przez pracowników, ryzyko nadmiernego lub niedostatecznego polegania przez pracowników na systemie, poziom umiejętności informatycznych oraz konkretnych umiejętności technicznych w ramach organu;

19. Czy system wpływa na warunki pracy w instytucji wdrażającej?¹⁴

20. Czy upewniono się, że personel rozumie działanie, możliwości i ograniczenia systemu tak, aby uniknąć nadmiernego lub niedostatecznego polegania na nim przez pracowników?

d) ocena środków podjętych w celu zapewnienia:

i. maksymalizacji korzyści, jakie można osiągnąć dzięki wdrożeniu systemu, w odniesieniu do celów publicznych określonych w obowiązującym prawie;

21. Czy rozważono, jak zmaksymalizować korzyści dla społeczeństwa wynikające z wdrożenia systemu?

ii. minimalizacji zidentyfikowanego ryzyka i złagodzenia ewentualnych negatywnych skutków;

22. Czy wdrożono mechanizmy wykrywania ryzyka i reagowania na nie, przy uwzględnieniu m.in. minimalizacji potencjalnych zagrożeń systemowych? Czy ustanowiono system zarządzania jakością lub system zarządzania ryzykiem?¹⁵

23. Jeśli nie zostało to wspomniane powyżej lub omówione w poprzednich pytaniach: czy wdrożono środki mające na celu zminimalizowanie zidentyfikowanego ryzyka lub złagodzenie ewentualnych negatywnych skutków?

iii. sprawczości człowieka oraz jego nadzoru i kontroli nad systemem;

24. Czy osoby zainteresowane są należycie informowane, że wchodzi w interakcję z algorytmicznym systemem decyzyjnym?¹⁶

25. Czy osoby zainteresowane mają do dyspozycji alternatywę wobec korzystania z systemu lub poddania się jego decyzji?

26. Jakie środki podjęto, aby zapewnić, że system może być skutecznie kontrolowany lub nadzorowany przez ludzi? Czy do podjęcia decyzji pracownicy mogą użyć środków innych niż sam system?

iv. wysokiej jakości danych;

27. Czy zastosowano środki zapewniające, że dane wykorzystywane w systemie mają wysoką jakość oraz są aktualne, kompletne i reprezentatywne dla środowiska, w którym system zostanie wdrożony?

v. dokładności we wszystkich grupach, a także precyzji i wrażliwości;

¹² Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 20; Rada Europy, Komitet ad hoc ds. sztucznej inteligencji (nr 4), 39–41.

¹³ KE (nr 2), Załącznik III do projektu rozporządzenia w sprawie sztucznej inteligencji.

¹⁴ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 20.

¹⁵ KE (nr 2), art. 9 i 17 projektu rozporządzenia w sprawie sztucznej inteligencji.

¹⁶ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 7.

28. Proszę opisać środki zapewniające odpowiedni poziom dokładności,¹⁷ precyzji¹⁸ i wrażliwości^{19,20} systemu, która pozwala uniknąć negatywnych konsekwencji.

²¹

vi. solidności i bezpieczeństwa technicznego, odporności na ataki, bezpieczeństwa danych, planów awaryjnych, niezawodności, a także powtarzalności decyzji;

29. Czy zastosowano wystarczające zabezpieczenia przed cyberatakami, niewłaściwym użyciem, manipulacją danymi, szkodliwym lub nieodpowiednim wykorzystaniem, usterekami technicznymi, wadami, awariami, atakami lub zagrożeniami środowiskowymi?²¹

30. Czy zdefiniowano sprawdzone plany awaryjne na wypadek błędów systemowych, usterek lub niespójności, bez względu na ich pochodzenie (zewnętrzne lub wewnętrzne), oraz czy wprowadzono procedury zarządzania umożliwiające ich uruchamianie?²²

31. Czy wdrożono środki pozwalające ocenić i zapewnić niezawodność oraz odtwarzalność systemu?²³

vii. przejrzystości systemu i możliwość wyjaśnienia jego decyzji;

32. W jaki sposób będą Państwo informować zainteresowane osoby i społeczeństwo o istnieniu i funkcjonowaniu systemu?²⁴

33. Czy są Państwo w stanie wyjaśnić podejmowane przez system decyzje osobom, których one dotyczą?²⁵

¹⁷Dokładność oznacza liczbę poprawnie przewidywanych punktów danych spośród wszystkich punktów danych, tzn. liczbę wyników prawdziwie dodatnich i wyników prawdziwie ujemnych podzieloną przez liczbę wyników prawdziwie dodatnich, prawdziwie ujemnych, fałszywie dodatnich oraz fałszywie ujemnych; <<https://deepai.org/machine-learning-glossary-and-terms/accuracy-error-rate>> dostęp: 14.12.2021 r.

¹⁸ Odsetek istotnych instancji wśród wszystkich wyszukanych instancji, tj. liczba wyników prawdziwie dodatnich podzielona przez sumę wyników prawdziwie i fałszywie dodatnich, <<https://deepai.org/machine-learning-glossary-and-terms/precision-and-recall>> dostęp: 14.12.2021 r.

¹⁹ Definiowana jako odsetek wyszukanych instancji wśród wszystkich istotnych instancji, tj. liczba wyników prawdziwie dodatnich podzielona przez sumę wyników prawdziwie i fałszywie ujemnych, <<https://deepai.org/machine-learning-glossary-and-terms/precision-and-recall>> dostęp: 14.12.2021 r.

viii. identyfikowalności umożliwiającej monitorowanie działania systemu;

34. Czy zastosowano środki zapewniające identyfikowalność systemu podczas całego cyklu jego życia (np. rejestrowanie procesów i wyników systemu)?²⁶

ix. odpowiedzialności, w szczególności w zakresie nadzoru oraz możliwości audytu, jasnego podziału obowiązków, samokontroli, benchmarkingu oraz możliwości zadośćuczynienia za szkody lub krzywdy spowodowane przez system;

35. Czy ustanowiono mechanizmy ułatwiające audyt systemu (np. dokumentację procesu rozwoju, pozyskiwanie danych treningowych i skarg dotyczących negatywnych skutków oraz rejestrowanie procesów w systemie)?²⁷

36. Czy określono jasny zakres odpowiedzialności za każdy etap funkcjonowania systemu (np. rozwój, wdrożenie, użytkowanie, nadzór, rozpatrywanie skarg i usuwanie błędów)?

e) o ile system nie jest określony jako „zawsze obarczony wysokim ryzykiem” w Załączniku 1 — końcowe określenie poziomu ryzyka;

f) ogólna ocena konieczności i proporcjonalności operacji przetwarzania w stosunku do celów, w szczególności kompromisów pomiędzy różnymi czynnikami określonymi w niniejszym artykule oraz tego, czy istnieją sensowne alternatywy dla przewidywanego projektu;

g) oświadczenie o legalności korzystania z systemu w świetle obowiązującego prawa, w szczególności prawa o ochronie danych, prawa

²⁰ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 10.

²¹ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 10.

²² Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 11.

²³ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 11.

²⁴ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 15.

²⁵ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 15.

²⁶ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 14.

²⁷ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 21.

o postępowaniu administracyjnym i obowiązujących przepisów sektorowych, wraz z uzasadnieniem;

Załącznik 4B: Kwestionariusz do sprawozdania z oceny skutków (wersja rozszerzona)

Komentarz:

Zawarte poniżej pytania, a także spora część sformułowań, opierają się na Liście kontrolnej oceny godnej zaufania sztucznej inteligencji (ALTAI) opracowanej przez Grupę Ekspertów Wysokiego Szczebla.²⁸ Zespół projektowy EIP dodał lub zmodyfikował kilka pytań. Niektóre z tych zmian inspirowane są projektem rozporządzenia Komisji Europejskiej w sprawie sztucznej inteligencji,²⁹ stanowiskiem niemieckiego stowarzyszenia „KI Bundesverband” w sprawie rzeczonego rozporządzenia UE,³⁰ Studium Wykonalności Komitetu ad hoc ds. sztucznej inteligencji Rady Europy (CAHAI),³¹ jak również przez sprawozdanie Europejskiej Agencji Praw Podstawowych pt. „Getting the Future Right”.³²

Uwagi ogólne

Udzielając odpowiedzi należy podawać merytoryczne wyjaśnienia i unikać podsumowań zdawkowych, jednowyrazowych. Jeśli pytanie nie wydaje się odpowiednie dla danego systemu, należy wyjaśnić przyczynę.

We wszystkich poniższych sekcjach należy rozważyć:

- Czynności szkoleniowe mające na celu zaznajomienie pracowników korzystających z systemu z istotnymi kwestiami technicznymi, etycznymi i prawnymi;
- Bieżące monitorowanie podczas użytkowania systemu;
- Odpowiednie informowanie/komunikowanie się z zainteresowanymi osobami, zwłaszcza gdy wymagana jest ich współpraca;
- Mechanizmy zgłaszania przez zainteresowane osoby wszelkich napotkanych problemów;

- Mechanizmy rozwiązywania problemów, które mogą pojawić się podczas korzystania z systemu. Struktura kwestionariusza opiera się na art. 6.

a) opis przeznaczenia i działania systemu, w szczególności w zakresie:

i. rozwoju systemu, w szczególności jego algorytmów;

1. Kto zaprojektował system i w jaki sposób został on opracowany?³³ Od kogo zakupiono system?

1.1 W jaki sposób wybrano projektanta lub producenta systemu? Na czym polegała ich przewaga nad konkurencją?

1.2 Czy system wprowadzono na rynek lub wdrożono do użytku także w innym miejscu?

1.3 Jakie metody zastosowano podczas tworzenia systemu i jakie kroki podjęto w ramach tego procesu? Czy strony trzecie dostarczyły wstępnie przetrenowane systemy lub narzędzia? Jeśli tak, to czy dokonano ich modyfikacji?³⁴

1.4 Jakie zasoby obliczeniowe wykorzystano do opracowania, trenowania, testowania i walidacji systemu?

2. Czy istnieją normy zharmonizowane opublikowane w Dzienniku Urzędowym UE lub specyfikacje techniczne, które mają (częściowo lub w całości) zastosowanie do posiadanego systemu?

ii. charakter i parametry techniczne systemu;

3. Proszę opisać, w miarę możliwości w sposób nietechniczny, technologię lub technologie, których zamierzają Państwo użyć.

3.1. Opis powinien obejmować³⁶: (1) datę i wersję systemu; (2) opis sprzętu, na którym system ma działać; (3) w przypadku gdy system stanowi komponent produktów — fotografie lub ilustracje przedstawiające cechy zewnętrzne, oznakowanie i układ wewnętrzny takich produktów.

3.2. Z technicznego punktu widzenia, jakie są właściwości systemu? Jaki jest sposób jego

²⁸ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1).

²⁹ KE, projekt rozporządzenia w sprawie sztucznej inteligencji (COM (2021) 206 wersja ostateczna).

³⁰ KI Bundesverband (nr 3).

³¹ Rada Europy, Komitet ad hoc ds. sztucznej inteligencji (nr 4).

³² Agencja Praw Podstawowych UE (nr 5).

³³ Zob. KE (nr 2), Załącznik 4 do projektu rozporządzenia w sprawie sztucznej inteligencji, 2.

³⁴ Zob. KE (nr 2), Załącznik 4 do projektu rozporządzenia w sprawie sztucznej inteligencji, 2 (a). ³⁶ Zob. KE (nr 2), Załącznik 4 do projektu rozporządzenia w sprawie sztucznej inteligencji (c–f).

działania? Należy opisać architekturę systemu i wyjaśnić, w jaki sposób komponenty oprogramowania opierają się na sobie lub wzajemnie na sobie wpływają oraz jak integrują się w całość procesu przetwarzania.

Zob. np.³⁵

3.2.1 Czy jest oparty na regułach i stosuje jasne reguły „if-then” („jeżeli X, to Y”)?

3.2.2 Czy w celu znalezienia korelacji system opiera się na bardziej tradycyjnych metodach statystycznych, np. analizie regresji?

3.2.3 Czy stosuje się w nim podejście oparte na logice czy oparte na wiedzy?

3.2.4 Czy jest to algorytm samouczący się/uczący się maszynowo, wykorzystujący np. uczenie nadzorowane, nienadzorowane lub uczenie przez wzmacnianie?

3.2.5 Czy model jest trenowany tylko raz, czy też jest stale uaktualniany?

3.2.6 Czy stosuje uczenie głębokie?

3.3. Jaki jest stopień automatyzacji systemu?³⁶ Czy system podejmuje ostateczne decyzje, czy jedynie przekazuje zalecenia człowiekowi?

3.4. Jakie są specyfikacje projektowe? Jaka jest ogólna logika systemu i jego algorytmów?

3.5. Jakie były kluczowe decyzje projektowe, w tym uzasadnienie i przyjęte założenia (np. dotyczące osób, w stosunku do których system ma być używany)?

3.6. Jakie były główne decyzje w zakresie klasyfikacji?

3.7. Pod jakim kątem docelowo ma być zoptymalizowany wybrany system?

3.8. Jakie jest znaczenie poszczególnych parametrów?

3.9. Jakie były kluczowe kompromisy, na które zdecydowano się w zakresie przyjętych rozwiązań technicznych?

4. W stosownych przypadkach należy także podać opis przewidywanych lub planowanych zmian w systemie i jego działaniu.

iii. wybór danych treningowych, walidacyjnych i testowych;

5. Proszę opisać stosowane metodologie i techniki szkoleniowe. Opis powinien obejmować informacje o pochodzeniu takich zbiorów danych, jak również ich zakresie i głównych cechach, sposobie pozyskania i selekcji danych, a także o procedurach etykietowania i metodologiach czyszczenia danych.³⁷

W szczególności należy opisać, jakie dane wykorzystano do trenowania systemu.

