POLITYKA OCHRONY DANYCH OSOBOWYCH

Polityka ochrony danych osobowych (PODO) w Warszawskim Instytucie Ekonomicznym zawiera zakres zabezpieczeń stosowanych w odniesieniu do danych osobowych, wskazanie obowiązujących środków organizacyjnych i technicznych oraz mechanizmy ochrony tych danych przetwarzanych w zbiorach zarówno w formie papierowej, jak i elektronicznej, a także danych osobowych przetwarzanych poza zbiorem. PODO normuje mechanizmy aktualizacji dokumentacji związanej z ochroną danych osobowych, a także wprowadza jednolite zasady wydawania upoważnień do przetwarzania danych osobowych, pozwala zarazem monitorować proces udostępniania tych danych i inne aspekty związane z ich przetwarzaniem.

1. Podstawowe pojęcia i skróty

Poniżej przedstawiono najważniejsze pojęcia i definicje obowiązujące w treści niniejszego dokumentu.

1) Rozporządzenie ogólne (RODO) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, opublikowane w Dzienniku Urzędowym Unii Europejskiej L 119/1.

2) Administrator – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania. W znaczeniu powyżej administratorem jest Warszawski Instytut Ekonomiczny a czynności operacyjne związane z realizacją zadań Administratora spoczywają na dyrektorze Instytutu.

3) Organ nadzorczy – oznacza niezależny organ publiczny zgodnie z art. 51 Rozporządzenia ogólnego.

4) Polityka Ochrony Danych Osobowych – dokument opracowany w celu określania obowiązujących zasad w trakcie procesu przetwarzania danych osobowych. Jest on zestawem zasad, praw, procedur i praktycznych rozwiązań regulujących sposób zarządzania tym procesem, w szczególności jego zabezpieczenia i ochrony, a także w kontaktach z otoczeniem.

5) Inspektor Ochrony Danych Osobowych (IODO) – osoba wyznaczona przez Administratora, której zadania polegają na realizacji celów powierzonych jej przez Administratora, w tym wymagań stawianych przed nią na podstawie niniejszej polityki, zgodnie z przepisami rozporządzenia ogólnego, w szczególności art. 39.

6) Administrator systemu informatycznego (ASI) – osoba wyznaczona przez Administratora, której zadaniem jest zapewnienie bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych.

7) Dane osobowe – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, której dotyczą. Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w tym na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka czynników określających fizyczną, ekonomiczną, kulturową lub społeczną tożsamość osoby.

8) Minimalizacja danych – przetwarzanie danych osobowych w sposób adekwatny, stosowny oraz ograniczony do tego, co niezbędne do celów, w których są przetwarzane.

9) Prawidłowość i aktualność danych – właściwość rozumiana jako konieczność podjęcia wszelkich rozsądnych działań, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.

10) Zabezpieczenie danych w systemie informatycznym – wdrożenie, utrzymywanie, eksploatacja, dostosowywanie i zmiana stosownych środków technicznych i organizacyjnych zapewniających ochronę danych

przed ich nieuprawnionym przetwarzaniem oraz przypadkową utratą, zmianą, zniszczeniem lub uszkodzeniem.

11) Integralność danych – właściwość danych polegająca na braku możliwości wprowadzenia do nich zmian w sposób nieautoryzowany.

12) Dostępność danych - właściwość danych polegająca na tym, że są one osiągalne i możliwe do wykorzystania na żądanie, w założonym czasie przez autoryzowany podmiot.

13) Obszar przetwarzania danych osobowych – budynki, pomieszczenia lub części pomieszczeń Instytutu, w których są przetwarzane dane osobowe zarówno w formie papierowej, jak i elektronicznej, a także wszystkie obszary, w których ma miejsce przetwarzanie danych osobowych przez podmioty przetwarzające w związku z działalnością prowadzoną przez Instytut.

14) Zgoda osoby, której dane dotyczą – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

15) Przetwarzanie danych osobowych – operacja lub zestaw operacji wykonywanych na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie, pobieranie, przeglądanie, przesyłanie, rozpowszechnianie, usuwanie lub niszczenie.

16) System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

17) Profilowanie – dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególnosci do analizy lub prognozy aspektów dotyczących pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

18) 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.

19) Naruszenie ochrony danych osobowych – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfkowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

20) Bezpieczeństwo informacji – stan rozumiany jako zachowanie trzech podstawych atrybutów związanych z przetwarzaniem informacje tj. poufności, integralności oraz dostępności, a jednocześnie zapewnienia odporności systemów i usług dotego służących.

