POLITYKA OCHRONY DANYCH OSOBOWYCH

W MINISTERSTWIE SPORTU I TURYSTYKI

Rozdział 1

Przepisy ogólne

§ 1. 1. Polityka ochrony danych osobowych w Ministerstwie, zwana dalej „Polityką”, realizując przepis art. 24 ust. 1 i 2 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, str. 1, Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 04.03.2021, str. 35), zwanego dalej „RODO”, określa środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych oraz szczegółowe warunki dotyczące sposobu zarządzania, ochrony i przetwarzania danych osobowych w Ministerstwie, dla których:

1) minister właściwy do spraw kultury fizycznej lub turystyki, zwany dalej „Ministrem”, jest administratorem;
2) Minister nie jest administratorem, chyba że zawarte przez Ministra porozumienia z administratorami danych stanowią inaczej;
3) Minister jest współadministratorem lub podmiotem przetwarzającym, chyba że zawarte przez Ministra umowy lub porozumienia z administratorami stanowią inaczej.

2. Politykę stosuje się do danych osobowych przetwarzanych:

1) w sposób całkowicie lub częściowo zautomatyzowany, w szczególności w systemie Elektronicznego Zarządzania Dokumentacją, zwanego dalej „EZD”, innych systemach teleinformatycznych, poczcie elektronicznej, informatycznych nośnikach danych;
2) w sposób inny niż zautomatyzowany, stanowiących część zbioru danych lub mających stanowić część zbioru danych;
3) w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych oraz dokumentach Ministerstwa, stanowiących zbiory danych w rozumieniu RODO.

3. Celem Polityki jest zapewnienie ochrony interesów osób, których dane osobowe są przetwarzane w Ministerstwie lub dla których Minister występuje w roli administratora, współadministratora lub podmiotu przetwarzającego, a w szczególności zapewnienie, aby dane te były przetwarzane zgodnie z ogólnymi zasadami przetwarzania danych osobowych, o których mowa w art. 5 RODO, a w szczególności aby dane te były:

1) przetwarzane zgodnie z prawem, w oparciu o co najmniej jedną przesłankę legalności przetwarzania danych osobowych wskazaną w art. 6 lub 9 RODO (zasada legalności);
2) przetwarzane rzetelnie, rozumiane jako obowiązek starannego działania i należytego wypełniania obowiązków, ale także postępowanie uczciwe (zasada rzetelności);
3) przetwarzane w sposób przejrzysty dla osoby, której dane dotyczą (zasada przejrzystości), w szczególności poprzez realizowanie obowiązków informacyjnych wynikających z art. 13 i art. 14 RODO oraz w ramach uprawnień przysługujących osobom, których dane dotyczą wynikających z art. 15-22 RODO;
4) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami ze wskazaniem odpowiedniej podstawy dopuszczalności przetwarzania danych, o których mowa w art. 6, 9 i 10 RODO (zasada ograniczenia celu);

5) adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, w których są przetwarzane (zasada minimalizacji danych);
6) prawidłowe i w razie potrzeby uaktualniane, w szczególności w trybie art. 16 RODO (zasada prawidłowości);
7) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą przez okres nie dłuższy, niż jest to niezbędne do osiągniecia celów, w których są one przetwarzane, przy czym po osiągnięciu celu dane powinny zostać usunięte lub zanonimizowane (zasada ograniczenia przechowywania);
8) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem zgodnie z regulacjami wewnętrznymi obowiązującymi w Ministerstwie w zakresie zabezpieczeń technicznych i organizacyjnych (zasada integralności i poufności).

4. Przetwarzanie danych osobowych powinno odbywać się w taki sposób, aby można było wykazać przestrzeganie zasad, o których mowa w ust. 5, zgodnie z zasadą rozliczalności.

5. Polityka nie ma zastosowania do danych osobowych przetwarzanych zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2025 r. poz. 1209).

§ 2. Politykę stosują pracownik, stażysta, wolontariusz, praktykant lub inna osoba fizyczna, realizująca zadania na rzecz Ministra lub Ministerstwa, w tym osoba fizyczna świadcząca usługi na podstawie umowy zlecenia, umowy o dzieło lub innej umowy cywilnoprawej bądź porozumienia, przetwarzający dane osobowe, upoważnieni w rozumieniu art. 29 RODO, zwani dalej „użytkownikami".

§ 3. 1. Minister deklaruje pełne zaangażowanie i wsparcie dla zapewnienia bezpieczeństwa danych osobowych i wszelkich działań na rzecz ochrony danych osobowych.

2. Minister jest administratorem w Ministerstwie.

3. Polityka określa odpowiedzialność osób upoważnionych do przetwarzania danych osobowych, a także wskazuje na konieczność zapewnienia wsparcia przez Członków kierownictwa Ministerstwa oraz kierownictwo komórek organizacyjnych działań na rzecz ochrony danych osobowych.

§ 4. W przypadku przetwarzania danych osobowych w systemach teleinformatycznych, pracowników oraz inne osoby, które z upoważnienia administratora uzyskały dostęp do danych osobowych przetwarzanych w tych systemach, obowiązują również polityki bezpieczeństwa dotyczące tych systemów.

§ 5. W przypadku pojawienia się wątpliwości w zakresie stosowania Polityki, należy rozstrzygać je w taki sposób, aby zapewnić ochronę danych osobowych oraz realizację praw osób, których dane dotyczą, z uwzględnieniem zasady rozliczalności.

§ 6. 1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania danych osobowych oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

2. Środki techniczne i organizacyjne zapewniające bezpieczeństwo danych osobowych przetwarzanych w Ministerstwie określają regulacje wewnętrzne obowiązujące w Ministerstwie.

§ 7. Obszar przetwarzania danych osobowych, określany jako przetwarzanie danych osobowych w obrębie Ministerstwa, obejmuje:
1) pomieszczenia znajdujące się w budynkach zlokalizowanych w Warszawie, użytkowanych przez Ministerstwo oraz
2) dodatkowe miejsca przetwarzania danych osobowych takie jak komputery oraz inne nośniki danych znajdujące się poza obszarem wskazanym w pkt 1, posiadające zabezpieczenia funkcjonujące w Ministerstwie, w tym w miejscach wykonywania pracy w formie zdalnej przez osoby upoważnione do przetwarzania danych osobowych lub w miejscach realizacji powierzonych im zadań.

§ 8. Przetwarzanie danych osobowych w Ministerstwa odbywa się zgodnie z przepisami obowiązującymi w zakresie ochrony danych osobowych, w szczególności zgodnie z RODO oraz ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781), zwaną dalej „Ustawą", z uwzględnieniem rekomendacji Prezesa Urzędu Ochrony Danych Osobowych (także organu poprzedzającego – Głównego Inspektora Ochrony Danych Osobowych), zwanego dalej „PUODO", oraz wytycznymi i zaleceniami określonymi dobrymi praktykami Europejskiej Rady Ochrony Danych oraz wytycznymi organu poprzedzającego – Grupy Roboczej Art. 29 ds. Ochrony Danych.

§ 9. Użyte w Polityce określenia oznaczają:

1) administrator – podmiot w rozumieniu art. 4 pkt 7 RODO;
2) współadministrator – administrator, który wspólnie z innymi administratorami ustala cele i sposoby przetwarzania danych osobowych;
3) podmiot przetwarzający – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu i na rzecz administratora;
4) IOD – Inspektor Ochrony Danych wyznaczony przez Ministra, posiadający kwalifikacje zawodowe, wiedzę, wykształcenie i doświadczenie w zakresie ochrony danych osobowych, realizujący zadania określone w art. 39 RODO;
5) osoba zastępująca IOD – osoba zastępująca IOD w czasie jego nieobecności, spełniająca wymagania właściwe dla IOD, o których mowa w pkt 4;
6) pracownik – osoba zatrudniona w Ministerstwie na podstawie umowy o pracę, mianowania, powołania, bez względu na rodzaj i formę pracy oraz zajmowane stanowisko;
7) kierujący komórką organizacyjną – dyrektor lub zastępca dyrektora departamentu lub biura, Szef Gabinetu Politycznego Ministra;
8) komórka organizacyjna – departament, biuro lub Gabinet Polityczny Ministra określone w statucie Ministerstwa;
9) komórka organizacyjna właściwa do spraw ryzyka – komórka organizacyjna realizująca zadania z zakresu koordynacji procesu zarządzania ryzykiem w Ministerstwie;
10) dane osobowe – wszelkie informacje o osobie fizycznej zidentyfikowanej lub możliwej do zidentyfikowania, w rozumieniu art. 4 pkt 1 RODO;
11) przetwarzanie danych osobowych – operacja lub zestaw operacji wykonywanych na danych osobowych lub ich zbiorach, w rozumieniu art. 4 pkt 2 RODO;
12) pseudonimizacja - przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
13) anonimizacja danych osobowych – przetworzenie danych osobowych w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować;
14) usunięcie danych osobowych – zniszczenie danych osobowych poprzez np. zniszczenie nośnika danych osobowych skutkujące trwałą utratą tych danych, trwałe usunięcie (wymazanie) danych osobowych przy pozostawieniu nośnika danych; usunięciem danych osobowych nie jest takie zniszczenie nośnika, które nie wyklucza możliwości odzyskania danych na nim zapisanych;
15) naruszenie ochrony danych osobowych – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
16) system teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz. U. poz. 1221 oraz z 2025 r. poz. 637 i 820);

17) rejestr czynności przetwarzania – rejestr czynności przetwarzania danych osobowych, o którym mowa w art. 30 ust. 1 RODO;
18) rejestr kategorii czynności przetwarzania – rejestr kategorii czynności przetwarzania danych osobowych, o którym mowa w art. 30 ust. 2 RODO;
19) ryzyko naruszenia praw lub wolności osób, których dane dotyczą - ryzyko, którego prawdopodobieństwo i powagę należy określić poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych; oceniając ryzyko w zakresie bezpieczeństwa danych, należy wziąć pod uwagę ryzyko związane z przetwarzaniem danych osobowych - takie jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych - i mogące w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych, bądź też wywołać inne skutki, o których mowa w motywie 75 RODO; ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko;
20) analiza DPIA (Data Protection Impact Assessment) – analiza ryzyka wraz z oceną skutków dla ochrony danych osobowych, przeprowadzana przez administratora przed rozpoczęciem przetwarzania, gdy dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

§ 10. 1. Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z przepisami RODO, Ustawą, Polityką, a także zgodnymi z Polityką regulacjami wewnętrznymi, odpowiadają:
1) Minister występujący w roli administratora, współadministratora lub podmiotu przetwarzającego;
2) IOD;
3) kierujący komórką organizacyjną;
4) użytkownik.

2. Minister może udzielić pełnomocnictwa do wykonywania zadań administratora, współadministratora lub podmiotu przetwarzającego w zakresie zgodnym z przepisami RODO.

3. Udzielenie pełnomocnictwa, o którym mowa w ust. 2, nie wyłącza odpowiedzialności Ministra jako administratora.

4. Administrator:
1) wyznacza i odwołuje IOD oraz osobę zastępującą IOD;
2) informuje PUODO o wyznaczeniu i odwołaniu IOD oraz zamieszczeniu stosownej informacji na stronie internetowej Ministerstwa;
3) wdraża odpowiednie procedury ochrony danych osobowych;
4) wdraża odpowiednie środki organizacyjne i techniczne w celu zapewnienia stopnia bezpieczeństwa odpowiadającego istniejącemu ryzyku naruszenia praw lub wolności osób, których dane dotyczą;
5) zapewnia środki umożliwiające prawidłową realizację praw osób, których dane dotyczą;
6) nadzoruje przetwarzanie danych osobowych w Ministerstwie;
7) nadzoruje prowadzenie w Ministerstwie rejestru czynności przetwarzania danych osobowych;
8) udziela upoważnień do przetwarzania danych osobowych;
9) wspiera IOD w wypełnianiu przez niego zadań, o których mowa w art. 39 RODO, w szczególności:
   a) zapewnia zasoby niezbędne do wykonania zadań IOD oraz dostępu do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania fachowej wiedzy IOD,
   b) umożliwia IOD należyte wykonywanie swoich obowiązków bez presji lub instrukcji dotyczących sposobu realizacji zadań i osiągania celów;
10) zgłasza naruszenia ochrony danych osobowych PUODO, a w przypadku, gdy zajdą ku temu odpowiednie przesłanki – informuje osobę, której dane dotyczą;
11) nadzoruje dokumentowanie wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia, jego skutków oraz podjętych działań zaradczych;

12) włącza IOD w kluczowe kwestie i decyzje podejmowane w Ministerstwie, które mogą mieć związek z przetwarzaniem danych osobowych.

§ 11. 1. W celu wdrażania przepisów o ochronie danych osobowych i nadzorowania ich przestrzegania w Ministerstwie funkcjonuje IOD wyznaczony przez administratora.

2. Dane IOD, obejmujące jego imię i nazwisko oraz e-mail, udostępnia się na stronie internetowej Ministerstwa.

3. IOD wykonuje zadania, o których mowa w art. 39 RODO, w szczególności:

1) informuje administratora, podmiot przetwarzający oraz użytkowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii Europejskiej lub przepisów krajowych o ochronie danych osobowych i doradza im w tej sprawie;
2) monitoruje przestrzeganie przepisów z zakresu ochrony danych osobowych, w tym RODO, oraz Polityki;
3) udziela na żądanie zaleceń co do oceny skutków dla ochrony danych osobowych oraz monitoruje jej wykonanie, zgodnie z art. 35 RODO;
4) współpracuje z organem nadzorczym;
5) pełni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzi konsultacje w innych sprawach;
6) opiniuje projekty dokumentów rządowych, projekty wewnętrznych aktów prawnych i innych dokumentów związanych z ochroną danych osobowych;
7) opiniuje projekty umów i porozumień o współadministrowaniu oraz projekty umów powierzenia przetwarzania danych osobowych;
8) wydaje zalecenia i rekomendacje w zakresie ochrony danych osobowych;
9) prowadzi zbiorcze rejestry: czynności przetwarzania, kategorii czynności przetwarzania, zawartych umów powierzenia przetwarzania danych osobowych oraz umów i porozumień o współadministrowaniu danymi osobowymi;
10) opracowuje roczny planu audytów, realizuje ten plan oraz sporządza z niego sprawozdanie;
11) przedstawia administratorowi sprawozdania z podejmowanych przez siebie działań, wydawanych zaleceń i rekomendacji, a także innych kwestii związanych z ochroną danych osobowych w Ministerstwie, co najmniej raz w roku, najpóźniej do końca I kwartału roku następującego po roku, za który składane jest sprawozdanie;
12) współpracuje z kierującymi komórkami organizacyjnymi w sprawach z zakresu ochrony danych osobowych;
13) dokumentuje w EZD podejmowane przez siebie czynności w zakresie ochrony danych osobowych w celu wykazania działania z należytą starannością, zgodnie z zasadą rozliczalności;
14) zapewnia obsługę adresu e-mail: iod@msit.gov.pl;
15) przekazuje do zamieszczenia w Intranecie w zakładce poświęconej ochronie danych osobowych wzory dokumentów oraz wszelkie materiały o charakterze edukacyjnym w celu stosowania oraz zwiększania świadomości użytkowników w zakresie ochrony danych osobowych.

