DZIENNIK URZĘDOWY

GENERALNEJ DYREKCJI DRÓG KRAJOWYCH I AUTOSTRAD

Warszawa, dnia czwartek, 29 września 2022 r.

Poz. 21

ZARZĄDZENIE NR 21

GENERALNEGO DYREKTORA DRÓG KRAJOWYCH I AUTOSTRAD

z dnia 28 września 2022 r.

w sprawie Polityki Ochrony Danych Osobowych w Generalnej Dyrekcji Dróg Krajowych i Autostrad

Na podstawie § 5 ust. 2 pkt 1 załącznika do zarządzenia Nr 36 Generalnego Dyrektora Dróg Krajowych i Autostrad z dnia 4 grudnia 2018 r. w sprawie ustalenia regulaminu organizacyjnego Generalnej Dyrekcji Dróg Krajowych i Autostrad[1)], w związku z art. 24 ust. 2 rozporządzenia 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 i Dz. Urz. UE L 127 z 23.05.2018, str. 2), zarządza się, co następuje:

§ 1. W Generalnej Dyrekcji Dróg Krajowych i Autostrad ustala się Politykę Ochrony Danych Osobowych, stanowiącą załącznik do zarządzenia.

---

1) Niniejsze zarządzenie zostało zmienione zarządzeniem Nr 13 Generalnego Dyrektora Dróg Krajowych i Autostrad z dnia 6 maja 2020 r. zmieniającym zarządzenie w sprawie ustalenia regulaminu organizacyjnego Generalnej Dyrekcji Dróg Krajowych i Autostrad, zarządzeniem Nr 25 Generalnego Dyrektora Dróg Krajowych i Autostrad z dnia 13 lipca 2020 r. zmieniającym zarządzenie w sprawie ustalenia regulaminu organizacyjnego Generalnej Dyrekcji Dróg Krajowych i Autostrad, zarządzeniem Nr 34 Generalnego Dyrektora Dróg Krajowych i Autostrad z dnia 17 września 2020 r. zmieniającym zarządzenie w sprawie ustalenia regulaminu organizacyjnego Generalnej Dyrekcji Dróg Krajowych i Autostrad oraz zarządzeniem Nr 39 Generalnego Dyrektora Dróg Krajowych i Autostrad z dnia 1 października 2020 r. zmieniającym zarządzenie w sprawie ustalenia regulaminu organizacyjnego Generalnej Dyrekcji Dróg Krajowych i Autostrad.

§ 2. 1. Politykę, o której mowa w § 1, stosuje się do przetwarzania danych osobowych, o którym mowa w rozporządzeniu 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 i Dz. Urz. UE L 127 z 23.05.2018, str. 2), dalej „RODO".

2. Polityka, o której mowa w § 1, może być pomocniczo stosowana również w sprawach związanych z przetwarzaniem danych osobowych, które nie jest regulowane przepisami RODO lub do którego odrębne ustawy nie przewidują obowiązku stosowania przepisów RODO.

§ 3. Niezwłocznie po dniu wejścia w życie niniejszego zarządzenia, nie później niż w terminie 5 dni roboczych, pełnomocnik ds. bezpieczeństwa informacji poinformuje wszystkich pracowników Generalnej Dyrekcji Dróg Krajowych i Autostrad o ustaleniu w Generalnej Dyrekcji Dróg Krajowych i Autostrad Polityki Ochrony Danych Osobowych, w sposób określony w § 4 ust. 4 zarządzenia Nr 23 Generalnego Dyrektora Dróg Krajowych i Autostrad z dnia 1 września 2021 r. w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Dróg Krajowych i Autostrad i określenia sposobu wprowadzania dokumentacji tego systemu, właściwy dla dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

§ 4. Zarządzenie wchodzi w życie z dniem następującym po dniu ogłoszenia.

P.O. GENERALNY DYREKTOR
DRÓG KRAJOWYCH I AUTOSTRAD

Tomasz Żuchowski

Załącznik do zarządzenia Nr 21
Generalnego Dyrektora Dróg
Krajowych i Autostrad
z dnia 28 września 2022 r.

Polityka Ochrony Danych Osobowych w Generalnej Dyrekcji Dróg Krajowych i Autostrad

Spis treści

Rozdział 1
Przepisy ogólne

§ 1.

Polityka Ochrony Danych Osobowych w Generalnej Dyrekcji Dróg Krajowych i Autostrad, zwana dalej „PODO", została opracowana na podstawie art. 24 ust. 2 rozporządzenia 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), zwanego dalej „RODO".

§ 2.

1. PODO ma na celu ustanowienie w Generalnej Dyrekcji Dróg Krajowych i Autostrad, zwanej dalej „GDDKiA", właściwego, z punktu widzenia praw i wolności osób, których dane dotyczą, poziomu ochrony danych osobowych poprzez zapewnienie realizacji zasad, o których mowa w art. 5 RODO, tj.:
   1) zgodności z prawem;
   2) rzetelności;
   3) przejrzystości;
   4) ograniczenia celu;
   5) minimalizacji danych;
   6) prawidłowości;
   7) ograniczenia okresu przechowywania.
2. Sposób zapewnienia zgodności przetwarzania danych osobowych z zasadami, o których mowa w ust. 1, podlega dokumentowaniu w celu zapewnienia rozliczalności ich realizacji.

§ 3.

1. PODO określa w szczególności:
   1) podział obowiązków i odpowiedzialności osób zobowiązanych do realizacji zadań określonych w PODO;
   2) jednolite reguły postępowania w zakresie przetwarzania danych osobowych w całej GDDKiA;
   3) sposób wdrażania środków ochrony danych osobowych zapewniających zgodność ich przetwarzania z prawem i uwzględniających wyniki analiz ryzyka dla praw i wolności osób, których dane osobowe przetwarzane są w GDDKiA;
   4) sposób zapewnienia realizacji praw osób, których dane osobowe przetwarzane są w GDDKiA.

2. Szczegółowe procedury przetwarzania i ochrony danych osobowych określa dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Dróg Krajowych i Autostrad, zwana dalej „dokumentacją SZBI", wprowadzona do stosowania w sposób określony w załączniku nr 3 do zarządzenia Nr 23 Generalnego Dyrektora Dróg Krajowych i Autostrad z dnia 1 września 2021 r. w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Dróg Krajowych i Autostrad i określenia sposobu wprowadzania dokumentacji tego systemu.
3. Przetwarzając dane osobowe w GDDKiA uwzględnia się rekomendacje, stanowiska i wytyczne:
   1) Prezesa Urzędu Ochrony Danych Osobowych, a także organu poprzedzającego – Generalnego Inspektora Ochrony Danych Osobowych;
   2) Europejskiej Rady Ochrony Danych;
   3) Europejskiego Inspektora Ochrony Danych.

§ 4.

Administratorem danych osobowych przetwarzanych w GDDKiA jest Generalny Dyrektor Dróg Krajowych i Autostrad.

§ 5.