21) Bezpieczeństwo systemu informatycznego – zapewnienie odporności sieci lub każdej części systemu, na danym poziomie poufności na przypadkowe zdarzenia albo niezgodne z prawem lub nieprzyjazne działania naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przesyłanych danych osobowych przy zastosowaniu środków technicznych i organizacyjnych.

22) Rozliczalność – konieczność przestrzegania przepisów Rozporządzenia ogólnego przez Administratora, a także możliwość wykazania tego przestrzegania.

23) Uwierzytelnienie – działnie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

24) Usuwanie danych osobowych – działanie bez zbędnej zwłoki polegające na zniszczeniu danych

osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.

25) Zbiór danych – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany, czy też rozproszony funkcjonalnie lub geograficznie.

26) Szczególne kategorie danych osobowych – dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej ososby.

27) Wnioski o skorzystanie z praw – żądania od osób, których dane dotyczą, skierowane do Instytutu w celu skorzystania z przysługujących im praw w odniesieniu do problematyki danych osobowych.

28) System ochrony danych osobowych – system składający się ze zbioru środków prawnych, zarządczych, organizacyjnych i technicznych, utworzony w celu zapewnienia pożądanego przez Administratora poziomu bezpieczeństwa tych danych.

30) Sytuacja kryzysowa – to zazwyczaj niespodziewane i niepożądane zdarzenie lub seria wydarzeń, które mogą stanowić istotne zagrożenie dla pozycji oraz stabilności organizacji jako całości, lub tylko jej części.

2. Cele, zakres i znaczenie bezpieczeństwa ochrony danych osobowych

1. Celem niniejszej Polityki Ochrony Danych Osobowych (zwanej dalej Polityką) jest określenie zasad przetwarzania danych osobowych, jako zestaw praw, reguł, procedur i praktycznych doświadczeń regulujących sposób ich zarządzania, ochrony i dystrybucji wewnątrz Instytutu, jak i w kontaktach z otoczeniem zewnętrznym. Polityka Ochrony Danych Osobowych stanowi dokument odnoszący się całościowo do problemu zabezpieczenia i zgodnego z przepisami prawa tych danych u Administratora, z uwzględnieniem i poszanowaniem praw osob, których dane dotyczą.

2. Zakres bezpieczeństwa dotyczy wszelkich procesów wykonywanych w obszarze przetwarzania danych osobowych w powiązaniu z prowadzoną działalnością i stanowi część całościowego systemu kierowania Instytutem.

3. Polityka Ochrony Danych Osobowych ma zastosowanie do:

- danych osobowych przetwarzanych w związku z realizacją przez Instytut wszelakich procesów biznesowych i świadczenia uslug, które dokonywane może być w systemach informatycznych oraz w tradycyjnej – papierowej formie,
- przechowywania danych osobowych na wszelkich nośnikach danych (magnetycznych, optycznych, elektronicznych takich jak: zewnętrzny dysk, dysk twardy, płyta CD/DVD, pamięć masowa typu flash), a także w książkach i kartotekach ewidencyjnych,
- danych osobowych przetwarzanych zarówno w zbiorach danych, zestawach oraz pojedynczych informacjach dotyczących osoby fizyczndej,
- informacji dotyczących bezpieczeństwa danych osobowych, w szczególności informacji służących do uwierzytelniania się w systemach informatycznych, w których mogą występować dane osobowe.

3. Cele Instytutu w zakresie realizacji zasad bezpieczeństwa informacji

1. Dyrektor Instytutu stojąc na stanowisku, że dane osobowe są priorytetowym zasobem każdej organizacji, wdrożyło niniejszą Politykę. Gwarancją sprawnej i skutecznej ochrony informacji, szczególnie danych osobowych, jest zapewnienie odpowiedniego do wymogów poziomu ich bezpieczeństwa oraz zastosowanie rozwiązań technicznych i organizacyjnych, zapewniających skuteczne tego spełnienie. Dyrektor Instytutu wprowadzając Politykę Ochrony Danych Osobowych deklaruje, że będzie ona podlegała ciągłemu doskonaleniu, uwzględniając w szczególności zmiany w otoczeniu prawnym, biznesowym oraz wynikające ze stanowiska Organu nadzorczego, a

także właściwych organów Unii Europejskiej.

2. Podejście do ochrony danych osobowych w Instytucie opiera się na czterech regułach:
   a) reguła poufności informacji – zapewnienie, że informacja jest udostępniana jedynie osobom upoważnionym,
   b) regula integralności informacji – zapewnienie zupełnej dokładności i kompletności informacji oraz metod jej przetwarzania,
   c) reguła dostępności informacji – zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów tylko wtedy, gdy istnieje taka potrzeba,
   d) regula odporności systemów i usług przetwarzania – zapewnienie odporności sieci lub systemu informacyjnego na danym poziomie poufności na przypadkowe zdarzenia albo niezgodne z prawem lub nieprzyjazne działania naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przesyłanych danych osobowych.