4. Administrator może wyznaczyć osobę zastępującą IOD, wykonującą zadania, o których mowa w ust. 3, wyłącznie w czasie nieobecności IOD.

§ 12. 1. Za ochronę danych osobowych przetwarzanych w komórce organizacyjnej Ministerstwa odpowiada kierujący tą komórką organizacyjną.

2. Do zadań kierującego komórką organizacyjną należy:

1) nadzór nad przestrzeganiem zasad ochrony danych osobowych zgodnie z przepisami RODO i Ustawą, Polityką oraz innymi zgodnymi z Polityką regulacjami wewnętrznymi, przez użytkowników realizujących zadania w tej komórce organizacyjnej. Nadzór, o którym mowa w zdaniu pierwszym, dotyczy również pracowników wykonujących pracę zdalną;

2) zgłaszanie IOD zmian, uzupełnień i aktualizacji do zbiorczego rejestru czynności przetwarzania danych osobowych, w tym identyfikowanie nowych czynności przetwarzania, oraz zbiorczego rejestru kategorii czynności przetwarzania danych osobowych;
3) realizowanie obowiązku informacyjnego, w sposób określony w § 27 Polityki;
4) przekazywanie do akceptacji przez IOD projektów klauzul informacyjnych, zgodnie z § 28 Polityki;
5) informowanie IOD o pracach dotyczących planowania, projektowania lub przygotowania przedsięwzięć o charakterze programowym, projektowym lub legislacyjnym, w tym wprowadzenia do użytkowania nowych systemów teleinformatycznych, jeżeli ich realizacja będzie związana z przetwarzaniem danych osobowych oraz umożliwienie IOD włączenia się w te prace od jak najwcześniejszego etapu;
6) podejmowanie działań zmierzających do wyeliminowania ewentualnych zagrożeń bezpieczeństwa danych osobowych i minimalizacji ryzyka oraz ich konsultowanie z IOD;
7) identyfikowanie potrzeb organizacyjnych i technicznych niezbędnych do prawidłowego przetwarzania danych osobowych oraz współpraca z IOD w tym zakresie;
8) informowanie IOD o stwierdzonych w komórce organizacyjnej nieprawidłowościach związanych z przetwarzaniem danych osobowych;
9) określenie sposobu i terminu realizacji zaleceń bądź podejmowanie decyzji o odstąpieniu od ich realizacji po wystąpieniu naruszenia ochrony danych osobowych bądź podejrzenia naruszenia ochrony danych osobowych oraz przeprowadzonym audycie w zakresie ochrony danych osobowych;
10) aktualizacja opisu stanowisk podległych pracowników zatrudnionych na podstawie stosunku pracy w zakresie dotyczącym ochrony danych osobowych, w szczególności w zakresie właściwego określenia czynności przez nich wykonywanych;
11) wystąpienie z wnioskiem o wydanie upoważnienia do przetwarzania danych osobowych oraz zapewnienie ich aktualności;
12) przygotowywanie projektów umów i porozumień o współadministrowaniu oraz projektów umów powierzenia przetwarzania danych osobowych;
13) przeprowadzanie analizy planowanego powierzenia przetwarzania danych osobowych zgodnie art. 28 RODO we współpracy z IOD;
14) przeprowadzanie oceny skutków dla ochrony danych osobowych;
15) zgłaszanie IOD potrzeb w zakresie dodatkowego przeszkolenia użytkowników z zakresu bezpieczeństwa przetwarzania i ochrony danych osobowych;
16) przeprowadzanie analizy ryzyka naruszenia praw lub wolności osób fizycznych, o której mowa w § 32 Polityki;
17) współpraca z IOD w zakresie ochrony danych osobowych.

§ 13. Do zadań użytkowników należy:
1) przestrzeganie przepisów z zakresu ochrony danych osobowych, w tym RODO, Ustawy, Polityki oraz zgodnych z nią regulacji wewnętrznych;
2) zapoznanie się z treścią Polityki oraz złożenie oświadczenia potwierdzającego ten fakt wraz z zobowiązaniem do bezterminowego zachowania w tajemnicy przetwarzanych danych osobowych oraz sposobów ich zabezpieczania;
3) przetwarzanie danych osobowych zgodnie z zasadami, o których mowa w § 1 ust. 3;
4) zgłaszanie IOD zdarzenia, w którym doszło do naruszenia ochrony danych osobowych lub mogło dojść do naruszenia ochrony danych osobowych;
5) udział w audycie, o którym mowa w rozdziale 12, w tym umożliwienie IOD przeprowadzenia czynności w toku audytu;
6) współpraca z IOD w zakresie ochrony danych osobowych;
7) zabezpieczanie danych osobowych oraz dokumentów zawierających dane osobowe przed przypadkowym lub niezgodnym z prawem zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do przetwarzanych danych osobowych.

2. Oświadczenie, o którym mowa w ust. 1 pkt 2 dołącza się do akt osobowych pracownika bądź do umowy zawartej z użytkownikiem innym niż pracownik bądź do sprawy z udziałem użytkownika innego niż pracownik.

§ 14. Nieprzestrzeganie Polityki może skutkować odpowiedzialnością dyscyplinarną lub inną odpowiedzialnością wynikającą z przepisów prawa.

Rozdział 2

Rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania

§ 15. 1. Kierujący komórką organizacyjną prowadzi, uzupełnia oraz aktualizuje rejestr czynności przetwarzania zgodnie z właściwością komórki, której pracą kieruje.

2. Rejestr, o którym mowa w ust. 1, zawiera informacje o procesach przetwarzania realizowanych przez komórkę organizacyjną, związanych z czynnościami przetwarzania, rozumianych jako 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 czynności te są podejmowane.

3. Kierujący komórką organizacyjną dokonuje czynności, o których mowa w ust. 1 i 2 we współpracy z IOD.

4. W przypadku zmian w realizowanych procesach przetwarzania, w tym dotyczących danych osobowych powierzonych przez inne podmioty, polegających na ich rozszerzeniu lub ograniczeniu, wynikających w szczególności ze zmian przepisów prawa powszechnie obowiązującego lub zmian organizacyjnych w Ministerstwie, kierujący komórką organizacyjną niezwłocznie uwzględnia ten fakt w rejestrze, o którym mowa w ust. 1.

5. Rejestr czynności przetwarzania oraz każda jego aktualizacja jest przekazywana do IOD przy wykorzystaniu EZD, w celu prowadzenia zbiorczego rejestru czynności przetwarzania, po podpisaniu przez kierującego komórką organizacyjną.

6. Formularz rejestru czynności przetwarzania stanowi załącznik nr 1 do Polityki.

§ 16. 1. Kierujący komórką organizacyjną prowadzi, uzupełnia oraz aktualizuje rejestr kategorii czynności przetwarzania zgodnie z właściwością komórki, której pracą kieruje.

2. Rejestr, o którym mowa w ust. 1, zawiera informacje o procesach przetwarzania realizowanych przez komórkę organizacyjną w przypadku, w którym Ministrowi powierzono przetwarzanie danych osobowych na podstawie umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego.

3. Kierujący komórką organizacyjną dokonuje czynności, o których mowa w ust. 1 i 2 we współpracy z IOD.

4. W przypadku zmian w realizowanych procesach przetwarzania związanych z powierzeniem Ministrowi przetwarzania danych osobowych, w szczególności zawarcia nowych umów lub porozumień w tym zakresie, kierujący komórką organizacyjną niezwłocznie uwzględnia ten fakt w rejestrze, o którym mowa w ust. 1.

5. Rejestr kategorii czynności przetwarzania oraz każda jego aktualizacja jest przekazywana do IOD przy wykorzystaniu EZD, w celu prowadzenia zbiorczego rejestru kategorii czynności przetwarzania, po podpisaniu przez kierującego komórką organizacyjną.

6. Minister nadzoruje prowadzenie w Ministerstwie rejestru kategorii czynności przetwarzania danych osobowych.

7. Formularz rejestru kategorii czynności przetwarzania stanowi załącznik nr 2 do Polityki.

§ 17. 1. Komórki organizacyjne prowadzą rejestry, o których mowa w § 15 i 16, w formie elektronicznej.

2. IOD prowadzi rejestry zbiorcze obejmujące rejestry, o których mowa w § 15 i 16, w formie elektronicznej.

3. IOD, raz na pół roku, organizuje dokonywanie przeglądu rejestrów, o których mowa w § 15 i 16, w celu zapewnienia ich aktualności.

Rozdział 3

Udzielanie upoważnień do przetwarzania danych osobowych i ewidencja osób upoważnionych

§ 18. 1. Do przetwarzania danych osobowych mogą być dopuszczone jedynie osoby posiadające pisemne upoważnienie udzielone przez administratora albo osobę przez niego upoważnioną.

2. Warunkiem przekazania przez administratora upoważnienia, o którym mowa w ust. 1, jest odbycie przez osobę, która ma otrzymać upoważnienie szkolenia z zakresu ochrony danych osobowych, które prowadzone jest zgodnie z § 36 ust. 2.

3. Osoba, o której mowa w ust. 2, przed rozpoczęciem przetwarzania danych osobowych składa oświadczenie o zapoznaniu się z przepisami RODO, Ustawy oraz procedurami i zasadami dotyczącymi ochrony danych osobowych wynikającymi z Polityki.

4. Do złożenia wniosku - poprzez przygotowanie projektu upoważnienia oraz jego zatwierdzenie w EZD - o udzielenie upoważnienia do przetwarzania danych osobowych jest obowiązany kierujący komórką organizacyjną, w której zatrudniony jest pracownik objęty wnioskowaniem, kierujący komórką organizacyjną właściwą w sprawie z udziałem osoby innej niż pracownik, realizującej zadania na rzecz Ministra lub Ministerstwa, a w przypadku zawarcia z taką osobą umowy cywilnoprawnej, w tym umowy bądź porozumienia w sprawie stażu, wolontariatu lub praktyki - kierujący komórką organizacyjną, na wniosek której zawarto taką umowę lub powstał inny stosunek prawny.

5. W przypadku powierzenia osobie, o której mowa w ust. 2 funkcji wynikających z przepisów powszechnie obowiązujących bądź przyjętych regulacji, do złożenia wniosku - poprzez przygotowanie projektu upoważnienia oraz jego zatwierdzenie w EZD - o udzielenie upoważnienia do przetwarzania danych osobowych jest obowiązany kierujący komórką organizacyjną właściwą w danym obszarze.

6. Projekt upoważnienia, o którym mowa w ust. 4 lub 5, kierujący komórką organizacyjną przygotowuje zgodnie z wzorem, stanowiącym załącznik nr 3 do Polityki, a następnie przekazuje do podpisu administratorowi lub osobie przez niego upoważnionej.

7. Upoważnienie, o którym mowa w ust. 1, traci moc w przypadku:

1) jego odwołania;
2) odwołania ze stanowiska – w przypadku wyższych stanowisk w służbie cywilnej;
3) ustania stosunku pracy;
4) ustania stosunku zobowiązaniowego wynikającego z umowy cywilnoprawnej;
5) zakończenia stażu;
6) zakończenia wolontariatu;
7) zakończenia praktyki;
8) przeniesienia pracownika do innej komórki organizacyjnej w Ministerstwie;
9) ustania innego stosunku prawnego, na podstawie którego przetwarzane są dane osobowe;
10) zakończenia pełnienia powierzonej funkcji;
11) zakończenia wykonywania zadań na rzecz Ministra lub Ministerstwa w oparciu o przepisy powszechnie obowiązujące bądź przyjęte regulacje stanowiące podstawę wykonywania zadań;
12) upływu czasu, na który zostało wydane.

8. Na wniosek kierującego komórką organizacyjną administrator albo osoba przez niego upoważniona może odwołać udzielone upoważnienie, o którym mowa w ust. 1, w szczególności w przypadku niewłaściwego przetwarzania danych osobowych przez osobę upoważnioną.

9. Formularz wniosku o odwołanie upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 4 do Polityki.

10. Komórka organizacyjna właściwa do spraw kadr niezwłocznie powiadamia administratora albo osobę przez niego upoważnioną, o każdym przypadku ustania stosunku pracy, odwołania ze stanowiska lub zakończenia pełnienia powierzonej funkcji. O ustaniu stosunku zobowiązaniowego z tytułu umowy cywilnoprawnej, zakończeniu stażu, wolontariatu lub praktyki lub innego stosunku prawnego powiadamia kierujący komórką organizacyjną, na wniosek której została zawarta taka umowa bądź powstał inny stosunek

prawny, a w pozostałych przypadkach o zakończeniu wykonywania zadań na rzecz Ministra lub Ministerstwa powiadamia kierujący komórką organizacyjną właściwą w danym obszarze.

11. Upoważnienie do przetwarzania danych osobowych jest udzielane przez administratora albo osobę przez niego upoważnioną, a następnie przekazywane pracownikowi oraz komórce organizacyjnej właściwej do spraw kadr w przypadku pracownika, a w pozostałych przypadkach o których mowa w ust. 4 i 5 do komórki wnioskującej.

12. Użytkownik potwierdza otrzymanie i zapoznanie się z upoważnieniem do przetwarzania danych osobowych, w zależności od sposobu jego przekazania: notatką zaakceptowaną w EZD, wiadomością elektroniczną (e-mail) albo podpisem na upoważnieniu do przetwarzania danych osobowych w formie papierowej.

§ 19. 1. Administrator albo osoba przez niego upoważniona prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych. W przypadku, jeżeli osobą upoważnioną do udzielania upoważnień do przetwarzania danych osobowych jest kierujący komórką organizacyjną, ewidencja, o której mowa w zdaniu pierwszym, jest prowadzona przez sekretariat tej komórki organizacyjnej.