5.1 Czy zbiór danych jest statyczny (tzn. ustalony i jasno określony), czy dynamiczny (tzn. na bieżąco zasilany nowymi danymi)?

5.2 Czy dane i proces ich generowania są jawne lub znajdują się pod kontrolą?

5.3 Czy system trenowany jest na danych osobowych, czy też na danych neutralnych?

iv. kontekst, w którym system jest wykorzystywany, w szczególności cele publiczne określone w obowiązującym prawie;

6. Jakie zadanie lub zadania administracyjne wykonuje system? Jaki jest cel jego funkcjonowania? Kto odpowiada za jego wdrożenie, a także nadzór nad nim oraz rozpatrywanie reklamacji?

6.1 Dlaczego zdecydowali się Państwo na zastosowanie tego systemu?

6.2 Czy Państwa organ publiczny ma już doświadczenie w wykorzystaniu podobnych systemów (tj. podobnych technologii)?

v. wzajemne powiązania systemu z innymi systemami cyfrowymi wdrożonymi przez organ wdrażający lub inne organy publiczne;

7. Czy system współdziała z innymi systemami sprzętowymi bądź systemami oprogramowania? Jeśli tak, to w jaki sposób?

³⁵ Agencja Praw Podstawowych UE (nr 5), 27; KI Bundesverband, Position Paper on EU-Regulation of Artificial Intelligence [pol.: Stanowisko w sprawie unijnych regulacji w zakresie sztucznej inteligencji], 8.

³⁶ Agencja Praw Podstawowych UE (nr 5) 27.

³⁷ KE (nr 2), Załącznik 4 do projektu rozporządzenia w sprawie sztucznej inteligencji, 2 (d).

b) ocena działania, skuteczności i wydajności systemu w odniesieniu do celów publicznych określonych w obowiązującym prawie, w szczególności w zakresie tego, czy działanie systemu może być zakłócone przez dostarczenie niskiej jakości danych podczas jego stosowania.

8. W jaki sposób system pozwoli skuteczniej wykonać odpowiednie zadania administracyjne w porównaniu ze stanem aktualnym (np. zapewni szybsze przetwarzanie, zwiększoną dokładność, niższe koszty)?

9. Czy system oraz podejmowane przez niego decyzje będą możliwe do zaakceptowania przez społeczeństwo i osoby zainteresowane?

9.1 Czy Państwa system opiera się na inicjatywie, współpracy lub zaufaniu osób objętych jego działaniami? Jeśli tak, to jak zapewniają Państwo współpracę z ich strony? Czy wprowadzono zachęty do korzystania z systemu?

10. Czy wzięto pod uwagę ryzyko celowego lub innego niewłaściwego wykorzystania systemu? Czy

wprowadzono środki mające na celu złagodzenie lub uniknięcie skutków takiego działania?

c) ocena konkretnych i systemowego skutków zastosowania systemu;

Przy rozpatrywaniu poniższych pytań należy wziąć pod uwagę oddziaływanie bezpośrednie i pośrednie, jak również ich dotkliwość, czas trwania i odwracalność.³⁸ Należy rozważyć wpływu systemu na:

i. podstawowe lub inne indywidualne prawa lub interesy, w szczególności prawo do prywatności i ochrony danych, prawo do niedyskryminacji oraz prawo do dobrej administracji;

11. Czy Państwa system został opracowany lub jest obsługiwany przy użyciu danych osobowych bądź jest trenowany z ich wykorzystaniem (w tym szczególnych kategorii danych osobowych)? Jeśli tak, to jakie wprowadzono zabezpieczenia

gwarantujące przestrzeganie obowiązków w zakresie ochrony danych?³⁹

11.1 Czy rozważono wpływ nieosobowych danych treningowych lub innych przetwarzanych danych nieosobowych na interesy osób prawnych w zakresie prywatności lub tajemnic?⁴⁰

11.2 W jaki sposób Państwa system zachowuje zgodność z koncepcją domyślnej ochrony danych [*ang.*: *privacy by design*]?⁴¹

12. Czy system może dyskryminować osoby ze względu na (lista niewyczerpująca): płeć biologiczną, tożsamość płciową, rasę, kolor skóry, pochodzenie etniczne lub społeczne, cechy genetyczne, język, religię lub przekonania, poglądy polityczne lub inne, przynależność do mniejszości narodowej, status materialny, miejsce urodzenia, niepełnosprawność, wiek lub orientację seksualną?⁴²

12.1 Czy rozważono różnorodność i reprezentatywność osób, których dotyczą dane?⁴³

12.2 Czy przeprowadzono testy pod kątem określonych grup docelowych lub problematycznych przypadków użycia rozwiązania?⁴⁴

12.3 Czy ustanowili Państwo definicję uczciwości? Czy Państwa definicja uczciwości jest powszechnie stosowana i wdrażana na każdym etapie procesu tworzenia systemu?

12.4 Czy wprowadzili Państwo w swoim systemie mechanizmy gwarantujące uczciwość?

13. Jeżeli system posiada ogólnodostępny interfejs — czy dokonano oceny tego, czy wspomniany interfejs uwzględnia zróżnicowane umiejętności informatyczne społeczeństwa i czy mogą z niego korzystać osoby o szczególnych potrzebach, a także niepełnosprawne lub zagrożone wykluczeniem?⁴⁵

13.1 Czy na etapie planowania i tworzenia systemu konsultowano się z zainteresowanymi

³⁸ Kryteria częściowo zaczerpnięte z Canadian Algorithmic Impact Assessment [*pol.*: *Kanadyjska Ocena Skutków Stosowania Algorytmów*].

³⁹ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 6; Rada Europy, Komitet ad hoc ds. sztucznej inteligencji (nr 4), 35–37.

⁴⁰ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 13.

⁴¹ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 12.

⁴² Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 5; Rada Europy, Komitet ad hoc ds. sztucznej inteligencji (nr 4), 31–33.

⁴³ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 16.

⁴⁴ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 16.

⁴⁵ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 17.

osobami, które wymagają technologii ułatwiającej funkcjonowanie, lub też zaangażowano takie osoby w ten proces?⁴⁶

13.2 Czy upewniono się, że uniwersalne zasady projektowania⁴⁷ i normy w zakresie dostępności⁴⁸ zostały uwzględnione na każdym etapie procesu planowania i rozwoju (jeśli dotyczy)?⁴⁹

14. Czy system zapewnia ochronę prawa do bycia wysłuchanym, a także zgodność z obowiązkiem uzasadnienia, prawem dostępu do akt i innymi elementami prawa do dobrej administracji, zgodnie z obowiązującymi przepisami?

15. Czy istnieje inne prawo podstawowe o szczególnym znaczeniu dla Państwa systemu?

ii. demokracja, dobrobyt społeczny i środowiskowy;

16. Czy system może mieć negatywny wpływ na procesy wyborcze, dyskurs publiczny i inne równie ważne aspekty demokracji i czy podjęto kroki w celu zminimalizowania go?⁵⁰

17. Czy system kontroluje lub wpływa na krytyczną infrastrukturę publiczną (np. transport, komunikację lub sektor energetyczny)?⁵¹

18. Czy występują dowolne inne skutki w zakresie dobrobytu społecznego i środowiskowego (np. edukacja, umiejętności informatyczne, dysproporcje regionalne, zużycie energii lub emisja gazów cieplarnianych), które są szczególnie istotne w odniesieniu do Państwa systemu?

iii. sam organ administracyjny, w szczególności szacowany odbiór systemu i jego decyzji przez pracowników, ryzyko nadmiernego lub niedostatecznego polegania przez pracowników na systemie, poziom umiejętności informatycznych oraz

konkretnych umiejętności technicznych w ramach organu;

19. Czy system wpływa na warunki pracy w instytucji wdrażającej?⁵²

19.1 Czy system może stwarzać ryzyko utraty umiejętności przez pracowników [*ang.: de-skilling*]? Czy podjęto działania w celu przeciwdziałania ryzyku utraty umiejętności?⁵³

19.2 Czy system wymaga nowych umiejętności (informatycznych) lub promuje ich nabycie? Czy zapewniają Państwo możliwości szkoleniowe i materiały do ponownego szkolenia oraz podnoszenia umiejętności?⁵⁴

19.3 Czy system korzysta z danych objętych klauzulą tajności? Jakie specjalne środki wdrożono w celu ochrony tych danych przed nieuprawnionym dostępem przez pracowników?

19.4 Czy zastosowanie systemu skutkuje zmniejszeniem liczby pracowników zatrudnionych w Państwa agencji administracyjnej, czy też wymaga specjalnych umiejętności, których obecni pracownicy nie posiadają?

19.5 Czy przygotowanie do wdrożenia systemu w Państwa organizacji obejmowało poinformowanie pracowników lub ich przedstawicieli o tym fakcie oraz konsultacje z nimi w tym zakresie?⁵⁵

20. Czy upewniono się, że personel rozumie działanie, możliwości i ograniczenia systemu tak, aby uniknąć nadmiernego lub niedostatecznego polegania na nim przez pracowników?

d) ocena środków podjętych w celu zapewnienia:

i. maksymalizacji korzyści, jakie można osiągnąć dzięki wdrożeniu systemu, w odniesieniu do celów publicznych określonych w obowiązującym prawie;

⁴⁶ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 17.

⁴⁷ <www.cen.eu/news/brief-news/Pages/NEWS-2019-014.aspx> Dostęp: 14.12.2021 r.

⁴⁸ <www.iso.org/standard/58625.html; <www.iso.org/standard/33987.html> dostęp: 14.12.2021 r.; <www.iso.org/obp/ui/#iso:std:iso:9241:171:ed-1:v1:en> dostęp: 14.12.2021 r.; <<http://mandate376.standards.eu/standard>> dostęp: 14.12.2021 r.

⁴⁹ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 17.

⁵⁰ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 20; Komitet ad hoc ds. sztucznej inteligencji (2020) 23, 39–41.

⁵¹ KE (nr 2), Załącznik III do projektu rozporządzenia w sprawie sztucznej inteligencji.

⁵² Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 20.

⁵³ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 20.

⁵⁴ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 20.

⁵⁵ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 20.

21. Czy rozważono, jak zmaksymalizować korzyści dla społeczeństwa wynikające z wdrożenia systemu?

21.1 Czy rozważono możliwości wypełnienia celu administracyjnego w innowacyjny sposób poprzez wykorzystanie potencjału systemu?

ii. minimalizacji zidentyfikowanego ryzyka i złagodzenia ewentualnych negatywnych skutków;

22. Czy wdrożono mechanizmy wykrywania ryzyka i reagowania na nie, przy uwzględnieniu m.in. minimalizacji potencjalnych zagrożeń systemowych? Czy ustanowiono system zarządzania jakością lub system zarządzania ryzykiem?⁵⁶

23. Jeśli nie zostało to wspomniane powyżej lub omówione w poprzednich pytaniach: czy wdrożono środki mające na celu zminimalizowanie zidentyfikowanego ryzyka lub złagodzenie ewentualnych negatywnych skutków?

iii. sprawczości człowieka oraz jego nadzoru i kontroli nad systemem;

24. Czy osoby zainteresowane są należycie informowane, że wchodzi w interakcję z algorytmicznym systemem decyzyjnym?⁵⁷

24.1 Czy system może manipulować działaniami lub reakcjami osób zainteresowanych, np. poprzez „popychanie” do zrobienia czegoś [ang.: nudging]?

25. Czy osoby zainteresowane mają do dyspozycji alternatywę wobec korzystania z systemu lub poddania się jego decyzji?

26. Jakie środki podjęto, aby zapewnić, że system może być skutecznie kontrolowany lub nadzorowany przez ludzi? Czy do podjęcia decyzji pracownicy mogą użyć środków innych niż sam system?

26.1 Czy system jest kontrolowany lub nadzorowany na zasadzie „Human-in-the-Loop”, „Human-on-the-Loop” bądź „Human-in-Command”?⁵⁸

26.2 Czy wymóg nadzoru ze strony człowieka jest już wbudowany w system, czy też konieczne jest podjęcie specjalnych działań organizacyjnych z Państwa strony?⁵⁹

26.3 W szczególności, czy osoby nadzorujące system otrzymały specjalnie przeszkolenie w zakresie sprawowania nadzoru?⁶⁰

26.4 Czy wspomniane przeszkolenie zapewnia, że takie osoby:

a. rozumieją możliwości i ograniczenia systemu?

b. rozumieją ryzyko tzw. „automation bias” — nadmiernego polegania na wyniku działania systemu?

c. potrafią poprawnie zinterpretować dane wyjściowe systemu?

d. otrzymały kryteria lub instrukcje odnośnie tego, kiedy nie należy korzystać z systemu lub polegać na nim?

