DZIENNIK URZĘDOWY

MINISTRA FUNDUSZY I POLITYKI REGIONALNEJ

Warszawa, dnia 17 stycznia 2022 r.

Poz. 1

ZARZĄDZENIE

MINISTRA FUNDUSZY I POLITYKI REGIONALNEJ[1)]

z dnia 14 stycznia 2022 r.

w sprawie Polityki ochrony danych osobowych w Ministerstwie Funduszy i Polityki Regionalnej

Na podstawie art. 34 ust. 1 ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów (Dz. U. z 2021 r. poz. 178, 1192, 1535 i 2105) zarządza się, co następuje:

§ 1. W Ministerstwie Funduszy i Polityki Regionalnej wprowadza się Politykę ochrony danych osobowych, stanowiącą załącznik do zarządzenia.

§ 2. Pełnomocnicy i koordynatorzy wyznaczeni na mocy zarządzenia Ministra Finansów, Inwestycji i Rozwoju z dnia 3 października 2019 r. w sprawie Polityki ochrony danych osobowych w Ministerstwie Inwestycji i Rozwoju (Dz. Urz. Min. Fin., Inw. i Roz. poz. 5) są pełnomocnikami i koordynatorami w rozumieniu niniejszego zarządzenia.

§ 3. Upoważnienia do przetwarzania danych osobowych wydane przed dniem wejścia w życie niniejszego zarządzenia pozostają w mocy.

§ 4. Użytkownicy, w terminie 14 dni od dnia wejścia w życie zarządzenia albo 14 dni od dnia nawiązania stosunku prawnego zobowiązującego ich do stosowania zarządzenia, potwierdzają zapoznanie się z jego treścią na piśmie lub w innej formie, która w sposób jednoznaczny zapewni potwierdzenie tego faktu w zakresie spełnienia zasady rozliczalności. Dyrektor komórki organizacyjnej właściwej do spraw koordynacji ochrony danych osobowych określi sposób i formę potwierdzenia czynności zapoznania się z treścią zarządzenia.

[1)] Minister Funduszy i Polityki Regionalnej kieruje działem administracji rządowej – rozwój regionalny, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 27 października 2021 r. w sprawie szczegółowego zakresu działania Ministra Funduszy i Polityki Regionalnej (Dz. U. poz. 1948).

§ 5. Traci moc zarządzenie Ministra Finansów, Inwestycji i Rozwoju z dnia 3 października 2019 r. w sprawie Polityki ochrony danych osobowych w Ministerstwie Inwestycji i Rozwoju (Dz. Urz. Min. Fin., Inw. i Roz. poz. 5).

§ 6. Zarządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

MINISTER

FUNDUSZY I POLITYKI REGIONALNEJ

Załącznik do zarządzenia
Ministra Funduszy i Polityki Regionalnej
z dnia 14 stycznia 2022 r. (poz. 1)

POLITYKA OCHRONY DANYCH OSOBOWYCH

Rozdział 1

Postanowienia ogólne

§ 1. 1. Polityka ochrony danych osobowych, zwana dalej „Polityką”, określa zasady przetwarzania danych osobowych, dla których minister właściwy do spraw rozwoju regionalnego, zwany dalej „Ministrem”, jest administratorem, zarówno w Ministerstwie Funduszy i Polityki Regionalnej, zwanym dalej „Ministerstwem”, jak i poza jego siedzibą.

2. Politykę stosuje się do danych osobowych przetwarzanych:

1) w sposób całkowicie lub częściowo zautomatyzowany, w szczególności w systemie Elektronicznego Zarządzania Dokumentacją, zwanym dalej „EZD”, innych systemach teleinformatycznych, poczcie elektronicznej, informatycznych nośnikach danych;
2) w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych oraz dokumentach Ministerstwa, stanowiących zbiory danych w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 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 r., str. 1, Dz. Urz. UE L 127 z 23.05.2018 r., str. 2 oraz Dz. Urz. UE L 74 z 04.03.2021 r., str. 35), zwanego dalej „RODO”.

3. Politykę stosuje się także do przetwarzanych w Ministerstwie danych osobowych, których administratorem nie jest Minister, chyba że zawarte przez Ministra porozumienia z administratorami danych stanowią inaczej.

4. Ochronie podlegają wszelkie informacje zawierające dane osobowe przetwarzane w ramach realizacji celów Ministerstwa. Ochrona danych jest adekwatna do zagrożeń, dane osobowe zabezpiecza się w sposób uwzględniający potencjalne ryzyka dla interesów i praw osób, których dane dotyczą.

5. Ze względu na specyfikę przetwarzania danych osobowych w programach operacyjnych oraz w Centralnym systemie teleinformatycznym (CST) wspierającym realizację programów operacyjnych oraz CST2021 wspierającym realizację programów Funduszy Europejskich (FE), Krajowego Planu

Odbudowy i Zwiększania Odporności (KPO) i pobrexitowej rezerwy dostosowawczej, dopuszcza się uregulowanie zasad przetwarzania danych osobowych w powyższych obszarach w odrębnych regulacjach wewnętrznych, które muszą uwzględniać postanowienia Polityki.

6. Regulacje, o których mowa w ust. 5, mają charakter przepisów szczególnych wobec Polityki oraz wydanych na jej podstawie wytycznych, metodyk, instrukcji, zaleceń i wzorów dokumentów, a także wdrożonych w Ministerstwie standardowych środków organizacyjnych i technicznych przetwarzania danych osobowych.

7. Zasady oraz zakres obowiązków i odpowiedzialności użytkowników systemów teleinformatycznych w zakresie ochrony danych osobowych określają odrębne przepisy, w tym dedykowane im regulacje z zakresu bezpieczeństwa informacji i ochrony danych osobowych.

8. Dyrektor komórki organizacyjnej właściwej do spraw koordynacji ochrony danych osobowych może dopuścić stosowanie w Ministerstwie regulacji, w tym w szczególności polityk, regulaminów, metodyk, instrukcji zarządzania systemami informatycznymi przetwarzającymi dane osobowe dla wyodrębnionych systemów informatycznych, o ile będą one zgodne z Polityką. Użytkownicy tych systemów mają obowiązek zapoznania się z tymi regulacjami.

§ 2. Celem Polityki jest zapewnienie ochrony interesów osób, których dane osobowe przetwarzane są w Ministerstwie lub dla których Minister jest administratorem, a w szczególności zapewnienie, aby dane te były:

1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
2) zbierane i przetwarzane dla oznaczonych, zgodnych z prawem celów i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
3) merytorycznie poprawne i adekwatne w stosunku do celu przetwarzania;
4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania;
5) chronione przed niedozwolonym lub niezgodnym z prawem przetwarzaniem;
6) przetwarzane przez osoby upoważnione.