2. Ewidencja, o której mowa w ust. 1, jest prowadzona w formie elektronicznej i zawiera w szczególności:

1) numer upoważnienia w rejestrze i datę jego udzielenia;
2) imię i nazwisko osoby upoważnionej;
3) wskazanie komórki organizacyjnej, w której pracownik jest zatrudniony, dana osoba wykonuje czynności na podstawie stosunku zobowiązaniowego z tytułu umowy cywilnoprawnej, stażu, wolontariatu lub praktyki lub na innej podstawie;
4) datę złożenia przez pracownika lub osobę, o której mowa w pkt 3, oświadczenia o zapoznaniu się z treścią Polityki oraz o zobowiązaniu do bezterminowego zachowania w tajemnicy przetwarzanych danych osobowych oraz sposobów ich zabezpieczania;
5) zakres upoważnienia;
6) datę wygaśnięcia upoważnienia lub jego odwołania;
7) inne uwagi dotyczące udzielonego upoważnienia lub jego odwołania.

3. Dopuszcza się wydawanie innych upoważnień do przetwarzania danych osobowych, niż określonych w niniejszej Polityce w przypadku, gdy obowiązek ten wynika z przepisów prawa powszechnie obowiązującego lub w innych szczególnie uzasadnionych przypadkach wiążących się z poleceniem przetwarzania wydanym przez Ministra występującego w roli administratora, współadministratora lub podmiotu przetwarzającego. Treść i forma takiego upoważnienia jest opiniowana przez IOD. W przypadku, gdy IOD wyda opinię negatywną, ostateczną decyzję podejmuje administrator.

Rozdział 4

Powierzenie przetwarzania danych osobowych

§ 20. 1. Przetwarzanie danych osobowych, dla których administratorem jest Minister, może zostać powierzone innemu podmiotowi, pod warunkiem zawarcia przez Ministra z tym podmiotem pisemnej umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego, zgodnie z art. 28 RODO.

2. W Ministerstwie funkcjonuje wzór umowy powierzenia przetwarzania danych osobowych, który jest dostępny na stronie intranetowej Ministerstwa oraz w EZD. Wzór określa istotne postanowienia umowne, które w szczególnie uzasadnionych przypadkach mogą ulegać zmianom mającym na celu dostosowanie ich do stanu faktycznego sprawy, w tym do treści innych stosunków prawnych i uzgodnień stron, jednakże wyłącznie w zakresie, który:

1) nie narusza interesu prawnego lub faktycznego administratora;
2) nie prowadzi do zapewnienia niższej ochrony danych osobowych niż przewidziana w tym wzorze.

3. Dopuszcza się stosowanie standardowych klauzul umownych określonych w decyzji wykonawczej Komisji (UE) 2021/915 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi na podstawie art. 28 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 oraz art. 29 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 (Dz. Urz. UE L 199 z 07.06.2021, str. 18).

4. Umowy powierzenia przetwarzania danych osobowych, o których mowa w ust. 1, mogą być zawierane w imieniu administratora, na podstawie pełnomocnictwa do tej czynności prawnej udzielonego przez administratora.

§ 21. 1. Kierujący komórką organizacyjną konsultuje z IOD konieczność zawarcia umowy powierzenia przetwarzania danych osobowych w związku z realizowanym zadaniem związanym z przetwarzaniem danych osobowych z zachowaniem zasady rozliczalności.

2. Kierujący komórką organizacyjną przygotowuje projekt umowy powierzenia przetwarzania danych osobowych i jest obowiązany uzyskać opinię IOD.

3. Kierujący komórką organizacyjną każdorazowo, przed zawarciem umowy, porozumienia lub innego stosunku prawnego, w ramach którego dochodzi lub może dojść do przetwarzania danych osobowych, zobowiązany jest do konsultacji z IOD w zakresie konieczności zawarcia umowy powierzenia przetwarzania danych osobowych.

4. Kierujący komórką organizacyjną, realizując zadania skutkujące powierzeniem przetwarzania danych osobowych innemu podmiotowi, odpowiada za wybór podmiotu przetwarzającego, który zapewni wystarczającą gwarancję wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie chroniło prawa osób, których dane dotyczą.

5. Podstawowym warunkiem dopuszczalności powierzenia przetwarzania danych osobowych w imieniu administratora jest dokonanie oceny podmiotu przetwarzającego dane osobowe przez komórkę organizacyjną właściwą w sprawie zawarcia umowy, o której mowa w ust. 1.

6. Ocena, o której mowa w ust. 5, musi wykazać, że wybór podmiotu przetwarzającego został uzależniony od zapewnienia wystarczających gwarancji ochrony danych osobowych zgodnie z arkuszem oceny podmiotu przetwarzającego dane osobowe, którego wzór jest określony w załączniku nr 5 do Polityki, lub za pomocą co najmniej jednego z następujących instrumentów: list kontrolnych, żądania oświadczeń o określonej treści, żądania możliwości przeprowadzenia audytu przedwdrożeniowego oraz żądania stosowania określonych standardów praktyk, certyfikatów i norm.

7. W przypadku zastosowania arkusza oceny podmiotu przetwarzającego dane osobowe, o którym mowa w ust. 6, jest on uzupełniany przez podmiot, który będzie przetwarzał powierzone dane osobowe w imieniu administratora.

8. Ocena, o której mowa w ust. 5, bez względu na formę i sposób, przeprowadzana jest przed zawarciem umowy powierzenia przetwarzania danych osobowych, a dokument lub oświadczenie stwierdzające dokonanie tej oceny, jest załączane do tej umowy.

9. Projekt umowy powierzenia przetwarzania danych osobowych oraz uzupełniony arkusz oceny, o którym mowa w ust. 6, albo zastosowanie innych instrumentów oceny wskazanych w ust. 6, są opiniowane przez IOD.

10. Oryginał umowy powierzenia przetwarzania danych osobowych przechowuje komórka organizacyjna zawierająca umowę, chyba że przepisy wewnętrznie obowiązujące w Ministerstwie dotyczące przechowywania umów określają inny tryb.

11. Informacja o zawartej umowie powierzenia przetwarzania danych osobowych, wraz z umową, na podstawie której będą przetwarzane dane osobowe oraz opinią w zakresie oceny podmiotu przetwarzającego jest udostępniania IOD w EZD przez pracownika komórki organizacyjnej, która procedowała jej zawarcie, celem odnotowania jej w rejestrze umów powierzenia przetwarzania danych osobowych.

§ 22. 1. Kierujący komórką organizacyjną sprawuje nadzór nad podmiotem przetwarzającym w zakresie wynikającym z umowy powierzenia przetwarzania danych osobowych.

2. Kierujący komórką organizacyjną wnioskuje o przeprowadzenie czynności kontrolnych w podmiotach, którym zostało powierzone przetwarzanie danych osobowych, do komórki organizacyjnej właściwej do spraw kontroli. Czynności kontrolne przeprowadza komórka organizacyjna właściwa do spraw kontroli, w porozumieniu z IOD, oraz przy udziale wnioskującej komórki organizacyjnej.

3. W ramach czynności kontrolnych, o których mowa w ust. 2, na wniosek kierującego komórką organizacyjną, udział może wziąć inna komórka organizacyjna, której wsparcie jest uzasadnione zakresem kontroli.

4. Z przeprowadzonych czynności kontrolnych jest sporządzana informacja pokontrolna wraz z zaleceniami, do której podmiot kontrolowany może zgłosić swoje uwagi.

5. Kopia informacji pokontrolnej jest przekazywana do wiadomości IOD.

6. Arkusz oceny podmiotu przetwarzającego, o którym mowa w § 21 ust. 6, może być przekazany temu podmiotowi na każdym etapie wykonywania umowy powierzenia przetwarzania danych osobowych celem sprawowania nadzoru nad powierzonymi danymi.

§ 23. Zbiorczy rejestr zawartych umów powierzenia jest prowadzony w formie elektronicznej i zawiera w szczególności:

1) numer oraz datę zawarcia umowy powierzenia przetwarzania danych osobowych;
2) wskazanie komórki organizacyjnej, w zakresie działania której zawarto umowę powierzenia przetwarzania danych osobowych;
3) podmiot, z którym zawarto umowę powierzenia przetwarzania danych osobowych;
4) przedmiot umowy powierzenia przetwarzania danych osobowych;
5) nazwa czynności przetwarzania danych osobowych;
6) datę uzyskania opinii IOD;
7) datę wygaśnięcia umowy powierzenia przetwarzania danych osobowych;
8) istotne uwagi dotyczące umowy.

Rozdział 5

Współadministrowanie danymi osobowymi

§ 24. 1. Kierujący komórką organizacyjną konsultuje z IOD konieczność zawarcia umowy lub porozumienia o współadministrowaniu danymi osobowymi w związku z realizowanym zadaniem związanym z przetwarzaniem danych osobowych z zachowaniem zasady rozliczalności.

2. Współadministrowanie danymi osobowymi wymaga zawarcia umowy lub porozumienia w formie pisemnej lub elektronicznej oraz zastosowania wymogów wynikających z art. 26 RODO.

3. Kierujący komórką organizacyjną przygotowuje projekt umowy lub porozumienia o współadministrowaniu danymi osobowymi i jest obowiązany uzyskać opinię IOD.

4. Oryginał umowy lub porozumienia o współadministrowaniu danymi osobowymi przechowuje komórka organizacyjna zawierająca umowę lub porozumienie, chyba że przepisy wewnętrznie obowiązujące w Ministerstwie dotyczące przechowywania umów i porozumień określają inny tryb.

5. Oryginał umowy lub porozumienia o współadministrowaniu danymi osobowymi przechowuje komórka organizacyjna zawierająca umowę lub porozumienie, chyba że przepisy wewnętrznie obowiązujące w Ministerstwie dotyczące przechowywania umów i porozumień określają inny tryb.

6. Informacja o zawartej umowie lub porozumieniu o współadministrowania jest udostępniania przez pracownika komórki organizacyjnej, która procedowała jej zawarcie, IOD w EZD celem odnotowania jej w rejestrze umów i porozumień o współadministrowaniu danymi osobowymi.

§ 25. Zbiorczy rejestr zawartych umów i porozumień o współadministrowaniu danymi osobowymi jest prowadzony w formie elektronicznej i zawiera w szczególności:

1) numer oraz datę zawarcia umowy lub porozumienia o współadministrowaniu danymi osobowymi;
2) wskazanie komórki organizacyjnej, w zakresie działania której zawarto umowę lub porozumienie o współadministrowaniu danymi osobowymi;
3) podmiot z którym zawarto umowę lub porozumienie o współadministrowaniu danymi osobowymi;
4) przedmiot umowy lub porozumienia o współadministrowaniu danymi osobowymi;
5) nazwa czynności przetwarzania danych osobowych;
6) data uzyskania opinii IOD;
7) data wygaśnięcia umowy lub porozumienia o współadministrowaniu danymi osobowymi;
8) istotne uwagi dotyczące umowy lub porozumienia o współadministrowaniu danymi osobowymi.

Rozdział 6

Obowiązek informacyjny

§ 26. 1. Administrator podejmuje niezbędne środki w zakresie wypełnienia obowiązku informacyjnego, o którym mowa w art. 13 i 14 RODO, wobec osoby, której dane dotyczą tak, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, niespecjalistycznym językiem przekazać informacje, o których mowa w art. 13 RODO (w przypadku zbierania danych osobowych od osoby, której dane dotyczą) i art. 14 RODO (w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą).

2. Informacji, o których mowa w ust. 1, udziela się w formie pisemnej lub elektronicznej, zgodnie z zasadą rozliczalności.

3. Informacja, o której mowa w ust. 2, jest sporządzana w formie klauzuli informacyjnej i dostosowywana do procesu przetwarzania danych osobowych realizowanego przez komórkę organizacyjną.

4. Elementy klauzuli informacyjnej określa załącznik nr 6 do Polityki.

§ 27. 1. Za wypełnianie obowiązków informacyjnych, o których mowa w § 26 ust. 1 i 2, odpowiedzialny jest kierujący komórką organizacyjną, w której dane będą przetwarzane albo podmiot, któremu powierzono przetwarzanie danych osobowych zgodnie z § 20 i 21, jeżeli umowa powierzenia przetwarzania danych osobowych taki obowiązek określa.

2. Kierujący komórką organizacyjną realizującą proces przetwarzania danych osobowych, z którym wiąże się konieczność spełnienia obowiązku informacyjnego, o którym mowa w § 26, dokumentuje realizację spełnienia tego obowiązku za pomocą EZD, z wyjątkiem systemów i narzędzi komunikacji elektronicznej lub systemów teleinformatycznych przeznaczonych do realizacji określonych wyspecjalizowanych usług oraz spraw, w przypadku których kierujący komórką organizacyjną potwierdza spełnienie realizacji obowiązku informacyjnego w tych systemach lub narzędziach komunikacji elektronicznej.

3. W przypadku zbierania danych osobowych bezpośrednio od osoby, której dane dotyczą, kierujący komórką organizacyjną jest obowiązany do wypełnienia wobec tej osoby obowiązku informacyjnego przez przekazanie podczas pozyskiwania danych klauzuli informacyjnej zawierającej informacje, o których mowa w art. 13 RODO.

4. W przypadku zbierania danych osobowych w sposób inny, niż od osoby, której dane dotyczą, kierujący komórką organizacyjną jest obowiązany do wypełnienia wobec tej osoby obowiązku informacyjnego, o którym mowa w art. 14 RODO, przez przekazanie klauzuli informacyjnej:

1) w rozsądnym terminie po pozyskaniu danych osobowych - najpóźniej w ciągu miesiąca - mając na uwadze konkretne okoliczności przetwarzania danych osobowych;
2) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą - najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą;
3) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.

5. Obowiązek informacyjny nie jest realizowany, jeżeli istnieją przesłanki zwalniające z tego obowiązku, o których mowa w art. 13 ust. 4 i art. 14 ust. 5 RODO.

§ 28. 1. Za aktualność i zgodność klauzul informacyjnych, o których mowa w § 26 z przepisami prawa powszechnie obowiązującego oraz wymaganiami Polityki, jest odpowiedzialny, kierujący komórką organizacyjną, w której realizowany jest proces przetwarzania danych osobowych, z wyłączeniem przypadków, w których klauzula informacyjna dotyczy zadania realizowanego w więcej niż jednej komórce organizacyjnej.

2. W przypadkach, o których mowa w ust. 1, w których dana klauzula informacyjna dotyczy zadania realizowanego w więcej niż jednej komórce organizacyjnej, za aktualność i zgodność klauzul informacyjnych z przepisami prawa powszechnie obowiązującego oraz wymaganiami Polityki odpowiadają kierujący komórkami organizacyjnymi stosujący daną klauzulę informacyjną, przy czym IOD koordynuje proces uzgadniania jednolitej treści takiej klauzuli.

3. Kierujący komórką organizacyjną przygotowuje projekt klauzuli informacyjnej i jest obowiązany uzyskać akceptację IOD.

4. Do stosowania są dopuszczone wyłącznie klauzule informacyjne zaakceptowane przez IOD z zachowaniem zasady rozliczalności.