3. Celem wdrożonego w Instytucie systemu ochrony danych osobowych jest osiągnięcie poziomu organizacyjnego i technicznego, który:
   - będzie gwarantem pełnej ochrony danych wsystkich osob związanych z Instytutem (kandydaci na kursy i szkolenia, kandydaci do pracy, uczestnicy kursów, wykładowcy, instruktorzy) oraz ciągłości procesu ich przetwarzania,
   - zapewni zachowanie poufności informacji chronionych, integralności i dostępności danych osobowych,
   - zapewni odporność systemów i usług przetwarzania danych osobowych,
   - zagwarantuje odpowiedni poziom bezpieczeństwa danych osobowych, bez względu na jej postać, we wszystkich systemach jej przetwarzania,
   - maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa danych osobowych, które wynikają z celowej bądź przypadkowej działalności człowiekowi oraz ich ewentualnego wykorzystania na szkodę Instytutu,
   - zapewni poprawne i bezpieczne funkcjonowanie wszystkich systemów przetwarzania danych osobowych,
   - zapewni gotowość do podjęcia działań w sytuacjach kryzysowych dla bezpieczeństwa Instytutu, jego interesów oraz posiadanych i powierzonych mu informacji.

4. W ramach modyfkacji lub wprowadzania nowych systemów oraz procesów mających związek z przetwarzaniem danych osobowych w Instytucie wprowadza się wymagania związane z uwzględnianiem ochrony danych w fazie projektowania. W ramach w/w procesów uwzględnia się również domyślną ochronę danych, co oznacza wprowadzanie takich ustawień systemu informatycznego czy oprogramowania, które jako ustawienia pierwotne zapewnią ochronę tych danych. Zmiana tych ustawień powinna następować jedynie na wyraźne żądanie użytkownika oprogramowania/systemu. W ramach opisanych działań należy brać pod uwagę koszt nowego wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania, a w szczególności ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i jego wadze. Wdrożone środki mają zapewnić aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania.

4. Standardy i wymagania stanowiące podstawę dla Polityki Ochrony Danych Osobowych

1. Przepisy prawa
   - krajowe akty prawne:

Konstytucja Rzeczypospolitej Polskiej:

Art. 47 Każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

Art. 51 1) Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.

2) Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.

3) Każdy ma prawo dostępu do dotyczących go urzędowych dokumentow i zbiorów danych. Ograniczenie tego prawa może określić ustawa.

4) Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.

5) Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

Ustawa „Kodeks cywilny" - w odniesieniu do warunków zawierania i wykonywania umów (art. 66 i następne kc).

- przepisy prawa Unii Europejskiej

Rozporządzenia:

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony oób 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 lub RODO),

Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie danych fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych.

Dyrektywy:

Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej (Dyrektywa o ochronie prywatności i komunikacji elektronicznej).

Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym).

Dyrektywa 2016/680 Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r. w sprawie ochrony osob fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ściagania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW.

5. Zasady ochrony danych osobowych

1. Ochrona danych osobowych w Instytucie opiera się na następujących zasadach:
- zasadzie indywidualnej odpowiedzialności za utrzymanie właściwego poziomu ochrony odpowiadają, zgodnie z zakresem swoich obowiązków i uprawnień konkretne osoby,
- zasadzie uzasadnionej odpowiedzialności – prawo przebywania w określonych pomieszczeniach Instytutu mają wyłącznie osoby, które są do tego uprawnione,
- zasadzie uprawnień koniecznych – każdy użytkownik systemu informatycznego posiada prawa ograniczone wyłącznie do zasobów, które są niezbędne do wykonywania powierzonych mu zadań służbowych,
- zasadzie stałej gotowości – system związany z ochroną danych osobowych funkcjonuje w sposób nieprzerwany, odpowiednio do warunków realizacji zadań Instytutu,
- zasadzie wyceny aktyów informacyjnych, w szczególności danych osobowych Instytutu w oparciu o jednolite metody i wzorce.

6. Zasady przetwarzania danych osobowych według rozporządzenia ogólnego

Zgodnie z przepisami rozporządzenia ogólnego w Instytucie wprowadza się następujące zasady przetwarzania danych osobowych:

1) Zasada przetwarzania danych – dane osobowe przetwarza się z zapewnieniem osobom fizycznym informacji o tym, jak, dlaczego i jak długo te dane są przetwarzane. Instytut zapewnia, że osoby, których dane dotyczą zostaną poinformowane o przetwarzaniu ich danych osobowych przez Instytut, w tym o celu ich przetwarzania oraz o podmiotach przetwarzajacych, którym te dane przekazuje.