26.5 Czy istnieje „przycisk stop” lub procedura umożliwiająca bezpieczne przerwanie operacji w razie potrzeby?

26.6 Czy wdrożono szczególne środki nadzoru i kontroli w celu uwzględnienia samouczącej się lub autonomicznej natury systemu?⁶¹

iv. wysokiej jakości danych;

27. Czy zastosowano środki zapewniające, że dane wykorzystywane w systemie mają wysoką jakość oraz są aktualne, kompletne i reprezentatywne dla środowiska, w którym system zostanie wdrożony?⁶²

27.1 Czy zestawy danych treningowych, walidacyjnych i testowych uwzględniają — w zakresie, w jakim wymaga tego przeznaczenie systemu — specyficzne środowisko geograficzne, behawioralne lub funkcjonalne, w którym system jest używany?⁶³

27.2 Czy istnieje ryzyko dużego rozproszenia danych wraz z ekstremalnymi wartościami skrajnymi, które mogą zaburzyć

⁵⁶ KE (nr 2), art. 14 i 17 projektu rozporządzenia w sprawie sztucznej inteligencji.

⁵⁷ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 7.

⁵⁸ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 8.

⁵⁹ KE (nr 2), art. 14 ust. 1 i 3 projektu rozporządzenia w sprawie sztucznej inteligencji.

⁶⁰ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 8.

⁶¹ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 8.

⁶² Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 10.

⁶³ KE (nr 2), art. 10 ust. 4 projektu rozporządzenia w sprawie sztucznej inteligencji.

działanie algorytmu? Jeśli tak, to jakie środki podjęto w celu zapobieżenia temu ryzyku?

27.3 Czy ustanowiono odpowiednie praktyki w zakresie zarządzania danymi, takie jak: wybór projektu, gromadzenie danych, operacje przetwarzania danych (np. adnotacje, etykietowanie, czyszczenie, wzbogacanie i agregacja), formułowanie odpowiednich założeń (w szczególności w zakresie tego, jakie informacje mają mierzyć i reprezentować konkretne dane), ocena dostępności, ilości i przydatności zbiorów danych, które są potrzebne, badanie ewentualnych błędów systemowych, identyfikacja ewentualnych braków lub niedociągnięć w danych oraz sposoby ich uzupełnienia?^{64,65}

v. dokładności we wszystkich grupach, a także precyzji i wrażliwości;

28. Proszę opisać środki zapewniające odpowiedni poziom dokładności,⁶⁶ precyzji i wrażliwości⁶⁷ systemu, pozwalający uniknąć negatywnych konsekwencji.⁶⁸

28.1 Czy rozważono już, czy działanie systemu może unieważnić dane lub założenia, na których został on przetestowany, a także sposób, w jaki może to doprowadzić do niepożądanych skutków?⁶⁹

28.2 Czy wdrożono procedury zapewniające odpowiednie informowanie o poziomie dokładności i precyzji systemu, jakiego mogą oczekiwać osoby zainteresowane?⁷⁰

28.3 Czy zawarli Państwo informacje o poziomie dokładności oraz odpowiednie

wskaźniki w instrukcji obsługi lub udostępnił je w inny sposób?⁷⁴

vi. solidności i bezpieczeństwa technicznego, odporności na ataki, bezpieczeństwa danych, planów awaryjnych, niezawodności, a także powtarzalności decyzji;

29. Czy zastosowano wystarczające zabezpieczenia przed cyberatakami, niewłaściwym użyciem, manipulacją danymi, szkodliwym lub nieodpowiednim wykorzystaniem, usterkami technicznymi, wadami, awariami, atakami lub zagrożeniami środowiskowymi?⁷¹

29.1 Czy system może mieć niekorzystne, istotne lub szkodliwe skutki (np. dla bezpieczeństwa ludzi lub społeczeństwa) w przypadku wystąpienia tego typu zagrożeń?

29.2 Czy system jest zgodny z ogólnymi lub szczegółowymi normami bezpieczeństwa cybernetycznego? Czy posiada on certyfikat bezpieczeństwa cybernetycznego (np. system certyfikacji stworzony na mocy ustawy o bezpieczeństwie cybernetycznym w Europie⁷²)?⁷³

29.3 Czy wdrożono odpowiednie do zagrożeń i okoliczności środki zapewniające integralność, niezawodność i ogólne zabezpieczenie systemu przed potencjalnymi atakami w całym jego cyklu życia?⁷⁴ Czy wspomniane środki zostały poddane testom penetracyjnym?

⁶⁴ Por. KE (nr 2), art. 10 ust. 2 projektu rozporządzenia w sprawie sztucznej inteligencji.

⁶⁵ Dokładność oznacza liczbę poprawnie przewidywanych punktów danych spośród wszystkich punktów danych, tzn. liczbę wyników prawdziwie dodatnich i wyników prawdziwie ujemnych podzieloną przez liczbę wyników prawdziwie dodatnich, prawdziwie ujemnych, fałszywie dodatnich oraz fałszywie ujemnych; <<https://deepai.org/machine-learning-glossary-and-terms/accuracy-error-rate>> dostęp: 14.12.2021 r.

⁶⁶ Odsetek istotnych instancji wśród wszystkich wyszukanych instancji, tj. liczba wyników prawdziwie dodatnich podzielona przez sumę wyników prawdziwie i fałszywie dodatnich, <<https://deepai.org/machine-learning-glossary-and-terms/precision-and-recall>> dostęp: 14.12.2021 r.

⁶⁷ Definiowana jako odsetek wyszukanych instancji wśród wszystkich istotnych instancji, tj. liczba wyników prawdziwie dodatnich podzielona przez sumę wyników prawdziwie i fałszywie ujemnych, <<https://deepai.org/machine-learning-glossary-and-terms/precision-and-recall>> dostęp: 14.12.2021 r.

⁶⁸ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 10.

⁶⁹ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 10.

⁷⁰ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 8.

⁷¹ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 10.

⁷² Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych.

⁷³ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 9.

⁷⁴ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 9.

- 29.4 Jaki jest przewidywany okres dostarczania aktualizacji zabezpieczeń dla systemu?⁷⁵
30. Czy zdefiniowano sprawdzone plany awaryjne na wypadek błędów systemowych, usterek lub niespójności, bez względu na ich pochodzenie (zewnętrzne lub wewnętrzne), oraz czy wprowadzono procedury zarządzania umożliwiające ich uruchamianie?⁷⁶
31. Czy wdrożono środki pozwalające ocenić i zapewnić niezawodność oraz odtwarzalność systemu?⁷⁷
- 31.1 Czy sprawdzono, czy w celu zapewnienia odtwarzalności należy brać pod uwagę określone konteksty lub warunki?
- 31.2 Czy dokonano oceny zależności decyzji podejmowanych przez system od jego stabilnej i niezawodnej pracy?
- 31.3 Czy dopasowano wymagania dotyczące niezawodności lub testowania do odpowiednich poziomów stabilności i niezawodności systemu?
- vii. przejrzystości systemu i możliwość wyjaśnienia jego decyzji;**
32. W jaki sposób będą Państwo informować zainteresowane osoby i społeczeństwo o istnieniu i funkcjonowaniu systemu?⁷⁸
33. Czy są Państwo w stanie wyjaśnić podejmowane przez system decyzje osobom, których one dotyczą?⁷⁹
- 33.1 Czy na bieżąco przeprowadzają Państwo ankiety wśród osób zainteresowanych w celu potwierdzenia, że rozumieją one decyzje podejmowane przez system?⁸⁰
- viii. identyfikowalności umożliwiającej monitorowanie działania systemu;**
34. Czy zastosowano środki zapewniające identyfikowalność systemu podczas całego cyklu jego życia (np. rejestrowanie procesów i wyników systemu)?⁸¹
- 34.1 Czy można prześledzić, jakie algorytmy, reguły lub dane zostały wykorzystane przez system do podjęcia określonej decyzji lub wydania konkretnego zalecenia?⁸²
- 34.2 Czy wdrożono środki pozwalające na ciągłą ocenę jakości wyników systemu?⁸³
- 34.3 Czy wprowadzono odpowiednie praktyki rejestrowania decyzji lub zaleceń systemu? Czy takie rejestry przechowywane są przez odpowiedni okres czasu?⁸⁴
- ix. odpowiedzialności, w szczególności w zakresie nadzoru oraz możliwości audytu, jasnego podziału obowiązków, samokontroli, benchmarkingu oraz możliwości zadośćuczynienia za szkody lub krzywdy spowodowane przez system;**
35. Czy ustanowiono mechanizmy ułatwiające audyt systemu (np. dokumentację procesu rozwoju, pozyskiwanie danych treningowych i skarg dotyczących negatywnych skutków oraz rejestrowanie procesów w systemie)?⁸⁵
36. Czy określono jasny zakres odpowiedzialności za każdy etap funkcjonowania systemu (np. rozwój, wdrożenie, użytkowanie, nadzór, rozpatrywanie skarg i usuwanie błędów)?
- 36.1 Czy rozważono ustanowienie rady ds. przeglądu etyki SI lub podobnego mechanizmu w celu omówienia ogólnej odpowiedzialności i praktyk etycznych, w tym potencjalnych niejasności?⁸⁶

⁷⁵ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 9.

⁷⁶ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 11.

⁷⁷ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 11.

⁷⁸ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 15.

⁷⁹ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 15.

⁸⁰ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 15.

⁸¹ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 14.

⁸² Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 14.

⁸³ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 14.

⁸⁴ KE (nr 2), art. 20 i art. 29 ust. 5 projektu rozporządzenia w sprawie sztucznej inteligencji.

⁸⁵ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 21.

⁸⁶ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 22.

36.2 Czy rozważono wprowadzenie procedur benchmarkingu w celu porównania wydajności i ryzyka w przypadku wyników pracy systemu z tymi, które występują w przypadku decyzji podejmowanych przez człowieka w tych samych obszarach?

36.3 Czy ustanowiono procedurę umożliwiającą stronom trzecim (np. dostawcom, osobom zainteresowanym, dystrybutorom/sprzedawcom, pracownikom lub organizacjom społeczeństwa obywatelskiego) zgłaszanie potencjalnych słabych punktów, zagrożeń lub błędów w systemie? Czy proces ten sprzyja aktualizowaniu procesu zarządzania ryzykiem?⁸⁷

36.4 Czy w przypadku systemów, które mogą mieć negatywny wpływ na jednostki, wprowadzono mechanizmy samokontroli (w szczególności mechanizmy zadośćuczynienia wbudowane w fazie projektowania (*ang. redress by design*))?⁸⁸

e) o ile system nie jest określony jako „zawsze obciążony wysokim ryzykiem” w Załączniku 1 — końcowe określenie poziomu ryzyka;

37.1 Jeśli system nie został wymieniony w Załączniku 1: Czy po szczegółowym wypełnieniu pytań zawartych w niniejszym załączniku zdecydowałoby się Państwo na zmianę swojej oceny ryzyka zgodnie z Załącznikiem 3? W szczególności, czy teraz uważają Państwo, że Państwa system stwarza wysokie ryzyko?

37.2 Jeżeli system został wyszczególniony w Załączniku 1 jako „obciążony istotnym ryzykiem”: Prosimy o wypełnienie kwestionariusza w Załączniku 3 z wykorzystaniem informacji uzyskanych podczas oceny skutków. Czy według kwestionariusza system obciążony jest wysokim ryzykiem?

f) ogólna ocena konieczności i proporcjonalności operacji przetwarzania w stosunku do celów, w szczególności kompromisów pomiędzy różnymi czynnikami określonymi w niniejszym artykule oraz tego, czy istnieją sensowne alternatywy dla przewidywanego projektu;

38.1 Jakie są alternatywy dla korzystania z tego systemu?

a. Czy w miarę możliwości rozważano zastosowanie innych systemów lub rozwiązań niewykorzystujących algorytmicznego podejmowania decyzji?

b. Dlaczego ostatecznie zdecydowano się na ten system?

38.2 Dlaczego Państwa zdaniem dopuszczalne jest podjęcie ryzyka wynikającego z użytkowania systemu?

g) oświadczenie o legalności korzystania z systemu w świetle obowiązującego prawa, w szczególności prawa o ochronie danych, prawa o postępowaniu administracyjnym i obowiązujących przepisów sektorowych, wraz z uzasadnieniem.

⁸⁷ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 22.

⁸⁸ Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji (nr 1), 22.

Wzorcowe zasady EIP w zakresie oceny skutków wykorzystania algorytmicznych systemów decyzyjnych w administracji publicznej wraz z komentarzami i źródłami

Artykuł 1: Cel i zakres

Źródła

Art. 1 ust. 1 i 4 Ocena oddziaływania na środowisko Dyrektywa 2011/92/UE:

Uwagi

(1.1.) Ustęp 1 określa cel niniejszych Wzorcowych Zasad. Należy podkreślić, że niniejsze Wzorcowe Zasady przewidują zastosowanie procedury oceny skutków, nie zaś (nowych) norm podstawowych. Wyszczególniając odpowiednie „skutki dla społeczeństwa”, o których mowa w ust. 1, można kierować się listą zamieszczoną w art. 6 ust. 2 lit. c) i w Załączniku 4.