5. Każda zmiana klauzul informacyjnych, o których mowa w ust. 4, wymaga akceptacji IOD.

6. Obowiązujące klauzule informacyjne są zamieszczane przez IOD na stronie intranetowej Ministerstwa.

Rozdział 7

Realizacja praw osób, których dane osobowe dotyczą

§ 29. 1. Administrator umożliwia osobom, których dane dotyczą wykonywanie praw przysługujących im na mocy przepisów RODO, w tym postępowania w przypadku złożenia przez osobę, której dane dotyczą żądania realizacji jej praw przysługujących na mocy art. 7 i art. 15-22 RODO oraz postępowania w przypadku konieczności zawiadomienia osoby fizycznej o naruszeniu jej danych osobowych na mocy art. 34 RODO (prawo do bycia poinformowanym o naruszeniu danych osobowych).

2. W przypadku wystąpienia z żądaniem realizacji praw osób, których dane dotyczą, o których mowa w art. 15–22 RODO, wobec których Minister występuje w roli administratora, kierujący komórkami organizacyjnymi oraz upoważnieni przez administratora mają obowiązek udzielenia odpowiedzi tym osobom, bez zbędnej zwłoki, jednak nie później, niż w terminie miesiąca od dnia otrzymania żądania.

3. W razie potrzeby, termin określony w ust. 2, można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań, po uprzednim poinformowaniu osoby, która wystąpiła z żądaniem, z podaniem przyczyn opóźnienia. Jeżeli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

4. Za przygotowanie odpowiedzi na żądanie, o którym mowa w ust. 2, oraz przekazanie wnioskodawcy kopii danych osobowych, jest odpowiedzialny kierujący komórką organizacyjną odpowiedzialną za proces przetwarzania danych osobowych, w której są przetwarzane przedmiotowe dane osobowe.

5. W przypadku, gdy żądanie, o którym mowa w ust. 2, jest kierowane do Ministra będącego podmiotem przetwarzającym, odpowiedź jest konsultowana z właściwym administratorem w trybie i terminie przewidzianym w zawartej umowie powierzenia przetwarzania danych osobowych.

6. Projekt odpowiedzi, o której mowa w ust. 4 i 5, wymaga uzyskania uprzedniej opinii IOD w EZD.

7. Realizacja praw osób, których dane osobowe dotyczą, odbywa się w trybie określonym w RODO z uwzględnieniem przepisów Ustawy.

Rozdział 8

Postępowanie w przypadku podejrzenia naruszenia ochrony danych osobowych

§ 30. 1. Użytkownik jest obowiązany do niezwłocznego – po jego zidentyfikowaniu – zgłoszenia IOD każdego zdarzenia stanowiącego naruszenie ochrony danych osobowych lub mogącego stanowić naruszenie ochrony danych osobowych, o którym mowa w art. 4 pkt 12 RODO, na adres iod@msit.gov.pl.

2. Użytkownik o zgłoszeniu informuje także bezpośredniego przełożonego lub przełożonego kierującego komórką organizacyjną Ministerstwa.

3. Formularz zgłoszenia stanowi załącznik nr 7 do Polityki.

4. Użytkownik po dokonaniu zgłoszenia, o którym mowa w ust. 1, jest obowiązany w szczególności do:

1) powstrzymania się od rozpoczęcia lub kontynuowania pracy, jak również podejmowania jakichkolwiek czynności, mogących mieć wpływ na ustalenie przyczyn zaistniałego zdarzenia;
2) podjęcia niezbędnych działań w celu zapobieżenia dalszym naruszeniom;
3) udzielenia IOD niezbędnych wyjaśnień dotyczących zaistniałego zdarzenia;
4) zebrania danych, dokumentów i dowodów mających na celu umożliwienie przeprowadzenia postępowania wyjaśniającego.

5. Użytkownik, który dokonał zgłoszenia podejmuje wraz z IOD niezbędne czynności w celu udokumentowania zdarzenia stanowiącego naruszenie ochrony danych osobowych lub mogącego stanowić naruszenie ochrony danych osobowych, w tym okoliczności wystąpienia zdarzenia, jego skutków oraz podjętych działań zaradczych.

6. Po otrzymaniu zgłoszenia, o którym mowa w ust. 1, IOD niezwłocznie przeprowadza czynności wyjaśniające.

7. IOD podejmuje działania, o których mowa w ust. 6, w celu doradzenia administratorowi w zakresie:

1) podjęcia decyzji czy zgłoszone zdarzenie stanowi naruszenie ochrony danych osobowych;
2) przeprowadzenia oceny wagi naruszenia;
3) konieczności poinformowania organu nadzorczego o naruszeniu;
4) konieczności poinformowania osób, których dane dotyczą o naruszeniu;
5) wydania zaleceń komórce organizacyjnej właściwej ze względu na przedmiot naruszenia.

8. IOD, w ramach przeprowadzanych czynności wyjaśniających, jest uprawniony w szczególności do:

1) wystąpienia o dodatkowe wyjaśnienia do użytkownika, który dokonał zgłoszenia oraz do innych osób, których wyjaśnienia mogą mieć wpływ na ocenę zdarzenia, wskazując termin na przekazanie wyjaśnień;
2) żądania przekazania przez właściwą komórkę organizacyjną dowodów wystąpienia zdarzenia stanowiącego naruszenie ochrony danych osobowych lub mogącego stanowić naruszenie ochrony danych osobowych;
3) dokonania sprawdzenia, w szczególności uzyskania dostępu do pomieszczeń, urządzeń i systemów teleinformatycznych lub dokumentacji;
4) nakazania powstrzymania się od kontynuowania pracy w zakresie przetwarzania danych osobowych;
5) czasowego odebrania lub ograniczenia uprawnień wskazanym użytkownikom lub wszystkim użytkownikom danego systemu teleinformatycznego.

9. Dokonując oceny IOD uwzględnia okoliczności naruszenia, w tym jego ciężar, skalę, możliwy wpływ na sytuację osób fizycznych, lub prawdopodobieństwo wystąpienia wpływu, a w szczególności bierze pod uwagę:

1) rodzaj naruszenia, w tym czy doszło do nieuprawnionego ujawnienia, utraty, zniszczenia, zmodyfikowania danych osobowych lub nieuprawnionego uzyskania dostępu do danych osobowych;
2) rodzaj, poziom wrażliwości i skalę danych osobowych, których dotyczy naruszenie, zwłaszcza czy naruszenie dotyczy danych osobowych szczególnych kategorii;
3) czy dane osobowe, których dotyczy naruszenie, można łatwo powiązać z osobą fizyczną, której te dane dotyczą;
4) wagę potencjalnych konsekwencji dla osób fizycznych;

5) specjalne cechy osób fizycznych, których dane dotyczą;
6) liczbę osób fizycznych, których dotyczy naruszenie.

10. Z przeprowadzonych czynności wyjaśniających, z uwzględnieniem elementów o których mowa w ust. 7 i 8, IOD sporządza notatkę i po złożeniu podpisu podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu albo podpisem tradycyjnym niezwłocznie przedkłada ją administratorowi albo osobie przez niego upoważnionej.

11. Na podstawie notatki, o której mowa w ust. 10, administrator albo osoba przez niego upoważniona, podejmuje decyzję co do sposobu realizacji w związku ze zgłoszonym zdarzeniem w postaci notatki zatwierdzonej w EZD albo odpowiedniej adnotacji złożonej w sposób tradycyjny na notatce, o której mowa w ust. 10.

12. W przypadku naruszenia ochrony danych osobowych, administrator albo osoba przez niego upoważniona bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu.

13. W przypadku gdy przekazanie wymaganych przez PUODO informacji nie jest możliwe w terminie 72 godzin, administrator w porozumieniu z IOD przesyła część informacji, wskazując jednocześnie termin ich uzupełnienia, a w przypadku uchybienia temu terminowi dokonuje zgłoszenia, wyjaśniając powody niedotrzymania tego terminu.

14. Kierujący komórką organizacyjną upoważniony przez administratora, we współpracy z IOD, zawiadamia osoby, których dane dotyczą, o naruszeniu ochrony danych osobowych, zgodnie z art. 34 RODO, których dotyczy naruszenie, w najkrótszym możliwym czasie, zgodnie z formularzem stanowiącym załącznik nr 8 do Polityki.

15. W przypadku gdy indywidualne zawiadomienie osób fizycznych o naruszeniu, o którym mowa w ust. 14, nie jest możliwe, administrator w porozumieniu z IOD, przekazuje komórce organizacyjnej Ministerstwa właściwej do spraw realizacji zadań informacyjno-promocyjnych projekt publicznego komunikatu w celu jego zamieszczenia na stronie internetowej Ministerstwa.

16. IOD, w imieniu administratora, przekazuje zalecenia zawarte w notatce, o której mowa w ust. 9, kierującemu komórką organizacyjną, w której doszło do naruszenia ochrony danych osobowych i kierującemu komórką organizacyjną, której zakres realizowanych zadań może mieć wpływ na minimalizację ryzyka wystąpienia naruszenia w przyszłości.

17. Kierujący komórką organizacyjną, w terminie 7 dni od dnia otrzymania zaleceń, ustala sposób i termin ich realizacji, powiadamiając o tym w formie pisemnej IOD.

18. W przypadku odmowy realizacji zaleceń, kierujący komórką organizacyjną przedstawia, w terminie 7 dni od dnia otrzymania zaleceń, swoje stanowisko w formie pisemnej administratorowi albo osobie przez niego upoważnionej i IOD.

19. W sytuacji, o której mowa w ust. 18, administrator albo osoba przez niego upoważniona podejmuje decyzję dotyczącą realizacji zaleceń, informując o tym kierującego komórką organizacyjną i IOD.

20. W przypadkach gdy po dokonanym zgłoszeniu, o którym mowa w ust. 1, IOD nie stwierdzi naruszenia ochrony danych osobowych, sporządza notatkę i po złożeniu podpisu podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu lub podpisu tradycyjnego niezwłocznie przedkłada ją administratorowi albo osobie przez niego upoważnionej.

21. Przepisy ust. 1-19 stosuje się także w przypadkach, w których naruszenie dotyczy danych osobowych powierzonych do przetwarzania Ministrowi, dla których nie jest on administratorem.

22. W przypadku gdy naruszenie dotyczy danych osobowych, wobec których Minister występuje w roli podmiotu przetwarzającego, administrator w porozumieniu z IOD wysyła informacje i dokumenty do administratora w trybie i terminie wynikającym z umowy powierzenia przetwarzania danych osobowych.

23. W przypadku umów powierzenia przetwarzania danych osobowych, o których mowa w § 20, zawieranych z osobami trzecimi innymi niż osoby upoważnione, zasady zgłaszania naruszeń określa ta umowa.

§ 31. 1. IOD, w imieniu administratora, prowadzi rejestr incydentów i naruszeń ochrony danych osobowych, w którym dokumentuje zdarzenia mogące stanowić naruszenie ochrony danych osobowych oraz

w których stwierdzono naruszenie ochrony danych osobowych, w szczególności okoliczności zdarzenia, jego skutki oraz podjęte działania zaradcze.

2. Formularz rejestru stanowi załącznik nr 9 do Polityki.

3. Rejestr jest prowadzony w formie elektronicznej.

Rozdział 9

Analiza ryzyka naruszenia praw lub wolności osób fizycznych

§ 32. 1. W Ministerstwie przetwarzanie danych osobowych odbywa się z uwzględnieniem ryzyka naruszenia praw lub wolności osób fizycznych przy uwzględnieniu charakteru, zakresu, kontekstu i celów przetwarzania danych osobowych.

2. Analizę ryzyka przeprowadza się w celu:

1) dokonania przeglądu technicznych i organizacyjnych środków ochrony danych osobowych;
2) zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzania danych osobowych;
3) weryfikacji skuteczności stosowanych środków ochrony.

3. W razie konieczności administrator, po przeprowadzeniu analizy ryzyka i zidentyfikowaniu zagrożeń, wdraża dodatkowe środki służące zwiększeniu bezpieczeństwa danych osobowych.

4. Analizę ryzyka naruszenia praw lub wolności osób fizycznych dokonuje się nie rzadziej niż raz w roku na wniosek komórki właściwej do spraw zarządzania ryzykiem w Ministerstwie.

5. Poza dokonywaną cyklicznie raz w roku analizą ryzyka dla naruszenia praw lub wolności osób fizycznych, analiza ryzyka jest przeprowadzana także w przypadku:

1) planowania nowej czynności przetwarzania danych osobowych, a także planowania zmian w zarejestrowanej czynności przetwarzania danych osobowych mających wpływ na bezpieczeństwo danych osobowych, szczególnie w przypadku planowania użytkowania systemu informatycznego, w którym będzie dokonywana dana czynność przetwarzania danych osobowych lub planowania uregulowania legislacyjnego danej czynności przetwarzania danych osobowych, przy czym analiza musi być przeprowadzona co najmniej na etapie dokonywania oceny skutków regulacji dla danego projektu ustawy lub rozporządzenia, w szczególności zmiany charakteru, celu lub zakresu przetwarzanych danych osobowych – przeprowadza ją kierujący komórką organizacyjną odpowiadającą za realizację czynności przetwarzania danych osobowych, we współpracy z IOD;
2) naruszenia ochrony danych osobowych – przeprowadza ją administrator, zgodnie z ustaloną procedurą, po zasięgnięciu opinii IOD w sposób określony w § 23 ust. 7, 8 i 10.

6. W przypadkach, o których mowa w ust. 5 informacja o przeprowadzonej identyfikacji i analizie ryzyka jest przekazywana do komórki właściwej do spraw ryzyka w Ministerstwie.

7. Komórka właściwa do spraw ryzyka ustala z administratorem metodę przeprowadzania analizy ryzyka naruszenia praw lub wolności osób fizycznych w Ministerstwie oraz procedurę dotyczącą procesu przeprowadzania w Ministerstwie analizy ryzyka naruszenia praw lub wolności osób fizycznych.

Rozdział 10

Przeprowadzenie oceny skutków dla ochrony danych osobowych

§ 33. 1. Kierujący komórką organizacyjną, w fazie planowania wdrażania nowego zadania, w przypadku gdy jego realizacja będzie związana z przetwarzaniem danych osobowych, których administratorem lub współadministratorem jest lub będzie Minister, w szczególności w sytuacji planowania, projektowania lub przygotowania przedsięwzięć o charakterze programowym, projektowym lub legislacyjnym, w tym wprowadzenia do użytkowania nowych systemów teleinformatycznych, jeżeli ich realizacja będzie związana z przetwarzaniem danych osobowych w szczególności w sytuacji planowania wdrożenia systemu informatycznego w którym będą przetwarzane dane osobowe związane z realizacją nowego zadania lub

planowania uregulowania legislacyjnego danego zagadnienia, przeprowadza ocenę, w ramach której dokonuje się opisu operacji przetwarzania oraz badania kryteriów DPIA, zgodnie z formularzem stanowiącym załącznik nr 10 do Polityki. Sporządzoną ocenę kierujący komórką organizacyjną przekazuje do konsultacji IOD, który może wydać zalecenie wykonania analizy, o której mowa w ust. 2.