§ 3. 1. Przetwarzanie danych osobowych w Ministerstwie odbywa się zgodnie z:

1) RODO;
2) ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781), zwaną dalej „UODO”.

2. Przetwarzając dane osobowe w Ministerstwie uwzględnia się rekomendacje, stanowiska i wytyczne:

1) Prezesa Urzędu Ochrony Danych Osobowych oraz organu poprzedzającego, w zakresie w jakim pozostają aktualne;
2) Europejskiej Rady Ochrony Danych oraz w zakresie, w jakim pozostają aktualne - Grupy Roboczej powołanej na mocy art. 29 Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.;
3) ministra właściwego do spraw informatyzacji, realizującego zadania w zakresie kształtowania polityki państwa w zakresie ochrony danych osobowych;
4) Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa (ENISA).

§ 4. Dokumentacja opisująca sposób przetwarzania danych osobowych oraz sposoby ich zabezpieczenia, w tym w systemach informatycznych służących do przetwarzania danych osobowych w Ministerstwie, stanowi informacje wrażliwe.

Rozdział 2

Definicje

§ 5. 1. Użyte w Polityce określenia i skróty oznaczają:

1) analiza DPIA – ocenę skutków planowanych czynności lub operacji przetwarzania dla ochrony danych osobowych, której dokonuje administrator, jeżeli dany rodzaj przetwarzania, w szczególności z użyciem nowych technologii, ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych; przeprowadzenie takiej analizy wymagane jest w przypadkach określonych w art. 35 ust. 3 RODO, oraz danych rodzajów przetwarzania, które zostały wskazane w wykazie podanym do publicznej wiadomości przez krajowy organ nadzorczy, zgodnie z art. 35 ust. 4 RODO;
2) analiza ryzyka naruszenia praw lub wolności osób fizycznych – analizę możliwości nieosiągnięcia celów ochrony danych osobowych lub braku możliwości zapewnienia ochrony danych osobowych na akceptowalnym poziomie;
3) BA – komórkę organizacyjną właściwą do spraw ochrony fizycznej;
4) BPB – komórkę organizacyjną właściwą do spraw koordynacji ochrony danych osobowych;
5) BZL – komórkę organizacyjną właściwą do spraw szkoleń;
6) członek kierownictwa Ministerstwa – Ministra, sekretarzy stanu i podsekretarzy stanu oraz dyrektora generalnego;
7) DI – komórkę organizacyjną właściwą do spraw informatyki;

8) dyrektor – dyrektora departamentu, biura, osobę kierującą komórką organizacyjną, szefa Gabinetu Politycznego Ministra;
9) dyrektor generalny – Dyrektora Generalnego Ministerstwa;
10) intranet – wewnętrzny serwis informacyjny Ministerstwa;
11) IOD – Inspektora Ochrony Danych, czyli pracownika Ministerstwa wyznaczonego przez Administratora, nadzorującego i kontrolującego przestrzeganie zasad ochrony danych osobowych w Ministerstwie;
12) koordynator do spraw ochrony danych osobowych – osobę wyznaczoną przez dyrektora w celu wsparcia realizacji zadań z zakresu ochrony danych osobowych w komórce organizacyjnej;
13) komórka organizacyjna – departament, biuro, Gabinet Polityczny Ministra;
14) komunikat PUODO – wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych wydany przez Prezesa Urzędu Ochrony Danych Osobowych na podstawie art. 54 ust. 1 pkt 1 UODO, w związku z art. 35 ust. 4 RODO;
15) operacja przetwarzania danych osobowych – zbiór czynności przetwarzania danych osobowych;
16) pełnomocnik do spraw ochrony danych osobowych – osobę wyznaczoną przez członka kierownictwa Ministerstwa do wykonywania określonych w Polityce zadań z zakresu ochrony danych osobowych w komórce organizacyjnej lub obszarze wskazanym przez administratora;
17) podwyższony poziom ryzyka – poziom ryzyka naruszenia praw i wolności osób fizycznych, w którym następuje warunkowa akceptacja ryzyka z jednoczesnym podjęciem działań w celu jego ograniczenia; jest to poziom ryzyka nieakceptowalnego;
18) pracownik – osobę zatrudnioną w Ministerstwie na podstawie stosunku pracy;
19) privacy by default – zasadę prywatności w ustawieniach domyślnych, polegającą na uwzględnieniu ochrony danych osobowych w ustawieniach domyślnych każdego programu (systemu) teleinformatycznego; zmiana tego ustawienia powinna następować jedynie na wyraźne żądanie gestora programu (systemu);
20) privacy by design – zasadę prywatności w fazie projektowania, uwzględniającą ochronę danych osobowych w fazie projektowania, zakładającą przetwarzanie danych osobowych w taki sposób, aby od samego początku istnienia każdego projektu ochrona prywatności stanowiła jego część składową;
21) ryzyko akceptowalne – poziom ryzyka naruszenia praw i wolności osób fizycznych, który jest akceptowany w procesie formalnego szacowania ryzyka;
22) ryzyko nieakceptowalne – poziom ryzyka naruszenia praw i wolności osób fizycznych, który nie może zostać zaakceptowany bez podjęcia skutecznych działań ograniczających ryzyko do poziomu akceptowalnego, a w przypadku braku możliwości ograniczenia tego ryzyka należy

zrezygnować z tych operacji przetwarzania, które są głównym źródłem wysokiego ryzyka; proces szczegółowo określa odrębna metodyka;

23) użytkownik – pracownika, stażystę, wolontariusza, praktykanta lub inną osobę wykonującą pracę albo świadczącą usługi na rzecz Ministra lub Ministerstwa, albo powołaną przez członka kierownictwa Ministerstwa do wykonywania określonych czynności, w tym członka zespołu lub komisji;

24) wysoki poziom ryzyka – poziom ryzyka naruszenia praw i wolności osób fizycznych, wymagający formalnie przeprowadzenia oceny DPIA i ograniczenia ryzyka do poziomu akceptowalnego, a w przypadku braku takiej możliwości, wymagający konsultacji z Prezesem Urzędu Ochrony Danych Osobowych; jakościowa miara poziomu ryzyka obejmuje następujące wartości: brak ryzyka (ryzyko niskie), ryzyko (średnie), poważne ryzyko (podwyższone) oraz wysokie ryzyko; skalę ryzyka określa szczegółowo odrębna metodyka; jest to poziom ryzyka nieakceptowalnego;

2. Dla niezdefiniowanych pojęć przyjmuje się ich znaczenie przedstawione w Polityce bezpieczeństwa informacji i RODO.

Rozdział 3

Zasady i organizacja przetwarzania danych osobowych

§ 6. 1. Przed rozpoczęciem przetwarzania danych osobowych dyrektor dokonuje analizy planowanej czynności przetwarzania, która obejmuje w szczególności określenie:

1) celu i podstawy prawnej przetwarzania danych osobowych;
2) rodzajów przetwarzanych danych osobowych oraz kategorii osób, których dane dotyczą;
3) okresu przetwarzania danych osobowych;
4) sposobu pozyskania i przechowywania danych osobowych oraz rodzajów podmiotów, którym dane te będą udostępnianie;
5) sposobu realizacji obowiązku informacyjnego, o którym mowa w art. 13 i 14 RODO.