(1.2.) W ust. 2 określono, kiedy konieczne jest przeprowadzenie oceny skutków. Załącznik 1 powinien zawierać listę systemów, w przypadku których zawsze konieczna jest ocena skutków. To, które systemy zostaną wymienione w tym załączniku, zależy głównie od decyzji politycznej. Z tego względu Zespół Projektowy odstąpił od sporządzenia treści niniejszego Załącznika. Państwa dążące do wdrożenia niniejszych Wzorcowych Zasad mogą rozważyć wyszczególnienie w tym Załączniku systemów będących przedmiotem gorącej debaty politycznej lub takich, które są powszechnie uważane za obarczone wysokim ryzykiem. Dobrym punktem wyjścia do przygotowania jego treści byłby Załącznik III do unijnego projektu rozporządzenia w sprawie SI (COM (2021) 206, wersja ostateczna). Zespół Projektowy zrezygnował z bezpośredniego odniesienia do tego rozporządzenia z dwóch powodów: Po pierwsze, kraje spoza UE również mogą chcieć wdrożyć niniejsze Wzorcowe Zasady. Po drugie, treść Załącznika III do projektu rozporządzenia wydaje się pod pewnymi względami nadmiernie zawężona (np. zawarta w nim definicja infrastruktury krytycznej nie jest zgodna z istniejącym już prawem unijnym w tym zakresie (dyrektywa NIS 2016/1148) i nie obejmuje np. telekomunikacji czy ruchu kolejowego). Zespół Projektowy zachęca państwa członkowskie do wyjścia poza definicję SI wysokiego ryzyka zawartą w unijnym projekcie rozporządzenia w sprawie SI przy opracowywaniu treści Załącznika 1. Projekt rozporządzenia w sprawie SI ma zastosowanie zarówno do wykorzystania SI w celach publicznych, jak

i prywatnych, dlatego też należy unikać nadmiernych obciążeń dla prywatnych przedsiębiorstw. Z kolei niniejsze Wzorcowe Zasady mają zastosowanie wyłącznie do ASD używanych w sektorze publicznym, które powinny podlegać większej kontroli niż systemy SI w ogóle.

(1.3.) Systemy nieobjęte postanowieniami Załącznika 1 lub ust. 3 muszą być poddane procedurze screeningu (art. 4) w celu ustalenia, czy konieczne będzie przeprowadzenie oceny skutków.

(1.4.) Systemy wyszczególnione w Załączniku 2 nie podlegają ocenie skutków. Zespół Projektowy pozostawia treść Załącznika 2 do ustalenia w ramach decyzji politycznych. W zamierzeniu Załącznik 2 zawierałby różne rodzaje systemów: systemy, które w oczywisty sposób obarczone są niskim ryzykiem (np. popularne czatboty), systemy tak powszechne, że związane z nimi ryzyko jest dobrze znane i łatwe do opanowania, jak również systemy, w przypadku których nie można zastosować wysokiego stopnia kontroli publicznej, jaki zapewnia ocena skutków (głównie systemy stosowane w dziedzinie bezpieczeństwa narodowego). Z tej ostatniej opcji należy korzystać oszczędnie — art. 8 Wzorcowych Zasad dopuszcza bowiem ochronę tajemnicy. Załącznik 2 powinien również obejmować systemy, które używane są jako komponenty produktów podlegających już obszernym regulacjom w zakresie bezpieczeństwa, jeżeli takie regulacje odnoszą się do konkretnych zagrożeń związanych z procesami podejmowania decyzji opartymi na algorytmach. Załącznik II do projektu rozporządzenia w sprawie SI określa szereg przykładów takich systemów, zwłaszcza samochodów autonomicznych. Zespół Projektowy zakłada, że ryzyko związane z takimi systemami jest już w pełni uwzględnione w odpowiednich przepisach. Niemniej w przypadku gdy takie produkty będą używane przez władze publiczne w sposób, który istotnie różni się od powszechnych praktyk zakładanych przez ogólne zasady bezpieczeństwa produktów, może być konieczne zastosowanie wyjątku.

(1.5.) Sposób aktualizacji załączników musi być dostosowany do danego systemu prawnego. Przykładowo w kwestii dyrektyw może być konieczne

przyniesienie parlamentom narodowym prawa do zmiany załączników.

(1.6.) W ust. 4 przewidziano ograniczony wyjątek dotyczący sytuacji nadzwyczajnych, który pozwala na odroczenie oceny do czasu po wdrożeniu systemu. Klauzula ta obejmuje sytuacje nadzwyczajne, takie jak pandemia Covid-19. W takich przypadkach wymagana jest szybka reakcja (np. w celu wykrywania kontaktów osób zakażonych lub ustalania terminów szczepień), co przeważa nad obawami w zakresie przejrzystości i konieczności szczegółowego zarządzania ryzykiem. Ustęp ten nie dotyczy ogólnych zagrożeń przestępczością lub terroryzmem.

(1.7.) W takim przypadku organ wdrażający musi przeprowadzić ocenę skutków przed rozpoczęciem korzystania z systemu. Nie jest możliwe wyznaczenie konkretnego terminu na ocenę skutków. Powinna ona towarzyszyć procesowi rozwoju systemu. Ocena skutków powinna rozpocząć się na tyle wcześnie, by umożliwić wprowadzenie istotnych zmian, jeśli organ wdrażający wykryje problemy w jej trakcie. Jednakże w przypadku zbyt wczesnego rozpoczęcia prac często okazuje się, że specyfika systemu nie jest jeszcze znana. Dokładny termin przeprowadzenia oceny skutków zależy także od tego, czy instytucja wdrażająca opracuje system samodzielnie, czy też zakupi go od zewnętrznego dostawcy. W drugim przypadku kwestią szczególnie ważną dla pomyślnego przeprowadzenia oceny skutków jest współpraca z dostawcą. Zasady takiej współpracy określa art. 7.

Artykuł 2: Definicje

Źródła

Art. 1 ust. 2 dyrektywy 2011/92/UE w sprawie oceny skutków wywieranych przez niektóre przedsięwzięcia publiczne i prywatne na środowisko; art. 3 ust. 9 dyrektywy 2007/2/WE (INSPIRE); załącznik A do dyrektywy w sprawie zautomatyzowanego podejmowania decyzji (Kanada); art. 2 ust. 4 ustawy senackiej stanu Waszyngton nr 5116; art. III-2 ust. 1 Modelu kodeksu postępowania administracyjnego ReNEUAL

Uwagi

Wykorzystanie algorytmicznych systemów decyzyjnych

(2.1.) Zespół Projektowy zdecydował się na wykorzystanie terminu „algorytmiczny system

decyzyjny” (ASD) [ang.: *algorithmic decision-making system* — ADMS] zamiast pojęcia „sztuczna inteligencja”, gdyż ma on szersze znaczenie i jest neutralny technologicznie. ASD nie ogranicza się do systemów SI lub uczenia maszynowego. To, czy system ASD wykorzystuje technologię sztucznej inteligencji, czy też nie, jest nierzadko kwestią sporną. Dodatkowo nawet bardziej konwencjonalne systemy algorytmiczne mogą stwarzać istotne ryzyko. Zespół Projektowy jest świadomy, że Komisja Europejska stosuje termin „sztuczna inteligencja” w projekcie rozporządzenia w sprawie sztucznej inteligencji. Zespół uważa jednak, że termin „algorytmiczne podejmowanie decyzji” [ang.: *algorithmic decision-making*] jest bardziej odpowiedni, przynajmniej w odniesieniu do administracji publicznej. Administracja publiczna korzysta nie tylko z bardzo złożonych systemów, które powszechnie określa się mianem SI, ale także z prostszych systemów, co do których można mieć wątpliwości, czy rzeczywiście są sztuczną inteligencją. Aby uniknąć takich kontrowersji, zespół projektowy wybrał bardziej neutralny termin, czyli właśnie „algorytmiczne podejmowanie decyzji”. W przeciwieństwie do przepisów o ochronie danych osobowych, w tym przypadku nie ma znaczenia, czy system przetwarza dane osobowe, czy też nie.

(2.2.) Termin ASD jest szeroki i obejmuje szeroką gamę systemów komputerowych — nawet tych, które nie są obciążone wysokim ryzykiem. Jednocześnie dzięki zastosowaniu procedury screeningu przewidzianej w art. 4 ocenie skutków zostanie poddana znacznie mniejsza liczba systemów. Niektóre ASD, które są bardzo powszechne i w oczywisty sposób nie stanowią zagrożenia (np. oprogramowanie antywirusowe, rozwiązania do automatycznego sprawdzania pisowni itp.), powinny być uwzględnione w załączniku 2, ponieważ nie wymagają przeprowadzania procedury screeningu. Władze publiczne mają swobodę w przeprowadzaniu ocen skutków zastosowania systemów, które nie są objęte niniejszymi Zasadami.

(2.3.) Definicja obejmuje systemy wspierające podejmowanie decyzji przez człowieka. Nawet jeśli ostateczną decyzję podejmuje człowiek, to systemy, które przygotowują lub analizują dane na potrzeby takiej decyzji, lub choćby przedstawiają konkretne propozycje, mogą wywierać znaczący wpływ na decydenta i w związku z tym nie powinny pozostawać bez kontroli.

Organ publiczny

(2.4.) Definicja została zaczerpnięta z art. 3 ust. 9 dyrektywy 2007/2/WE (INSPIRE). Obejmuje ona

wszystkie szczeble administracji publicznej. Na mocy litery „c” wspomnianego ustępu, definicja obejmuje również podmioty prywatne pełniące funkcje administracyjne.

(2.5.) Definicja nie obejmuje sądownictwa, chyba że działa ono w charakterze administracyjnym. Zespół Projektowy opowiada się za wdrożeniem oceny skutków stosowania rozwiązań ASD w sądownictwie. Wpływ takich systemów (np. takich, które przewidują szansę na powrotność do przestępstwa u kryminalistów) może być co najmniej tak duży, jak wpływ systemów stosowanych przez władzę wykonawczą. Zasada niezawisłości sądownictwa byłaby jednak sprzeczna z niektórymi zapisami Wzorcowych Zasad (zwłaszcza z kompetencjami organu nadzorczego określonymi w art. 15). Prawodawcy pragnący wprowadzić ocenę skutków w sądownictwie mogą wykorzystać niniejsze Zasady jako wzorzec, lecz powinni je starannie dostosować do tego obszaru.

Decyzja

(2.6.) Termin „decyzja” ma szersze znaczenie niż to przewidziane w typowych definicjach decyzji administracyjnej w krajowym ustawodawstwie dotyczącym postępowania administracyjnego lub sądownictwa administracyjnego (por. np. art. III-2 ust. 1 Modelu kodeksu postępowania administracyjnego ReNEUAL). Działanie w rozumieniu art. 2 nie musi być prawnie wiążące. Termin ten obejmuje również działania czysto merytoryczne (np. ostrzeżenia lub porady). Decyzja w rozumieniu niniejszych Wzorcowych Zasad nie ogranicza się do pojedynczej sprawy. Definicja obejmuje także zmianę polityki (np. zainstalowanie monitoringu w obszarze, w którym system algorytmiczny wykrył wzrost przestępczości). Obejmuje ona ponadto decyzje deklaratoryjne stwierdzające określony fakt — np. decyzje o zaszeregowaniu, w ramach których ustala się, że dana osoba kwalifikuje się do objęcia ubezpieczeniem zdrowotnym. Definicja ta obejmuje działania organów administracyjnych zarówno na gruncie prawa publicznego, jak i prywatnego. Nie jest tutaj konieczne, aby osoba poszkodowana zdawała sobie sprawę, że podjęto konkretne działanie, a zatem definicja ta obejmuje np. potajemną inwigilację. Termin „określenie” nie ogranicza się do prostego pytania o to, czy należy działać, czy też nie. Obejmuje również pytanie o to, jak należy postąpić (np. czy zastosować surową czy łagodną karę).

Spółeczeństwo

(2.7.) Z punktu widzenia udziału społeczeństwa zgodnie z artykułem 11, definicja tego, czym jest społeczeństwo, ma istotne znaczenie. Została ona zaczerpnięta z art. 1 ust. 2 lit. d) dyrektywy w sprawie oceny skutków wywieranych przez niektóre przedsięwzięcia publiczne i prywatne na środowisko (dyrektywa 2011/92/UE), który ustanawia porównywalny mechanizm partycypacji społeczeństwa.

Dostawca systemu/Dostawca danych

(2.8.) Definicja ta związana jest z art. 7, który reguluje współpracę organu wdrażającego z tymi podmiotami. Różni się ona od definicji dostawcy zawartej w art. 3 ust. 2 projektu rozporządzenia w sprawie SI (COM (2021) 206, wersja ostateczna), która koncentruje się na podmiocie wprowadzającym system na rynek UE lub oddającym go do użytku. Z kolei dostawcą systemu (lub danych) może być każdy, kto dostarcza elementy systemu bądź odpowiednie dane — bez względu na swoją pozycję w łańcuchu dostaw. Może to być również dystrybutor w rozumieniu art. 3 ust. 7 projektu rozporządzenia w sprawie SI. Ponadto definicja dostawcy danych różni się nieco od tej zawartej w treści zasady 3 pkt 1 lit. n) Zasad EIP dotyczących gospodarki opartej na danych [*ang.: ELI Principles for a Data Economy*]. Definicja zawarta we wspomnianych Zasadach odnosi się do każdego podmiotu, który przekazuje dane innemu podmiotowi lub zobowiązuje się do tego. W myśl niniejszych Wzorcowych Zasad dane muszą zostać dostarczone organowi wdrażającemu, a samo podjęcie się ich dostarczenia nie jest wystarczające.