1. Ilekroć w PODO jest mowa o:
   1) Administratorze danych – rozumie się przez to Generalnego Dyrektora Dróg Krajowych i Autostrad;
   2) czynności przetwarzania – rozumie się przez to zespół powiązanych ze sobą operacji na danych osobowych, wykonywanych przez jedną lub kilka osób, które można określić w sposób zbiorczy, w związku z celem, w jakim te operacje są podejmowane;
   3) intranetowej bazie wiedzy o ochronie danych osobowych – rozumie się przez to witrynę „Ochrona danych osobowych" opublikowaną w ramach Portalu intranetowego GDDKiA, dostępną dla pracowników GDDKiA;
   4) IOD – rozumie się przez to Inspektora Ochrony Danych w GDDKiA;
   5) koordynatorze ds. ochrony danych osobowych w Oddziale GDDKiA lub Koordynatorze – rozumie się przez to pracownika Oddziału GDDKiA, wyznaczonego przez Dyrektora Oddziału GDDKiA do koordynowania realizacji zadań w zakresie ochrony danych osobowych;
   6) operacji przetwarzania – rozumie się przez to każdą operację na danych osobowych realizowaną w ramach czynności przetwarzania, a w szczególności zbieranie lub pobieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, przeglądanie, wykorzystywanie, ujawnianie

poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

7) organie nadzorczym – rozumie się przez to Prezesa Urzędu Ochrony Danych Osobowych;

8) osobach pełniących funkcje kierownicze - rozumie się przez to Generalnego Dyrektora Dróg Krajowych i Autostrad, jego zastępców oraz Dyrektora Generalnego GDDKiA, dyrektorów oddziałów GDDKiA i ich zastępców, kierujących komórkami organizacyjnymi Centrali GDDKiA i ich zastępców;

9) osobie upoważnionej – rozumie się przez to osobę uprawnioną do przetwarzania danych osobowych poprzez nadanie jej upoważnienia do przetwarzania danych osobowych w trybie określonym w rozdziale 3 PODO;

10) Polityce Bezpieczeństwa Informacji – rozumie się przez to Politykę Bezpieczeństwa Informacji w GDDKiA wprowadzoną do stosowania na mocy zarządzenia Nr 23 Generalnego Dyrektora Dróg Krajowych i Autostrad z dnia 1 września 2021 r. w sprawie ustanowienia Systemu Zarządzania Bezpieczeństwem Informacji w Generalnej Dyrekcji Dróg Krajowych i Autostrad i określenia sposobu wprowadzania dokumentacji tego systemu;

11) zasobie teleinformatycznym – rozumie się przez to system, bazę danych, aplikację, udział sieciowy, w szczególności folder na dysku sieciowym lub w chmurze obliczeniowej, w którym przetwarza się dane.

2. Pojęcia niezdefiniowane w PODO mają znaczenie nadane im w Polityce Bezpieczeństwa Informacji w GDDKiA oraz RODO.

§ 6.

1. Wszystkie osoby upoważnione do przetwarzania danych osobowych w GDDKiA mają obowiązek stosowania PODO.

2. PODO ma zastosowanie wobec danych osobowych, których przetwarzanie regulowane jest przepisami RODO:

1) przetwarzanych w GDDKiA, będących jej własnością lub jej powierzonych w ramach umów lub porozumień z podmiotami zewnętrznymi, chyba, że umowy te lub porozumienia stanowią inaczej;

2) przetwarzanych we wszystkich obiektach i zasobach teleinformatycznych użytkowanych przez GDDKiA, jak również innych miejscach, w których realizowany jest dostęp do danych osobowych, w szczególności za pośrednictwem zdalnego korzystania z cyberprzestrzeni GDDKiA i pracy w formule BYOD.

3. PODO nie ma zastosowania do przetwarzania danych osobowych, które nie jest regulowane przepisami RODO lub do którego odrębne ustawy nie przewidują obowiązku stosowania przepisów RODO, w szczególności PODO nie ma zastosowania do przetwarzania danych osobowych na potrzeby bezpieczeństwa i obronności państwa.

4. Generalny Dyrektor Dróg Krajowych i Autostrad nie jest zobligowany do stosowania przepisów o ochronie danych osobowych w związku z zapobieganiem i zwalczeniem przestępczości.

Rozdział 2
Obowiązki i odpowiedzialność w zakresie zarządzania ochroną danych osobowych

§ 7.

Administrator danych zapewnia bezpieczeństwo danych osobowych oraz realizuje inne obowiązki wynikające z RODO i z przepisów powszechnie obowiązujących. Zadania te wykonuje samodzielnie lub powierza ich wykonanie osobom upoważnionym wskazanym w PODO, innej dokumentacji SZBI lub w pełnomocnictwach.

§ 8.

Administrator danych stosuje środki fizyczne, techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności zabezpiecza dane osobowe przechowywane, przesyłane lub w inny sposób przetwarzane przed przypadkowym lub niezgodnym z prawem zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem.

§ 9.

Osoby pełniące funkcje kierownicze w GDDKiA:

1) organizują przetwarzanie i ochronę danych osobowych w podległych im komórkach organizacyjnych;
2) zapewniają przestrzeganie przepisów o ochronie danych osobowych w podległych im komórkach organizacyjnych;
3) tworzą warunki do zapewnienia właściwego poziomu ochrony danych osobowych w podległych im komórkach, w tym poprzez stosowanie fizycznych, technicznych i organizacyjnych środków zapewniających ochronę tych danych;
4) zapewniają włączenie odpowiednio IOD i Koordynatorów do wszystkich spraw dotyczących ochrony danych osobowych na ich początkowym etapie, poprzez przekazanie im niezbędnych informacji o planowanym procesie przetwarzania danych, w tym informacji określonych w art. 38 RODO.

§ 10.

1. Do zadań kierujących komórkami organizacyjnymi należy realizacja obowiązków Administratora danych niezastrzeżonych dla innych osób, w szczególności:
   1) uwzględnianie ochrony danych osobowych w fazie projektowania i realizacji procesów zachodzących w kierowanej komórce organizacyjnej oraz stosowanie zasady domyślnej ochrony danych;
   2) identyfikowanie ryzyka naruszenia ochrony danych osobowych i naruszenia praw i wolności osób, których dane są przetwarzane w kierowanej komórce organizacyjnej, a także zarządzanie tym ryzykiem;

3) dokonywanie oceny skutków planowanych operacji przetwarzania danych osobowych dla ich ochrony oraz wnioskowanie do Administratora o uprzednie konsultacje, o których mowa w art. 36 RODO;

4) wnioskowanie o rejestrację, aktualizację lub usunięcie czynności z Rejestru czynności przetwarzania;

5) wypełnianie obowiązków informacyjnych, względem osób fizycznych, których dane przetwarzane są w GDDKiA;

6) przygotowywanie umów dotyczących powierzenia przetwarzania danych i nadzór nad ich realizacją;

7) udostępnianie danych osobowych przetwarzanych w podległej komórce organizacyjnej;

8) rozpatrywanie, w porozumieniu z IOD lub Koordynatorami, skarg, wniosków i żądań osób, których dane dotyczą w związku z przetwarzaniem ich danych osobowych;

9) nadzór nad przestrzeganiem przez podległą komórkę organizacyjną przepisów w zakresie ochrony danych osobowych.

2. Kierujący komórkami organizacyjnymi Centrali GDDKiA mogą powierzyć realizację wybranych zadań, o których mowa w ust. 1, kierującym wewnętrznymi komórkami organizacyjnymi tych komórek organizacyjnych.

§ 11.

1. Kierujący komórką właściwą w sprawach ochrony fizycznej w Centrali GDDKiA i dyrektorzy oddziałów GDDKiA zapewniają środki fizycznej ochrony danych osobowych. Szczegółowy zakres zadań w tym zakresie określa Polityka Bezpieczeństwa Fizycznego w GDDKiA.

2. Dobierając środki ochrony fizycznej danych osobowych uwzględnia się wyniki analiz ryzyka przetwarzania tych danych dla praw i obowiązków osób, których dane dotyczą.

§ 12.