W związku z tym, gromadząc dane określonej osoby, Instytut udostępnia osobie, której te dane dotyczą informację zawierającą:

- nazwę i dane kontaktowe osoby, która będzie Administratorem danych osoby, której one dotyczą,
- dane kontaktowe Inspektora Ochrony Danych Osobowych (IODO),

- krótki opis celu, dla którego dane osoby, której dane dotyczą mogą być przetwarzane oraz podstawa prawna takiego przetwarzania,
- dane odbiorców lub kategorie odbiorców, którym dane osoby, której dane dotyczą mogą zostać ujawnione,
- w stosownych przypadkach informacje o tym, że dane osoby, której dane dotyczą mogą być przesyłane za granicę,
- okres przechowywania danych,
- istnienie prawa do dostępu, sprostwoania, usuwania, sprzeciwu i przenoszenia danych oraz w stosownych przypadkach prawo do wycofania zgody na przetwarzanie danych osobowych,
- prawo do złożenia skargi do Organu nadzorczego,
- informację czy podanie danych osobowych jest wymogiem ustawowym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania oraz jakie są konsekwencje niepodania danych,
- informację o stosowaniu zautomatyzowanego procesu podejmowania decyzji oraz informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

2) Zasada zgodności z prawem: Instytut przetwarza tylko dane osobowe, włączając w to szczególne kategorie danych osobowych, w sytuacji posiadania ważnej do tego podstawy. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy i w takim zakresie, w jakim spełniony jest co najmniej jeden z poniższych warunków:
   - osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
   - przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
   - przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
   - przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
   - przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
   - przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesu lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

W przypadku szczególnych kategorii danych osobowych należy spełnić co najmniej jeden z poniższych warunków:
- osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach,
- przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej,
- przetwarzanie jest niezbędne do cohrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody,
- przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą,
- przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń,
- przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej.

7. Struktura zarządzania ochroną danych osobowych

W Instytucie tworzy się następującą strukturę zarządzania ochroną danych osobowych:

1) Administrator Danych Osobowych (ADO) określony zgodnie z definicją
2) Inspektor Ochrony Danych Osobowych (IODO), który jest odpowiedzialny za realizację następujących zadań:

- informowanie Administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na podstawie przepisów prawa odnoszących się do ochrony danych osobowych i doradzanie im w tej sprawie,
- monitorowanie przestrzegania przepisów prawa oraz polityk Administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków,
- działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwrzania oraz powiązane z tym audyty,
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania,
- współpraca z organem nadzorczym,
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,
- inne zadania określone w niniejszym dokumencie, dotyczące zapewnienia bezpieczeństwa danych osobowych.

3) Administrator Systemu Informatycznego (ASI), funkcję tę pełni główny informatyk, który wykonuje polecenia Inspektora Ochrony Danych Osobowych w wyznaczonym przez niego obszarze działania. Do obowiązków ASI należy:

- rejestrowanie i wyrejestrowywanie użytkowników systemu informatycznego na podstawie wniosku zaakceptowanego przez kierownika jednostki organizacyjnej i/lub przełożonego,
- dokonywanie zmiany uprawnień użytkowników systemu na podstawie wniosku zaakceptowanego przez przełożonego,
- przestrzeganie opracowanych dla systemu procedur bezpieczeństwa,
- utrzymanie systemu w sprawności technicznej w stopniu określonym w dokumentacji powykonawczej,
- konfigurowanie urządzeń i oprogramowania,
- aktualizowanie i konfigurowanie oprogramowania antywirusowego,
- reagowanie na naruszenia bezpieczeństwa i usuwanie ich skutków,
- nadzorowanie właściwego użytkowania oraz serwisowania urządzeń i oprogramowania,
- wykonywanie kopii bezpieczeństwa informatycznych baz danych osobowych oraz systemów informatycznych.

8. Zasady postępowania w przypadku naruszenia ochrony danych osobowych

Przetwarzanie danych osobowych powinno mieć miejsce w zakresie niezbędnym i proporcjonalnym do zapewnienia bezpieczeństwa sieci i informnacji, a zarazem do realizowanych czynności przetwarzania związanych z potrzebami biznesowymi użytkowników systemów informatycznych. Za monitorowanie stanu bezpieczeństwa informacyjnego, a w przypadku jego naruszenia za podjęcie niezwłocznie działań związanych z ich eliminacją odpowiada IODO we współpracy z ASI.