2. Dyrektor, dokonując analizy, o której mowa w ust. 1, uwzględnia:

1) zasady określone w art. 5 RODO, w tym zasadę minimalizacji danych;
2) zasady: privacy by design oraz privacy by default.

§ 7. 1. Dyrektor, we współpracy z dyrektorami BPB, DI oraz BA, dokonuje analizy ryzyka naruszenia praw lub wolności osób fizycznych, a w przypadku, gdy jest to konieczne, również analizy DPIA, zgodnie z metodyką sporządzania tych analiz.

2. W przypadku, gdy w wyniku dokonania analizy ryzyka nie zostanie zidentyfikowany podwyższony lub wysoki poziom ryzyka (czyli ryzyko jest akceptowalne), dyrektor wdraża

standardowe środki organizacyjne i techniczne przetwarzania danych osobowych, z uwzględnieniem § 1 ust. 5 i 6, a następnie rozpoczyna przetwarzanie danych osobowych.

3. W przypadku, gdy w wyniku przeprowadzenia analizy ryzyka zidentyfikowany zostanie podwyższony lub wysoki poziom ryzyka (czyli ryzyko jest nieakceptowalne), dyrektor, we współpracy z dyrektorem BPB, DI i BA oraz IOD:

1) określa i wdraża dodatkowe środki organizacyjne i techniczne przetwarzania danych osobowych;
2) wykonuje inne czynności zmierzające do obniżenia poziomu ryzyka lub
3) przedstawia właściwemu członkowi kierownictwa Ministerstwa wniosek o akceptację poziomu ryzyka wraz z uzasadnieniem.

4. W przypadku, gdy w wyniku przeprowadzenia analizy ryzyka zidentyfikowany zostanie podwyższony lub wysoki poziom ryzyka (ryzyko nieakceptowalne), a także w przypadkach, o których mowa w art. 35 RODO i komunikacie PUODO, dyrektor, we współpracy z dyrektorem BPB, DI i BA oraz IOD, dokonuje analizy DPIA.

5. Analizę ryzyka naruszenia praw lub wolności osób fizycznych oraz analizę DPIA ponawia się nie rzadziej niż raz w roku oraz w przypadku wprowadzenia istotnych zmian w czynności przetwarzania danych osobowych, w szczególności dotyczących:

1) rozszerzenia zakresu przetwarzanych danych osobowych;
2) zmiany celu przetwarzania danych osobowych;
3) zmiany podstawy prawnej przetwarzania danych osobowych;
4) zmiany środków organizacyjno-technicznych;
5) zmiany otoczenia prawnego.

6. Dyrektor dokumentuje wykonanie czynności, o których mowa w ust. 1-5 oraz § 6 ust. 1i 2.

Rozdział 4

Udostępnienie danych osobowych

§ 8. 1. Dane osobowe przetwarzane w Ministerstwie mogą być przekazywane innym podmiotom przez udostępnienie.

§ 9. 1. Udostępnienie danych osobowych odbywa się na podstawie obowiązujących przepisów prawa powszechnie obowiązującego albo wiążących umów lub porozumień, zawartych między Ministerstwem a podmiotem zewnętrznym.

2. Dane udostępnia się na wniosek uprawnionego podmiotu albo na podstawie umowy lub porozumienia.

3. W przypadku udostępnienia danych osobowych na podstawie umowy/porozumienia udostępnienie danych może nastąpić po jej/jego zawarciu.

4. Umowy/porozumienia, które przewidują udostępnienie danych osobowych pomiędzy stronami, regulują zasady postępowania z tymi danymi.

5. Umowę/porozumienie sporządza się w formie pisemnej: papierowej albo elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym.

6. Projekt umowy/porozumienia sporządza się z uwzględnieniem wzoru określonego przez dyrektora BPB lub zaopiniowanego przez BPB.

7. Projekt umowy/porozumienia o udostępnieniu danych osobowych do państw spoza Europejskiego Obszaru Gospodarczego (EOG) podlega zaopiniowaniu przez BPB.

8. Oryginał umowy/porozumienia przechowuje komórka organizacyjna, która je zawiera.

§ 10. 1. Komórka organizacyjna prowadzi rejestr:

1) udostępnień danych osobowych, zawierający co najmniej następujące informacje: komu, jakie dane i na jakiej podstawie udostępniono;
2) zawartych umów/porozumień w sprawie udostępnienia danych osobowych. Wzór rejestru jest określony w załączniku nr 1 do Polityki.

2. Do końca miesiąca następującego po zakończeniu półrocza, komórki organizacyjne - za pośrednictwem EZD - udostępniają do BPB oraz IOD aktualne rejestry zawartych umów oraz porozumień w sprawie udostępnienia danych osobowych. Dyrektor BPB może zwrócić się do komórek organizacyjnych o udostępnienie aktualnego rejestru także w innym czasie. BPB monitoruje poprawność przekazywanych rejestrów.

Rozdział 5

Powierzenie przetwarzania danych osobowych

§ 11.1. Powierzenie przetwarzania danych osobowych odbywa się z uwzględnieniem art. 28 RODO.

2. Określenie zadań i obowiązków administratorów i podmiotu przetwarzającego wymaga zawarcia umowy w formie pisemnej: papierowej albo elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym.

3. Projekt umowy powierzenia przetwarzania danych osobowych sporządza się zgodnie ze wzorem określonym przez dyrektora BPB lub zaopiniowanym przez BPB.

4. W przypadku umowy, w której wprowadzono istotne modyfikacje względem wzoru, w szczególności dokonano zmiany elementów umowy, które we wzorze nie zostały przewidziane do modyfikacji, obowiązkowe jest uzyskanie opinii BPB.

5. Oryginał umowy powierzenia przetwarzania danych osobowych przechowuje komórka organizacyjna zawierająca umowę.

6. Projekt umowy o powierzeniu danych osobowych do państw spoza Europejskiego Obszaru Gospodarczego (EOG) podlega zaopiniowaniu przez BPB.

§ 12. W przypadku, gdy w ramach zawartej umowy powierzenia przetwarzania danych osobowych zawierane są dalsze umowy powierzenia przetwarzania danych osobowych, dyrektor komórki organizacyjnej prowadzącej sprawę dokonuje oceny zgodności dalszych umów z umową pierwotną i przechowuje ich kopię.

§ 13. 1. Komórka organizacyjna prowadzi rejestr zawartych umów powierzenia danych osobowych. Wzór rejestru jest określony w załączniku nr 1 do Polityki.

2. Do końca miesiąca następującego po zakończeniu kwartału komórki organizacyjne - za pośrednictwem EZD - udostępniają do BPB oraz IOD aktualny rejestr zawartych umów powierzenia danych osobowych. Dyrektor BPB może zwrócić się do komórek organizacyjnych o udostępnienie aktualnego rejestru także w innym czasie. BPB monitoruje poprawność przekazanych rejestrów.

Rozdział 6

Współadministrowanie danymi osobowymi

§ 14. 1. Współadministrowanie danymi osobowymi wymaga zawarcia umowy/porozumienia.

2. Umowę/porozumienie o współadministrowaniu zawiera się w formie pisemnej: papierowej albo elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym.

3.Projekt umowy/porozumienia w sprawie współadministrowania danymi osobowymi, związany z przekazaniem danych osobowych do państw spoza Europejskiego Obszaru Gospodarczego (EOG), podlega zaopiniowaniu przez BPB.

4. Oryginał umowy/porozumienia współadministrowania przechowuje komórka organizacyjna, która je zawiera.

§ 15. 1. Komórka organizacyjna prowadzi rejestr zawartych umów/porozumień współadministrowania. Wzór rejestru jest określony w załączniku nr 1 do Polityki.

2. Do końca miesiąca następującego po zakończeniu kwartału komórki organizacyjne - za pośrednictwem EZD - udostępniają do BPB oraz IOD aktualny rejestr umów lub porozumień o

współadministrowaniu. Dyrektor BPB może zwrócić się do komórek organizacyjnych o udostępnienie aktualnego rejestru także w innym czasie. BPB monitoruje poprawność przekazywanych rejestrów.

Rozdział 7

Rejestr czynności przetwarzania danych osobowych

§ 16. 1. BPB prowadzi rejestr czynności przetwarzania danych osobowych oraz rejestr kategorii czynności przetwarzania danych osobowych. Wnioskujący o wpis do rejestrów odpowiada za merytoryczną poprawność przekazanych danych, a BPB za kompletność i spójność tych rejestrów.

2. Wzory rejestrów są określone odpowiednio w załączniku nr 2 i nr 3 do Polityki. Rejestry publikowane są w intranecie Ministerstwa.

3. Wpis do rejestru czynności przetwarzania danych osobowych lub do rejestru kategorii czynności przetwarzania danych osobowych dokonywany jest na wniosek właściwej komórki organizacyjnej, na samodzielny wniosek BPB albo IOD - po przeprowadzeniu analizy ryzyka lub odpowiednio czynności kontrolnych, lub sprawdzających.

4. Wpis do rejestru polega na zdefiniowaniu, opisaniu czynności przetwarzania, zgodnie z wytycznymi PODO (załącznik nr 2 i nr 3 do Polityki).

5. Zmiany w rejestrze czynności przetwarzania danych osobowych oraz rejestrze kategorii czynności przetwarzania danych osobowych zatwierdza dyrektor BPB, po uzyskaniu opinii IOD, na wniosek dyrektora.

§ 17. W przypadku braku przyporządkowania czynności przetwarzania danych osobowych danej komórce organizacyjnej lub niemożliwości ustalenia komórki wiodącej (właściciela czynności przetwarzania), właściwym do realizacji zadań, o których mowa w § 16, jest dyrektor BPB lub dyrektor wskazany przez dyrektora generalnego.

§ 18. Dyrektor BPB, we współpracy z innymi dyrektorami, dokonuje przeglądu rejestrów, o których mowa w § 16 ust. 1, nie rzadziej niż raz w roku oraz w przypadku wprowadzenia istotnych zmian organizacyjnych w Ministerstwie - na podstawie oceny przeprowadzonej przez dyrektora BPB. Wyniki przeglądów przekazywane są do wiadomości IOD.

Rozdział 8

Upoważnienia do przetwarzania danych osobowych oraz rejestr upoważnień

§ 19. Użytkownicy ujęci w ewidencji uprawnień do EZD upoważnieni są do przetwarzania danych osobowych w zakresie, w jakim jest to niezbędne do wykonywania przez nich obowiązków wynikających z:

1) przepisów prawa powszechnie obowiązującego;

2) wewnętrznych aktów normatywnych obowiązujących w Ministerstwie;
3) umów wiążących Ministra i Ministerstwo;
4) umów zawartych z użytkownikami, w szczególności umów o pracę, i opisów stanowisk pracy;
5) poleceń wydawanych użytkownikom EZD przez dyrektorów.

§ 20. 1. W przypadku użytkowników innych, niż wskazani w § 19, oraz jeżeli przepisy prawa powszechnie obowiązującego dopuszczają możliwość przetwarzania danych osobowych wyłącznie przez osoby posiadające imienne upoważnienie, upoważnienia do przetwarzania danych osobowych w ramach określonych czynności przetwarzania wydają:

1) dyrektor BPB, pełnomocnik do spraw ochrony danych osobowych w BPB lub jego zastępca – w odniesieniu do komórek organizacyjnych, dla których nie został ustanowiony pełnomocnik do spraw ochrony danych osobowych w komórce organizacyjnej, lub w sytuacji gdy nie jest możliwe jednoznaczne ustalenie dyrektora odpowiedzialnego za daną czynność przetwarzania;
2) pełnomocnik do spraw ochrony danych osobowych w komórce organizacyjnej lub jego zastępca – w odniesieniu do czynności przetwarzania, dla których został ustanowiony.

2. W przypadku, gdy analiza ryzyka wykaże podwyższony lub wysoki poziom ryzyka naruszenia praw i wolności osób fizycznych, w celu ograniczenia tego ryzyka, dyrektor komórki organizacyjnej w uzgodnieniu z dyrektorem BPB może ograniczyć krąg użytkowników posiadających dostęp do danych osobowych, do użytkowników posiadających imienne upoważnienie do przetwarzania danych osobowych. Dyrektor BPB opracowuje i udostępnia w intranecie Ministerstwa wykaz danych osobowych, których przetwarzanie wymaga posiadania imiennego upoważnienia.