Organ wdrażający

(2.9.) Obowiązki wynikające z niniejszych Wzorcowych Zasad są zaadresowane głównie do organu wdrażającego. Definicja ta koncentruje się na organie, który korzysta lub zamierza korzystać z systemu. Jeśli jednak nadrzędny organ publiczny (np. ministerstwo finansów) zdecyduje, że organy podległe (np. lokalne urzędy skarbowe) muszą korzystać z systemu, to wówczas za ocenę skutków odpowiada organ nadrzędny. Może on wówczas podjąć decyzję o samodzielnym przeprowadzeniu oceny skutków — w razie potrzeby przy wsparciu jednego z organów niższego szczebla — lub nawet o powierzeniu jej jednemu z takich organów.

Artykuł 3: Koordynacja z innymi procedurami

Źródła

Art. 9 i 35 projektu rozporządzenia w sprawie SI (wniosek Komisji; COM (2021) 206, wersja ostateczna); Art. 35 ogólnego rozporządzenia o ochronie danych (UE) 2016/679

Uwagi

(3.) W celu uniknięcia dublowania się przeprowadzanych ocen, ważne jest, aby zapewnić koordynację pomiędzy procedurami określonymi w niniejszych Wzorcowych Zasadach a procedurami przewidzianymi w innych aktach prawnych. Przykładowo jasne jest, że ocena skutków przewidziana w art. 35 RODO (rozporządzenie (UE) 2016/679) mogłaby dostarczyć przynajmniej część informacji wymaganych w ramach sprawozdania na podstawie art. 6. Podobnie unijne przepisy dotyczące bezpieczeństwa produktów wymagają przeprowadzenia oceny zgodności, która już teraz może obejmować niektóre kwestie, które byłyby omawiane w sprawozdaniu na podstawie art. 6. W szczególności obecny projekt rozporządzenia UE w sprawie sztucznej inteligencji (COM (2021) 206, wersja ostateczna), jeśli zostanie przyjęty, może wymusić wykonanie pewnych ocen, które mogą być przydatne przy sporządzaniu sprawozdania wymaganego w art. 6. Dotyczy to w szczególności oceny zgodności (art. 43) oraz systemu zarządzania ryzykiem (art. 9). Poprzez wprowadzenie w życie niniejszych Wzorcowych Zasad, każdy system prawny powinien z góry określić istniejące procedury, które mogą częściowo spełniać wymogi sprawozdania wymaganego na podstawie art. 6.

Mimo iż nie można opisać wszystkich sytuacji, w których konieczna jest koordynacja procedur, zwłaszcza w przypadku istnienia sprzecznych przepisów, pragniemy zwrócić uwagę ustawodawcy na tę kwestię.

Artykuł 4: Ustalanie obowiązku przeprowadzenia oceny (screening)

Źródła

Artykuł 4 dyrektywy 2011/92/UE w sprawie oceny skutków wywieranych przez niektóre przedsięwzięcia publiczne i prywatne na środowisko oraz załącznik III do niej; art. 35 ust. 1 ogólnego rozporządzenia o ochronie danych (UE) 2016/679;

Number 6.1.1 Directive on Automated Decision-Making [pol.: Ppkt 6.1.1 Dyrektywy w sprawie zautomatyzowanego podejmowania decyzji] (Kanada),

Uwagi

(4.1.) Artykuł 4 przewiduje procedurę screeningu mającą na celu ustalenie, czy systemy niewymienione w załączniku 1 lub 2 będą podlegać ocenie skutków. Pojęcie screeningu lub oceny wstępnej jest już znane, gdyż proces ten przeprowadzany jest także w przypadku oceny oddziaływania na środowisko i ochrony danych. Procedura screeningu nie musi być tak szczegółowa jak właściwa ocena skutków.

(4.2.) Szczegółowy kwestionariusz do procedury screeningu znajduje się w Załączniku 3. Jego ogólny zamysł bazuje na procesie Canadian Algorithmic Impact Assessment [pol.: Kanadyjska Ocena Skutków Stosowania Algorytmów]. Zawiera on głównie pytania wielokrotnego wyboru. Każdej odpowiedzi należy przypisać określoną wartość ryzyka. Suma wszystkich odpowiedzi daje wynik oceny ryzyka, który określa poziom ryzyka. Do niektórych odpowiedzi wskazujących na to, że wdrożono środki zarządzania ryzykiem, należy przypisać wartości ujemne. Zespół Projektowy nie przypisał konkretnych wartości do każdej z odpowiedzi, gdyż nie posiada praktycznego doświadczenia z systemami sztucznej inteligencji w sektorze publicznym. Rządy, które pragną wdrożyć Wzorcowe Zasady, powinny zasięgnąć opinii ekspertów i praktyków w celu ustalenia konkretnych wartości.

(4.3.) Rezultatem procedury screeningu jest ustalenie jednego z trzech możliwych poziomów ryzyka:

- Niskie ryzyko — ocena skutków nie jest wymagana.
- Istotne ryzyko — konieczna jest ocena skutków, jednak nie mają zastosowania postanowienia rozdziału 3;
- Wysokie ryzyko — konieczne jest przeprowadzenie oceny skutków, w tym konsultacji społecznych i eksperckich zgodnie z wymogami zawartymi w rozdziale 3.

(4.4.) Używane w niniejszych Wzorcowych Zasadach określenie „wysokie ryzyko” nie jest tożsame z tym stosowanym w projekcie rozporządzenia UE w sprawie SI, choć znaczenie tych sformułowań może się pokrywać. Projekt rozporządzenia w sprawie SI określa tym mianem produkty zawierające zintegrowany system SI bądź też obszary, w których wykorzystuje się systemy SI. Z kolei niniejsze Wzorcowe Zasady opierają się na indywidualnej ocenie każdego przypadku przy

uwzględnieniu konkretnego kontekstu, w którym system jest używany.

(4.5.) Jeśli ocena skutków jest konieczna, organ wdrażający będzie musiał dokonać przeglądu wstępnej oceny ryzyka po sporządzeniu sprawozdania z oceny skutków (art. 6 ust. 2 lit. f)). Gwarantuje to, że w ocenie ryzyka uwzględnione zostaną wyniki szczegółowego badania.

(4.6.) Zgodnie z ust. 2 organ wdrażający publikuje wyniki procedury sprawdzającej. Zapewnia to pewien poziom przejrzystości nawet przy zastosowaniu systemów, w przypadku których nie jest wymagana właściwa ocena skutków. Z racji, iż kwestionariusz wstępny jest testem wielokrotnego wyboru, organ wdrażający nie musi wyjaśniać wyników procedury screeningu. Dodając wyjaśnienie możemy jednak dodatkowo zwiększyć przejrzystość, na przykład w sytuacji, gdy system był bliski zakwalifikowania do wyższego poziomu ryzyka.

(4.7.) Nie można wykluczyć, że wyniki screeningu będą zawierały dane poufne, dlatego też treść ust. 2 kończy się odniesieniem do art. 13 ust. 3, który jest głównym przepisem dotyczącym tej kwestii.

Artykuł 5: Ustalanie zakresu oceny (scoping)

Źródła

Art. 5 ust. 2 Ocena oddziaływania na środowisko dyrektywa 2011/92/UE; art. 4 ust. 2 rozporządzenia (UE) 182/2011; § 15

Umweltverträglichkeitsprüfungsgesetz (niemiecka ustawa o ocenie oddziaływania na środowisko)

Uwagi

(5.1.) Ustalenie zakresu (scoping) nie jest obowiązkowe, ale pomaga organowi wdrażającemu określić najważniejsze kwestie do uwzględnienia w sprawozdaniu wymaganym przez art. 6. Z racji, iż poszczególnym organom wdrażającym może brakować wiedzy na temat SI, szczególnie ważne jest konsultowanie się z ekspertami lub, w stosownych przypadkach, z organem nadzorczym ustanowionym na mocy art. 15.

(5.2.) Na podstawie ust. 2 organ wdrażający może zwrócić się do organu nadzorczego z wnioskiem o ustalenie zakresu oceny. Umożliwia to organowi wdrażającemu jak najlepsze wykorzystanie wiedzy fachowej organu nadzorczego. W ust. 2 wyjaśniono również, że organ wdrażający musi w jak największym

stopniu uwzględniać wyniki ustalania zakresu przez organ nadzorczy. Sformułowanie „uwzględniając w jak największym stopniu” jest typowe dla unijnego prawa administracyjnego — zob. np. art. 4 ust. 2 rozporządzenia (UE) nr 182/2011 ustanawiającego przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję.

(5.3.) Ważną częścią ustalania zakresu jest wyjaśnienie, na jakich zagadnieniach powinna się skupić ocena. Zwykle nie wszystkie spośród aspektów wymienionych w art. 6 będą wymagały szczegółowej analizy. Ustalenie zakresu dotyczy jednak wyłącznie określenia priorytetów, nie zaś wyłączenia z oceny skutków aspektów wymienionych w art. 6.

Artykuł 6: Sprawozdanie z oceny skutków

Źródła

Artykuły 6–20 projektu rozporządzenia UE w sprawie SI (wniosek Komisji; COM (2021) 206, wersja ostateczna); art. 35 ust. 1 i 7 ogólnego rozporządzenia o ochronie danych (UE) 2016/679; art. 5 ust. 3 dyrektywy 2011/92/UE w sprawie oceny skutków wywieranych przez niektóre przedsięwzięcia publiczne i prywatne na środowisko; Lista kontrolna oceny godnej zaufania sztucznej inteligencji Grupy Ekspertów Wysokiego Szczebla UE ds. Sztucznej Inteligencji (2020); Zalecenie CM/Rec(2020)1 Komitetu Ministrów dla państw członkowskich w sprawie wpływu systemów algorytmicznych na prawa człowieka (Rada Europy); „The Impact of Artificial Intelligence on Human Rights, Democracy and the Rule of Law” [pol.: *Wpływ sztucznej inteligencji na prawa człowieka, demokrację i praworządność*] (sprawozdanie Cateljine Muller; CAHAI (2020) 06; Studium wykonalności (Rada Europy, Komitet ad hoc ds. sztucznej inteligencji, CAHAI (2020) 23); „Human Rights, Democracy and Rule of Law Impact Assessment of AI Systems” [pol.: *Ocena wpływu systemów sztucznej inteligencji na prawa człowieka, demokrację i praworządność*] (Rada Europy, Komitet ad hoc ds. sztucznej inteligencji, CAHAIPDG (2021) 05; Ocena skutków na podstawie Dyrektywy w sprawie zautomatyzowanego podejmowania decyzji (Kanada); § 16 *Umweltverträglichkeitsprüfungsgesetz* (niemiecka ustawa o ocenie oddziaływania na środowisko)

Uwagi

(6.1.) W art. 6 wykorzystano różne dokumenty dotyczące wymogów prawnych i etycznych, tworząc

obszerną i szczegółową listę zagadnień, które należy poddać ocenie. Celem zespołu projektowego było opracowanie artykułu, który byłby bardziej szczegółowy niż większość dokumentów dotyczących etyki w zakresie SI, a jednocześnie na tyle obszerny, aby objąć wszystkie kwestie prawne i etyczne, które zwykle omawiane są w odniesieniu do ASD. Ponadto zespół projektowy dążył do stworzenia przejrzystej struktury „prawnej” dla różnych kryteriów oceny. Szeroki zakres artykułu uzasadniony jest dużą różnorodnością skutków, jakie mogą wywierać ASD, a z których personel administracyjny nie zawsze zdaje sobie sprawę. Dlatego ważne jest, aby zapewnić stosunkowo szczegółowe wytyczne dotyczące odpowiednich aspektów. W przeciwieństwie do większości propozycji dotyczących oceny skutków oraz zapisów art. 35 RODO, w projekcie nie skupiono się wyłącznie na ryzyku, ale także zapytano, w jaki sposób organ wdrażający może zoptymalizować korzyści wynikające z zastosowania systemów. Kryteria oceny nie są wiążącymi normami, które musi spełnić każdy system: niniejsze Wzorcowe Zasady przewidują zastosowanie procedury oceny skutków, nie zaś norm podstawowych. Jeśli organ wdrażający nie może lub nie chce podjąć działań w celu spełnienia kryterium określonego w niniejszym artykule, to powody ku temu może wyjaśnić w sprawozdaniu. Przykładowo zapewnienie konfiguracji zapewniającej maksymalną przejrzystość systemu może być niewykonalne z technicznego punktu widzenia lub zbyt kosztowne. W konsekwencji organy nadzorcze, sądy lub opinia publiczna muszą zdecydować, czy korzystanie z systemu jest dopuszczalne (z prawnego lub politycznego punktu widzenia).

(6.2.) Treść art. 6 jest już wprawdzie stosunkowo szczegółowa, jednakże korzystne byłoby doprecyzowanie go poprzez sporządzenie wytycznych i metodologii. Załączniki 4A i 4B stanowią punkt wyjścia do opracowania takich metodologii lub wytycznych. Stworzenie jednej metodologii dla wszystkich typów systemów prawdopodobnie okaże się niemożliwe. Metody oceny skutków należy zawsze opracowywać i dostosowywać zgodnie z rozwojem technologicznym, prawnym i społecznym. Właściwe może być również dostosowanie ich do konkretnych kontekstów prawnych, kulturowych lub społecznych, szczególnie gdy występują znaczne różnice w postrzeganiu zagrożeń związanych z algorytmicznym podejmowaniem decyzji w tych kontekstach.