9. Dane współadministrowane

W przypadku gdy dane osobowe będą współadministrowane przez dwóch lub większą liczbę Administratorów - przetwarzanie danych może odbywać się jedynie na podstawie umowy, w której Administratorzy w przejrzysty sposób określą odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z przepisów prawa dotyczących ochrony danych osobowych. Za monitorowanie przestrzegania zgodności przetwarzania z właściwymi umowami odpowiedzialny jest IODO.

10. Czynności związane z realizacją praw osób, których dane dotyczą

1) Informacje ogólne: Instytut ma obowiązek umożliwiania osobom, których dane dotyczą, korzystania z ich praw dostępu, usuwania, sprostowania, sprzeciwu i przenoszenia danych osobowych.

Podstawowe prawa osób, których dane dotyczą, a także sposób umożliwiania korzystania z tych praw zostały

zdefiniowane w niniejszym dokumencie. Określono w szczególności to, w jaki sposób Instytut powinien ułatwiać osobom fizycznym korzystanie ze swoich praw oraz w jaki sposób odpowiadać na konkretne prośby osób, których dane dotyczą, w zakresie wykonywania ich praw. W kontekście realizowania określonych praw osób, których dane dotyczą, należy pamiętać o każdorazowym pouczeniu tych osób o możliwości złożenia skargi do organu nadzorczego w sytuacji, gdyby rozstrzygnięcie Instytutu w jej sprawie byłoby uznane za niesatysfakcjonujące.

Udzielanie informacji o przetwarzaniu danych osobowych, a także w sprawach związanych z realizacją określonych żądań osób, których dane dotyczą, jest realizowane co do zasady nieodpłatnie. Odpłatny tryb udzielania informacji, może być zastosowany wyłącznie w szczególnych, indywidualnych przypadkach, powodowanych oceną nadmiarowego kierowania tego rodzaju wniosków. W takich okolicznościach opłata za udzielenie informacji musi uwzględniać faktycznie poniesione w tym zakresie przez Instytut koszty. IODO nadzoruje w sposób bezpośredni każdy proces działań związanych z realizacją praw osób. Dane dotyczące jego numeru telefonu oraz adresu poczty elektronicznej muszą być dostępne na stronie internetowej Instytutu, a także na formularzach wykorzystywanych w procesie pozyskiwania danych od tych osób.

2) Instytut umożliwia w szczególności realizację następujących praw:

- Prawo dostępu do danych: osoby, których dane dotyczą mają prawo do informacji, jakie dane osobowe przetwarza na ich temat Instytut oraz mają prawo do uzyskania kopii tych danych osobowych.
- Prawo do bycia zapomnianym: osoby, których dane dotyczą, mają prawo do usunięcia danych osobowych, jeśli Instytut nie ma podstawy wynikającej z zasady zgodności z prawem do dalszego przetwarzania danych.
- Prawo do sprostowania danych: osoby, których dane dotyczą mają prawo sprzeciwić się wykorzystaniu ich danych osobowych do określonego celu, na przykład do profilowania podejmowania decyzji zautomatyzowanych.
- Prawo do przenoszenia danych: osoby, których dane dotyczą, mają prawo do otrzymywania danych osobowych, które dostarczyły Instytutowi w powszechnie używanym formacie nadającym się do odczytu maszynowego oraz mają prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony Instytutu.
- Prawo do ograniczenia przetwarzania: osoba, której dane dotyczą, ma prawo żądania od Administratora ograniczenia przetwarzania, w razie zrealizowania się przesłanej wynikających z aktualnych przepisów prawa.

Prawa, o których mowa powyżej są realizowane poprzez umożliwienie podmiotowi wykonywania m.in. następujących czynności:

- przeglądanie danych osobowych, które przetwarza na ich temat Instytut,
- żądanie usunięcia wszelkich informacji, co do których wyrażają wolę, aby Instytut już nie miał dostępu,
- żądanie skorygowania wszelkich niedokładności i błędów danych i aktualizacja tych danych, które tego wymagają,
- żądanie zmiany ustawienia swojego konta w systemie informatycznym, tak aby ich dane osobowe nie były już wykorzystywane do określonego celu np. rezygnacja z możliwości marketingu,
- żądanie uzyskania kopii danych w powszechnie używanym i przeznaczonym do odczytu maszynowego formacie.

3) Realizacja wniosków w sprawach o dostęp do danych

Zgodnie z zasadą przejrzystego przetwarzania Instytut informuje osobę, której dane dotyczą o przysługujących jej prawach, prostym, jasnym i zrozumiałym językiem. Proces realizacji praw osób podlega w każdym indywidualnym przypadku analizie pod kątem zgodności z prawem powzechnym i wewnętrznymi przepisami Instytutu.
Osoby, których dane dotyczą są również uprawnione do złożenia pisemnego lub ustnego wniosku do Instytutu, w celu skorzystania z przysługujących im praw.