3. Procedura wydania imiennego upoważnienia do przetwarzania danych osobowych obejmuje:

1) wydanie upoważnienia przez dyrektora BPB lub właściwego pełnomocnika i następuje zgodnie z zasadą nadawania dostępu wyłącznie do zasobów koniecznych w celu realizacji zadań, z wykorzystaniem załączników do Polityki o numerach: 4a, 4b, 4c, 4d, lub 4e;
2) czynność wydania upoważnienia następuje po sprawdzeniu i zaakceptowaniu przez dyrektora BPB lub właściwego pełnomocnika wniosku podpisanego przez przełożonego osoby, której wniosek dotyczy, zgodnie z załącznikiem nr 5 do Polityki.

§ 21. Dyrektor BPB oraz pełnomocnicy do spraw ochrony danych osobowych prowadzą, zgodnie z właściwością, rejestry imiennych upoważnień do przetwarzania danych osobowych. Wzór rejestru imiennych upoważnień do przetwarzania danych osobowych jest określony w załączniku nr 6 do Polityki. Jeżeli dedykowany system informatyczny, w tym CST wspierający realizację programów operacyjnych oraz CST2021 wspierający realizację programów FE, KPO i pobrexitowej rezerwy

dostosowawczej, umożliwia rejestrowanie wydanych upoważnień imiennych, prowadzenie rejestru nie jest obligatoryjne.

§ 22. 1. Upoważnienia, o których mowa w § 20 ust. 2, tracą moc z dniem ustania stosunku prawnego, na podstawie którego użytkownicy wykonują czynności w komórce organizacyjnej lub zmiany zakresu obowiązków powodującej zaprzestanie przetwarzania danych osobowych w ramach wskazanej w upoważnieniu czynności przetwarzania.

2. Dyrektor komórki organizacyjnej niezwłocznie informuje BPB o okolicznościach, o których mowa w ust. 1.

§ 23. Kierujący BPB przy udziale pełnomocników do spraw ochrony danych osobowych, dyrektorów lub koordynatorów, dokonuje raz w roku przeglądu wydanych upoważnień do przetwarzania danych osobowych w celu weryfikacji ich aktualności. Wyniki przeglądu przekazywane są do wiadomości IOD.

Rozdział 9

Obowiązki użytkowników i odpowiedzialność za bezpieczeństwo danych osobowych

§ 24. W doborze i stosowaniu środków ochrony przetwarzanych danych osobowych należy kierować się kryterium należytego ich zabezpieczenia przed udostępnieniem osobom nieuprawnionym, kradzieżą, uszkodzeniem, nieuprawnioną modyfikacją, utratą lub zniszczeniem.

§ 25. Użytkownicy są zobowiązani w szczególności do:

1) przetwarzania danych osobowych zgodnie z RODO i UODO, wewnętrznymi aktami normatywnymi obowiązującymi w Ministerstwie, w tym Polityką, wytycznymi dyrektora BPB, oraz zgodnie z celem, dla którego te dane zostały zebrane;
2) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczania, również po ustaniu zatrudnienia lub innego zobowiązania wynikającego z zawartych umów;
3) przetwarzania danych osobowych w odpowiednio zabezpieczonych pomieszczeniach służbowych lub wyznaczonych ich częściach;
4) bezwzględnego przestrzegania zasad bezpieczeństwa przetwarzania informacji w systemie teleinformatycznym, określonych w dokumentacji systemu zawierających zasady oraz zakresy obowiązków i odpowiedzialności użytkowników systemów teleinformatycznych w zakresie ochrony danych osobowych, przyjętych do stosowania na podstawie wewnętrznych aktów normatywnych obowiązujących w Ministerstwie lub umów zawartych przez Ministerstwo;
5) zabezpieczania danych osobowych oraz dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych;

6) niszczenia wszystkich, niepodlegających archiwizacji dokumentów zawierających dane osobowe, w sposób uniemożliwiający ich odczytanie lub odtworzenie;
7) nieudzielania innym podmiotom informacji o przetwarzanych danych osobowych, chyba że obowiązek taki wynika wprost z przepisów prawa powszechnie obowiązującego i tylko w sytuacji, gdy przesłanki określone w tych przepisach zostały spełnione - z uwzględnieniem zasady minimalizacji danych;
8) udziału w obowiązkowych szkoleniach z zakresu ochrony danych osobowych, określonych przez dyrektora BZL;
9) współpracy z IOD przy realizacji jego zadań dotyczących ochrony danych osobowych.

§ 26. 1. Za naruszenie obowiązków w zakresie ochrony danych osobowych, pracownicy podlegają odpowiedzialności na podstawie przepisów prawa powszechnie obowiązującego, w tym UODO, odpowiedzialności dyscyplinarnej wynikającej z przepisów ustawy z dnia 21 listopada 2008 r. o służbie cywilnej (Dz. U. z 2021 r. poz. 1233) lub porządkowej wynikającej z przepisów prawa pracy.

2. Użytkownicy niebędący pracownikami, za naruszenie obowiązków, o których mowa w ust. 1, podlegają odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, w tym UODO, oraz umowach lub aktach powołania.

Rozdział 10

Zgłaszanie naruszeń ochrony danych osobowych

§ 27. Zasady zgłaszania naruszeń ochrony danych osobowych i postępowania z nimi, w tym oceny spełnienia przesłanek, o których mowa w art. 33 i 34 RODO, regulują wewnętrzne akty normatywne obowiązujące w Ministerstwie.

§ 28. Każdy użytkownik ma obowiązek niezwłocznego zgłoszenia zdarzenia lub podejrzenia naruszenia ochrony danych osobowych na adres IOD@mfipr.gov.pl. Sposób postępowania wskazano w Procedurze postępowania ze zgłoszeniami związanymi z bezpieczeństwem informacji w Ministerstwie Funduszy i Polityki Regionalnej w rozdziale 2.

§ 29.1. Zgłoszenie do Prezesa Urzędu Ochrony Danych Osobowych powinno być zrealizowane bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia ochrony danych osobowych.

2. Proces zgłaszania naruszenia ochrony danych osobowych koordynuje IOD, zgodnie z § 41 ust. 1 pkt 5.

Rozdział 11

Realizacja praw osób, których dane dotyczą

§ 30. 1. Rozpatrywaniem wniosków, o których mowa w art. 15-22 RODO, zajmuje się dyrektor komórki właściwej ze względu na przedmiot wniosku.

2. O ile jest to konieczne, komórki współpracują ze sobą w ramach ww. wniosków i przekazują informacje IOD, który zajmuje się koordynacją procesu.

§ 31. W przypadku kontaktu z osobami, których dotyczą przetwarzane dane należy każdorazowo potwierdzić tożsamość tych osób. Dotyczy to także kontaktu zdalnego, w tym telefonicznego i za pomocą wideo komunikatorów. Tożsamość można potwierdzić za pomocą dokumentów identyfikacyjnych lub weryfikacji posiadanych informacji dotyczących osoby.

Rozdział 12

Realizacja zadań związanych z ochroną danych osobowych

§ 32. 1. Członkowie kierownictwa Ministerstwa sprawują, zgodnie z ustalonym podziałem pracy w kierownictwie, nadzór nad przetwarzaniem danych osobowych w nadzorowanych przez siebie komórkach organizacyjnych.

2. Członek kierownictwa Ministerstwa, z zastrzeżeniem ust. 4 oraz § 27, jest uprawniony do wykonywania wszystkich czynności administratora, w zakresie w jakim jest to niezbędne do wykonywania jego zadań – zgodnie z ustalonym podziałem pracy w kierownictwie, w tym do udzielenia upoważnień/pełnomocnictw pełnomocnikom do spraw ochrony danych osobowych, o których mowa w § 37 i § 38.

3. Członek kierownictwa Ministerstwa może, w uzasadnionym przypadku, wyznaczyć pracowników podległej mu komórki organizacyjnej do pełnienia funkcji pełnomocników do spraw ochrony danych osobowych lub jego zastępców. Wyznaczenie pełnomocników oraz ich zastępców następuje zgodnie z zarządzeniem w sprawie wydawania upoważnień i pełnomocnictw. W komórce organizacyjnej można wyznaczyć więcej niż jednego pełnomocnika lub zastępcę, o ile jest to uzasadnione z uwagi na wykonywane przez tę komórkę zadania.

4. Dyrektor generalny, w imieniu Ministra, wykonuje czynności administratora danych wobec IOD oraz wspiera go w wykonywaniu jego zadań, w szczególności:

1) zapewnia właściwe i niezwłoczne włączanie IOD we wszystkie sprawy dotyczące ochrony danych osobowych w Ministerstwie;
2) wspiera IOD w wypełnianiu przez niego zadań, o których mowa w art. 39 RODO, zapewniając mu zasoby niezbędne do wykonywania tych zadań oraz dostęp do danych osobowych i

czynności przetwarzania danych osobowych, a także zasobów niezbędnych do utrzymania fachowej wiedzy;

3) wyznacza IOD inne zadania i obowiązki, niewynikające z RODO, w zakresie niepowodującym konfliktu interesów;

4) konsultuje z IOD ocenę skutków planowanych czynności lub operacji przetwarzania danych osobowych dla ochrony danych osobowych.

§ 33. 1. Do zadań dyrektora należy, w zakresie właściwości kierowanej przez niego komórki organizacyjnej, wykonywanie czynności administratora niezastrzeżonych do właściwości innych podmiotów, w szczególności:

1) zbieranie, przechowywanie, udostępnianie i usuwanie danych osobowych;

2) zawieranie umów/porozumień dotyczących przetwarzania danych osobowych, w tym umów powierzenia przetwarzania danych osobowych, udzielanie dalszych pełnomocnictw do ich zawierania oraz upoważnień, w szczególności zastępcom dyrektora i koordynatorom do spraw ochrony danych osobowych;

3) prowadzenie rejestru umów powierzenia danych osobowych oraz udostępnienia i współadministrowania tymi danymi;

4) przeprowadzanie analizy planowanych czynności lub operacji przetwarzania danych osobowych w zakresie określonym w § 6, w tym przeprowadzanie analizy ryzyka naruszenia praw lub wolności osób fizycznych oraz analizy DPIA;

5) realizacja obowiązku informacyjnego, o którym mowa w art. 13 i 14 RODO;

6) rozpatrywanie wniosków, o których mowa w art. 15-22 RODO, w terminie określonym w art. 12. ust. 3 i 4 RODO oraz niezwłoczna realizacja praw osób, których dane dotyczą;

7) zgłaszanie konieczności wprowadzenia zmian w rejestrach prowadzonych przez BPB, o których mowa w § 16 ust. 1;

8) współpraca z BPB i IOD przy realizacji ich zadań;

9) informowanie IOD o pracach dotyczących planowania/projektowania/przygotowania przedsięwzięć zarówno o charakterze programowym, legislacyjnym jak i projektowym, jeżeli ich realizacja będzie związana z przetwarzaniem danych osobowych oraz umożliwienie IOD włączenia się w te prace;

10) zapewnienie prawidłowego przetwarzania danych osobowych, z zastrzeżeniem zadań przypisanych DI, BA i BPB.

2. Do zadań dyrektora komórki organizacyjnej realizującej zadania związane z obsługą Ministra pełniącego funkcję instytucji zarządzającej programem operacyjnym oraz dyrektora komórki organizacyjnej odpowiedzialnej za koordynację realizacji programów operacyjnych należy

wykonywanie czynności administratora, o których mowa w ust. 1, a ponadto opracowanie projektów wewnętrznych aktów normatywnych, metodyk, wytycznych, zaleceń, wzorów dokumentów oraz standardowych środków organizacyjnych i technicznych przetwarzania danych osobowych regulujących zasady przetwarzania danych osobowych w programach operacyjnych albo w CST wspierającym realizację programów operacyjnych oraz CST2021 wspierającym realizację programów FE, KPO i pobrexitowej rezerwy dostosowawczej - w zakresie właściwości tych komórek organizacyjnych, o ile jest to uzasadnione specyfiką przetwarzania danych osobowych w powyższych obszarach.

3. Dyrektor może wyznaczyć koordynatora do spraw ochrony danych osobowych i jego zastępcę (lub zastępców), z zastrzeżeniem ust. 4, w celu realizacji niektórych lub wszystkich zadań, o których mowa w Polityce, określając jednocześnie zakres uprawnień i obowiązków. Wyznaczenie koordynatora oraz jego zastępców następuje zgodnie z zarządzeniem w sprawie upoważnień i pełnomocnictw. O wyznaczeniu koordynatora do spraw ochrony danych osobowych oraz jego zastępców oraz o zakresie uprawnień i obowiązków dyrektor informuje niezwłocznie, za pośrednictwem EZD, dyrektora BPB oraz IOD.

4. Udzielenie dalszego pełnomocnictwa do zawierania umów i porozumień dotyczących przetwarzania danych osobowych, w tym umów powierzenia przetwarzania danych osobowych, następuje zgodnie z zarządzeniem w sprawie upoważnień i pełnomocnictw.

5. Dyrektor podczas realizacji zadań może stosować dokumenty opracowane przez BPB, w tym wytyczne, zalecenia, interpretacje, wyjaśnienia, metodyki oraz wskazówki.

6. Dyrektor dokumentuje wykonywane czynności, o których mowa w ust. 1 i 2.

§ 34. 1. Do zadań dyrektora BPB należy realizacja czynności administratora, o których mowa w § 33 ust. 1, a ponadto:

1) wydawanie upoważnień do przetwarzania danych osobowych;
2) prowadzenie rejestru upoważnień do przetwarzania danych osobowych;
3) opiniowanie projektów aktów normatywnych, dokumentów związanych z ochroną danych osobowych, w tym projektów umów o współadministrowaniu, porozumień i umów dotyczących udostępnienia danych osobowych lub powierzenia przetwarzania danych osobowych;
4) koordynacja procesu przetwarzania danych osobowych w Ministerstwie, w szczególności opracowywanie, aktualizacja i publikowanie w intranecie Ministerstwa wzorów dokumentów, instrukcji, standardowych środków organizacyjnych i technicznych przetwarzania danych osobowych oraz metodyki sporządzania analizy ryzyka zagrożeń i analizy DPIA, a także formułowanie zaleceń i wytycznych - z własnej inicjatywy, na polecenie dyrektora generalnego albo wniosek IOD;

5) współpraca z dyrektorami przy realizacji czynności, o których mowa w § 6 ust. 1 oraz § 7 ust. 1-5;

2. Przed udostępnieniem do stosowania dokumentów opracowanych przez BPB (zgodnie z ust. 1 pkt 4), dyrektor BPB występuje o opinię do dyrektorów właściwych komórek organizacyjnych oraz IOD.

3. Projekt wykazu standardowych środków organizacyjnych i technicznych przetwarzania danych osobowych podlega uzgodnieniu z dyrektorami.

4. Stosowanie wytycznych, metodyk oraz standardowych środków organizacyjnych i technicznych przetwarzania danych osobowych jest obowiązkowe.

§ 35. Do zadań dyrektora BA należy realizacja czynności administratora, o których mowa w § 33 ust. 1, a ponadto:

1) zapewnienie w Ministerstwie warunków umożliwiających wdrożenie standardowych środków organizacyjnych i technicznych przetwarzania danych osobowych w formie papierowej;
2) współpraca przy opracowywaniu i wdrażaniu dodatkowych środków organizacyjnych i technicznych przetwarzania danych osobowych w formie papierowej, przy realizacji czynności, o których mowa w § 6 ust. 1 oraz § 7 ust. 1 - 5.

§ 36. Do zadań dyrektora DI należy realizacja czynności administratora, o których mowa w § 33 ust. 1, a ponadto:

1) zapewnienie w Ministerstwie warunków umożliwiających wdrożenie standardowych środków organizacyjnych i technicznych przetwarzania danych osobowych w systemach teleinformatycznych i zapisywanych na informatycznych nośnikach danych;
2) współpraca przy opracowywaniu i wdrażaniu dodatkowych środków organizacyjnych i technicznych przetwarzania danych osobowych w systemach teleinformatycznych przy realizacji czynności, o których mowa w § 6 ust. 1 i 2 oraz § 7 ust. 1 - 5;
3) opracowanie oraz opiniowanie projektów wewnętrznych aktów normatywnych w zakresie przetwarzania danych osobowych w systemach teleinformatycznych.

§ 37. Do zadań pełnomocnika do spraw ochrony danych osobowych w BPB oraz jego zastępcy należy:

1) wydawanie upoważnień do przetwarzania danych osobowych,
2) prowadzenie rejestru upoważnień, o którym mowa w § 21,
3) opiniowanie projektów aktów normatywnych, wewnętrznych aktów normatywnych, umów oraz innych dokumentów związanych z ochroną danych osobowych, w tym projektów umów o

współadministrowaniu, porozumień/umów dotyczących udostępnienia danych osobowych lub powierzenia przetwarzania danych osobowych;

4) koordynacja realizacji zadań przez pełnomocników do spraw ochrony danych osobowych,

5) współpraca z IOD przy realizacji jego zadań

- w odniesieniu do czynności przetwarzania danych osobowych wskazanych w upoważnieniu/pełnomocnictwie wydanym przez właściwego członka kierownictwa.

§ 38. 1. Do zadań pełnomocnika do spraw ochrony danych osobowych w komórce organizacyjnej oraz jego zastępcy należy:

1) wydawanie upoważnień do przetwarzania danych osobowych oraz udzielanie dalszych pełnomocnictw do wydawania upoważnień,

2) prowadzenie rejestru upoważnień, o którym mowa w § 21,

3) współpraca z dyrektorem BPB w zakresie koordynacji procesu przetwarzania danych osobowych,

4) współpraca z IOD w obszarze przetwarzania danych osobowych,

5) przeprowadzanie, jeżeli zaistnieje taka konieczność, czynności kontrolnych przestrzegania zasad przetwarzania danych osobowych w macierzystych komórkach organizacyjnych oraz czynności kontrolnych w podmiotach, którym zostało powierzone przetwarzanie danych osobowych

- w odniesieniu do czynności przetwarzania danych osobowych wskazanych w upoważnieniu/pełnomocnictwie wydanym przez właściwego członka kierownictwa.

2. Upoważnienia do przetwarzania danych osobowych oraz umocowania dla pełnomocników oraz ich zastępców w ramach SL2014-PT, są wydawane na podstawie Zasad zarządzania uprawnieniami w aplikacji SL2014-PT Centralnego Systemu Teleinformatycznego.

3. Upoważnienia do przetwarzania danych osobowych oraz umocowania dla pełnomocników oraz ich zastępców w ramach obowiązującej i zatwierdzonej w przyszłości dokumentacji regulującej zasady przetwarzania danych osobowych w programach operacyjnych albo w CST wspierającym realizację programów operacyjnych oraz CST2021 wspierającym realizację programów FE, KPO i pobrexitowej rezerwy dostosowawczej mogą przewidywać odmienny tryb umocowań i upoważnień, ale muszą uwzględniać postanowienia Polityki.

§ 39**.** 1. Do zadań koordynatora do spraw ochrony danych osobowych w komórce organizacyjnej oraz jego zastępcy należy realizacja zadań zgodnie z zakresem upoważnienia nadanego przez dyrektora.

2. Wyznaczenie koordynatora do spraw ochrony danych osobowych i jego zastępców następuje zgodnie z zarządzeniem w sprawie upoważnień i pełnomocnictw.

3. O wyznaczeniu koordynatora do spraw ochrony danych osobowych oraz jego zastępców oraz o zakresie ich działania dyrektor informuje niezwłocznie, za pośrednictwem EZD, dyrektora BPB oraz IOD.

Rozdział 13

Inspektor ochrony danych

§ 40. W celu zapewnienia przestrzegania przepisów o ochronie danych osobowych w Ministerstwie administrator wyznacza IOD.

§ 41. 1. IOD wykonuje zadania, o których mowa w art. 39 RODO, w szczególności:

1) opiniuje przekazane projekty aktów normatywnych, projekty wewnętrznych aktów normatywnych, umów i innych dokumentów związanych z ochroną danych osobowych;
2) prowadzi szkolenia, warsztaty oraz udziela porad i konsultacji pracownikom i członkom kierownictwa Ministerstwa w zakresie ochrony danych osobowych;
3) monitoruje przestrzeganie przepisów z zakresu ochrony danych osobowych;
4) zapewnia obsługę adresu email: IOD@mfipr.gov.pl, w tym koordynuje udzielanie odpowiedzi na zapytania wysyłane na ten adres;
5) zapewnia koordynację procesu zgłaszania naruszeń ochrony danych osobowych do Prezesa Urzędu Ochrony Danych Osobowych i przedkłada dokument zgłoszenia do podpisu właściwemu członkowi kierownictwa Ministerstwa;
6) uczestniczy w procesie rozpatrywania wniosków, o których mowa w art. 15-22 RODO, skierowanych do Ministerstwa za pośrednictwem adresu e-mail: iod@mfipr.gov.pl oraz w przypadku, gdy wniosek dotyczy więcej niż jednej komórki organizacyjnej - koordynuje takie działania.

2. IOD pełni rolę punktu kontaktowego w komunikacji Ministerstwa z Urzędem Ochrony Danych Osobowych, w tym przygotowuje lub opiniuje projekty pism.

3. W trakcie realizacji swoich zadań IOD posiada, w niezbędnym zakresie, dostęp do wszystkich danych osobowych przetwarzanych w Ministerstwie.

§ 42. IOD nie podejmuje działań, które prowadziłyby do przejęcia przez niego obowiązków, odpowiedzialności lub uprawnień administratora.

§ 43. Administrator może powołać zastępcę IOD. Zastępca IOD w czasie nieobecności IOD wykonuje jego zadania.

Rozdział 14

Monitoring przestrzegania przepisów z zakresu ochrony danych osobowych

§ 44. Monitoring przestrzegania przepisów z zakresu ochrony danych osobowych w Ministerstwie obejmuje:

1) czynności sprawdzające (prowadzone przez IOD) oraz kontrolne (prowadzone przez dyrektora BPB), w zakresie zgodności przetwarzania danych osobowych z przepisami prawa powszechnie obowiązującego oraz wewnętrznymi aktami normatywnymi obowiązującymi w Ministerstwie;
2) audyty i kontrole realizowane na zasadach określonych w odrębnych przepisach;
3) czynności kontrolne realizowane przez pełnomocników do spraw ochrony danych osobowych w zakresie posiadanego pełnomocnictwa;
4) sprawowanie nadzoru nad czynnościami przetwarzania danych osobowych;
5) bieżące zgłaszanie dyrektorom i pozostałym użytkownikom uwag i propozycji dotyczących ochrony danych osobowych.

§ 45. 1. Czynności sprawdzające oraz kontrolne przeprowadza odpowiednio IOD lub dyrektor BPB. W uzasadnionych przypadkach czynności te może przeprowadzić zespół pod kierownictwem IOD lub dyrektora BPB, którego skład zatwierdza dyrektor generalny.

2. Dokonując czynności sprawdzających IOD i kontrolnych dyrektor BPB bierze pod uwagę kryteria legalności, skuteczności, efektywności oraz ryzyka przetwarzania danych osobowych.

3. IOD lub dyrektor BPB dokumentuje czynności sprawdzające lub kontrolne, w tym:

1) sporządza notatkę, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;
2) sporządza kopię dokumentu oraz obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych;
3) utrwala dane z systemu informatycznego służącego do przetwarzania danych osobowych lub zabezpiecza dane osobowe na informatycznym nośniku danych lub dokonuje wydruku tych danych;
4) sporządza kopie zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu.

4. IOD lub dyrektor BPB zawiadamia dyrektora komórki organizacyjnej objętej czynnościami sprawdzającymi lub kontrolnymi o zakresie planowanych czynności w terminie co najmniej 7 dni przed dniem ich przeprowadzenia. Czynności sprawdzające lub kontrolne mogą zostać

przeprowadzone bez uprzedzenia, jeżeli uzasadniają to okoliczności, w tym w sytuacji podejrzenia naruszenia bezpieczeństwa danych osobowych.

5. Z przeprowadzonych czynności sprawdzających lub kontrolnych sporządzane jest sprawozdanie w formie pisemnej: papierowej lub elektronicznej. Sprawozdanie przedkładane jest dyrektorowi generalnemu do zatwierdzenia, niezwłocznie po zakończeniu czynności, a także do wiadomości właściwemu członkowi kierownictwa, nadzorującemu daną komórkę organizacyjną.

§ 46. 1. W sprawozdaniu z czynności sprawdzających lub kontrolnych, o którym mowa w § 45 ust. 5, IOD lub dyrektor BPB może wystosować rekomendacje i zalecenia dotyczące ochrony danych osobowych w Ministerstwie.

2. Podsumowanie wyników czynności sprawdzających lub jego część jest udostępniana komórkom organizacyjnym, których dotyczą wystosowane rekomendacje. Określenie sposobu i terminu wykonania poszczególnych rekomendacji pozostaje we właściwości dyrektora komórki organizacyjnej, odpowiedzialnej za dany zakres.

3. Rekomendacje są realizowane we współpracy z IOD lub z dyrektorem BPB.

Rozdział 15

Szkolenia

§ 47.1. Administrator zapewnia szkolenia dla użytkowników w zakresie obowiązujących przepisów, procedur oraz podstawowych zagrożeń związanych z przetwarzaniem danych osobowych.

2. Dyrektor BZL w uzgodnieniu z dyrektorami BPB, DI, BA oraz IOD określa zakres szkoleń obowiązkowych i fakultatywnych oraz wdraża mechanizmy mające na celu egzekwowanie udziału użytkowników w szkoleniach obowiązkowych.

§ 48. 1. Szkolenia prowadzi IOD.

2. BPB wspiera IOD w zakresie prowadzenia szkoleń, które mogą być prowadzone także przez wyspecjalizowane w tym zakresie podmioty zewnętrzne.