2. W przypadku gdy w wyniku oceny, o której mowa w ust. 1, zidentyfikowane zostaną potencjalne wysokie ryzyka wiążące się z przetwarzaniem danych osobowych, w tym wysokie ryzyka naruszenia praw i wolności osób, których dane będą przetwarzane, w szczególności kradzieży tożsamości, straty finansowej, naruszenia dobrego imienia, naruszenia poufności danych chronionych tajemnicą zawodową, nieuprawnionego odwrócenia pseudonimizacji, utraty przysługujących osobom praw i wolności lub sprawowania kontroli nad swoimi danymi osobowymi, ujawnienia danych szczególnej kategorii, kierujący komórką organizacyjną w porozumieniu z IOD przeprowadza analizę DPIA.

3. Formularz analizy DPIA stanowią załączniki nr 11-A do nr 11-D do Polityki.

4. Kierujący komórką organizacyjną, uwzględniając wynik analizy DPIA oraz charakter, zakres, kontekst i cele przetwarzania, wdraża odpowiednie środki techniczne i organizacyjne, w tym minimalizujące ryzyko naruszenia praw i wolności.

5. W przypadku gdy planowane przetwarzanie danych osobowych będzie powodować wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, a zminimalizowanie tego ryzyka jest utrudnione, w szczególności z uwagi na ograniczenia technologiczne i ekonomiczne, przed rozpoczęciem przetwarzania Minister występujący w roli administratora lub współadministratora konsultuje się z PUODO, zgodnie z art. 36 RODO.

Rozdział 11

Audyty zgodności przetwarzania danych osobowych

§ 34. 1. Audyt zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz Polityki jest przeprowadzany przez IOD.

2. IOD opracowuje roczny plan audytów, który przedstawia do wiadomości administratorowi najpóźniej do końca roku kalendarzowego poprzedzającego rok objęty tym planem.

3. Roczny plan audytów określa:

1) przedmiot, zakres oraz termin przeprowadzenia poszczególnych audytów;
2) czynności przetwarzania danych osobowych objęte audytem;
3) konieczność weryfikacji zgodności przetwarzania danych osobowych z:
   a) zasadami przetwarzania danych osobowych,
   b) zasadami dotyczącymi zabezpieczenia danych osobowych,
   c) zasadami przekazywania danych osobowych.

4. Niezależnie od rocznego planu audytów, IOD może przeprowadzać audyty doraźne, w szczególności:

1) po stwierdzeniu naruszenia ochrony danych osobowych;
2) na wniosek administratora lub z własnej inicjatywy, jeżeli uzna to za niezbędne dla zapewnienia zgodności przetwarzania danych z przepisami o ochronie danych osobowych.

§ 35. 1. IOD zawiadamia w EZD kierującego komórką organizacyjną objętą audytem o zakresie planowanych czynności w terminie co najmniej 7 dni przed dniem przeprowadzenia czynności, z wyłączeniem przypadków, o których mowa w **§ 34 ust. 4**.

2. IOD dokumentuje w EZD czynności przeprowadzone podczas audytu w komórce organizacyjnej objętej audytem.

3. Z przeprowadzonego audytu IOD sporządza sprawozdanie zawierające w szczególności ocenę i zalecenia w odniesieniu do zakresu objętego audytem.

4. Formularz sprawozdania, o którym mowa w ust. 3, stanowi załącznik nr 12 do Polityki.

5. Sprawozdanie, o którym mowa w ust. 3, jest udostępniane kierującemu komórką organizacyjną objętą audytem, który może zgłosić uwagi do sprawozdania w terminie 3 dni roboczych od dnia jego otrzymania.

6. IOD informuje kierującego komórką organizacyjną objętą audytem o uwzględnieniu bądź nieuwzględnieniu uwag do sprawozdania, o którym mowa w ust. 3, w terminie 3 dni roboczych od dnia ich otrzymania.

7. Sprawozdanie, o którym mowa w ust. 3, wraz z uwagami zgłoszonymi przez kierującego komórką organizacyjną i stanowiskiem IOD, IOD udostępnia administratorowi.

8. IOD przedkłada administratorowi roczne sprawozdanie z przeprowadzonych audytów w terminie do końca marca następnego roku kalendarzowego.

Rozdział 12

Szkolenia

§ 36. 1. Administrator zapewnia szkolenia dla pracowników w zakresie obowiązujących przepisów oraz podstawowych zagrożeń związanych z przetwarzaniem danych osobowych w celu pogłębiania ich wiedzy i poszerzania świadomości w zakresie ochrony danych osobowych.

2. Szkolenia dla nowych użytkowników z zakresu ochrony danych osobowych przeprowadza się niezwłocznie po rozpoczęciu przez nich pracy, stażu, praktyki, wolontariatu lub realizacji umowy cywilnoprawnej w Ministerstwie, przed rozpoczęciem przetwarzania danych osobowych.

3. Szkolenia prowadzi IOD lub inny pracownik Ministerstwa posiadający wiedzę z zakresu ochrony danych osobowych lub podmiot zewnętrzny posiadający wiedzę z zakresu ochrony danych osobowych.

4. W ramach pogłębiania wiedzy w zakresie ochrony danych osobowych IOD przygotowuje materiały pomocnicze do poszerzania wiedzy, zalecenia, wytyczne, opinie, które przekazuje pracownikom bezpośrednio lub za pośrednictwem kierujących komórkami organizacyjnymi lub zamieszcza je na stronie intranetowej Ministerstwa.

5. Kierujący komórką organizacyjną może wystąpić do IOD z wnioskiem o przeprowadzenie szkolenia dla osób upoważnionych, w zakresie ochrony danych osobowych zgodnie z potrzebami komórki organizacyjnej.

6. Administrator może zobowiązać użytkowników do odbywania szkoleń również po uzyskaniu upoważnienia do przetwarzania danych osobowych. Nieukończenie takiego szkolenia może skutkować odwołaniem upoważnienia do przetwarzania danych osobowych do momentu pozytywnego ukończenia szkolenia przez użytkownika.

7. IOD może wydawać dokumenty związane z przeprowadzonymi szkoleniami oraz prowadzi ewidencję osób przeszkolonych w zakresie ochrony danych osobowych.

Rozdział 13

Przegląd Polityki

§ 37. 1. Polityka podlega okresowemu przeglądowi dokonywanemu przez IOD, w zakresie jej aktualności i adekwatności, nie rzadziej niż raz do roku.

2. Informację o przeprowadzonym przeglądzie, o którym mowa w ust. 1, IOD przekazuje Ministrowi.

3. Polityka może podlegać także przeglądom w przypadku:

1) wystąpienia poważnego naruszenia ochrony danych osobowych;
2) pojawienia się nowych i istotnych rodzajów ryzyka;
3) zmian regulacji prawnych dotyczących ochrony danych osobowych;
4) istotnych zmian organizacyjnych w Ministerstwie;
5) zgłaszanych potrzeb w zakresie ujętym w Polityce.

Załącznik nr 1 do Polityki Ochrony Danych Osobowych w Ministerstwie Sportu i Turystyki

Rejestr czynności przetwarzania danych osobowych w Ministerstwie Sportu i Turystyki

Nazwa i dane kontaktowe administratora		Inspektor Ochrony Danych
Nazwa		
Adres		
Email		
Telefon		

Lp.	Komórka organizacyjna	ID zbioru	Kategoria danych osobowych i ich rodzaj (ze szczególnym wskazaniem danych osobowych szczególnej kategorii, o których mowa w art. 9 RODO)	Czynności przetwarzania	Kategoria osób, których dane osobowe dotyczą	Podstawa prawna przetwarzania	Cel przetwarzania	Źródło pochodzenia danych (zbierane przez Ministerstwo czy otrzymane od innego podmiotu, jeśli tak, to od jakiego)	Kategorie odbiorców danych (o ile są one przez Ministerstwo przekazywane lub ujawniane)	Przekazywanie danych (do państwa trzeciego lub organizacji międzynarodowej)	Termin usunięcia danych (wynikający z przepisów prawa, z instrukcji archiwalnej i in.)	Rodzaje technicznych i organizacyjnych środków bezpieczeństwa(art. 32 RODO lub odwołanie do istniejących procedur wewnętrznych)	Sposób przetwarzania danych osobowych (przetwarzanie w postaci elektronicznej, w tym konkretne systemy informatyczne, przetwarzanie w postaci fizycznej)	Czy dane osobowe są aktualne i prawidłowe?	Utrzymywanie lub przetwarzanie zbioru przez podmiot zewnętrzny wskazać pod-stawę np. umowa przetwarzania

Załącznik nr 2 do Polityki Ochrony Danych Osobowych w Ministerstwie Sportu i Turystyki

Rejestr kategorii czynności przetwarzania danych osobowych w Ministerstwie Sportu i Turystyki

Nazwa i dane kontaktowe administratora		Inspektor Ochrony Danych
Nazwa		
Adres		
Email		
Telefon		

Lp.	Komórka organizacyjna MSiT	Kategorie przetwarzań	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (jeżeli jest to możliwe)	Administrator				Czas trwania przetwarzania	Nazwy państw trzecich lub organizacji międzynarodowych, do których dane są przekazywane	Dokumentacja odpowiednich zabezpieczeń danych osobowych przekazywanych na podstawie art. 49 ust. 1 akapit drugi	Podprzetwarzający (podwykonawca) - jeśli dotyczy	
				Nazwa i dane kontaktowe administratora	Nazwa i dane kontaktowe współadministratora (jeśli dotyczy)	Nazwa i dane kontaktowe przedstawiciela administratora (jeśli wyznaczono)	Inspektor ochrony danych administratora (jeśli powołano)				Nazwa i dane kontaktowe podprzetwarzającego (podwykonawcy)	Kategorie podpowierzonych przetwarzań

Minister
Sportu i Turystyki

UPOWAŻNIENIE nr ……../202…./AD

do przetwarzania danych osobowych

Na podstawie art. 29 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, str. 1, z późn. zm.), zwanego dalej „RODO", upoważniam Panią/Pana*:

Imię i nazwisko osoby upoważnionej: **Imię Nazwisko**

Komórka organizacyjna: **Nazwa Departamentu/Biura**

do przetwarzania danych osobowych[1], których administratorem, współadministratorem lub podmiotem przetwarzającym jest Minister Sportu i Turystyki, zgodnie z zakresem zadań:

1) określonych odpowiednio w regulaminie organizacyjnym Ministerstwa Sportu i Turystyki, regulaminie wewnętrznym komórki organizacyjnej Ministerstwa Sportu i Turystyki[2], wynikających ze stosunku pracy lub sprawowanej funkcji lub innych zadań powierzonych przez pracodawcę,
2) określonych w umowie cywilnoprawnej/ umowie o staż/ umowie praktyki/ porozumieniu o wolontariat/ innych umowach lub porozumieniach*
……
(podać numer umowy/porozumienia i datę zawarcia)
3) określonych w przepisach powszechnie obowiązujących bądź przyjętych regulacjach stanowiących podstawę do wykonywania zadań na rzecz Ministra Sportu i Turystyki lub obsługującego go urzędu tj. Ministerstwa Sportu i Turystyki*

[1] Zgodnie z art. 4 pkt 2 RODO „przetwarzanie" oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

[2] Komórka organizacyjna – departament, biuro, Gabinet Polityczny Ministra oraz jednoosobowe i wieloosobowe stanowiska pracy w Ministerstwie Sportu i Turystyki.

na podstawie których są realizowane polecenia administratora w rozumieniu art. 29 RODO[3].

Niniejsze upoważnienie może być w każdym czasie odwołane.

Niniejsze upoważnienie wygasa z chwilą jego odwołania lub przeniesienia do pracy w innym Departamencie/ Biurze w Ministerstwie Sportu i Turystyki lub ustania stosunku prawnego na podstawie, którego przetwarzane są dane osobowe w Ministerstwie Sportu i Turystyki, tj. odwołania z zajmowanego stanowiska lub ustania stosunku pracy na zajmowanym stanowisku, zakończenia sprawowanej funkcji, zakończenia wykonywania innych zadań powierzonych przez pracodawcę, zakończenia realizacji umowy cywilnoprawnej/umowy o staż/umowy o praktyki/porozumienia o wolontariat/innych umów lub porozumień.....

(podać nr umowy/porozumienia i przewidziany w umowie/porozumieniu okres na jaki została zawarta)

lub zakończenia wykonywania zadań na rzecz Ministra Sportu i Turystyki lub obsługującego go urzędu tj. Ministerstwa Sportu i Turystyki w oparciu o przepisy powszechnie obowiązujące bądź przyjęte regulacje stanowiące ich podstawę*

..... .

(podać planowaną datę zakończenia prac Komisji/Zespołu/Rady w której uczestniczy osoba fizyczna niebędąca pracownikiem)

Z upoważnienia Ministra Sportu i Turystyki

.....

Data, podpis/ podpis elektroniczny/

Potwierdzam przyjęcie upoważnienia

.....

(data i podpis)

* Niepotrzebne usunąć.

Osoba wskazana w upoważnieniu zapoznała się z Polityką ochrony danych osobowych oraz zobowiązała się do zachowania tajemnicy składając na tę okoliczność oświadczenie według wzoru stanowiącego załącznik nr 2 do zarządzenia Ministra Sportu i Turystyki z dnia 24 lutego 2026 r. w sprawie wprowadzenia Polityki ochrony danych osobowych w Ministerstwie Sportu i Turystyki.

[3] Zgodnie z art. 29 RODO podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.

Załącznik nr 4 do Polityki Ochrony Danych
Osobowych w Ministerstwie Sportu i Turystyki

WNIOSEK O ODWOŁANIE UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH
dla
……..
(imię i nazwisko)

Zgodnie z art. 29 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, z późn. zm.)