Żądania od osób, których dane dotyczą, skierowane do Instytutu w celu skorzystania z tych praw są określane jako wnioski o skorzystanie z praw i należy rejestrować datę ich otrzymania i sam wniosek.
Nie obowiązuje żaden określony wzór wniosku o skorzystanie z praw. Należy akceptować składane w tych sprawach wnioski w każdej dogodnej dla wnioskodawców formie. Jeżeli dana osoba odmawia złożenia wniosku na

piśmie, Instytut powinien wysłać wnioskodawcy pisemną informację potwierdzając charakter i zakres wniosku. Przed podjęciem jakichkolwiek działań należy dokonać uwierzytelnienia tożsamości osoby, której dane dotyczą lub osoby upoważnionej do działania w jej imieniu.

Instytut ma obowiązek odpowiedzieć na wniosek w ciągu jednego miesiąca. Jeżeli żądanie jest według oceny IODO szczególnie skomplikowane udzielenie odpowiedzi może zostać przedłużone do okresu nie przekraczającego 2 miesięcy. W takich przypadkach Instytut ma obowiązek udzielenia wstępnej odpowiedzi żądającemu w ciągu jednego miesiąca, wyjaśniając, dlaczego konieczne jest wydłużenie okresu.
Etapami odpowiedzi na wniosek o skorzystanie z praw są następujące działania:

- poinformowanie IODO oraz jednostek biznesowych, w których kompetencji jest dalsze działanie o wpłynięciu wniosku,
- zidentyfikowanie, które systemy, bazy danych, zestawy informacji w formie papierowej mogą zawierać informacje dotyczące jednostek organizacyjnych odpowiedzialnych za przetwarzanie informacji będących przedmiotem wniosku,
- po zakończeniu działań przez odpowiednią jednostkę biznesową dostarcza ona kopię wszelkich informacji zidentyfikowanych do IODO,
- IODO dokonuje przeglądu informacji w celu zidenttyfikowania wszelkich danych osobowych dotyczących wnioskodawcy. W przypadku stwierdzenia braku przeciwskazań natury prawnej, IODO podejmuje decyzję o przesłaniu kopii danych osobowych wymaganych przez daną osobę.

Instytut nie powinien ujawniać, usuwać ani w inny sposób wpływać na dane osobowe dotyczące osób innych niż sam wnioskodawca, chyba że strona trzecia wyrazi na to zgodę lub uzasadnione jest dostarczenie lub usunięcie danych bez ich zgody.

4) Realizacja wniosków o usunięcie danych i prawo do bycia zapomnianym

Prawo do usunięcia danych i do bycia zapomnianym nie są prawami absolutnymi. Instytut nie musi usuwać danych osobowych, które należy zachować:

- w celu ochrony przed roszczeniami prawnymi np. umowy, historia zatrudnienia lub korespondencja w sprawie skargi,
- w celu spełnienia obowiązku prawnego,
- w celu wykonania umowy.

Osoba, które dane dotyczą, nie ma prawa do wyrażenia sprzeciwu wobec wykorzystywania jej informacji w celu, który jest niezbędny do wypełnienia zobowiązań prawnych. Instytut powinien spełnić żądanie usunięcia i/lub sprzeciwu wobec przetwarzania w odniesieniu do następujących danych (o ile nie są one przedmiotem skargi lub postępowania sądowego):

- informacje o profilowaniu klienta,
- pliki cookie,
- zebrane w celach marketingowych
- niezrealizowane wnioski o nawiązanie stosunku pracy, po okresie, na jaki zostały przekazane dane do rekrutacji.

Jeśli zapadnie decyzja odmowna w sprawie wniosku (w całości lub w odniesieniu do określonego prawa), odpowiedź musi zawierać powody odrzucenia wniosku. Jeśli zdecydowano się na spełnienie żądania usunięcia przez „ograniczenie" danych osobowych, należy to wskazać i wyjaśnić w odpowiedzi.

Odpowiedź powinna zostać dostarczona w sposób zgodny z przepisami prawa właściwymi do komunikacji z osobami, których dane dotyczą lub w sposób, na który dana osoba wyraziła zgodę.

5) Realizacja wniosków w sprawie przeniesienia danych
Prawo do przenoszenia danych uprawnia wnioskodawcę do kopii danych w powszechnie używanym i nadającym się do odczytu komputerowego formacie. Ma zastosowanie tylko w przypadku kiedy:

- dane osobowe są zapisywane elektronicznie tj. nie ma zastosowania do plików papierowych,
- dane osobowe zostały zebrane od osoby, której dane dotyczą,
- osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie lub dane zostały przetworzone w celu wykonania umowy lub czynności poprzedzających zawarcie umowy z osobą fizyczną.