(6.3.) Art. 6 ust. 2 lit. a) wymaga opisu odpowiednich cech systemu. Opis ten pomoże zrozumieć funkcjonowanie systemu i ocenić jego zalety i wady nie

tylko ekspertom i opinii publicznej, ale także samemu organowi wdrażającemu. Jako jedno z kryteriów rozważano także „złożoność” [*ang.: complexity*], jednakże pomysł ten został odrzucony przez Zespół Projektowy EIP po konsultacjach z ekspertami ds. SI, którzy wskazali na brak definicji takiego terminu. Zawarte poniżej kryteria w zakresie przejrzystości i wytłumaczalności odzwierciedlają tę trudność w zrozumieniu lub wyjaśnieniu działania systemu.

(6.4.) Art. 6 ust. 2 lit. b) odnosi się do problemu polegającego na tym, że debaty publiczne dotyczące SI, a także niektóre inne modele oceny skutków często koncentrują się wyłącznie na ryzyku. To zaś grozi zlekceważeniem potencjału rozwiązań ASD w zakresie usprawniania pracy administracji publicznej. Celem jest jednak również uniknięcie przesadnego optymizmu: niektóre władze publiczne przyjmują ASD bezkrytycznie, nie oceniając ich funkcjonalności. To z kolei może prowadzić do osiągnięcia rozczarowujących wyników i marnowania zasobów (finansowych). Dlatego ważne jest, aby dokładnie określić i zbadać potencjalne korzyści płynące z zastosowania systemu oraz wymagania dotyczące ich osiągnięcia (np. architektura systemu, dostępność dla społeczeństwa, wszechstronność i jakość danych itp.)

(6.5.) Art. 6 ust. 2 lit. c) dotyczy zewnętrznego wpływu systemu. Wymaga to zbadania zarówno skutków specyficznych, jak i systemowych. Skutki specyficzne to takie występujące w poszczególnych przypadkach zastosowania danego rozwiązania. Skutki systemowe wynikają z faktu, że decyzje, które wcześniej były w zdecentralizowany sposób, zastępowane są scentralizowanymi systemami algorytmicznymi, co zwiększa potencjalne szkody w przypadku awarii takich systemów.⁹³ Art. 6 ust. 2 lit. c) pkt (i) dotyczy praw podstawowych. Ocena może obejmować wszystkie prawa podstawowe. W tym przypadku wymieniono jednak tylko te, które są najczęściej omawiane w kontekście sztucznej inteligencji. To, jakie prawa będą musiały być dogłębnie zbadane w ramach oceny indywidualnej, zależy od kontekstu, w którym system jest używany. Prawa te powinny zostać określone podczas ustalania zakresu, zgodnie z art. 5. Mimo iż ocena powinna koncentrować się na prawach określonych w prawnie wiążących dokumentach (np. w Karcie praw podstawowych UE, Europejskiej konwencji praw człowieka lub konstytucjach krajowych), instytucja wdrażająca powinna także rozważyć aspekty etyczne. Ze względu na fakt, że w debacie publicznej często nie rozróżnia się aspektów prawnych od etycznych, zapewnienie

ochrony praw wykraczającej poza minimum wymagane w przepisach może zwiększyć zaufanie opinii publicznej do systemu. W odróżnieniu od projektu rozporządzenia Komisji (COM (2021) 206, wersja ostateczna), zespół projektowy nie skupił się na kwestii „zdrowia i bezpieczeństwa”, gdyż ma ona największe znaczenie dla robotyki i jazdy autonomicznej, które nie są typowymi przypadkami zastosowania algorytmów w administracji publicznej. W przeciwieństwie do art. 35 RODO, ocena obejmuje również aspekty społeczne i środowiskowe, a także sam organ administracyjny. Druga część oceny ma na celu zapewnienie akceptacji systemu przez administrację oraz skuteczną realizację zmian, jakie nieuchronnie przynosi cyfryzacja.

(6.6.) W art. 6 ust. 2 lit. d) jest mowa o ocenie cech i ustawień systemu w celu jego optymalizacji, a także zarządzania ryzykiem. Są to cechy „wewnętrzne” — w odróżnieniu od „zewnętrznych” skutków systemu, o których mowa w art. 6 ust. 2 lit. c). Art. 6 ust. 2 lit. d) pkt (i) zawiera pytanie o środki podejmowane w celu przeciwdziałania skutkom zewnętrznym, z kolei pkt (ii)–(ix) opisują cechy, jakie powinien posiadać każdy system SI. Znaczenie niektórych kryteriów zawartych w tym ustępie nie zostało w pełni wyjaśnione w ramach dyskusji prawnej na temat SI. W szczególności Zespół Projektowy omówił pojęcia „ochrona” [ang.: *security*] i „bezpieczeństwo” [ang.: *safety*]. Zespół interpretuje te terminy zgodnie z terminologią informatyczną, w której nie są one zamiennie. Bezpieczeństwo oznacza, że system nie powoduje szkód zewnętrznych (tzn. unika wypadków). Ochrona polega na zapobieganiu nieuprawnionemu dostępowi do systemu i jego danych. W przypadku systemów informatycznych terminy te pokrywają się, gdyż osoby atakujące system mogą manipulować nim w celu wyrządzenia krzywdy innym⁹⁴. Zespół projektowy rozważał także dokładne znaczenie „przejrzystości” [ang.: *transparency*] i „wytłumaczalności” [ang.: *explainability*], jak również powiązania pomiędzy tymi pojęciami. Przejrzystość jest tu rozumiana jako ujawnienie logiki stosowanej przez system (np. poprzez publikację kodu źródłowego), zaś wytłumaczalność oznacza, że poszczególne decyzje

(6.7.) Art. 6 ust. 2 lit. e) wymaga od organu wdrażającego ostatecznego określenia poziomu ryzyka, bowiem podczas procedury screeningu organ ten podjął jedynie wstępną decyzję w tym zakresie.

(6.8.) Art. 6 ust. 2 lit. f) wymaga ogólnej oceny proporcjonalności użycia systemu. Zespół Projektowy postanowił nie używać terminu „analiza kosztów i korzyści”, ponieważ może on sugerować, że należy skupić się głównie na efektywności (ekonomicznej), podczas gdy Zespół pragnie zachęcić do przyjęcia bardziej holistycznego spojrzenia, uwzględniającego interesy społeczne i prawa jednostki.

(6.9.) Art. 6 ust. 2 lit. g) wymaga sprawdzenia zgodności z prawem. W idealnym przypadku na tym etapie wiele kwestii związanych z legalnością zostało już omówionych podczas przeprowadzania ocen wymaganych w poprzednich punktach — zwłaszcza ocen w zakresie praw podstawowych. Osoba oceniająca musi jednak nadal sprawdzić zgodność z przepisami o ochronie danych osobowych lub innymi przepisami obowiązującymi w danym sektorze. Ostatnim elementem zawartym w tym ustępie jest kontrola legalności. Jest to zmotywowane tym, że Zespół Projektowy pragnie, aby władza wykonawcza podeszła do oceny z otwartym umysłem i rozważyła wszystkie skutki zastosowania systemu jeszcze przed przystąpieniem do kontroli zgodności, której zakres jest stosunkowo wąski.

(6.9.) Ustęp 3 odsyła do listy kontrolnej zawartej w Załączniku 4. Zawarte w niej pytania są jeszcze bardziej szczegółowe, jednak jej struktura jest podobna do tej opisanej w art. 6. Lista kontrolna opiera się głównie na „Liście kontrolnej oceny godnej zaufania sztucznej inteligencji” autorstwa Niezależnej Grupy Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji, jednak została rozszerzona na podstawie innych źródeł. Zespół Projektowy przygotował zarówno standardową wersję aneksu (Aneks 4A), jak i wersję rozszerzoną, zawierającą bardziej szczegółowe pytania (Aneks 4B). Wersja standardowa ma być jak najkrótsza i koncentruje się na pytaniach, które Zespół Projektowy

⁹³Catelijne Muller, „The Impact of Artificial Intelligence on Human Rights, Democracy and the Rule of Law” [pol.: *Wpływ sztucznej inteligencji na prawa człowieka, demokrację i praworządność*] (CAHAI (2020) 06), ust. 49. ⁹⁴ Na definicję tę wskazują również Wytyczne Grupy Ekspertów Wysokiego Szczebla UE w zakresie etyki, 16–17

można wyjaśnić w sensowny sposób. Oznacza to, że osoby zainteresowane będą mogły zrozumieć powody poszczególnych decyzji — w idealnym przypadku i na tyle, na ile jest to technicznie możliwe.

uznał za najważniejsze. Z kolei wersja rozszerzona może pomóc organowi wdrażającemu nie przeoczyć istotnych szczegółów. Właściwe organy ustawodawcze muszą zdecydować, którą z tych dwóch opcji preferują. Alternatywnie mogą również powierzyć rozstrzygnięcie

tej kwestii organowi wdrażającemu lub nadzorczemu. Stosowanie się do listy kontrolnej w najdrobniejszych szczegółach nie jest obowiązkowe. Organ wdrażający może zastąpić ją innymi listami, które będą lepiej dostosowane do danego sektora.

(6.11.) W ust. 4 wyraźnie zaznaczono, że poziom szczegółowości sprawozdania zgodnego z art. 6 zależy od konkretnego przypadku i poziomu ryzyka. Ustęp ten instruuje również organ wdrażający, aby dążył do sporządzenia sprawozdania, które będzie zarówno dokładne, jak i zrozumiałe. Jeśli cele te są sprzeczne, instytucja wdrażająca musi przedstawić ogólnie zrozumiałe podsumowanie.

Artykuł 7: Współpraca i komunikacja z dostawcą systemu i dostawcą danych

Uwagi

(7.1.) Choć odpowiedzialność za przeprowadzenie oceny skutków i sporządzenie sprawozdania na podstawie art. 6 spoczywa przede wszystkim na organie wdrażającym, w rzeczywistości wykonanie tego zadania nie będzie możliwe bez aktywnej współpracy z dostawcą systemu oraz dostawcą danych. Ponadto organ wdrażający musi mieć dostęp do informacji o systemie dostarczonych przez osoby, które go zaprojektowały, opracowały, przetestowały i przetestowały — szczególnie ze względu na fakt, że np. opisy rozwoju systemu, jego właściwości technicznych i doboru danych stanowią elementy sprawozdania na podstawie art. 6.

(7.2.) Ważne jest także, aby wymiana informacji była rejestrowana i możliwa do odtworzenia, zgodnie z postanowieniami punktu 1. Głównym tego powodem, poza udowodnieniem wypełnienia zobowiązań, jest ustalenie przyczyn oraz podmiotu odpowiedzialnego w przypadku gdy system przestanie działać zgodnie z przeznaczeniem z powodu błędu technicznego, błędu ludzkiego, tendencyjności zbiorów danych itp.

(7.3.) Aby uniknąć nieporozumień i zapewnić prawidłowe działanie systemu po jego wdrożeniu w instytucji publicznej, należy ustanowić minimalne praktyczne zasady współpracy. Obejmuje to np. wspólny zespół projektowy obejmujący przedstawicieli organu wdrażającego, dostawcy systemu i dostawcy danych posiadających wystarczającą wiedzę i doświadczenie, aby aktywnie uczestniczyć w jego pracach.

(7.4.) Z tych samych powodów ust. 4 wymaga, aby system został poddany ostatecznym testom na sprzęcie organu wdrażającego lub innym sprzęcie używanym przez ów organ w toku zwykłej działalności (np. usługi w chmurze), a testy te powinny być przeprowadzone przez jego pracowników. Wyniki takich testów końcowych należy także uwzględnić w sprawozdaniu sporządzanym zgodnie z art. 6. Pozwoli to w wiarygodny sposób wykazać, że system powinien działać zgodnie z założeniami, gdy zostanie wdrożony na dużą skalę przez organ wdrażający, ze względu na fakt, że organ ten dysponuje odpowiednim sprzętem, a jego pracownicy wiedzą, jak go używać.

(7.5.) Wreszcie, ustęp 5 zapewnia, że cel niniejszego artykułu zostanie osiągnięty w praktyce poprzez ustanowienie wymogu, aby jego postanowienia były zawarte w umowie o zamówienie publiczne w przypadku gdy taka metoda nabycia systemu zostanie wybrana przez organ wdrażający. W innym przypadku — np. jeśli organ wdrażający zamierza stworzyć system własnymi siłami — powinien mimo wszystko zapewnić, że przepisy niniejszego artykułu zostaną uwzględnione i wdrożone w tym procesie

Artykuł 8: Przejrzystość i ochrona tajemnic

Źródła

Dyrektywa (UE) 2019/1024 w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego; Dyrektywa 2009/24/WE w sprawie ochrony prawnej programów komputerowych; Dyrektywa 96/9/WE w sprawie ochrony prawnej baz danych; Dyrektywa Rady 91/250/EWG w sprawie ochrony prawnej programów komputerowych; Rozporządzenie (UE) 2018/1807 w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej

Uwagi

(8.1.) Niniejsze Wzorcowe Zasady mają na celu ochronę uzasadnionych interesów zarówno organu wdrażającego, jak i dostawcy systemu lub dostawcy danych — niezależnie od tego, czy jest to zespół działający w ramach organu wdrażającego, czy też odrębny podmiot prywatny, który wygrał przetarg na stworzenie systemu. Ich zadaniem jest także ochrona interesów innych osób i podmiotów zaangażowanych w proces przeprowadzania oceny skutków. W tym przypadku, interesy chronione w ramach artykułu 8 dotyczą szeroko rozumianych „tajemnic”, czyli informacji umożliwiających identyfikację osób, jak

również dotyczących prywatności, własności intelektualnej, tajemnic handlowych (lub innych uzasadnionych interesów handlowych), bezpieczeństwa narodowego, obronności i bezpieczeństwa publicznego.