Dane	
Nazwa komórki organizacyjnej	
Rodzaj zatrudnienia/inny stosunek prawny (pracownik, praktykant, stażysta, zleceniobiorca, inna [jaka?])	
Wnioskowana data odwołania upoważnienia do przetwarzania danych osobowych	**dd-mm-rrrr**
Data i numer odwoływanego upoważnienia do przetwarzania danych osobowych	**Upoważnienie z dnia dd-mm-rrrr nr ……**

_____
(data i podpis kierującego komórką organizacyjną)

Ministerstwo Sportu i Turystyki			
Arkusz oceny podmiotu przetwarzającego			
Ankieta dla podmiotu przetwarzającego			
Dane podmiotu przetwarzającego	Nazwa		
	Adres		
	Dane kontaktowe		
Data wypełnienia dokumentu	dd-mm-rrrr		
Uprzejmie prosimy o udzielenie wyczerpujących odpowiedzi na pytania w tabeli (arkusz drugi - pytania) oraz dołączenie załączników, jeżeli jest to konieczne			
Osoba uprawniona do wypełnienia ankiety po stronie podmiotu przetwarzającego	Imię, nazwisko, stanowisko		
Pytania: **Uwaga: rodzaj pytań powinien być dostosowany do przedmiotu umowy powierzenia - zawarte tu pytania są przykładowe**			
Lp.	**Pytanie**	**Odpowiedź**	**Uwagi**
Pytania organizacyjne			
1.	Czy wyznaczono Inspektora Ochrony Danych (IOD) lub osobę odpowiedzialną za obszar ochrony danych? Jeżeli IOD nie został wyznaczony, czy dokonano analizy pod kątem obowiązku wyznaczenia IOD i czy analiza ta została udokumentowana? Podaj kontakt do IOD lub wskaż inną osobę do kontaktu w zakresie ochrony danych osobowych.		
2.	Czy stosowana jest zasada ochrony danych w fazie projektowania oraz zasada domyślnej ochrony danych dla wprowadzanych zmian? Podaj, w jaki sposób organizacja wykazuje stosowanie zasad.		
3.	Czy wdrożono proces analizy ryzyka naruszenia praw lub wolności osób fizycznych? Podaj ogólne zasady działania procesu.		

4.	Czy osoby wyznaczone do wykonywania zadań z zakresu powierzenia przetwarzania posiadają odpowiednią wiedzę i przygotowanie praktyczne do wykonywania swoich obowiązków z zakresu przetwarzania powierzonych danych? Uzasadnij odpowiedź np. fakt odbycia szkolenia.		
5.	Czy osoby delegowane do obsługi danych powierzonych przez administratora posiadają nadane upoważnienia do przetwarzania danych?		
6.	Czy wdrożono politykę ochrony danych i zasady zarządzania systemami informatycznymi? Jeśli wprowadzono inne polityki lub procedury z zakresu ochrony danych osobowych, podaj ich nazwy.		
7.	Czy osoby przetwarzające dane zostały poinformowane o konieczności stosowania dokumentów wskazanych w poprzednim punkcie? Podaj, w jaki sposób.		
8.	Czy osoby upoważnione do przetwarzania danych osobowych zostały zobowiązane do zachowania danych osobowych w tajemnicy? Przedstaw wzór upoważnienia do przetwarzania danych osobowych wraz z obowiązkiem zachowania tajemnicy co do przetwarzanych danych lub wskazaniem w jakim dokumencie osoby upoważnione do przetwarzania danych zostały zobowiązane do zachowania tajemnicy.		
9.	Jak wygląda procedura realizacji praw osób, których dane dotyczą uwzględniającą wspieranie administratora w realizacji tych praw? Wskaż odpowiedni wyciągu z procedury albo opisz mechanizm.		
10.	Czy podmiot przetwarzający miał kontrolę, postępowanie wyjaśniające lub inne działania prowadzone przez organ nadzorczy w związku z powierzeniem przetwarzania? Jeśli tak, wskaż co było przedmiotem działań organu nadzorczego i jakie są wyniki przeprowadzonych działań.		
Inwentaryzacja danych oraz Rejestr Kategorii Czynność Przetwarzania (RKCP)			
11.	Czy dokonano inwentaryzacji danych osobowych poprzez np. przeprowadzenie audytu?		
12.	Czy istnieje Rejestr Kategorii Czynności Przetwarzania i czy jest on zgodny z art. 30 RODO?		
Naruszenie ochrony danych osobowych i jego zgłoszenie			
13.	Czy wdrożona została procedura zarządzania incydentami bezpieczeństwa i naruszeniami ochrony danych osobowych? Wskaż lub opisz odpowiednią procedurę lub przyjęty w podmiocie sposób		

	postępowania.		
14.	Czy prowadzony jest wewnętrzny rejestr incydentów bezpieczeństwa i naruszeń ochrony danych osobowych? (incydent poufności, integralności oraz dostępności danych) Podaj ilość wpisów dotyczących incydentów i naruszeń.		
15.	Czy w podmiocie przetwarzającym występowały naruszenia, które były zgłaszane do organu nadzorczego w zakresie ochrony danych osobowych? Jeśli tak, podaj kiedy oraz ich przedmiot.		
Podmioty podprzetwarzające (subprocesorzy)			
16.	Czy prowadzony jest rejestr umów podmiotów, którym dane są dalej powierzane?		
17.	Czy podmiot przetwarzający podpisał stosowne umowy powierzenia z podwykonawcami?		
18.	Czy podmiot przetwarzający korzysta z usług tylko takich podmiotów zewnętrznych/podwykonawców, którzy zostali wcześniej przez niego sprawdzeni pod kątem zapewnienia odpowiedniego poziomu ochrony danych osobowych? Opisz krótko, jak wybierani są i weryfikowani subprocesorzy.		
19.	Czy podmiot przetwarzający zbadał aby wszyscy podwykonawcy zostali zobowiązani do zachowania poufności przetwarzanych danych osobowych?		
20.	Czy serwery podwykonawców znajdują się na terenie UE?		
21.	Czy w ramach planowanego powierzenia przetwarzania danych osobowych w ramach umowy z Urzędem Ochrony Konkurencji i Konsumentów nastąpi przekazanie danych do państwa trzeciego? Jeżeli tak, podaj nazwy państw.		
Środki ochrony			
22.	Czy w oparciu o analizę ryzyka wdrożono adekwatne środki organizacyjne i techniczne zapewniające odpowiedni poziom bezpieczeństwa dla poufności, integralności, dostępności i odporności systemów oraz usług? Podaj stosowane organizacyjne i techniczne środki bezpieczeństwa.		
23.	Czy stosowane są adekwatne do ryzyka techniczne środki zabezpieczeń, np. IDS, firewalle, monitoring sieci, licencje aktualizowane na bieżąco?		

	Podaj jakie.		
24.	Czy stosowana jest pseudonimizacja lub/i szyfrowanie danych osobowych? Jeżeli tak, podaj, jakie techniki/rozwiązania są stosowane będą dla przedmiotowej umowy.		
25.	Czy podmiot przetwarzający stosuje fizyczne zabezpieczenia pomieszczeń/obszarów przetwarzania danych osobowych przed dostępem osób nieuprawnionych? Podaj jakie.		
26.	Czy opracowano plan ciągłości działania dla utrzymania zdolności do szybkiego przywrócenia dostępności danych w razie incydentu fizycznego lub technicznego? Podaj datę ostatniego testu planu ciągłości działania.		
27.	Czy stosowane jest regularne testowanie i ocenianie skuteczności wdrożonych środków organizacyjnych i technicznych mających zapewnić odpowiedni poziom bezpieczeństwa przetwarzania? Podaj, jak wygląda proces.		
28.	Czy podmiot przetwarzający zarządza dostępem do systemów oraz programów komputerowych, w którym są przetwarzane dane osobowe, poprzez proces nadawania, przeglądu i odbierania uprawnień oraz stosuje bezpieczne mechanizmy uwierzytelniania? Wskaż odpowiednią procedurę nadawania dostępu.		
29.	Czy podmiot przetwarzający wdrożył i stosuje zasady udzielania dostępu tylko do informacji niezbędnych do zakresu wykonywanych obowiązków oraz zasady ograniczonego dostępu? W myśl zasady ograniczonego dostępu użytkownik ma mieć dostęp tylko do tych informacji i zasobów, które są mu niezbędne do wykonywania swojej pracy.		
30.	Czy podmiot przetwarzający przechowuje kopie bezpieczeństwa w bezpiecznej lokalizacji oraz zabezpiecza kopie przed ich nieuprawnionym dostępem?		
31.	Czy podmiot przetwarzający prowadzi regularnie audyty dotyczące zasad bezpieczeństwa informacji, w tym danych osobowych, w celu weryfikacji spełniania wymogów polityki ochrony danych lub innej wewnętrznej procedury, w tym ocena skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania? Przekaż informację z jaką regularnością takie audyty się odbywają oraz o wskazanie raportu/ odpowiednich wniosków z raportu audytowego.		

32.	Czy system informatyczny służący do przetwarzania danych osobowych zabezpiecza się przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej? Podaj w jaki sposób.		
33.	Czy komputery, na których są przetwarzane dane osobowe mają włączone automatyczne blokowanie ekranu po zdefiniowanym okresie bezczynności pracownika?		
34.	Czy dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych?		
35.	Czy kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem?		
36.	Czy podmiot przetwarzający jest właścicielem infrastruktury fizycznej (serwerownia, serwery), na której funkcjonują systemy informatyczne, w których są przetwarzane dane osobowe?		
37.	Czy serwery podmiotu przetwarzającego znajdują się na terenie UE?		
38.	Czy stosuje się szyfrowanie dysków komputerów przenośnych?		
Pytania inne			
39.			
Osoba uprawniona do wypełnienia ankiety po stronie podmiotu przetwarzającego		Imię, nazwisko, stanowisko	

Elementy wymagane przez art. 13 i 14 RODO w klauzuli informacyjnej dotyczącej przetwarzania danych osobowych ….

(należy doprecyzować kto jest adresatem tej klauzuli poprzez wskazanie kategorii osób, np. dla kandydatów do pracy, w związku z udzielaniem świadczeń z Zakładowego Funduszu Świadczeń Socjalnych, dla stron umowy itd)

Zgodnie z art. 13 ust. 1 i 2 (jeśli dane osobowe są zbierane bezpośrednio od osoby, której dotyczą)/art. 14 ust. 1 i 2 (jeśli dane pozyskiwane są z innego źródła niż bezpośrednio od osoby, której dotyczą) 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 (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.), dalej jako: RODO, Ministerstwo Sportu i Turystyki uprzejmie informuje, że:

Tożsamość administratora

1. Administratorem Pani/Pana danych jest: Minister Sportu i Turystyki, z siedzibą w Warszawie (00-082), przy ul. Senatorskiej 14, kontakt e-mail:……

Dane kontaktowe inspektora ochrony danych osobowych

2. Kontakt do inspektora ochrony danych: Inspektor Ochrony Danych Ministerstwo Sportu i Turystyki, ul. Senatorska 14, 00-082 Warszawa, adres e-mail: iod@msit.gov.pl .

Z inspektorem ochrony danych można kontaktować się we wszystkich sprawach dotyczących przetwarzania danych osobowych oraz korzystania z praw związanych z przetwarzaniem danych.

3. Źródło pochodzenia danych *(ten punkt należy wpisać i uzupełnić wówczas jeśli dane pozyskiwane są z innego źródła niż bezpośrednio od osoby, której dotyczą)*

Źródłem Pani/Pana danych osobowych jest…/W przypadku kiedy Pani/Pana dane nie zostały bezpośrednio przez Panią/Pana udostępnione, zostały udostępnione przez …. /Dane osobowe otrzymaliśmy bezpośrednio od Pani/Pana lub od Pani/Pana pracodawcy/Wykonawcy będącego stroną zawartej z MSiT umowy - w celu zawarcia oraz prawidłowej realizacji umowy itp.

4. Kategorie przetwarzanych danych osobowych *(ten punkt należy wpisać i uzupełnić wówczas jeśli dane pozyskiwane są z innego źródła niż bezpośrednio od osoby, której dotyczą, należy wskazać rodzaje kategorii danych, które będą przetwarzane)*

- np. imię i nazwisko,
- np. służbowy nr telefonu,
- np. służbowy adres e-mail,
- np. miejsce pracy.

5. Cele przetwarzania danych osobowych i podstawa prawna

Pani/Pana dane osobowe będą przetwarzane w celu:

- *(podać cel/cele przetwarzania danych osobowych, np. zawarcie i realizacja umowy świadczenia usług/ przeprowadzenie konkursu i wyłonienie laureatów/realizacji wniosku o uzyskanie świadczenia socjalnego oraz wskazać cel w zakresie archiwizacji czy publikacji danych z wyszczególnieniem przesłanek legalności)*[4].

6. Odbiorcy danych lub kategorie odbiorców danych

Pani/Pana dane osobowe są udostępniane podmiotowi, który przetwarza dane osobowe w imieniu Administratora na podstawie zawartej umowy powierzenia przetwarzania danych osobowych (tzw. podmiot przetwarzający), tj. …. *(należy wskazać nazwę podmiotu, jeśli to możliwe, bądź wskazać rodzaj podmiotów, np. firmy świadczące usługi informatyczne, jeśli nie ma to zastosowania – usunąć to zdanie)* oraz …….. *(wskazać inne podmioty jeśli istnieją)./* Pani/Pana dane mogą zostać przekazane do podmiotów, które dysponują informacjami niezbędnymi do prawidłowej realizacji umowy, podmiotom świadczącym na rzecz administratora usługi IT.
Pani/Pana dane osobowe mogą zostać przekazane organom i podmiotom upoważnionymi do pozyskiwania danych osobowych na podstawie przepisów prawa *(można wskazać z nazwy)*

7. Okres przechowywania danych osobowych

Pani/Pana dane osobowe będą przechowywane przez czas niezbędny do realizacji celu przetwarzania, tj. ……*(wskazać kiedy ten cel zostanie osiągnięty poprzez wskazanie konkretnego okresu np. 3 miesiące od dnia zawarcia porozumienia,* a następnie przez okres (…) (określenie na podstawie Instrukcji Kancelaryjnej obowiązującej w Ministerstwie Sportu i Turystyki (kat. archiwalna …) i przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach. *(podać okres przechowywania danych osobowych z uwzględnieniem okresu archiwizacji (zgodnego z JRWA). Jeżeli nie ma możliwości wskazania okresu przechowywania, należy podać kryterium ustalania tego okresu).*

8. Osoba, której dane osobowe są przetwarzane ma prawo do:

- dostępu do danych i uzyskania ich kopii, zgodnie z art. 15 RODO,
- sprostowania (poprawiania) swoich danych osobowych, jeśli są błędne lub nieaktualne, zgodnie z art. 16 RODO,
- usunięcia przetwarzanych danych osobowych, zgodnie z art. 17 RODO, z zastrzeżeniem ust. 3 *(w przypadku przetwarzania w celu realizacji obowiązku prawnego jakim jest obowiązek archiwizacyjny dane mogą zostać usunięte po zakończeniu okresu archiwizacji),*
- ograniczenia przetwarzania danych osobowych, zgodnie z art. 18 RODO;
- wniesienia sprzeciwu wobec przetwarzania, zgodnie z art. 21 RODO (*jeśli przetwarzanie danych osobowych jest oparte na art. 6 ust. 1 lit. e lub f RODO)*
- przenoszenia danych, zgodnie z art. 20 RODO, z zastrzeżeniem ust. 3 *(jeśli przetwarzanie odbywa się na podstawie zgody, o której mowa w art. 6 ust. 1 lit a lub art. 9 ust. 2 lit. a albo umowy w myśl art. 6 ust. 1 lit b RODO oraz w sposób zautomatyzowany)*
- wycofania zgody na przetwarzanie danych osobowych w dowolnym momencie, bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem *(jeśli przetwarzanie odbywa się na podstawie zgody, o której mowa w art. 6 ust. 1 lit a lub art. 9 ust. 2 lit. a RODO).*

Aby skorzystać z powyższych praw należy skontaktować się z nami lub z naszym inspektorem ochrony danych

---

[4] Art …. RODO *(wskazać odpowiednią przesłankę z art. 6 lub 9 RODO) w* zw. z…*(jeśli dotyczy, wskazać przepis prawa materialnego). Przy wyborze art. 6 ust. 1 lit. c lub e RODO należy dodatkowo podać przepis prawa materialnego stanowiący źródło obowiązku prawnego ciążącego na administratorze / zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.*

(dane kontaktowe zawarte są powyżej).