1. Kierujący komórką właściwą w sprawach informatyki w Centrali GDDKiA zapewnia środki bezpieczeństwa danych osobowych przetwarzanych w systemach teleinformatycznych. Szczegółowy zakres zadań w tym zakresie określa Polityka Bezpieczeństwa Teleinformatycznego w GDDKiA.

2. Dobierając środki ochrony teleinformatycznej danych osobowych uwzględnia się wyniki analiz ryzyka przetwarzania tych danych dla praw i obowiązków osób, których dane dotyczą.

§ 13.

Osoby upoważnione realizują zadania i obowiązki określone w RODO, PODO i w pozostałej dokumentacji SZBI w odniesieniu do danych osobowych przekazanych im do przetwarzania w ramach obowiązków służbowych. W szczególności są one zobowiązane do:

1) zachowania szczególnej staranności przy przetwarzaniu danych osobowych, z uwzględnieniem zasad zgodności z prawem, rzetelności, przejrzystości, ograniczenia celu, minimalizacji danych, prawidłowości i ograniczenia przechowywania;
2) przestrzegania zasad bezpieczeństwa i ochrony informacji określonych w Polityce Bezpieczeństwa Informacji;
3) przestrzegania zasad i stosowania procedur ochrony danych osobowych określonych w PODO oraz dokumentacji SZBI;
4) przestrzegania zakresu udzielonego im upoważnienia;
5) zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczania.

§ 14.

Do zadań IOD należy:

1) monitorowanie przestrzegania przepisów RODO i innych aktów prawnych dotyczących ochrony danych osobowych, w tym prowadzenie sprawdzeń z zakresu ochrony danych osobowych;
2) monitorowanie przestrzegania regulacji wewnętrznych dotyczących ochrony danych osobowych;
3) koordynacja procesu prowadzenia sprawdzeń w Oddziałach GDDKiA;
4) szkolenie osób upoważnionych z przepisów i zasad dotyczących ochrony danych osobowych;
5) opiniowanie projektów wewnętrznych i zewnętrznych aktów prawnych, a w razie potrzeby również innych dokumentów, w zakresie ich zgodności z przepisami o ochronie danych osobowych;
6) doradzanie osobom przetwarzającym dane osobowe w GDDKiA we wszelkich sprawach związanych z ochroną danych osobowych, a także informowanie o obowiązkach spoczywających na nich na mocy przepisów Unii Europejskiej lub krajowych przepisów o ochronie danych osobowych;
7) udzielanie zaleceń co do oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych i monitorowanie jej wykonania;
8) pełnienie roli punktu kontaktowego dla organu nadzorczego i współpraca z tym organem;
9) uzgadnianie sposobu i treści odpowiedzi na wpływające do Centrali GDDKiA żądania osób fizycznych, których dane osobowe są przetwarzane w GDDKiA;
10) udzielanie Koordynatorom wsparcia w zakresie realizacji ich obowiązków, o których mowa w § 16 oraz w dokumentacji SZBI;

11) sporządzanie i przedkładanie Administratorowi danych, do dnia 31 marca każdego roku, rocznego sprawozdania o stanie ochrony danych osobowych w GDDKiA oraz realizacji zadań IOD;

12) realizacja zadań IOD w zakresie rozwiązywania naruszeń ochrony danych osobowych, zgodnie z procedurą reagowania na incydenty lub podejrzenia wystąpienia incydentu bezpieczeństwa informacji, o której mowa w Polityce Bezpieczeństwa Informacji;

13) udział w procesie analizy ryzyka przetwarzania danych osobowych poprzez realizację zadań określonych w procedurach analizy ryzyka, o których mowa w Polityce Bezpieczeństwa Informacji;

14) obsługa skrzynki poczty elektronicznej: iod@gddkia.gov.pl.

§ 15.

Do zadań wewnętrznej komórki organizacyjnej do spraw bezpieczeństwa informacji w Centrali GDDKiA należy koordynowanie funkcjonowania systemu ochrony danych osobowych w GDDKiA poprzez:

1) prowadzenie i aktualizowanie Rejestru czynności przetwarzania danych osobowych oraz rejestru kategorii czynności przetwarzania danych osobowych na podstawie informacji przekazanych przez kierowników komórek organizacyjnych;

2) opracowywanie projektów wytycznych i procedur w zakresie sposobu realizacji obowiązków wynikających z przepisów o ochronie danych osobowych;

3) opiniowanie projektów umów powierzenia przetwarzania danych i dokumentacji zamówień publicznych w zakresie ochrony danych osobowych w Centrali GDDKiA;

4) opiniowanie treści i sposobu realizacji obowiązków informacyjnych względem osób, których dane osobowe są przetwarzane w Centrali GDDKiA;

5) koordynacja sposobu realizacji obowiązku informacyjnego w GDDKiA;

6) opiniowanie udostępnienia danych osobowych przez Centralę GDDKiA, w tym w ramach dostępu do informacji publicznej;

7) prowadzenie intranetowej bazy wiedzy o ochronie danych osobowych dla pracowników GDDKiA;

8) współpraca z Koordynatorami w zakresie realizacji przez nich obowiązków, o których mowa w § 16 oraz w dokumentacji SZBI;

9) realizacja zadań w zakresie rozwiązywania naruszeń ochrony danych osobowych, zgodnie z procedurą reagowania na incydenty lub podejrzenia wystąpienia incydentu bezpieczeństwa informacji, o której mowa w Polityce Bezpieczeństwa Informacji;

10) udział w procesie analizy ryzyka przetwarzania danych osobowych poprzez realizację zadań określonych w procedurach analizy ryzyka, o których mowa w Polityce Bezpieczeństwa Informacji.

11) doradzanie pracownikom GDDKiA w ramach procesu planowania ochrony danych osobowych w fazie projektowania i domyślnej ochrony danych.

§ 16.

Do zadań Koordynatora ds. ochrony danych w Oddziale GDDKiA należy:

1) monitorowanie przestrzegania przepisów RODO i innych aktów prawnych dotyczących ochrony danych osobowych w Oddziale GDDKiA, w tym prowadzenie sprawdzeń z zakresu ochrony danych osobowych;
2) monitorowanie przestrzegania w Oddziale GDDKiA regulacji wewnętrznych dotyczących ochrony danych osobowych;
3) szkolenie osób upoważnionych w Oddziale GDDKiA z przepisów i zasad dotyczących ochrony danych osobowych;
4) opiniowanie projektów wewnętrznych aktów prawnych Oddziału GDDKiA, a także innych dokumentów w zakresie ich zgodności z przepisami o ochronie danych osobowych;
5) doradzanie osobom przetwarzającym dane osobowe w Oddziale GDDKiA we wszelkich sprawach związanych z ochroną danych osobowych, a także informowanie o obowiązkach spoczywających na nich na mocy przepisów Unii Europejskiej lub krajowych przepisów o ochronie danych osobowych;
6) uzgadnianie sposobu i treści odpowiedzi na wpływające do Oddziału GDDKiA żądania osób fizycznych, których dane osobowe są przetwarzane w Oddziale GDDKiA;
7) sporządzanie i przedkładanie Dyrektorowi Oddziału GDDKiA do dnia 31 stycznia każdego roku rocznego sprawozdania o stanie ochrony danych osobowych w Oddziale GDDKiA oraz realizacji zadań Koordynatora;
8) opiniowanie projektów umów powierzenia przetwarzania danych i dokumentacji zamówień publicznych w zakresie ochrony danych osobowych w Oddziale GDDKiA;
9) opiniowanie treści i sposobu realizacji obowiązku informacyjnego, o którym mowa w RODO względem osób których dane osobowe są przetwarzane w Oddziale GDDKiA;
10) opiniowanie udostępniania danych osobowych przez Oddział GDDKiA, w tym w ramach dostępu do informacji publicznej;
11) realizacja zadań w zakresie rozwiązywania naruszeń ochrony danych osobowych w Oddziale GDDKiA, zgodnie z procedurą reagowania na incydenty lub podejrzenia wystąpienia incydentu bezpieczeństwa informacji, o której mowa w Polityce Bezpieczeństwa Informacji;
12) udział w procesie analizy ryzyka przetwarzania danych osobowych w Oddziale GDDKiA poprzez realizację zadań określonych w procedurach analizy ryzyka, o których mowa w Polityce Bezpieczeństwa Informacji;
13) doradzanie pracownikom Oddziału GDDKiA w ramach procesu planowania ochrony danych osobowych w fazie projektowania i domyślnej ochrony danych.

Rozdział 3
Nadawanie dostępu do danych osobowych

§ 17.

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby upoważnione przez Administratora danych lub podmiot przetwarzający, zapoznane z przepisami o ochronie danych osobowych oraz zobowiązane do zachowania w tajemnicy danych osobowych i sposobów ich ochrony w GDDKiA.
2. Zasady nadawania dostępu do danych osobowych osobom upoważnionym przez podmioty przetwarzające działające na polecenie Administratora danych określają każdorazowo umowy powierzenia przetwarzania, a w zakresie w nich nieuregulowanym regulacje wewnętrzne stosowane przez podmiot przetwarzający.

§ 18.

Upoważnienia do przetwarzania danych osobowych dla:

1) pracowników zajmujących stanowisko, z którym wiąże się przetwarzanie danych osobowych – są wypełniane, przedkładane do podpisu oraz wydawane pracownikowi, przez kierującego komórką właściwą do spraw pracowniczych odpowiednio w Centrali GDDKiA lub Oddziale GDDKiA, a następnie przechowywane w aktach osobowych pracownika;
2) stażystów, praktykantów lub wolontariuszy realizujących zadania, z którymi wiąże się przetwarzanie danych osobowych – są wypełniane, przedkładane do podpisu oraz wydawane, przez kierującego komórką właściwą do spraw pracowniczych odpowiednio w Centrali GDDKiA lub Oddziale GDDKiA, a następnie przechowywane w aktach sprawy dotyczącej organizacji stażu, praktyki lub wolontariatu;
3) osób wykonujących zadania na podstawie umów cywilnoprawnych - stanowią załączniki do umowy zawieranej z tą osobą;
4) osób świadczących usługi na rzecz GDDKiA na innej podstawie – są opracowywane, przedkładane do podpisu oraz wydawane, przez kierującego komórką organizacyjną na rzecz której ta osoba wykonuje działania, a następnie przechowywane we właściwych aktach sprawy.

§ 19.

Upoważnienia do przetwarzania danych osobowych podpisuje:

1) w odniesieniu do osób zatrudnionych lub wykonujących zadania na rzecz Centrali GDDKiA – Administrator danych, Dyrektor Generalny GDDKiA lub inna osoba upoważniona przez Administratora danych;
2) w odniesieniu do osób zatrudnionych lub wykonujących zadania na rzecz Oddziału GDDKiA – Dyrektor Oddziału GDDKiA lub, w uzasadnionych przypadkach, osoba go zastępująca.

§ 20.

Upoważnienia do przetwarzania danych osobowych są wypełniane lub opracowywane z wykorzystaniem wzoru, który stanowi załącznik do PODO.

§ 21.

W przypadku wątpliwości, co do zakresu upoważnienia do przetwarzania danych osobowych, o zakresie tym decyduje kierujący komórką organizacyjną, w której osoba upoważniona jest zatrudniona na podstawie umowy o pracę lub z którą współpracuje na innej podstawie.

§ 22.

Tryb nadawania, zmiany i odbierania uprawnień dostępu do danych osobowych przetwarzanych w systemach teleinformatycznych określa Polityka Bezpieczeństwa Teleinformatycznego.

§ 23.

Kierujący komórką organizacyjną, w której zatrudniony jest pracownik lub na rzecz której wykonuje działania osoba, o której mowa w § 18 pkt 2-4, kieruje pracownika lub tę osobę na szkolenie adaptacyjne z bezpieczeństwa informacji, o którym mowa w Polityce Bezpieczeństwa Informacji.

Rozdział 4
Dopuszczalność przetwarzania danych osobowych

§ 24.

1. Przetwarzanie danych osobowych jest dopuszczalne po spełnieniu co najmniej jednej z przesłanek wymienionych w art. 6 ust. 1 RODO i z uwzględnieniem zasad, o których mowa w art. 5 RODO.
2. W przypadku zamiaru przetwarzania danych szczególnych kategorii, o których mowa w art. 9 RODO, konieczne jest spełnienie co najmniej jednej z przesłanek wymienionych w art. 6 ust. 1 RODO oraz jednej z przesłanek wymienionych w art. 9 ust. 2 RODO.
3. Przetwarzanie danych osobowych o wyrokach skazujących i naruszeniach prawa jest możliwe wyłącznie w sytuacji, gdy wymagają tego przepisy prawa.

§ 25.

1. W przypadku uznania, że przesłanką do przetwarzania danych osobowych jest zgoda osoby, której dane dotyczą, zgoda ta jest odbierana najpóźniej w chwili zbierania danych od tej osoby.
2. Zgoda może zostać odebrana w dowolnej formie, pod warunkiem, że forma ta umożliwia jednoznaczne określenie jakich danych osobowych dotyczy zgoda oraz w jakim celu mają być one przetwarzane. W szczególności zgoda może być odebrana w formie:
   1) pisemnej;
   2) elektronicznej potwierdzonej podpisem elektronicznym;
   3) dokumentowej, w rozumieniu art. 77^2 Kodeksu cywilnego;
   4) świadomego działania wyrażonego poprzez załączenie danych osobowych do pisma, e-maila lub podanie danych osobowych w rozmowie telefonicznej, która jest rejestrowana.
3. W przypadku, gdy dane osobowe przetwarzane na podstawie zgody zbierane są z inicjatywy GDDKiA, zgoda powinna zostać udzielona poprzez podpisanie formularza zgody lub zaznaczenie odpowiedniej opcji (*checkbox*) w systemie teleinformatycznym. Dopuszcza się możliwość dokumentowania faktu udzielenia zgody poprzez przechowywanie skanu podpisanego dokumentu.
4. Formularz zgody, o którym mowa w ust. 3, musi zawierać pełną treść klauzuli informacyjnej. Osoba, której dane dotyczą musi mieć możliwość zapoznania się z treścią klauzuli przed wyrażeniem zgody.
5. W przypadku odbierania zgody za pośrednictwem systemu teleinformatycznego system ten musi zapewniać rozliczalność udzielonych zgód poprzez odnotowanie co najmniej

imienia i nazwiska lub identyfikowalnego loginu osoby, wyrażającej zgodę oraz daty udzielonej zgody.

6. Niedopuszczalne jest:

   1) uznawanie za zgodę milczenia lub niepodjęcia określonego działania przez osobę, której dane dotyczą;

   2) domyślne oznaczenie opcji zgody w systemie teleinformatycznym, za pośrednictwem którego zbierane są dane osobowe.

7. Kierujący komórką organizacyjną odpowiedzialną za realizację czynności przetwarzania, w ramach której dane osobowe przetwarzane są na podstawie zgody, zapewnia rozliczalność odebranych zgód co najmniej przez okres realizacji tej czynności przetwarzania.

§ 26.

1. W przypadku uznania, że przesłanką do przetwarzania danych osobowych jest prawnie uzasadniony interes Administratora danych, kierujący komórką organizacyjną odpowiedzialną za realizację czynności przetwarzania, w ramach której, na tej podstawie, dane osobowe są przetwarzane, przeprowadza test równowagi.

2. Test równowagi polega na wykazaniu równowagi pomiędzy interesem Administratora danych a sposobem zabezpieczenia realizacji praw i wolności osoby, której dane mają być przetwarzane w ramach czynności przetwarzania, i zapewnia:

   1) identyfikację interesów Administratora danych realizowanych za pośrednictwem czynności przetwarzania oraz praw i wolności, które przetwarzanie może naruszyć;

   2) ocenę wagi interesów Administratora danych, względem zakresu gromadzonych w ramach czynności przetwarzania danych osobowych;

   3) ocenę zabezpieczeń, które Administrator danych planuje zastosować w celu ochrony praw i wolności które przetwarzanie może naruszyć.

3. W sytuacji gdy test, o którym mowa w ust. 1, wykaże brak możliwości zapewnienia równowagi pomiędzy interesem Administratora danych a sposobem zabezpieczenia realizacji praw i wolności osoby, której mają być przetwarzane, określonej czynności przetwarzania nie realizuje się.

4. Kierujący komórką organizacyjną odpowiedzialną za realizację czynności przetwarzania, w ramach której dane osobowe przetwarzane są na podstawie uzasadnionego interesu Administratora danych, zapewnia rzetelność wykonania testu równowagi i jego udokumentowanie.

5. W GDDKiA obowiązuje jednolity sposób wykonywania i dokumentowania testu równowagi określony w dokumentacji SZBI.

Rozdział 5
Ochrona danych osobowych w fazie projektowania i domyślna ochrona danych

§ 27.

Każdą nową czynność przetwarzania danych osobowych projektuje się w sposób zapewniający:

1) domyślną realizację zasad zgodności z prawem, rzetelności, przejrzystości, ograniczenia celu, minimalizacji danych, prawidłowości i ograniczenia przechowywania;
2) domyślną realizację praw osób, których dane dotyczą;
3) rozliczalność w zakresie, o którym mowa w pkt 1-2.

§ 28.

1. Przed rozpoczęciem przetwarzania danych osobowych, w ramach nowej czynności przetwarzania, kierujący komórką organizacyjną odpowiedzialną za realizację tej czynności przeprowadza analizę obejmującą co najmniej określenie:
   1) celu i podstawy prawnej przetwarzania danych osobowych;
   2) rodzajów przetwarzanych danych osobowych oraz kategorii osób, których dane dotyczą;
   3) planowanego okresu przetwarzania danych osobowych;
   4) sposobu pozyskania i przechowywania oraz zakresu operacji, jakie będą wykonywane na danych osobowych;
   5) rodzajów podmiotów, którym dane będą udostępnianie lub powierzane;
   6) sposobu realizacji obowiązku informacyjnego, o którym mowa w art. 13 i 14 RODO;
   7) ryzyk dla praw i wolności osób, których dane dotyczą i proponowanego sposobu zarządzania nimi w ramach planowanej czynności przetwarzania.
2. W sytuacji, o której mowa w § 26 ust. 1, niezbędnym elementem analizy, o której mowa w ust. 1, jest test równowagi, o którym mowa w § 26 ust. 2.
3. W GDDKiA obowiązuje jednolity sposób wykonywania i dokumentowania analizy, o której mowa w ust. 1, określony w dokumentacji SZBI.
4. Dokumentacja z wykonanej analizy stanowi podstawę wpisu nowej czynności przetwarzania do Rejestru czynności przetwarzania, o którym mowa w § 31.

§ 29.

1. Analizę, o której mowa w § 28 ust. 1, ponawia się w przypadku wprowadzenia istotnych zmian w czynności przetwarzania danych osobowych, w szczególności dotyczących:
   1) rozszerzenia zakresu przetwarzanych danych;

2) zmiany celu przetwarzania;

3) zmiany lub dodania nowej podstawy prawnej przetwarzania danych,;

4) zmiany środków organizacyjno-technicznych ochrony danych,;

5) zmiany otoczenia prawnego czynności przetwarzania;

6) a także innych wywierających wpływ na zapewnienie realizacji zasad i praw, o których mowa w § 27.

2. Dokumentacja z wykonanej analizy, o której mowa w ust. 1, stanowi podstawę aktualizacji wpisu czynności przetwarzania w Rejestrze czynności przetwarzania, o którym mowa w § 31.

Rozdział 6
Rejestrowanie czynności przetwarzania

§ 30.

1. W GDDKiA prowadzi się wspólny Rejestr czynności przetwarzania i wspólny rejestr kategorii czynności przetwarzania dla wszystkich jednostek organizacyjnych.
2. Rejestr czynności przetwarzania oraz rejestr kategorii czynności przetwarzania prowadzone są w wewnętrznej komórce organizacyjnej do spraw bezpieczeństwa informacji w Centrali GDDKiA.

§ 31.

1. W Rejestrze czynności przetwarzania zamieszcza się informacje dotyczące wszystkich czynności przetwarzania realizowanych w GDDKiA.
2. Wpis pojedynczej czynności przetwarzania w Rejestrze czynności przetwarzania zawiera co najmniej informacje o:
   1) celu przetwarzania danych osobowych;
   2) kategoriach osób i kategoriach danych osobowych jakie są przetwarzane w ramach czynności przetwarzania;
   3) podstawie prawnej przetwarzania danych osobowych;
   4) odbiorcach lub kategoriach odbiorców, którym dane osobowe mogą być przekazywane;
   5) planowanych terminach usunięcia poszczególnych kategorii danych osobowych;
   6) sposobach przetwarzania danych (papierowo, elektronicznie);
   7) ewentualnym przekazywaniu danych do państwa trzeciego lub organizacji międzynarodowych;
   8) fizycznych, technicznych i organizacyjnych środkach ochrony danych osobowych.
3. Rejestr czynności przetwarzania jest udostępniany pracownikom GDDKiA za pośrednictwem wewnętrznych elektronicznych kanałów komunikacji.

§ 32.

1. W Rejestrze kategorii czynności przetwarzania dokonuje się wpisu w każdej sytuacji, w której Generalny Dyrektor Dróg Krajowych i Autostrad przyjmuje na siebie obowiązki podmiotu przetwarzającego, w myśl art. 28 RODO.
2. Kierujący komórką organizacyjną, która zamierza przetwarzać dane osobowe w sytuacji, o której mowa w ust. 1, informuje wewnętrzną komórkę organizacyjną do spraw bezpieczeństwa informacji w Centrali GDDKiA o zawartej umowie lub innym instrumencie prawnym nakładającym na Generalnego Dyrektora Dróg Krajowych

i Autostrad obowiązki podmiotu przetwarzającego. Informacja ta stanowi podstawę wpisu do rejestru kategorii czynności przetwarzania.

3. Kierujący komórką organizacyjną w Oddziale GDDKiA przekazuje informację, o której mowa w ust. 2, za pośrednictwem Koordynatora.
4. Rejestr kategorii czynności przetwarzania zawiera co najmniej informacje o:
   1) celu przetwarzania danych osobowych;
   2) nazwie i danych kontaktowych administratora powierzającego dane;
   3) danych kontaktowych IOD administratora powierzającego dane, o ile został wyznaczony;
   4) kategoriach osób i kategoriach danych osobowych jakie są przetwarzane w ramach obowiązków, o których mowa w ust. 1;
   5) czasie na który powierzone zostały dane osobowe;
   6) ewentualnym przekazywaniu danych do państwa trzeciego lub organizacji międzynarodowych;
   7) fizycznych, technicznych i organizacyjnych środkach ochrony danych osobowych.
5. Rejestr kategorii czynności przetwarzania jest udostępniany pracownikom GDDKiA za pośrednictwem wewnętrznych elektronicznych kanałów komunikacji.

Rozdział 7
Zarządzanie ryzykiem i ocena skutków przetwarzania dla ochrony praw i wolności osób fizycznych

§ 33.

1. Przetwarzanie danych osobowych w GDDKiA odbywa się z uwzględnieniem ryzyka, jakie to przetwarzanie może wywoływać dla praw i wolności osób, których dane dotyczą.
2. Zarządzanie ryzykiem naruszenia praw i wolności osób, których dane dotyczą, ma na celu rzetelną ocenę wpływu operacji przetwarzania danych osobowych i stosowanych lub proponowanych do stosowania zabezpieczeń na prawa i wolności osoby, której dane dotyczą, na wszystkich etapach realizacji czynności przetwarzania oraz opracowanie planu postępowania ze zidentyfikowanym ryzykiem.

§ 34.

1. Analizę ryzyka przetwarzania danych osobowych dla praw i wolności osób, których dane dotyczą przeprowadza się podczas:
   1) planowania nowej czynności przetwarzania;
   2) planowania zmian w zarejestrowanej czynności przetwarzania;
   3) analizy naruszenia ochrony danych osobowych;
   4) cyklicznej analizy ryzyka, o której mowa w Polityce Bezpieczeństwa Informacji.
2. W analizie, o której mowa w ust. 1, uwzględnia się kontekst przetwarzanych danych osobowych oraz łatwość identyfikacji osoby fizycznej za pośrednictwem przetwarzanych danych.
3. Za przeprowadzenie analizy ryzyka odpowiedzialny jest:
   1) kierujący komórką organizacyjną odpowiedzialną za realizację czynności przetwarzania – w przypadkach określonych w ust. 1 pkt 1 i 2;
   2) zespół analizujący naruszenie ochrony danych osobowych – w przypadku określonym w ust. 1 pkt 3;
   3) Zespół ds. analizy ryzyka, o którym mowa w Polityce Bezpieczeństwa Informacji – w przypadku określonym w ust. 1 pkt 4.
4. Przeprowadzający analizę zapewnia udział w procesie analizy ryzyka pracownika komórki odpowiedzialnej za bezpieczeństwo informacji w GDDKiA oraz odpowiednio IOD lub Koordynatora.
5. Analizę ryzyka przeprowadza się w oparciu o procedurę, o której mowa w § 6 Polityki Bezpieczeństwa Informacji.

§ 35.

1. W sytuacji, gdy analiza ryzyka, o której mowa w § 34 ust. 1, wykaże duże prawdopodobieństwo wystąpienia wysokiego ryzyka naruszenia praw i wolności osób, których dane dotyczą oraz w przypadku planowania operacji przetwarzania wymienionej w wykazie, o którym mowa w art. 35 ust. 4 RODO, przeprowadzający analizę dokonuje oceny skutków planowanych operacji przetwarzania na ochronę danych osobowych.
2. Oceny, o której mowa w ust. 1, dokonuje się zgodnie z zaleceniami IOD.
3. W sytuacji, gdy ocena, o której mowa w ust. 1, wykaże wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą, przeprowadzający analizę wnioskuje do Administratora danych o przeprowadzenie konsultacji z organem nadzorczym. Przed podjęciem decyzji o przeprowadzeniu konsultacji z organem nadzorczym przeprowadzający analizę jest zobowiązany do wykazania przed Administratorem danych niezbędności realizacji operacji przetwarzania wskazujących na wysokie ryzyko.

Rozdział 8
Realizacja obowiązków informacyjnych

§ 36.

Obowiązki informacyjne, o których mowa w art. 13 i 14 RODO, realizuje się wobec osób fizycznych, których dane przetwarzane są w ramach czynności przetwarzania.

§ 37.

1. Obowiązki informacyjne realizuje się poprzez:
   1) publikację klauzul informacyjnych w miejscach zbierania danych od osób, których dane dotyczą;
   2) publikację klauzul informacyjnych na stronach internetowych i intranetowych GDDKiA, w tym na stronach za pośrednictwem których zbierane są dane osobowe;
   3) zamieszczenie klauzul informacyjnych we wzorach dokumentów, za pośrednictwem których zbierane są dane osobowe;
   4) przesyłanie i przekazywanie klauzul informacyjnych w korespondencji lub bezpośrednio osobom, których dane dotyczą;
   5) przekazywanie treści klauzul informacyjnych w postaci głosowej w sytuacji, gdy inny sposób ich przekazania nie jest możliwy.
2. Dopuszcza się realizację obowiązków informacyjnych w postaci warstwowej, przy czym pierwsza warstwa klauzuli informacyjnej musi zawierać bezpośrednie odesłanie do treści pełnej klauzuli informacyjnej.

§ 38.

1. Kierujący komórką organizacyjną odpowiedzialną za realizację czynności przetwarzania opracowuje treść klauzul informacyjnych w ramach analizy, o której mowa w § 28 ust. 1.
2. Treść klauzul informacyjnych może być modyfikowana w każdym czasie, w szczególności w przypadku stwierdzenia ich niepoprawności lub nieaktualności w całości lub części.
3. Treść klauzul opracowuje się zgodnie ze wzorem opublikowanym w intranetowej bazie wiedzy o ochronie danych osobowych dla pracowników GDDKiA.
4. Dla czynności przetwarzania powtarzalnych lub realizowanych w sposób ciągły stosuje się klauzule informacyjne opublikowane w intranetowej bazie wiedzy o ochronie danych osobowych.

§ 39.

Treść klauzul informacyjnych innych niż wymienione w § 38 ust. 4, modyfikacje dotychczas stosowanych klauzul oraz sposób realizacji obowiązku informacyjnego kierujący komórką

organizacyjną odpowiedzialną za realizację czynności przetwarzania uzgadnia z komórką do spraw bezpieczeństwa informacji w Centrali GDDKiA lub Koordynatorem.

Rozdział 9
Przekazywanie danych osobowych podmiotom zewnętrznym

§ 40.

Dane osobowe są udostępniane na wniosek osoby, której dane dotyczą, w ramach przysługującego jej prawa dostępu do danych i w trybie, o którym mowa w Rozdziale 11.

§ 41.

1. Dane osobowe mogą być udostępniane innemu niż określony w § 40 podmiotowi zewnętrznemu, o ile podmiot ten wykaże posiadanie podstawy prawnej do przetwarzania określonego zakresu danych osobowych.
2. Udostępnienia danych osobowych, o którym mowa w ust. 1, dokonuje kierujący komórką organizacyjną odpowiedzialną za współpracę z podmiotem zewnętrznym, na wniosek tego podmiotu i po potwierdzeniu istnienia podstawy prawnej, o której mowa w ust. 1.
3. Udostępnienia danych osobowych można dokonać w trybie bezwnioskowym wyłącznie w przypadku, gdy stanowi o tym przepis prawa lub umowa, albo inny instrument prawny wiążący GDDKiA z podmiotem, o którym mowa w ust. 1.

§ 42.

Przed rozpoczęciem współpracy z podmiotem zewnętrznym, z którą wiąże się przetwarzanie danych osobowych, kierujący komórką organizacyjną odpowiedzialną za tę współpracę dokonuje ustalenia ról, jakie pełnią strony w zakresie przetwarzania danych osobowych, w szczególności ustala:

1) która strona (strony) i w jakim zakresie pełni rolę administratora danych,
2) która strona (strony) i w jakim zakresie pełni rolę podmiotu przetwarzającego,
3) czy strony pełnią role współadministratorów danych osobowych.

§ 43.

1. Dane osobowe są powierzane podmiotowi zewnętrznemu w przypadku, gdy podmiot ten wykonuje w imieniu i na rzecz GDDKiA zadania związane z przetwarzaniem danych osobowych.
2. Powierzenie przetwarzania może nastąpić wyłącznie w drodze umowy zawartej w formie pisemnej, dokumentowej lub elektronicznej, pomiędzy podmiotem przetwarzającym, a Administratorem danych. Administratora danych oraz podmiot przetwarzający mogą reprezentować osoby odpowiednio umocowane.
3. Projekt umowy powierzenia przetwarzania opracowuje kierujący komórką organizacyjną odpowiedzialną za zlecenie podmiotowi zewnętrznemu zadania, o którym mowa w ust. 1. Projekt umowy powierzenia przetwarzania opracowuje się

zgodnie ze wzorem opublikowanym w intranetowej bazie wiedzy o ochronie danych osobowych dla pracowników GDDKiA.

4. Projekt umowy powierzenia przetwarzania danych osobowych wymaga zaopiniowania odpowiednio przez komórkę do spraw bezpieczeństwa informacji w Centrali GDDKiA, albo Koordynatora.

5. Komórka organizacyjna GDDKiA prowadzi rejestr powierzeń przetwarzania danych osobowych. Rejestr zawiera:

   1) nazwy i dane kontaktowe podmiotów przetwarzających;

   2) cel i zakres powierzanych danych osobowych;

   3) wykaz operacji przetwarzania powierzonych w ramach umowy powierzenia;

   4) daty zawarcia umów powierzenia;

   5) informacje dotyczące podpowiedzenia danych.

§ 44.

1. Dane osobowe mogą być przetwarzane wspólnie z podmiotem zewnętrznym w ramach współadministrowania.

2. W sytuacji gdy Generalny Dyrektor Dróg Krajowych i Autostrad wraz z innym podmiotem zamierzają współadministrować danymi osobowymi, kierujący komórką organizacyjną odpowiedzialną za współpracę z tym podmiotem opracowuje umowę lub porozumienie o współadministrowaniu.

3. Umowa lub porozumienie, o którym mowa w ust. 2, zawiera postanowienia dotyczące podziału zadań i odpowiedzialności pomiędzy stronami w zakresie zapewnienia zgodności przetwarzania danych osobowych z przepisami prawa.

4. Treść umowy lub porozumienia, o którym mowa w ust. 2, wymaga zaopiniowania przez komórkę do spraw bezpieczeństwa informacji w Centrali GDDKiA.

Rozdział 10
Retencja danych osobowych

§ 45.

1. Planowany okres przechowywania danych osobowych ustala się w procesie projektowania nowej czynności przetwarzania, o którym mowa w Rozdziale 5, z uwzględnieniem ust. 2 i 3.
2. Dane osobowe przetwarzane w aktach spraw podlegają archiwizacji wraz z aktami tych spraw. Szczegółowe zasady dotyczące archiwizacji reguluje instrukcja kancelaryjna.
3. Dane osobowe przetwarzane w ramach zbiorów nietworzących akt sprawy przechowywane są do czasu ustania celu, dla którego zostały zebrane lub do chwili, gdy są już zbędne do osiągnięcia tego celu.

§ 46.

1. Procedurę usuwania danych osobowych po upływie okresu ich przetwarzania ustala się indywidualnie dla każdej czynności przetwarzania, mając na uwadze sposoby zbierania i przechowywania danych osobowych w ramach tej czynności. W szczególności dane osobowe usuwa się poprzez anonimizację dokumentów lub nadpisanie danych przetwarzanych w systemach teleinformatycznych.
2. Kierujący komórką organizacyjną realizującą czynność przetwarzania, nie rzadziej niż raz na 2 lata zarządza przegląd zbiorów nie tworzących akt sprawy w celu usunięcia z nich danych osobowych, dla których ustał cel ich przetwarzania.

Rozdział 11
Realizacja praw osób, których dane dotyczą

§ 47.

Kierujący komórką organizacyjną Centrali GDDKiA oraz Dyrektor Oddziału GDDKiA, każdy w swoim zakresie, są zobowiązani do odpowiadania na żądania osób fizycznych, których dane są przetwarzane w związku z realizacją czynności przetwarzania w podległych im komórkach organizacyjnych.

§ 48.

1. W przypadku zgłoszenia przez osobę, której dane dotyczą, żądania dostępu do danych osobowych, które jej dotyczą, kierujący komórką organizacyjną realizującą czynność przetwarzania, w ramach której przetwarzane są te dane niezwłocznie podejmuje decyzję co do sposobu udostępnienia danych i ustala treść odpowiedzi.
2. Realizując prawo dostępu, o którym mowa w ust. 1, uwzględnia się prawo do prywatności innych osób, których dane są przetwarzane w związku z przetwarzaniem danych osoby żądającej dostępu do danych.

§ 49.

1. W przypadku zgłoszenia przez osobę, której dane dotyczą, żądania usunięcia lub ograniczenia przetwarzania jej danych osobowych lub sprzeciwu wobec przetwarzania jej danych osobowych, kierujący komórką organizacyjną realizującą czynność przetwarzania, w ramach której przetwarzane są te dane niezwłocznie podejmuje decyzję co do sposobu postępowania z tymi danymi i ustala treść odpowiedzi.
2. W przypadku, gdy dane, których dotyczy żądanie lub sprzeciw, o których mowa w ust. 1, przetwarzane są w systemie teleinformatycznym, sposób odpowiedzi na żądanie lub sprzeciw ustala się z właścicielem systemu oraz ASI merytorycznym.
3. Sposoby odpowiedzi na żądania, o których mowa w ust. 1., każdorazowo uzgadniane są odpowiednio z IOD lub Koordynatorem.
4. Udzielenie odpowiedzi na żądania, o których mowa w ust. 1, odbywa się na zasadach i w terminach określonych w art. 12 RODO.

Rozdział 12
Postępowanie w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych

§ 50.

1. Każdy pracownik GDDKiA jest zobowiązany do:
   1) natychmiastowego zgłaszania dostrzeżonych naruszeń ochrony danych osobowych oraz podejrzeń naruszenia ochrony tych danych;
   2) powstrzymania się od działań mogących spowodować zatarcie śladów, bądź dowodów naruszenia do chwili ich zebrania przez osoby obsługujące naruszenie;
   3) aktywnego włączania się w proces obsługi naruszenia, w szczególności niezwłocznego udzielania informacji i wyjaśnień dotyczących dostrzeżonego naruszenia osobom obsługującym naruszenie.
2. Informacje dotyczące naruszeń ochrony danych osobowych stwierdzonych w GDDKiA stanowią informację wewnętrzną i mogą być przekazywane poza struktury GDDKiA wyłącznie przez osoby do tego upoważnione.

§ 51.

Szczegółowe zasady zgłaszania oraz obsługi naruszeń ochrony danych osobowych określają procedury reagowania na incydenty lub podejrzenia wystąpienia incydentu bezpieczeństwa informacji, o których mowa w § 12 Polityki Bezpieczeństwa Informacji.

Rozdział 13
Monitorowanie zgodności przetwarzania danych osobowych z przepisami

§ 52.

1. Monitorowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz PODO jest zadaniem IOD oraz Koordynatorów.
2. Monitorowanie, o którym mowa w ust. 1, odbywa się w szczególności w formie sprawdzeń planowych lub doraźnych.
3. IOD przy udziale Koordynatorów opracowuje plan sprawdzeń na dany rok kalendarzowy i przedkłada go do wiadomości Administratora danych do końca stycznia danego roku.

§ 53.

1. IOD przeprowadza sprawdzenia planowe w Centrali GDDKiA i koordynuje proces sprawdzeń planowych w Oddziałach GDDKiA.
2. IOD przeprowadza sprawdzenia doraźne samodzielnie lub zleca ich przeprowadzenie Koordynatorom.
3. Sprawdzenia mogą być przeprowadzane przy wsparciu specjalistycznych podmiotów zewnętrznych.

§ 54.

1. Przeprowadzający sprawdzenie ma prawo do:
   1) wstępu do pomieszczeń, w których są przetwarzane dane osobowe w obecności osoby zajmującej to pomieszczenie lub powołanej komisji;
   2) żądania, w zakresie niezbędnym do przeprowadzenia sprawdzenia, złożenia pisemnych lub ustnych wyjaśnień oraz okazania dokumentów i wykonania ich kopii przez osoby przetwarzające dane osobowe;
   3) przeprowadzania oględzin urządzeń, nośników informacji i systemów informatycznych służących do przetwarzania danych osobowych.
2. Osoba przetwarzająca dane, których dotyczy sprawdzenie, ma obowiązek niezwłocznie udzielić informacji i wyjaśnień, o których mowa w ust. 1 pkt 2.

§ 55.

1. Z przeprowadzonego sprawdzenia sporządza się sprawozdanie zawierające w szczególności przedmiot sprawdzenia, stwierdzone nieprawidłowości i propozycje działań korygujących.
2. Koordynatorzy uzgadniają zakres sprawozdania z IOD.
3. Sprawozdanie przedkłada się kierującemu komórką organizacyjną, w której realizowano sprawdzenie, Pełnomocnikowi ds. Bezpieczeństwa Informacji oraz:

1) Dyrektorowi Generalnemu GDDKiA – w przypadku sprawdzeń w Centrali GDDKiA,

2) Dyrektorowi Oddziału – w przypadku sprawdzenia w Oddziale GDDKiA.

4. W przypadku stwierdzenia nieprawidłowości osoby, o których mowa w ust. 3 pkt 1 i 2, decydują o podjęciu działań korygujących i określają termin przywrócenia przetwarzania danych osobowych do stanu zgodnego z prawem.

5. Kierujący komórką organizacyjną, w której stwierdzono nieprawidłowości, informuje odpowiednio IOD lub Koordynatora oraz Pełnomocnika ds. Bezpieczeństwa Informacji o realizacji działań korygujących niezwłocznie po ich wdrożeniu.

Rozdział 14
Środki ochrony danych osobowych

§ 56.

Ochronę danych osobowych w GDDKiA zapewnia się poprzez zastosowanie:

1) środków organizacyjnych;
2) środków bezpieczeństwa fizycznego;
3) środków bezpieczeństwa teleinformatycznego.

§ 57.

1. Zastosowane środki ochrony danych osobowych uwzględniają stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania danych.
2. Przy doborze środków ochrony danych osobowych uwzględnia się wyniki analiz ryzyka, o których mowa w Rozdziale 7.
3. Ogólny opis środków ochrony danych osobowych właściwych dla danej czynności przetwarzania umieszcza się w Rejestrze czynności przetwarzania.

§ 58.

Do środków organizacyjnych zalicza się w szczególności:

1) wyznaczenie IOD w Centrali GDDKiA oraz wyznaczenie koordynatorów ds. ochrony danych osobowych w Oddziałach GDDKiA;
2) monitorowanie przestrzegania przepisów o ochronie danych osobowych;
3) dopuszczanie do przetwarzania danych osobowych wyłącznie osób posiadających upoważnienie;
4) zapewnianie zapoznania osób przetwarzających dane osobowe z przepisami o ochronie danych osobowych;
5) zobowiązanie osób przetwarzających dane osobowe do zachowania danych osobowych w tajemnicy;
6) niszczenie dokumentów zawierających dane osobowe po ustaniu ich przydatności, za pomocą mechanicznych niszczarek dokumentów;
7) zakaz pozostawiania bez nadzoru dokumentów zawierających dane osobowe.

§ 59.

Środki bezpieczeństwa teleinformatycznego danych osobowych określa Polityka Bezpieczeństwa Teleinformatycznego.

§ 60.

Środki bezpieczeństwa fizycznego danych osobowych określa Polityka Bezpieczeństwa Fizycznego.

Rozdział 15
Postanowienia końcowe

§ 61.

1. W sprawach nieuregulowanych w PODO zastosowanie mają przepisy RODO.
2. PODO podlega regularnym przeglądom, nie rzadziej niż w terminie przeglądów Systemu Zarzadzania Bezpieczeństwem Informacji, o których mowa w Polityce Bezpieczeństwa Informacji.
3. Wszelkie zmiany PODO są procedowane zgodnie z zasadami prowadzenia prac legislacyjnych w GDDKiA.

Załącznik

WZÓR

GENERALNY DYREKTOR
DRÓG KRAJOWYCH I AUTOSTRAD

Miejscowość, data ……..

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 oraz art. 32 ust. 4 rozporządzenia 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, Generalny Dyrektor Dróg Krajowych i Autostrad, jako Administrator Danych, upoważnia Panią/Pana

……

(imię, nazwisko)

do przetwarzania danych osobowych w formie papierowej lub elektronicznej, w zakresie niezbędnym do[1]:

1) realizacji zadań służbowych, zgodnie z zakresem czynności, oraz powierzonych jednorazowo lub na stałe przez przełożonego *(w przypadku pracowników)*;
2) realizacji zadań wynikających z: ……. *(w przypadku stron umów cywilnoprawnych, osób zaangażowanych do współpracy z GDDKiA na podstawie innych dokumentów)*;
3) realizacji zadań w ramach odbywanego stażu *(w przypadku stażystów)*;
4) realizacji zadań w ramach odbywanych praktyk *(w przypadku praktykantów*);

[1] niepotrzebne wykreślić

5) realizacji zadań w ramach świadczenia usług wolontarystycznych *(w przypadku wolontariuszy).*

Dla potrzeb realizacji zadań, upoważniam Panią/Pana do przetwarzania danych osobowych, z zachowaniem pełnej ich ochrony, przy zastosowaniu środków organizacyjnych oraz środków bezpieczeństwa fizycznego i teleinformatycznego wdrożonych w GDDKiA.

Upoważnienie jest ważne przez okres świadczenia pracy (*w przypadku pracowników*)/ od dnia …. do dnia …… (*w przypadku innych osób niż pracownicy*).

……

(podpis Administratora Danych

lub osoby umocowanej do nadania upoważnienia)

Przyjmuję do wiadomości i stosowania, a także zobowiązuję się do zachowania danych osobowych w tajemnicy.

……

(data i podpis osoby upoważnionej)