(8.2.) Zakres ust. 1 jest celowo bardzo szeroki i niewyczerpujący. Ma to na celu zapewnienie spójnego poziomu ochrony praw osób lub podmiotów oraz celów interesu publicznego w różnych kontekstach, co z natury rzeczy prowadzi do pokrywania się z różnymi systemami prawnymi, np. przepisami o ochronie danych. Z racji, iż wdrożenie Wzorcowych Zasad może potencjalnie nastąpić nie tylko w UE i jej państwach członkowskich, włączenie klauzul ogólnych dotyczących rodzajów tajemnic objętych niniejszym ustępem 1 miało kluczowe znaczenie. Ponadto przepis ten dotyczy zarówno przeprowadzania procesu oceny skutków, jak i opracowywania jej wyników w sprawozdaniu sporządzanym zgodnie z art. 6. Ponadto w przypadku ASD oznaczonych jako systemy wysokiego ryzyka, do których zastosowanie ma art. 10 (audyt i rada ekspertów), podczas przeprowadzania audytu i sporządzania sprawozdania z niego eksperci muszą również przestrzegać zapisów art. 8 (zob. ust. 2).

(8.3.) Dane szczególnie chronione, których nie można ujawniać na żadnym etapie procesu oceny skutków, obejmują informacje dotyczące bezpieczeństwa narodowego (czyli bezpieczeństwa państwa), obronności lub bezpieczeństwa publicznego. Dotyczy to zwłaszcza objętych szczególną ochroną informacji związanych z ochroną infrastruktury krytycznej. Chroniona jest własność intelektualna i tajemnice handlowe dotyczące systemu, a także dane osobowe wszystkich osób bezpośrednio lub pośrednio zaangażowanych w ten proces. Obejmuje to także sytuacje, gdy informacje zawarte w indywidualnym zbiorze danych treningowych lub testowych nie stwarzają ryzyka zidentyfikowania lub wyodrębnienia osoby fizycznej (ze względu na anonimizację lub podobny proces), jednakże mogą stwarzać takie ryzyko po połączeniu z innymi dostępnymi informacjami. Poufność danych statystycznych należy chronić w podobny sposób.

(8.4.) Aby uniknąć wątpliwości, termin „własność intelektualna” odnosi się wyłącznie do prawa autorskiego i praw pokrewnych, w tym do form ochrony na mocy prawa *sui generis*. Termin „tajemnica handlowa” obejmuje wszystkie formy chronionej własności przemysłowej i handlowej, takich jak patenty, zarejestrowane znaki towarowe, wzory i modele

przemysłowe, nieujawnione know-how i informacje biznesowe.

(8.5.) Jeśli chodzi o ASD i zbiory danych wykorzystywane do celów treningowych i testowych, dyrektywa 91/250/EWG zobowiązała wszystkie państwa członkowskie UE do tego, aby ich prawo autorskie chroniło programy komputerowe jako dzieła literackie w rozumieniu Konwencji berneńskiej o ochronie dzieł literackich i artystycznych. Zostało to skodyfikowane w Dyrektywie Parlamentu Europejskiego i Rady 2009/24/WE.

Dyrektywa 96/9/WE przewiduje ochronę prawną baz danych, definiując bazę danych jako „zbiór niezależnych utworów, danych lub innych materiałów uporządkowanych w sposób systematyczny lub metodyczny, indywidualnie dostępnych środkami elektronicznymi lub innymi sposobami”. Dyrektywa stanowi, że bazy danych chronione są zarówno prawem autorskim, które obejmuje twórczość intelektualną, jak i prawem *sui generis* chroniącym inwestycje (pieniądze, zasoby ludzkie, wysiłek i energię) w uzyskanie, weryfikację lub prezentację zawartości.

(8.6.) Ocenę skutków należy przeprowadzać z zastosowaniem odpowiednich środków w celu zabezpieczenia tajemnic prawnie chronionych. Ustęp 2 przyznaje organowi wdrażającemu oraz dostawcy systemu lub dostawcy danych prawo do zachowania poufności danych związanych z oceną skutków, ograniczając je jednak tylko do należycie uzasadnionych przypadków. Takie ograniczenie poufności należy zawsze rozważać w kontekście zasady przejrzystości. Wynika to z faktu, że istnieje potencjalny dysonans pomiędzy ochroną prawną szeroko rozumianych tajemnic a przejrzystością oceny skutków i ogólną zasadą przejrzystości administracji publicznej. Oznacza to, że chronione tajemnice (niezależnie od tego, czy są wyraźnie wymienione w ust. 1, czy nie) nie mają charakteru absolutnego, lecz powinny być zawsze rozpatrywane w konkretnym kontekście danego ASD i wymogów przejrzystości. Jest to istotne zwłaszcza ze względu na zgodność z ochroną prawną programów komputerowych (tu: kodu źródłowego ASD) oraz baz danych (tu: zbiorów danych do celów treningowych i testowych) z jednej strony, a także koncepcję wytłumaczalnej SI i zrozumienie przez opinię publiczną sposobu działania ASD z drugiej strony. W związku z tym w ust. 3 przedstawiono ogólne ramy umożliwiające ocenę kodu źródłowego systemu ASD i zbiorów danych wykorzystywanych do jego trenowania i testowania

(pod względem niezawodności, odporności, poprawności, adekwatności, niedyskryminacji itp.), co zapewni zgodność z wymogami w zakresie ochrony tajemnic. Decyzję o częściowym lub całkowitym ograniczeniu dostępu do kodu źródłowego oraz zbiorów danych szkoleniowych i testowych można pozostawić w gestii organu nadzorczego (o ile taki istnieje). W każdym przypadku taka decyzja wymaga jednak odpowiedniego uzasadnienia.

Artykuł 9: Zastosowanie niniejszego rozdziału

(9.) Artykuł 9 wyjaśnia, że artykuły dotyczące udziału społeczeństwa i ekspertów mają zastosowanie tylko w odniesieniu do systemów, które określone są jako „zawsze obciążone wysokim ryzykiem” w Załączniku 1 lub takich, w przypadku których stwierdzono występowanie wysokiego ryzyka w ramach sprawozdania sporządzanego na podstawie art. 6. Powodem tego ograniczenia jest uniknięcie stosowania nadmiernie uciążliwych procedur w odniesieniu do systemów, które stwarzają stosunkowo niewielkie ryzyko.

Artykuł 10: Audyt i Rada Ekspertów

Źródła

Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji, Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji, 19–20, 36, Rec. 33, Art. 5 Dyrektywy 2011/92/UE w sprawie oceny skutków wywieranych przez niektóre przedsięwzięcia publiczne i prywatne na środowisko; art. 6 ust. 3 Directive on Automated Decision-Making [pol.: *Dyrektywa w sprawie zautomatyzowanego podejmowania decyzji*] oraz załącznik 3 do niej (Kanada); Biuro Komisarza ds. Informacji Publicznej, „AI Auditing Framework” [pol.: *Ramy audytu SI*] (Zjednoczone Królestwo); opinia Komisji ds. etyki danych (Niemcy) 29, 159–184

Uwagi

(10.1.) Włączenie przeprowadzanego przez radę ekspertów audytu do procesu oceny skutków (sensu largo) zastosowania systemu wysokiego ryzyka ma na celu zapewnienie dodatkowej ochrony przed wdrożeniem takiego systemu na skalę masową. Wartość dodana zapewniana jest dzięki wiedzy

technicznej i doświadczeniu, dzięki którym rada ekspertów ponownie sprawdza system i wyszukuje zagrożenia, które organ wdrażający mógł przeoczyć. Głównym przedmiotem audytu jest raport sporządzany na podstawie art. 6 — w tym jego kompletność, jakość, dokładność itp. Niemniej eksperci powinni także uzyskać dostęp do samego systemu. Takie przeprowadzenie audytu powinno dać ekspertom możliwość zidentyfikowania brakujących elementów sprawozdania przewidzianego w art. 6, które nie zostały poddane ocenie, a także niespójności lub problemów z niską jakością, które mogłyby wskazywać, że ocena nie została przeprowadzona wystarczająco starannie. Audyt nie przenosi jednak odpowiedzialności za ocenę skutków z organu wdrażającego na ekspertów, co z kolei pozwala oszczędzić czas, gdyż eksperci nie muszą przeprowadzać pełnego audytu systemu.

(10.2.) W art. 10 położono nacisk m.in. na odpowiednią wiedzę tematyczną i niezależność ekspertów, co uznano za kluczowe dla zapewnienia bezstronnego i wiarygodnego audytu. Taką wiedzę fachową i niezależność zapewnia się, przyznając organowi nadzorcemu (a więc nie organowi wdrażającemu ani dostawcom systemu lub danych) prawo do powoływania i odwoływania ekspertów oraz tworzenia rady ekspertów na podstawie obiektywnych kryteriów przy uwzględnieniu kryterium różnorodności, a także wprowadzając zasady unikania konfliktów interesów.

Artykuł 11: Udział społeczeństwa

Źródła

Art. 6 Dyrektywy 2011/92/UE w sprawie oceny skutków wywieranych przez niektóre przedsięwzięcia publiczne i prywatne na środowisko; Artykuł III-25 Modelu kodeksu postępowania administracyjnego ReNEUAL

Uwagi

(11.1.) W przypadku systemów obciążonych znacznym ryzykiem przeprowadzenie konsultacji społecznych pozwala zapewnić, że wszystkie ich skutki zostały wzięte pod uwagę. Konsultacje umożliwiają również poinformowanie o systemie szerokiego grona osób, na które będzie on miał wpływ, poprzez umożliwienie im wyrażenia swoich opinii.

(11.2.) Ustęp 1 zobowiązuje organ wdrażający do przeprowadzenia procedury partycypacji społecznej. Organ wdrażający musi zapewnić możliwość udziału w tej procedurze zainteresowanym członkom społeczności. Oznacza to na przykład dostosowanie metod przekazywania informacji o procedurze i metod

konsultacji ze społeczeństwem, na które opracowany system ASD może mieć bezpośredni lub pośredni wpływ.

(11.3.) Ustęp 2 określa informacje o konsultacjach społecznych, które należy podać do wiadomości opinii publicznej. Podano w nim minimalne elementy pozwalające społeczeństwu dowiedzieć się o terminie i temacie konsultacji, jak również o podmiocie, który je organizuje. Jednocześnie o konsultacjach informowany jest organ nadzorczy. Ustęp 3 stanowi, że w ramach konsultacji należy udostępnić sprawozdanie zgodne z art. 6 oraz sprawozdanie z audytu.

(11.4.) Ustępy 4 i 5 odnoszą się do dwóch trybów konsultacji określonych w Artykule III-25 Modelu kodeksu postępowania administracyjnego ReNEUAL. Zasady ReNEUAL przewidują dwutygodniowe ramy czasowe na konsultacje społeczne. Na tym etapie nie proponuje się przedłużenia tego terminu, aby zachować prostotę tego procesu. W razie potrzeby przewidziane trzydziestodniowe ramy czasowe mogą zostać odpowiednio przedłużone.

(11.5.) Na konsultacje społeczne przeznaczają się co najmniej 30 dni (ust. 6). Uważa się, że jest to okres wystarczający do zagwarantowania partycypacji społecznej, a jednocześnie niezbyt długi, co pozwala uniknąć nadmiernych opóźnień we wdrażaniu ASD.

(11.6.) Oprócz zapewnienia udziału społeczeństwa należy przeprowadzić konsultacje z innymi właściwymi organami — na przykład z urzędem ochrony danych (ust. 7).

Artykuł 12: Ocena

Uwagi

(12.1.) Po konsultacjach publicznych sprawozdanie zgodne z art. 6 uzupełniane jest przez organ wdrażający. Odpowiedzi na sprawozdanie z audytu udzielane przez organ wdrażający zgodnie z art. 10 ust. 4 mogą zostać udzielone już po zakończeniu konsultacji publicznych. Z jednej strony umożliwia to organowi wdrażającemu uwzględnienie w tych odpowiedziach kwestii, na które uwagę zwróciła opinia publiczna, jednak z drugiej strony odpowiedzi te mogą nie być publicznie dostępne.

(12.2.) Sprawozdanie rozszerzone sporządzane jest przez organ wdrażający. Obejmuje ono wstępne sprawozdanie na podstawie art. 6, sprawozdanie z audytu, podsumowanie wyników udziału społeczeństwa, ocenę wszystkich wkładów (publicznego, rady ekspertów ds. audytu, a także innych

organów) przez wdrażającego, jak również uzasadnioną opinię końcową w sprawie wdrożenia ASD.

Artykuł 13: Publikacja

Źródła

Art. 9 ust. 2 Dyrektywy 2011/92/UE w sprawie oceny skutków wywieranych przez niektóre przedsięwzięcia publiczne i prywatne na środowisko; § 27 Ustawy o ocenie oddziaływania na środowisko [*niem.: Gesetz über die Umweltverträglichkeitsprüfung*] (Niemcy)

Uwagi

(13.1.) Ustęp 1 zobowiązuje do opublikowania ostatecznej wersji sprawozdania (w wersji przewidzianej w art. 6 bądź w wersji sprawozdania rozszerzonego) przynajmniej w internecie. Publikacja sprawozdania ma zasadnicze znaczenie dla przedstawienia społeczeństwu przejrzystej oceny skutków. Organ wdrażający ma obowiązek udostępnić sprawozdanie po zaprzestaniu użytkowania systemu, gdyż nawet po zakończeniu jego cyklu życia mogą pojawić się problemy prawne lub krytyka ze strony społeczeństwa. Jest to zgodne z ogólnymi przepisami dotyczącymi przechowywania plików — często bowiem przewidują one dość długie okresy przechowywania takich treści przed ich usunięciem.

(13.2.) Ustęp 2 nakazuje organowi wdrażającemu zawiadomienie ekspertów i członków społeczeństwa, którzy uczestniczyli w konsultacjach zgodnie z art. 10 i 11, o publikacji. Organ wdrażający ma w tym względzie swobodę proceduralną. Może opublikować zawiadomienie na swojej stronie internetowej lub skorzystać z systemu automatycznego powiadamiania na stronie przeznaczonej do prowadzenia konsultacji. Organ wdrażający przekazuje ponadto niezbędne dokumenty organowi nadzorczemu. Umożliwia to organowi nadzorczemu sprawdzenie, czy sprawozdanie jest zgodne z niniejszymi Wzorcowymi Zasadami, oraz, w razie potrzeby, skorzystanie z uprawnień przysługujących mu na mocy art. 15. Dzięki temu możliwe jest także opublikowanie sprawozdania w centralnym rejestrze publicznym (zob. art. 15 ust. 4).

(13.3.) Ustęp 3 dotyczy sprawozdań, które zawierają tajemnice określone w artykule 8. Organ wdrażający może odpowiednio zredagować sprawozdanie w celu ochrony wspomnianych tajemnic. Niemniej na mocy obowiązujących przepisów w zakresie wolności dostępu do informacji nadal będzie można uzyskać dostęp do

nieocenzurowanej wersji. Zespół Projektowy postanowił uwzględnić to odniesienie z uwagi na fakt, iż przepisy w sprawie wolności dostępu do informacji ustanawiają powszechnie akceptowaną równowagę pomiędzy związanym z informacjami interesem publicznym a ochroną tajemnicy.

(13.4.) Ustęp 4 odnosi się do art. 15 ust. 4, który reguluje kwestię publikacji odpowiednich dokumentów w rejestrze publicznym. Może to być np. publiczna baza danych dla systemów sztucznej inteligencji, tak jak zaproponowano w treści art. 60 unijnego projektu rozporządzenia w sprawie sztucznej inteligencji (COM (2021) 206, wersja ostateczna).

Artykuł 14: Przegląd i powtórzenie oceny

Źródła

Art. 35 ust. 11 ogólnego rozporządzenia o ochronie danych (UE) 2016/679; Art. 43 ust. 4 projektu rozporządzenia w sprawie SI (wniosek Komisji; COM (2021) 206 wersja ostateczna)

Uwagi

(14.1.) Ustęp 1 wymaga przeprowadzenia przeglądu, jeśli są dowody na istnienie znaczących negatywnych skutków, które nie zostały uwzględnione w odpowiednim pierwotnym sprawozdaniu (sprawozdaniu zgodnym z art. 6 lub sprawozdaniu rozszerzonym). Takie negatywne skutki mogą wynikać z nieoczekiwanego rozwoju algorytmów samouczących się, z niewykrytych błędów programistycznych, jak również z nieoczekiwanego zachowania personelu lub użytkowników. W ustępie 1 jako możliwą przyczynę istotnych negatywnych skutków wymieniono także celowe zmiany w systemie lub kontekście, w którym jest on używany. To, czy oddziaływanie jest znaczące, zależy od jego dotkliwości, a także od prawdopodobieństwa wystąpienia jego konsekwencji.

(14.2.) Ustęp 2 wymaga dokonania przeglądu sprawozdania po upływie określonego czasu, bez względu na to, czy miały miejsce negatywne zdarzenia. Tego typu przeglądy pozwalają uaktualnić sprawozdanie. Powinny odzwierciedlać rzeczywiste doświadczenia użytkownika podczas korzystania z systemu. Pozwoli to np. na dokładniejsze określenie liczby wyników fałszywie dodatnich i fałszywie ujemnych. Podane okresy stanowią jedynie propozycję i mogą być dostosowane do doświadczeń praktycznych

oraz typowego tempa wdrażania zmian w systemie lub zdobywania nowych doświadczeń.

(14.3.) Zgodnie z ustępem 3 zmienione sprawozdanie musi być ponownie poddane przeglądowi przez ekspertów, jeśli taki przegląd był wymagany w przypadku pierwotnego sprawozdania na mocy art. 10. Eksperti mogą jednak nie zgłosić żadnych dodatkowych uwag. Dalsze konsultacje społeczne nie są zalecane, ponieważ ponowne przeprowadzanie ich w przypadku stosunkowo niewielkich zmian wydaje się zbyt kosztowne. Organ wdrażający może jednak przeprowadzić takie konsultacje według uznania.

Artykuł 15: Organ nadzorczy

Źródła

Artykuły 51, 52, 57–59 ogólnego rozporządzenia o ochronie danych (UE) 2016/679; Art. 41, 42, 46, 47–49 dyrektywy (UE) 2016/680 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania lub ścigania przestępstw lub egzekwowania sankcji karnych i swobodnego przepływu takich danych; Art. 63 ust. 5 i art. 64 projektu rozporządzenia w sprawie SI (wniosek Komisji; COM (2021) 206, wersja ostateczna)

Uwagi

(15.1.) Procedura oceny skutków wymaga wsparcia i nadzoru ze strony wyspecjalizowanego organu dysponującego odpowiednimi zasobami. Z racji, że organ ten ma sprawować nadzór nad innymi jednostkami administracyjnymi, powinien on być niezależny.

(15.2.) Zamiast tworzyć odrębny organ nadzorczy, jego zadania i uprawnienia można powierzyć istniejącym instytucjom, które spełniają wymogi niniejszego ustępu lub są do nich dostosowane. W państwach członkowskich UE można do tego celu wykorzystać urzędy ochrony danych, działające na mocy odpowiednich przepisów unijnych.

(15.3.) Art. 15 ust. 3 wyszczególnia zadania organu nadzorczego. Powinien on wspierać procedurę oceny wpływu i monitorować przestrzeganie tych zasad przez organy wdrażające. Ponadto, gromadząc doświadczenia w ramach wielu ocen i obserwując rozwój sytuacji w tej dziedzinie, powinien stać się centrum wiedzy, zdolnym do dostarczania informacji i porad władzom

publicznym, zainteresowanym osobom i organizacjom oraz społeczeństwu w zakresie wykorzystania systemów przez instytucje publiczne.

(15.4.) Najważniejsze dokumenty z różnych ocen skutków powinny być stale dostępne dla opinii publicznej na stronie internetowej organu nadzorczego. Rejestr takich dokumentów ma na celu ułatwienie pracy instytucjom publicznym, które po raz pierwszy muszą ustalić obowiązek przeprowadzenia oceny lub przeprowadzić ocenę skutków, a także usprawnienie przyszłych procesów ocen oraz promowanie świadomej debaty publicznej i odpowiedzialnego korzystania z systemów. W zakresie zachowania tajemnicy art. 15 ust. 4 odnosi się do art. 13 ust. 3.

(15.5.) Art. 15 ust. 5 wymienia uprawnienia nadzorcze organu. Może on — tak z własnej inicjatywy, jak i na podstawie skargi — zbadać, czy ocena skutków lub powtórna ocena skutków wymagana na mocy tych przepisów rzeczywiście miała miejsce i czy została przeprowadzona zgodnie z nimi. Organ nadzorczy nie powinien być jednak uprawniony do kwestionowania decyzji organu wdrażającego o zastosowaniu systemu po przeprowadzeniu odpowiedniej oceny, niezależnie od jej wyniku. Organ nadzorczy powinien mieć prawo do uzyskiwania odpowiednich informacji bez względu na

ograniczenia wynikające z art. 8, jednakże w kontaktach z innymi powinien zachować poufność zgodnie z wymogami art. 8. W odpowiedzi na brak oceny lub ocenę niezgodną z prawem organ nadzorczy może wydać (niewiążące) zalecenie dla organu wdrażającego, by ów zaprzestał korzystania z systemu, a w razie potrzeby także uzyskać nakaz sądowy. Alternatywnie, w systemach prawnych, w których jest to zgodne z konstytucją, organ nadzorczy może otrzymać uprawnienia do wydania wiążącego nakazu. Organ nadzorczy (a ostatecznie również sąd) powinien mieć pewną swobodę w tolerowaniu drobnych błędów proceduralnych, które nie miały znaczenia dla wyniku oceny, lub zalecić ich naprawienie zamiast zarządzenia zaprzestania użytkowania systemu. W ramach pełnionej funkcji doradczej organ nadzorczy może wydawać wszelkiego rodzaju zalecenia, w tym takie dotyczące systemów wykorzystywanych zgodnie z prawem. Organ nadzorczy posiada również uprawnienia pomocnicze na mocy innych artykułów: uprawnienia do ustalania zakresu (jeśli jest to przewidziane w art. 5 ust. 2), uprawnienia do udostępniania i nadzorowania ekspertów przeprowadzających audyt na mocy art. 10, jak również uprawnienia do podejmowania decyzji w sprawie dostępu do informacji zgodnie z art. 8 ust. 3.

Artykuł 16: Skargi i ochrona prawna

Źródła

Artykuł 9 Konwencja z Aarhus

Uwagi

(16.1) Przepisy dotyczące ochrony prawnej stanowią standard minimalny, który może oczywiście zostać wzmocniony. Zasady te muszą być dostosowane do specyficznych procedur danego systemu prawnego. W szczególności w przypadku wystąpienia powtarzających się nieuzasadnionych skarg może zostać wprowadzony przepis zakładający szybkie rozpatrywanie ich.

(16.2.) Zapisy ustępów 1 i 2 wprowadzają możliwość złożenia skargi do organu nadzorczego (art. 15). Organ nadzorczy musi odpowiedzieć na każdą skargę, przy czym może odrzucić ją, jeżeli jest nieuzasadniona, wyraźnie bezpodstawna lub powtarzająca się. Ponadto organ nadzorczy może według własnego uznania dostosować intensywność dochodzenia do ewentualnej szkody wynikającej z domniemanego nielegalnego korzystania z systemu. W przypadku uznania skargi za uzasadnioną organ nadzorczy może

uruchomić procedurę mającą na celu naprawienie problemu (art. 15 ust. 5 lit. c) i d)) oraz informować o tym skarżącego. Zastosowanie takiego mechanizmu w dziedzinie, która jest wysoce techniczna i wymaga specjalnych umiejętności, jest kluczowe — organ nadzorczy może bowiem zostać zawiadomiony o problemie bezpośrednio przez osoby dotknięte działaniem systemu.

(16.3.) Najważniejszą kwestią jest zapewnienie możliwości odwołania się dla osób potencjalnie poszkodowanych. W przypadku decyzji indywidualnych na ogół nie stanowi to problemu, gdyż osoba, do której skierowana jest decyzja, może ją co najmniej zaskarżyć w sądzie. Jednakże w przypadku decyzji zbiorowych — np. w hipotetycznej sytuacji, gdy ASD określa strefy użytkowania gruntów w mieście — zainteresowanymi stronami są nie tylko właściciele działek, ale także inne podmioty, takie jak organizacje pozarządowe reprezentujące interesy różnych środowisk (edukacyjnych, społecznych, ekologicznych itp.), które mogą zakwestionować wdrożenie systemu.

(16.4.) Ustępy 3 i 4 stanowią, że kwestia dostępu do sądu powinna być rozumiana w sposób szeroki. Nie określono jednak żadnych szczegółowych obowiązków, aby zapewnić, że przepisy te będą mogły zostać wdrożone w różnych systemach prawnych. W tym miejscu podkreśla się rolę organizacji pozarządowych w zapewnieniu mechanizmu dochodzenia roszczeń zbiorowych wraz z dostępem do sądu po złożeniu skargi do organu nadzorczego (ust. 1).

(16.5.) W ust. 5 przypomniano niektóre z kwestii niezbędnych do zapewnienia skutecznego dostępu do wymiaru sprawiedliwości.

Europejski Instytut Prawa jest niezależną organizacją typu non-profit, powołaną w celu inicjowania, prowadzenia i wspierania badań, a także wydawania zaleceń i zapewniania praktycznych wskazówek w dziedzinie rozwoju prawa europejskiego. Instytut opiera się na bogactwie różnorodnych tradycji prawnych, zaś jego misją jest dążenie do lepszego stanowienia prawa w Europie oraz wzmocnienia europejskiej integracji w zakresie samego prawa. Poprzez swoje działania EIP stara się przyczynić do powstania bardziej dynamicznej europejskiej wspólnoty prawnej, integrującej osiągnięcia różnych kultur prawnych oraz zwiększającej wartość wiedzy porównawczej i przyjmującej prawdziwie paneuropejską perspektywę. W związku z tym praca EIP obejmuje wszystkie gałęzie prawa: materialne i proceduralne, a także prywatne i publiczne.



ELI

EUROPEAN
LAW
INSTITUTE