Niezależnie od powyższego przysługuje Pani/Panu uprawnienie do wniesienia skargi do organu nadzorczego, tj. Prezesa Urzędu Ochrony Danych Osobowych na adres Urzędu Ochrony Danych Osobowych (ul. St. Moniuszki 1A, 00-014 Warszawa), gdy uzna Pani/Pan, że przetwarzanie Pani/Pana danych osobowych narusza przepisy RODO.

Informacja o przekazywaniu danych osobowych do państw trzecich

Nie przekazujemy Pani/Pana danych do państw trzecich. (*Należy dostosować w przypadkach, gdy dane osobowe będą przekazywane poza Europejski Obszar Gospodarczy lub do organizacji międzynarodowych)*.

Informacja o zautomatyzowanym podejmowaniu decyzji

Pani/Pana dane osobowe nie podlegają zautomatyzowanemu przetwarzaniu, w tym profilowaniu (*Jeśli podlegają - wskazać istotne informacje o zasadach zautomatyzowanego podejmowania decyzji oraz znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą, np. w jaki sposób będą oceniane określone cechy osoby fizycznej. Przykładową konsekwencją takiego przetwarzania może być automatyczne odrzucenie przez system aplikacji w przypadku niespełnienia wymogów formalnych)*.

Informacja o dowolności lub obowiązku podania danych osobowych

Podanie przez Panią/Pana danych jest ….
a) wymogiem ustawowym/wynikającym z przepisów normatywnych,
b) warunkiem zawarcia umowy,
d) dobrowolne, ale niepodanie danych w zakresie wymaganym przez administratora może skutkować ……..;
Skutkiem niepodania danych może być np. niezawarcie umowy/ nierozpatrzenie aplikacji.

Zgłoszenie naruszenia ochrony danych osobowych

Lp.	ZGŁOSZENIE NARUSZENIA	
1.	Oznaczenie roli Ministra Sportu i Turystyki (administrator, współadministrator, podmiot przetwarzający)	*administrator, współadministrator, podmiot przetwarzający*
2.	Data i godzina wystąpienia naruszenia (jeśli jest znana)	*data i godzina*
3.	Data i godzina powzięcia informacji o naruszeniu	*data i godzina*
4.	Miejsce naruszenia	*adres, nazwa systemu, itp.*
5.	Opis naruszenia ochrony danych osobowych	*opis okoliczności zdarzenia stanowiącego naruszenie*
6.	Nośniki danych osobowych, których dotyczy naruszenie	*wskazanie nośników (np. dokument elektroniczny, pismo tradycyjne).*
7.	Kategorie osób, których danych osobowych dotyczy naruszenie	*wskazanie kategorii osób (np. pracownik, pacjent, usługobiorca, usługodawca, wnioskodawca)*
8.	Dokładna lub ewentualnie przybliżona liczba osób, których danych osobowych dotyczy naruszenie	*wskazanie dokładnej lub ewentualnie przybliżonej liczby osób*
9.	Kategorie danych osobowych, których dotyczy naruszenie (zakres danych osobowych)	*wskazanie jakich danych dotyczy naruszenie, tj. zwykłych (np. imię, nazwisko, adres zamieszkania, numer PESEL, numer telefonu, adres e-mail), szczególnej kategorii (np. danych dotyczące zdrowia, biometrycznych, genetycznych)*
10.	Określenie liczby wpisów danych osobowych, których dotyczy naruszenie (ewentualnie przybliżona liczba)	*liczba wpisów danych osobowych (na ilu dokumentach/nośnikach pojawiają się dane osobowe)*
11.	Skutki naruszenia, w tym możliwe konsekwencje naruszenia dla osób fizycznych	*opis faktycznie zaistniałych skutków naruszenia i możliwe konsekwencje (np. wykorzystanie danych osobowych przez osoby niepowołane, utrata kontroli nad danymi osobowymi, strata finansowa, ograniczenie możliwości realizacji praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, naruszenie dobrego imienia, utrata poufności danych osobowych chronionych tajemnicą zawodową).*
12.	Środki zastosowane w celu zaradzenia naruszeniu ochrony danych, w celu zminimalizowania jego ewentualnych negatywnych skutków (jeśli zostały już podjęte)	*opis działań podjętych w celu usunięcia skutków naruszenia oraz zminimalizowania ryzyka powtórzenia się naruszenia w przyszłości*
13.	W przypadku, gdy zgłoszenia naruszenia nie dokonano niezwłocznie od momentu powzięcia informacji o naruszeniu – wyjaśnienie przyczyn opóźnienia	*wyjaśnienie przyczyn opóźnienia*
14.	Imię, nazwisko, stanowisko, numer telefonu, adres e-mail, komórka organizacyjna osoby dokonującej zgłoszenia	*imię, nazwisko, stanowisko, numer telefonu, adres, e-mail, komórka organizacyjna (departament/biuro)*

Zawiadomienie o naruszeniu ochrony danych osobowych

Szanowna Pani/ Szanowny Panie,

na podstawie art. 34 ust. 1 i 2 RODO[5] w imieniu Ministra Sportu i Turystyki – administratora danych osobowych przetwarzanych w……. – uprzejmie informuję, że stwierdzono zdarzenie, które mogło skutkować/skutkowało naruszeniem Pani/Pana danych osobowych.

Naruszenie polegało na *[opis naruszenia]*.

Naruszenie dotyczyło danych osobowych obejmujących: *[zakres danych osobowych]*. Czas trwania nieprawidłowości obejmował okres od dnia ……do dnia……

Naruszenie ochrony danych osobowych zostało przez Ministra Sportu i Turystyki zgłoszone Prezesowi Urzędu Ochrony Danych Osobowych.

Zapewniamy, że podejmujemy wszelkie możliwe działania w celu zminimalizowania ryzyka i ewentualnych negatywnych konsekwencji naruszenia.

Potencjalnymi konsekwencjami dla osób, których dane mogły zostać naruszone przedmiotowym zdarzeniem, może być nieuprawnione wykorzystanie danych osobowych w następujący sposób *[wskazanie możliwych ryzyk wynikających z naruszenia]*.

Niezależnie od podjętych działań naprawczych, w celu minimalizacji ewentualnych negatywnych skutków podajemy informacje o krokach, które można podjąć w związku z naruszeniem *[opis rekomendowanych działań]*.

Informacje dotyczące naruszenia ochrony danych osobowych, można uzyskać, kontaktując się z……Inspektorem Ochrony Danych w Ministerstwie Sportu i Turystyki pod adresem e-mail: ……. Adres korespondencyjny: ……..

Z wyrazami szacunku

[5] Rozporządzenie 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, str. 1, z późn. zm.).

Załącznik nr 9 do Polityki Ochrony Danych Osobowych w Ministerstwie Sportu i Turystyki

Rejestr incydentów i naruszeń ochrony danych osobowych w Ministerstwie Sportu i Turystyki

Lp.	Miejsce wystąpienia naruszenia	Czy stwierdzono naruszenie	Data wystąpienia naruszenia	Data stwierdzenia naruszenia	Osoba zgłaszająca naruszenie/ nazwa komórki organizacyjnej	Okoliczności wystąpienia naruszenia	Skutki i konsekwencje wywołane naruszeniem	Podjęte środki zaradcze	Decyzja o zgłoszeniu do organu nadzorczego lub uzasadnienie niezgłoszenia naruszenia	Data zgłoszenia do organu nadzorczego	Decyzja o poinformo-waniu podmiotu danych	Data poinformowania podmiotu danych	Numer sprawy /ID koszulki	Uwagi

OCENA, W RAMACH KTÓREJ DOKONUJE SIĘ OPISU OPERACJI PRZETWARZANIA ORAZ BADANIA KRYTERIÓW DPIA	
I. DANE IDENTYFIKACYJNE	
(1) Nazwa zadania[1] podlegającego ocenie	
(2) Komórka organizacyjna Ministerstwa Sportu i Turystyki odpowiedzialna za wdrażanie nowego zadania	
(3) Kierujący komórką organizacyjną	
(4) Znak sprawy w EZD	
II. INFORMACJE WSTĘPNE	
(1) Czynność przetwarzania lub grupa czynności	
(2) Cel/-e przetwarzania	
(3) Kategorie osób i zakres danych	
(4) Rola Ministra Sportu i Turystyki (administrator/ podmiot przetwarzający/ współadministrator)	
III. OPIS OPERACJI PRZETWARZANIA – USTALENIE KONTEKSTU	
(1) Ogólne założenia i opis	
(2) Odbiorcy danych (podmioty, którym ujawnia się dane osobowe)	
(3) Ocena skali przetwarzania (ilu orientacyjnie osób fizycznych dotyczy przetwarzanie)	
(4) Retencja (okres przechowywania) danych	
(5) Zakres geograficzny (na terenie Polski albo krajów EOG)	

[1] Zadania/projektu/przedsięwzięcia – w znaczeniu zestawu czynności, które będą wiązać się z przetwarzaniem danych osobowych.

(6) Sposób/-y pozyskiwania danych (bezpośrednio lub pośrednio od osób fizycznych, wyjaśnienie, podstawa)	
(7) Częstotliwość zbierania	
(8) Przekazywanie danych poza EOG lub organizacjom międzynarodowym	
(9) Zgodność przetwarzania z prawem (należy wskazać przesłankę legalizującą przetwarzanie w oparciu o art. 6 ust. 1 RODO, jeśli dotyczy)	
(10) Podstawa prawna (w przypadku, gdy w pkt 9 wpisano art. 6 ust. 1 lit. c lub e RODO, należy wskazać stanowiące podstawę przepisy prawa krajowego lub UE)	
(11) Przetwarzanie szczególnych kategorii danych osobowych (należy wskazać przesłankę legalizującą przetwarzanie w oparciu o art. 9 ust. 2 RODO, jeśli dotyczy)	
(12) Zasoby lub aktywa – personel	
(13) Zasoby lub aktywa – sprzęt	
(14) Zasoby lub aktywa - oprogramowanie	
(15) Zasoby lub aktywa – siedziba	
(16) Zasoby lub aktywa – sieć	
(17) Współadministrator	
(18) Uzgodnienia ze współadministratorem	
(19) Podmiot/-y przetwarzając(y)/-e	
(20) Powierzenie przetwarzania	
(21) Weryfikacja podmiotu przetwarzającego	
(22) Operacje przetwarzania (zgodnie art. 4 pkt 2 RODO)	
(23) Niezbędność i proporcjonalność operacji przetwarzania do celu przetwarzania	

(24) Funkcjonalny opis operacji przetwarzania	
(25) Realizacja obowiązku informacyjnego	
(26) Środki techniczne i organizacyjne zapewniające bezpieczeństwo	
(27) Projekt klauzul/-i	
(28) Realizacja praw osób, których dane dotyczą	
(29) Sposób pozyskiwania, wycofywania oraz przechowywania zgody	
(30) Treść zgody	
(31) Termin rozpoczęcia przetwarzania	

IV. KRYTERIA KONIECZNOŚCI PRZEPROWADZENIA ANALIZY DPIA (kryteria o których mowa w art. 35 ust. 3 RODO)

(1) Art. 35 ust. 3 lit. a RODO	Systematyczna, kompleksowa ocena czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną	*tak/nie*
(2) Art. 35 ust. 3 lit. b RODO	Przetwarzanie na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o których mowa w art. 10	*tak/nie*
(3) Art. 35 ust. 3 lit. c RODO	Systematyczne monitorowanie na dużą skalę[2] miejsc dostępnych publicznie	*tak/nie*
(4) Art. 35 ust. 4 RODO	Wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych (komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony[3])	*tak/nie*

[2] Zgodnie z motywem 91 RODO operacje przetwarzania o dużej skali to operacje, które służą przetwarzaniu znacznej ilości danych osobowych na szczeblu regionalnym, krajowym lub ponadnarodowym i które mogą wpłynąć na dużą liczbę osób, których dane dotyczą, oraz które mogą powodować wysokie ryzyko.

[3] M.P. z 2019 r. poz. 666 (https://dziennikustaw.gov.pl/M2019000066601.pdf).

V. IDENTYFIKACJA I OCENA RYZYK DLA PRAW LUB WOLNOŚCI OSÓB FIZYCZNYCH	
(1) Czy zadanie może wiązać się z wysokim ryzykiem naruszenia praw i wolności osób[4]	*tak/nie*[5]
(2) Opis ryzyka	

[4] W szczególności: kradzieży tożsamości, straty finansowej, naruszenia dobrego imienia, naruszenia poufności danych chronionych tajemnicą zawodową, nieuprawnionego odwrócenia pseudonimizacji, utraty przysługujących osobom praw i wolności lub sprawowania kontroli nad swoimi danymi osobowymi, ujawnienia danych szczególnej kategorii.

[5] W przypadku, gdy spełniona jest przynajmniej jedna z przesłanek wymienionych z pkt IV (tj. gdy badanie kryteriów DPIA w przynajmniej jednym przypadku przyniesie efekt w postaci odpowiedzi „tak") wymagane jest zaznaczenie „tak").