Jeżeli osoba zwróciła się do Instytutu o przesłanie danych osobowych bezpośrednio do strony trzeciej, należy upewnić się, że otrzymane instrukcje są jasne i szczegółowe, w tym powinny uwzględniać informacje do kogo ze strony trzeciej należy przesłać dane osobowe oraz pisemne potwierdzenie od osoby składającej wniosek, że odbiorca spodziewa się danych osobowych. Jeśli nie uzyskano konkretnych instrukcji od osoby składającej wniosek, należy przesłać dane osobowe bezpośrednio do osoby składającej wniosek.

Instytut może utrzymywać dane osoby, której dane dotyczą, dotyczące otrzymanych zapytań i żądań oraz kopie wysłanych odpowiedzi, w celu prowadzenia dokumentacji i archiwizacji dotyczących zapytań i żądań od osoby, której dane dotyczą, a także wysłanych odpowiedzi pod warunkiem, że kontekst danych tej osoby będzie zrozumiały dla każdego pracownika Instytutu, który ma do nich dostęp. Dane takie powinny zostać usunięte niezwłocznie, w sytuacji kiedy dane takie nie spełniałyby dalej funkcji ewidencyjnej do celów ochrony przed roszczeniami prawnymi.

11. Pozyskiwanie zgody na przetwarzanie danych osobowych

1) Aby uzyskać zgodę na przetwarzanie danych osoby, której one dotyczą, muszą zostać spełnione następujące warunki:
- dobrowolność – osoba, której dane dotyczą, musi mieć rzeczywisty wybór, czy wyrazić zgodę na przetwarzanie. Może to być wybór, czy w ogóle podać swoje dane osobowe, a także czy wyraża zgodę na ich przetwarzanie.

- konkretność – zgoda powinna być ograniczona do wyraźnie określonego celu lub celów przetwarzania. Zgoda na wiele celów nie powinna być „łączona". Osoba, której dane dotyczą powinna mieć oddzielny wybór dla każdego celu.

- jednoznaczność – zgoda powinna wymagać pozytywnego działania ze strony osoby, której dane dotyczą. Zazwyczaj oznacza to zaznaczenie pola lub przesunięcie przełącznika lub wprowadzenie przez osobę, której dane dotyczą dodatkowych informacji, które nie będą wykorzystywane do celów innych niż przetwarzanie.

- odwoływalność – osoba, której dane dotyczą, musi mieć możliwość wycofania swojej zgody w dowolnym czasie, na przykład poprzez usunięcie danych osobowych, zmianę ustawień swojego konta lub skontaktowanie się z Instytutem.

W przypadku danych osobowych szczególnych kategorii zgoda musi być wyraźna, co oznacza, że musi być ona potwierdzona jednoznaczym w formie i treści oświadczeniem ustnym lub pisemnym przez osobę, której dane dotyczą, a nie tylko działaniem. Na przykład decyzja o podaniu opcjonalnych danych osobowych lub wyborze konkretnej usługi nie stanowi wyraźnej zgody, chyba że towarzyszy jej pole wyboru umożliwiające wyrażenie zgody na przetwarzanie.

2) W procesie pozyskiwania zgody oraz dalszego przetwarzania danych należy stosować się do zasad:

- Zasada ograniczenia celu przetwarzania – Instytut powinien zbierać dane klienta tylko w konkretnym, wyraźnym i prawnie uzasadnionym celu. Jeżeli Instytut przetwarza dane, osoby której dane dotyczą w sposób, który może być niezgodny z pierwotnym celem, dla którego został zebrany, Instytut jest zobligowny do uzyskania dobrowolnej, konkretnej, świadomej i jednoznacznej zgody osoby, której dane dotyczą na przetwarzanie lub dopilnowania, że osoba, której dane dotyczą, została poinformowana o możliwości nowego przetwarzania oraz, że Instytut może zgodnie z zasadą zgodności z prawem przetwarzać dane osoby, której dane dotyczą nawet bez zgody tej osoby. Działanie takie będzie wymagało każdorazowo zatwierdzenia przez IODO.
Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Instytut przed rozpoczęciem przetwarzania dokona oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.

- Minimalizacja danych – ilość danych klienta zebranych lub wykorzystanych w dowolnym celu musi być ograniczona do wielkości niezbędnej służącej realizacji tego celu. W przypadku gromadzenia przez Instytut danych osoby, której dane dotyczą za pomocą standardowego formularza w trybie online lub offline każde pytanie w

formularzu musi być bezpośrednio związane z celem, dla którego są one zbierane.
Jeśli Instytut zamierza zebrać dodatkowe „opcjonalne" dane osoby, której dane dotyczą w tym samym lub innym celu, Instytut musi wskazać tej osobie, jakie dane osobowe należy podać, a które są opcjonalne.

- Prawidłowość – Instytut podejmuje działania skutkujące tym, że dane osoby, której dane dotyczą są kompletne, dokładne i aktualne. Witryny internetowe Instytutu powinny umożliwiać osobie, której dane dotyczą, poprawianie i aktualizowanie własnych danych, pod warunkiem, że będzie ona możliwa do zweryfikowania swojej tożsamości zanim podejmie działania z tym związane.
Jeśli Instytut w inny sposób pozyska informację, że dane osoby, której dane dotyczą są niedokładne, niekompletne lub nieaktualne, musi podjąć uzasadnione kroki w celu skorygowania, uzupełnienia lub zaktualizowania tych danych. Instytut może również podejmować wewnętrzne kroki w celu utrzymania należytej jakości danych, w tym poprzez okresowe przeprowadzanie procesu czyszczenia danych.
Instytut a może utrzymywać dane osoby, której dane dotyczą, które są nieaktualne do celów prowadzenia dokumentacji i archiwizacji, pod warunkiem, że kontekst danych tej osoby będzie zrozumiały dla każdego pracownika Instytutu, który ma do nich dostęp.

- Ograniczenie przechowywania danych – Instytut może przechowywać dane osoby, których dane dotyczą wyłącznie w możliwej do zidentyfikowania formie tak długo, jak jest to konieczne do celów, dla których zostały pierwotnie zebrane. Po upływie tego okresu dane osoby, których one dotyczą, powinny zostać usunięte lub zniszczone, lub poddane procesowi anonimizacji, tak, aby nie można było już zidentyfikować danej osoby.
Instytut może przechowywać dane osoby, której dane dotyczą przez dłuższe okresy, jeśli uzna to za konieczne w związku z postępowaniem sądowym lub potencjalnym postępowaniem sądowym. Długość tego okresu jest uzależniona każdorazowo od długości przewidywanego okresu przedawnienia roszczeń wynikających z zawartych umów.
- Stosowanie odpowiednich środków bezpieczeństwa danych – Instytut musi stosować i utrzymywać odpowiednie środki techniczne i organizacyjne w celu ochrony danych oosby, której dane dotyczą przed nieuprawnionym dostępem i uniknięcia ich przypadkowej utraty, uszkodzenia lub zniszczenia. Środki te zostały opisane w niniejszym dokumencie.
Podstawą wdrożenia adekwatnych do zagrożeń środków bezpieczeństwa są wyniki realizowanej na bieżąco analizy ryzyka, a na etapie wdrażania nowych rozwiązań organizacyjnych i informatycznych również wyniki procesów oceny skutków dla oceny prywatności i domyślnej ochrony danych. Za koordynację wymienionych działań odpowiada IODO.

- Rozliczalność – wszyscy pracownicy zatrudnieni w Instytucie mający dostęp do danych osobowych muszą przestrzegać niniejszej Polityki i powinni być w stanie wykazać przestrzeganie jej przepisów.

12. Elementy analizy ryzyka informacyjnego

Analiza ryzyka informacyjnego stanowi integralną część procesu zapewnienia bezpieczeństwa danych osobowych. Konkretne mechanizmy i zakresy odpowiedzialności zostały zawarte w odrębnych procedurach. Wymienione poniżej elementy powinny być każdorazowo uwzględniane w ramach prowadzonej analizy ryzyka:

- mechanizmy dotyczące oceny ryzyka związanego z przetwarzaniem danych, które zawarte zostały w treści właściwych norm,
- mechanizmy dotyczące przeglądu stosowanych środków ochrony danych osobowych, w tym oceny ich skuteczności, które zostały zawarte w arkuszach analitycznych sporządzonych oddzielnie dla każdego z systemów przetwarzających dane osobowe,
- mechanizmy dotyczące kryteriów wyboru podmiotu przetwarzającego, pod kątem tego, czy zapewnia on adekwatne środki techniczne i organizacyjne, które zostały zawarte w procedurze outsourcingu,
- mechanizmy dotyczące bieżącej weryfikacji podmiotu przetwarzającego pod kątem spełnienia wymagań przewidzianych przepisami rozporządzenia ogólnego, a także wymagań umownych dotyczących zapewnienia bezpieczeństwa danych, w tym zasady dotyczące audytu zostały zawarte w procedurze outsourcingu oraz karcie audytu.