SZCZEGÓŁOWY OPIS OPERACJI PRZETWARZANIA ORAZ ZASTOSOWANYCH ŚRODKÓW OCHRONY		
NAZWA ZADANIA PODLEGAJĄCEGO OCENIE		
SZCZEGÓŁOWY OPIS ZADANIA		
Lp.	**TREŚĆ PYTANIA**	**ODPOWIEDŹ**
1.	**Opis operacji oraz charakteru przetwarzania danych** *(należy m.in. wskazać, czy zachodzi profilowanie lub zautomatyzowane podejmowanie decyzji)*	
2.	**Cele przetwarzania danych osobowych**	
3.	**Podstawy prawne przetwarzania danych osobowych** *(w tym profilowania oraz automatycznego podejmowania decyzji)*	
4.	**Opis prawnie uzasadnionych interesów realizowanych przez administratora** *(w przypadku, gdy podstawą przetwarzania jest uzasadniony interes administratora)*	
5.	**Kategorie podmiotów, których dane są przetwarzane**	
6.	**Kategorie danych osobowych, które są przetwarzane**	
7.	**Źródło pochodzenia danych** *(należy wskazać, czy dane pochodzą od podmiotu danych, czy są pozyskiwane z innych źródeł)*	
8.	**Podmioty, którym administrator powierza przetwarzanie danych osobowych**	
9.	**Podstawa prawna powierzenia danych**	
10.	**Podmioty, którym administrator udostępnia dane osobowe**	
11.	**Podstawa prawna udostępnienia danych przez administratora**	
12.	**Współadministratorzy danych**	
13.	**Odbiorcy danych poza Europejskim Obszarem Gospodarczym**	

14.	**Podstawa prawna transferu danych poza EOG**	
OPIS ZASOBÓW WYKORZYSTYWANYCH DO PRZETWARZANIA DANYCH		
Lp.	**TREŚĆ PYTANIA**	**OPIS**
1.	**Sprzęt wykorzystywany do przetwarzania danych osobowych** *(np. sprzęt komputerowy, sieci)*	
2.	**Systemy informatyczne (oprogramowanie) wykorzystywane do przetwarzania danych osobowych**	
FIZYCZNE ORAZ TECHNICZNE ŚRODKI OCHRONY DANYCH OSOBOWYCH		
Lp.	**TREŚĆ PYTANIA**	**ODPOWIEDŹ**
1.	**Środki fizyczne oraz techniczne**	

OCENA NIEZBĘDNOŚCI I PROPORCJONALNOŚCI ŚRODKÓW OCHRONY				
NAZWA ZADANIA PODLEGAJĄCEGO OCENIE				
ŚRODKI PRZYCZYNIAJĄCE SIĘ DO ZGODNOŚCI PRZETWARZANIA Z ZASADAMI OGÓLNYMI RODO				
Lp.	**TREŚĆ PYTANIA**	**OPIS PLANOWANYCH ŚRODKÓW ORGANIZACYJNYCH I TECHNICZNYCH**	**OCENA ADEKWATNOŚCI ŚRODKÓW ORAZ ZALECENIA WDROŻENIA DODATKOWYCH ŚRODKÓW**	**WDROŻONE ŚRODKI LUB UZASADNIENIE BRAKU WDROŻENIA**
1.	**Środki podjęte w celu zapewnienia legalności przetwarzania danych osobowych**			
2.	**Środki podjęte w celu zapewnienia zasady ograniczenia celu przetwarzania danych osobowych**			
3.	**Środki podjęte w celu zapewnienia zasady minimalizacji danych osobowych**			
4.	**Środki podjęte w celu zapewnienia zasady ograniczenia czasowego**			
ŚRODKI PRZYCZYNIAJĄCE SIĘ DO ZACHOWANIA PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ				
Lp.	**TREŚĆ PYTANIA**	**OPIS PLANOWANYCH ŚRODKÓW ORGANIZACYJNYCH I TECHNICZNYCH**	**OCENA ADEKWATNOŚCI ŚRODKÓW ORAZ ZALECENIA WDROŻENIA DODATKOWYCH ŚRODKÓW**	**WDROŻONE ŚRODKI LUB UZASADNIENIE BRAKU WDROŻENIA**
1.	**Środki podjęte w celu realizacji obowiązków informacyjnych w stosunku do osoby, której dane dotyczą (art. 12, 13 i 14 RODO).**			

2.	**Środki podjęte w celu realizacji prawa dostępu do danych osobowych (art. 15 ust. 1 RODO)**			
3.	**Środki podjęte w celu realizacji prawa do uzyskania kopii danych (art. 15 ust. 3 RODO)**			
4.	**Środki podjęte w celu realizacji prawa do przenoszenia danych (art. 20 RODO)**			
5.	**Środki podjęte w celu realizacji prawa do sprostowania (art. 16 i 19 RODO)**			
6.	**Środki podjęte w celu realizacji prawa do usunięcia danych (do bycia zapomnianym) (art. 17 i 19 RODO)**			
7.	**Środki podjęte w celu realizacji prawa do ograniczenia przetwarzania (art. 18 i 19 RODO)**			
8.	**Środki podjęte w celu realizacji prawa do wyrażenia sprzeciwu (art. 21 RODO)**			

OCENA ORAZ ZARZĄDZANIE RYZYKIEM			
NAZWA ZADANIA PODLEGAJĄCEGO OCENIE			
OPIS ZAGROŻEŃ MAJĄCYCH WPŁYW NA STOPIEŃ RYZYKA NARUSZENIA PRYWATNOŚCI			
LP.	**KATEGORIE ZAGROŻEŃ**	**KRYTERIA WYRÓŻNIANIA ORAZ PRZYKŁADY MOŻLIWYCH ZAGROŻEŃ**	**ZAGROŻENIA, KTÓRE MOGĄ WYSTĄPIĆ W OCENIANYM PROJEKCIE**
1.	**POUFNOŚĆ (ZAGROŻENIA ZWIĄZANE Z UZYSKANIEM BEZPRAWNEGO DOSTĘPU DO DANYCH)**	Wskazując zagrożenia dla zadania oraz oceniając ich wagę, należy uwzględnić w szczególności **następujące kryteria**: - **ilość danych**, do których osoba nieuprawniona może uzyskać dostęp (np. czy istnieje ryzyko dostępu do dużej bazy danych, czy tylko do pojedynczych dokumentów); - **rodzaj danych**, do których osoba nieuprawniona może otrzymać dostęp (w szczególności, czy są to szczególne kategorie danych - dane wrażliwe, przez które należy rozumieć kategorie danych wskazanych w art. 9 oraz 10 RODO oraz dane osobowe objęte tajemnicami zawodowymi); - **kategorie osób, których dane dotyczą -** np. dane dotyczą osób wymagających szczególnej opieki, tj. dzieci, pracowników, osób należących do bardziej wrażliwych grup społecznych wymagających szczególnej ochrony (osoby chore psychicznie, osoby ubiegające się o azyl lub osoby starsze, pacjenci itp.); **- kategorie osób, które mogą uzyskać bezprawny dostęp do danych** (w szczególności, czy z danymi mogą zapoznać się osoby z wewnątrz, czy z zewnątrz organizacji). **Przykładowe zagrożenia** podlegające ocenie: - Dostęp osoby nieuprawnionej z wewnątrz organizacji do systemów informatycznych służących do przetwarzania danych osobowych o stanie zdrowia. - Dostęp osoby nieuprawnionej z zewnątrz organizacji do nośników służących do przetwarzania danych pracowników (np. komputery służbowe, telefony służbowe).	
2.			
3.			
4.			
5.			
6.			
7.			
1.		Wskazując zagrożenia dla zadania oraz oceniając ich wagę, należy uwzględnić w szczególności **następujące kryteria**: - **ilość danych**, które mogą zostać w niepożądany sposób zmienione (np. czy istnieje ryzyko zmiany danych w dużej bazie danych, czy tylko w pojedynczych dokumentach); - **rodzaj danych**, które mogą ulec niepożądanej zmianie (w szczególności, czy są to szczególne kategorie danych (dane wrażliwe, przez które należy rozumieć	

2.		kategorie danych wskazanych w art. 9 oraz 10 RODO oraz dane osobowe objęte tajemnicami zawodowymi); - **kategorie osób, których dane dotyczą** - np. dane dotyczą osób wymagających szczególnej opieki, tj. dzieci, pracowników, osób należących do bardziej wrażliwych grup społecznych wymagających szczególnej ochrony (osoby chore psychicznie, osoby ubiegające się o azyl lub osoby starsze, pacjenci itp.). **Przykładowe zagrożenia** podlegające ocenie: - Niepożądana modyfikacja danych w systemach informatycznych służących do przetwarzania danych osobowych o stanie zdrowia. - Zmiana danych na nośnikach służących do przetwarzania danych pracowników (np. komputery służbowe, telefony służbowe).	
3.			
4.			
1.	**DOSTĘPNOŚĆ (ZAGROŻENIA ZWIĄZANE Z UTRATĄ DANYCH LUB BRAKIEM DOSTĘPU DO DANYCH PRZEZ ADMINISTRATORA)**	Wskazując zagrożenia dla zadania oraz oceniając ich wagę, należy uwzględnić w szczególności **następujące kryteria**: - **ilość danych**, do których osoba nieuprawniona może uzyskać dostęp (np. czy istnieje ryzyko dostępu do dużej bazy danych, czy tylko do pojedynczych dokumentów); - **rodzaj danych**, do których osoba nieuprawniona może otrzymać dostęp (w szczególności, czy są to szczególne kategorie danych - dane wrażliwe, przez które należy rozumieć kategorie danych wskazanych w art. 9 oraz 10 RODO oraz dane osobowe objęte tajemnicami zawodowymi); - **kategorie osób, których dane dotyczą** - np. dane dotyczą osób wymagających szczególnej opieki, tj. dzieci, pracowników, osób należących do bardziej wrażliwych grup społecznych wymagających szczególnej ochrony (osoby chore psychicznie, osoby ubiegające się o azyl lub osoby starsze, pacjenci itp.). **Przykładowe zagrożenia** podlegające ocenie: - Brak możliwości dostępu do systemów informatycznych służących do przetwarzania danych osobowych o stanie zdrowia. - Zgubienie nośników służących do przetwarzania danych pracowników (np. komputery służbowe, telefony służbowe).	
2.			
1.	**ZAGROŻENIA OGÓLNE**	Zagrożenia związane ze specyfiką zadania	

OCENA ORAZ ZARZĄDZANIE RYZYKIEM						
OCENA RYZYKA POTENCJALNEGO			ZALECENIA DOTYCZĄCE ŚRODKÓW MINIMALIZUJĄCYCH RYZYKO	OCENA RYZYKA SZCZĄTKOWEGO		
ISTOTNOŚĆ (WAGA) ZAGROŻENIA	PRAWDOPODO-BIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	STOPIEŃ RYZYKA POTENCJALNEGO	WDROŻONE ŚRODKI LUB UZASADNIENIE BRAKU WDROŻENIA	ISTOTNOŚĆ (WAGA) ZAGROŻENIA	PRAWDOPODO-BIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	STOPIEŃ SZCZĄTKOWEGO RYZYKA
		0				0
		0				0
		0				0
		0				0
		0				0
		0				0
		0				0
		0				0
		0				0
		0				0
		0				0
		0				0
		0				0
		0				0

OCENA ORAZ ZARZĄDZANIE RYZYKIEM

KONSULTACJE Z ORGANEM NADZORCZYM *(art. 36 RODO)*			KONSULTACJE Z PODMIOTAMI DANYCH *(art. 35 ust. 9 RODO)*			OCENA RYZYKA FINALNEGO		
KONIECZNOŚĆ KONSULTACJI Z ORGANEM (TAK/NIE)	WYNIK KONSULTACJI	WDROŻONE ŚRODKI LUB UZASADNIENIE BRAKU WDROŻENIA	KONIECZNOŚĆ KONSULTACJI Z PODMIOTAMI DANYCH (TAK/NIE)	WYNIK KONSULTACJI	WDROŻONE ŚRODKI LUB UZASADNIENIE BRAKU WDROŻENIA	ISTOTNOŚĆ (WAGA) ZAGROŻENIA	PRAWDOPODO-BIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	OSTATECZNY STOPIEŃ RYZYKA
								0
								0
								0
								0
								0
								0
								0
								0
								0
								0
								0
								0
								0
								0

METODA OCENY RYZYKA POTENCJALNEGO ORAZ SZCZĄTKOWEGO					
ISTOTNOŚĆ (WAGA) ZAGROŻENIA	PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA				
	pomijalne (1)	niskie (2)	średnie (3)	wysokie (4)	krytyczne (5)
pomijalna (1)	1	2	3	4	5
niska (2)	2	4	6	8	10
średnia (3)	3	6	9	12	15
wysoka (4)	4	8	12	16	20
krytyczna (5)	5	10	15	20	25
STOPIEŃ RYZYKA	mało prawdopodobne (1-7)	średnie (8-14)	wysokie (15-25)		

Sprawozdanie z audytu zgodności
przetwarzania danych osobowych z przepisami o ochronie danych osobowych

……..
(nazwa komórki organizacyjnej objętej audytem)

Po przeprowadzeniu czynności sprawdzających w…….....
…….....
(nazwa komórki organizacyjnej objętej audytem)

w okresie od……..do……..…., przedstawiam sprawozdanie z dokonanych czynności.

1.Przedmiot i zakres audytu

Audytem było objęte przetwarzanie danych osobowych w ramach realizowanego/nych przez komórkę organizacyjną procesu/ów określonego/ych w rejestrze czynności przetwarzania
……...……
……...
……...……
……...
(nazwa procesu/ów - z rejestru czynności przetwarzania)

W toku audytu ustalono, że dane osobowe w ramach audytowanego procesu są przetwarzane w sposób zautomatyzowany/niezautomatyzowany* i są wykonywane na tych danych następujące operacje*: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
*(*niepotrzebne skreślić)*

2.Podstawa prawna przeprowadzenia audytu
……
……
……
……

3.Przedmiot audytu
……
……
……
……

4.Zakres audytu
……
……
……
……

5.Podmioty zewnętrzne

……
……
……
……

6.Wykaz czynności podjętych przez Inspektora Ochrony Danych

W toku audytu (*np. odebrano pisemne/ustne wyjaśnienia, przeprowadzono oględziny miejsca przetwarzania danych osobowych, zapoznano się z dokumentacją opisującą przetwarzanie danych osobowych*).

……
……
……
……

7.Opis stanu faktycznego stwierdzonego w toku audytu

W toku audytu ustalono co następuje:

……
……
……
……

8. Ocena zgodności

……
……
……
……

9. Zalecenia w odniesieniu do zakresu objętego audytem

……

……

……

…….

Sporządzone i podpisane przez:

……
……

Załączniki: