załącznik do zarządzenia nr 15/2022
dyrektora Szkoły Podstawowej z Oddziałami Integracyjnymi nr 41
w Warszawie, ul. Drewniana 8 z dnia 13.09.2022r.

Polityka Bezpieczeństwa Danych Osobowych w Szkole Podstawowej z Oddziałami Integracyjnymi nr 41 im. Żołnierzy Armii Krajowej Grupy Bojowej „Krybar" w Warszawie, ul. Drewniana 8

Spis treści

Wstęp

Polityka Bezpieczeństwa Danych Osobowych (dalej: PBDO) ma na celu ochronę danych osobowych przetwarzanych w Szkole Podstawowej z Oddziałami Integracyjnymi nr 41 im. Żołnierzy Armii Krajowej Grupy Bojowej „Krybar" z siedzibą w Warszawie, ul. Drewniana 8 (dalej: placówka), na podstawie zobowiązań, wytycznych i zaleceń określonych w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych – dalej: RODO) oraz krajowych przepisach dotyczących ochrony danych osobowych, m.in. Ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz.U. 2018, poz. 1000).

Dokument jest aktem wewnętrznego stosowania, wprowadzonym zarządzeniem dyrektora szkoły. Dokument jest zgodny z powszechnie obowiązującymi aktami prawnymi, w tym regulującymi działalność jednostki.

PBDO ma na celu zapewnienie przetwarzania danych osobowych w Szkole w sposób zgodny z przepisami z zakresu ochrony danych osobowych oraz gwarantujący ich odpowiednie bezpieczeństwo w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych**.**

PBDO stosuje się w odniesieniu do wszelkich Danych osobowych, wobec których placówce przysługuje status Administratora Danych lub Podmiotu Przetwarzającego, przetwarzanych zarówno w Systemach informatycznych lub Aplikacjach, jak i w formie papierowej tj. księgach, wykazach i innych zbiorach ewidencyjnych.

Zasady opisane w PBDO obowiązują wszystkich pracowników, nauczycieli, pedagogów, logopedów, współpracowników (osoby współpracujące w oparciu o umowy cywilnoprawne, w tym umowy zlecenie, o dzieło), stażystów, praktykantów, a w szczególności Osoby upoważnione do przetwarzania danych osobowych.

Nad przestrzeganiem przepisów z zakresu ochrony danych osobowych w Placówce pieczę sprawuje dyrektor szkoły. W celu sprawnego nadzoru i gwarancji przestrzegania zasad dotyczący przetwarzania danych Dyrektor wyznacza Inspektora Ochrony Danych Osobowych (dalej IOD).

Wykaz użytych skrótów i terminów

Administrator danych/ADO – administrator w rozumieniu art. 4 pkt 7 RODO - osoba decydująca o celach i środkach przetwarzania danych osobowych. Administratorem danych jest Szkoła, reprezentowana przez Dyrektora.

Administrator Systemu Informatycznego – rozumie się przez to osobę wyznaczoną przez Dyrektora, odpowiedzialną za administrowanie, monitorowanie i zarządzanie uprawnieniami oraz procesami w środowisku informatycznym placówki, w tym za bezpieczeństwo oraz zapewnienie właściwego i ciągłego funkcjonowania nadzorowanych systemów teleinformatycznych/ informatycznego oraz sieci informatycznej.

Dane osobowe - oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Dostępność - zapewnienie, że dostęp do informacji mają osoby uprawnione zawsze, gdy istnieje taka potrzeba.

Incydent - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z naruszeniem ochrony danych osobowych, które stwarzają znaczne prawdopodobieństwo naruszenia praw lub wolności osób których dane dotyczą, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Integralność - zagwarantowanie dokładności i kompletności informacji oraz metod ich przetwarzania – zapewnienie, że dane nie zostały zmodyfikowane w nieautoryzowany sposób.

IOD - inspektor ochrony danych, osoba wyznaczona przez Administratora danych zgodnie z art. 37 RODO.

Obszar przetwarzania - miejsce, w którym przetwarzane są dane osobowe.

Organ nadzorczy – Prezes Urzędu Ochrony Danych Osobowych - organ powołany do spraw ochrony danych osobowych.

Osoba upoważniona – Pracownik lub osoba fizyczna, której zostało nadane upoważnienie do przetwarzania danych osobowych przez Administratora Danych,

PBDO/Polityka - niniejszy dokument Polityki Bezpieczeństwa Danych Osobowych,

Przetwarzanie danych - operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka 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.

Podmiot przetwarzający - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

Powierzenie przetwarzania danych osobowych – zlecenie wykonania czynności przetwarzania danych innemu podmiotowi, w drodze odrębnej umowy zawartej na piśmie lub stosownego zapisu do umowy, wyłącznie w zakresie i celu w niej przewidzianym.

Poufność - zapewnienie, że informacje nie są udostępniane bądź wyjawiane nieupoważnionym osobom lub podmiotom.

Pracownicy – osoba fizyczna zatrudniona w Szkole na podstawie stosunku pracy lub umowy cywilnoprawnej, nie prowadząca profesjonalnej działalności gospodarczej, w szczególności nauczyciele, pracownicy niepedagogiczni, stażyści, praktykanci, współpracownicy

RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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).

Rozliczalność - zapewnienie, że działania na informacjach mogą być jednoznacznie przypisane danej osobie, umożliwienie jednoznacznej identyfikacji,

Placówka – Szkoła Podstawowa z Oddziałami Integracyjnymi nr 41 im. Żołnierzy Armii Krajowej Grupy bojowej „Krybar" z siedzibą w Warszawie przy ul. Drewnianej 8,

System teleinformatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych, w tym również za pomocą obrazu i dźwięku.

Ustawa – ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz. U. 2018, poz. 1000).

1. Cel Polityki bezpieczeństwa danych osobowych

Celem Polityki bezpieczeństwa danych osobowych placówki jest:

1) zapewnienie przetwarzania danych osobowych zgodnie z przepisami o ochronie danych osobowych, w tym przepisami branżowymi dotyczącymi placówki,
2) zapewnienie odpowiedniej ochrony danych osobowych, uwzględniającej stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze,
3) ustanowienie systemu bezpiecznego przetwarzania danych osobowych,
4) realizacja obowiązków nałożonych na placówkę przez obowiązujące przepisy prawa, w ramach których przetwarzane są dane osobowe,
5) gwarancja nienaruszalności i realizacja praw osób, których dane dotyczą,
6) zapewnienie przetwarzania danych osobowych przez podmioty którym placówka zleciła wykonanie określonych usług zgodnie z wymaganiami określonymi w umowach powierzenia przetwarzania danych.

2. Podstawowe zasady przetwarzania Danych osobowych

Dane osobowe w Placówce muszą być przetwarzane zgodnie z zasadami, o których mowa w art. 5 RODO, tj.:

Zasadą zgodności z prawem, rzetelności i przejrzystości – przez co rozumiemy, że przetwarzanie dokonywanej jest zgodnie z prawem, rzetelnie i w sposób przejrzysty, dla osoby, której dane dotyczą,

Zasadą ograniczenia celu – przez co rozumiemy, że dane zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami,

Zasadą minimalizacji danych – przez co rozumiemy, że zbierane dane są adekwatne, stosowne oraz ograniczone do tego co jest niezbędne do celów, w których są przetwarzane,

Zasadą prawidłowości – przez co rozumiemy, że dane są zawsze prawidłowe i w razie konieczności uaktualniane,

Zasadą ograniczenia przechowywania – przez co rozumiemy, że dane przechowywane są przez okres nie dłuższy niż jest to niezbędne do celów, w których są przetwarzane,

Zasadą integralności i poufności – przez co rozumiemy, że dane przetwarzane są zawsze w sposób zapewniający im bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

3. Podstawowe zasady bezpieczeństwa obowiązujące przy przetwarzaniu danych osobowych

Osoby przetwarzające Dane osobowe, zobowiązane są do ochrony Danych osobowych na swoim stanowisku pracy oraz zachowania w tajemnicy Danych osobowych oraz sposobów ich zabezpieczenia, również po ustaniu zatrudnienia lub zakończenia współpracy z Placówką .

Osoby przetwarzające Dane osobowe zobowiązane są do zabezpieczenia Danych osobowych przetwarzanych zarówno w formie elektronicznej, jak i papierowej, w sposób uniemożliwiający nieuprawnione ujawnienie Danych osobowych, nieautoryzowany dostęp do Danych osobowych, niedozwolone: powielenie, modyfikację, zniszczenie, utratę, nieprawidłowe wykorzystanie lub kradzież.

Osoby mające dostęp do Danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy jak i poza nim, w zakresie wykraczającym poza wykonywanie obowiązków służbowych.

W pomieszczeniach, w których przetwarzane są Dane osobowe przebywać mogą Osoby upoważnione do przetwarzania Danych osobowych oraz inne osoby jedynie w obecności Osób upoważnionych do przetwarzania Danych osobowych albo posiadające upoważnienie do przebywania w obszarze przetwarzania danych nadane przez uprawnione osoby działające w tym zakresie w imieniu Placówki. Osoby nadające uprawnienie do przebywania odpowiadają za nadzór nad stosowaniem się osób uprawnionych do zasad i standardów bezpieczeństwa obowiązujących w Placówce. Osoby nieuprawnione do przebywania w Obszarze przetwarzania danych mogą poruszać się wyłącznie w strefach ogólnodostępnych takich jak korytarze, ciągi komunikacyjne na terenie przyległym do budynków oraz hole wejściowe do budynków.

Dokumenty papierowe zawierające Dane osobowe jak również elektroniczne nośniki informacji, na których są zapisane Dane osobowe należy przechowywać przynajmniej w meblach biurowych zamykanych na klucz.

Osoby upoważnione do przetwarzania Danych osobowych zobowiązane są do zamykania wszelkich pomieszczeń, w których przetwarzane są Dane osobowe w czasie ich nieobecności w pomieszczeniu.

Każdy dokument papierowy zawierający Dane osobowe sporządzony jako dokument roboczy należy najpóźniej na koniec dnia pracy zniszczyć lub zamknąć w miejscu uniemożliwiającym dostęp osób nieuprawnionych.

Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających Dane osobowe odbywać się musi w sposób uniemożliwiający odczytanie zawartej w nich treści, z wykorzystaniem niszczarek spełniających wymóg, co najmniej standardu DIN - 3.

Nie można udzielać informacji dotyczących Danych osobowych na podstawie prośby o takie dane w formie zapytania telefonicznego przekazywanego przez osoby reprezentujące instytucje zewnętrzne lub inne osoby fizyczne, za wyjątkiem spraw związanych ze zwykłymi czynnościami dnia codziennego, np. podania kontaktu w celach służbowych (imię i nazwisko pracownika, numer telefonu służbowego, numer fax, służbowy adres e-mail, stanowisko pracy, adres biura (w przypadku pracy zdalnej wykonywanej przez pracownika z domu nie podajemy adresu miejsca wykonywania pracy)). Wyjątek od powyższej zasady jest dopuszczalny wyłącznie w sytuacji, gdy przewidują to ustanowione w tym celu odrębne procedury dla wybranych procesów działalności placówki, po uprzedniej analizie ryzyk i ich akceptacji przez Dyrekcję.

Nauczyciele w przypadku kontaktu telefonicznego rodzica/ opiekuna prawnego mogą przekazać informacje w zakresie spraw związanych ze zwykłymi czynnościami dnia codziennego, dotyczącymi ucznia (np. nieobecności, umówienie się na spotkanie), będącego pod ich opieką, wyłącznie w sytuacji w których zweryfikowali tożsamość rodzica lub opiekuna prawnego lub mają ustaloną stałą ścieżkę komunikacji i są pewni tożsamości rozmówcy telefonicznego.

Pozostali Pracownicy Placówki w przypadku kontaktu telefonicznego osób trzecich, mogą przekazać informacje w zakresie spraw związanych ze zwykłymi czynnościami dnia codziennego, dotyczącymi przekazywania informacji niezawierających danych osobowych (np. dostępność składanych wniosków, terminy na składanie dokumentów, rodzaj dokumentów, umówienie się na spotkanie).

Niedopuszczalnym jest wynoszenie materiałów zawierających Dane osobowe poza Obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających Dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia. Przetwarzanie danych osobowych poza Obszarem przetwarzania danych możliwe jest po uzyskaniu zgody bezpośredniego przełożonego Pracownika. W przypadku przetwarzania Danych osobowych poza Obszarem przetwarzania danych ich zakres należy ograniczyć do niezbędnego minimum koniecznego dla czynności realizowanych poza Obszarem przetwarzania. W przypadku pracy zdalnej należy zastosować się do postanowień odpowiedniej procedury określającej ten sposób pracy.

Kopiowanie Danych osobowych może odbywać się wyłącznie w ramach posiadanego upoważnienia do przetwarzania danych, w związku z realizacją czynności służbowych.

Kopia Danych osobowych wykonana zgodnie z postanowieniami powyżej podlega zniszczeniu niezwłocznie po realizacji celu, dla którego została wykonana. W przypadku kopii Danych osobowych przetwarzanych w formie cyfrowej przy użyciu systemów teleinformatycznych zasady ich tworzenia i niszczenia określa odrębny dokument.

Zabezpieczenia fizyczne Danych osobowych opisane są w odrębnym dokumencie.

Organizację przetwarzania danych i odpowiedzialność poszczególnych osób tworzące system bezpiecznego przetwarzania danych określa odrębny dokument ***Regulamin organizacji przetwarzania danych,*** stanowiący **załącznik nr 1**.

4. Zasady nadawania upoważnień do przetwarzania danych

Dyrektor Placówki jest upoważniony do przetwarzania wszelkich danych osobowych, w zakresie niezbędnym do wykonywania czynności związanych z pełnioną funkcją i realizacją zadań placówki oświatowej.

Inspektor Ochrony Danych Osobowych jest upoważniony do przetwarzania danych osobowych w zakresie niezbędnym do wykonywania czynności związanych z pełnioną funkcją.

Administrator Systemów Informatycznych jest uprawniony do przetwarzania danych w zakresie w jakim jest to niezbędne do utrzymania i zapewnienia bezpieczeństwa i właściwego funkcjonowania środowiska informatycznego placówki w którym przetwarzane są dane osobowe.

Do przetwarzania Danych osobowych w Placówce są dopuszczone wyłącznie osoby upoważnione przez Administratora Danych, którego reprezentuje Dyrektor Placówki.

Upoważnienie do przetwarzania Danych osobowych ma formę dokumentu papierowego treść (upoważnienia stanowi ***załącznik nr 2*** do PBDO), nadawanego indywidualnie dla danej osoby oraz dla każdego procesu przetwarzania Danych osobowych oraz Aplikacji, w których przetwarzane są Dane osobowe. Dyrektor placówki wyraża również zgodę na nadanie dostępu i uprawnień przez Administratora Systemów Informatycznych do aplikacji, programów, Systemów informatycznych, narzędzi informatycznych w których przetwarzane są Dane osobowe

Upoważnienie do przetwarzania Danych osobowych nadawane jest przy przyjęciu do pracy lub zlecaniu czynności zgodnie z zakresem obowiązków na stanowisku pracy lub zakresem zleconych czynności.

Upoważnienie nadawane jest na czas powołania, zatrudnienia lub realizacji zleconych czynności. W przypadku zmiany stanowiska pracy lub zakresu obowiązków lub odpowiadających im procesów przetwarzania danych nadawane jest nowe upoważnienie, a dotychczasowe zostaje odwołane zgodnie z zasadami reprezentacji jak przy nadawaniu upoważnień.

Osoba, której zostało nadane upoważnienie do przetwarzania Danych osobowych otrzymuje kopię upoważnienia oraz podpisuje oświadczenie opatrzone datą, iż upoważnienie zostało jej przekazane oraz oświadczenie o zachowaniu tajemnicy danych osobowych oraz sposobów ich zabezpieczania.

Oryginał upoważnienia po jego podpisaniu przez osobę, której nadawane jest upoważnienie do przetwarzania danych osobowych oraz oświadczenie o zachowaniu w tajemnicy danych osobowych (treść oświadczenia stanowi ***załącznik nr 3*** do PBDO), przechowywane są w aktach osobowych pracowników lub razem z właściwą umową cywilnoprawną.

Upoważnienie do przetwarzania danych osobowych wygasa z dniem zakończenia stosunku prawnego wiążącego osobę upoważnioną ze placówką (umowa o pracę, umowa cywilnoprawna, itd.).

Nadzór nad wydawaniem upoważnień sprawuje Inspektor Ochrony Danych.

Nadawanie uprawnień do przetwarzania danych osobowych w Systemie informatycznym lub Aplikacji jest dokonywane zgodnie z upoważnieniem, o którym mowa powyżej przez Administratora Systemu Informatycznego, na wniosek Dyrektora.

Zasady nadawania uprawnień w systemach informatycznych i aplikacjach reguluje Instrukcja Zarządzania Systemem Informatycznym.

Procedura nadawania upoważnień do przetwarzania Danych osobowych stanowi ***załącznik nr 4***. Administrator danych prowadzi ewidencję osób upoważnionych do przetwarzania danych lub wyznacza w tym celu odpowiedniego pracownika. Nadzór nad ewidencją sprawuje IOD.

Ewidencja zawiera co najmniej następujący zakres informacji:

1) Imię i nazwisko osoby upoważnionej,
2) Datę nadania i ustania upoważnienia
3) zakres upoważnienia (wykonywane operacje – kategorie przetwarzań),
4) Nazwę komórki organizacyjnej
5) Identyfikator (login) użytkownika w systemie,

Datę zarejestrowania i wyrejestrowania z systemu, aplikacji, programu.

Wzór ewidencji stanowi ***załącznik nr 5***. Ewidencja prowadzona jest w formie elektronicznej i stanowi dokument powiązany z PBDO.

5. Administrator danych

Administrator danych decyduje o celach i środkach przetwarzania Danych osobowych, jest też odpowiedzialny za przestrzeganie zasad, o których mowa w PBDO oraz przepisach prawa. ADO wdraża odpowiednie środki techniczne i organizacyjne w celu zapewnienia przetwarzania danych w Placówce zgodnie z zapisami RODO i stwierdzonymi na ich podstawie ryzykami. Administratora danych osobowych reprezentuje Dyrektor placówki.

6. Inspektor ochrony danych

Placówka oświatowa jako instytucja publiczna, będąca jednostką sektora finansów publicznych, zobowiązana jest do wyznaczenia Inspektora ochrony danych (IOD) zgodnie z art.37 pkt 1a 1 RODO. Inspektor ochrony danych włączany jest we wszystkie sprawy dotyczące ochrony danych osobowych, podlega on bezpośrednio Administratorowi danych. Do jego zadań w szczególności należy:

1. informowanie Administratora danych i wszystkich pracowników/ współpracowników placówki o obowiązkach spoczywających na nich w obszarze zapewnienia bezpieczeństwa danych osobowych,
2. monitorowanie przestrzegania zapisów RODO i przyjętych zasad ochrony danych w placówce, podejmowanie działań zwiększających świadomość w obszarze ochrony danych,
3. współpraca z organem nadzorczym,
4. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych.

Dane osobowe (imię i nazwisko) i kontaktowe (adres e-mail lub telefon służbowy) IOD muszą zostać udostępnione na stronie internetowej placówki oświatowej.

Administrator danych może w formie odrębnego porozumienia ustalić inny zakres zadań IOD, z zastrzeżeniem aby te zadania nie stanowiły konfliktu interesów z zadaniami wykonywanymi przez IOD na podstawie przepisów RODO.

7. Administrator Systemów Informatycznych

Administrator Systemów Informatycznych jest wyznaczony przez Dyrektora, posiada kompetencje w zakresie informatyki i jest osobą odpowiedzialną za administrowanie powierzonym systemem informatycznym/teleinformatycznym, siecią informatyczną oraz infrastrukturą i środowiskiem informatycznym placówki, ich bezpieczeństwo oraz sprawne i ciągłe funkcjonowanie.

Zadania ASI określa *Regulamin organizacji przetwarzania danych osobowych* stanowiący **załącznik nr 1** do PBDO oraz IZSI.

8. Procesy przetwarzania danych w placówce.

W placówce stosuje się procesowe podejście do przetwarzania Danych osobowych, w ramach którego w pierwszej kolejności określa się cele przetwarzania danych niezbędne dla placówki z punktu widzenia realizacji jej zadań statutowych, a następnie weryfikuje się legalność i zakres niezbędnych danych. W dalszej kolejności określa się nazwy procesów i przypisuje tym procesom operacje i czynności przetwarzania danych osobowych. Dane osobowe przetwarzane są w procesach określonych w Rejestrze czynności przetwarzania danych osobowych (RCPD) prowadzonym przez IOD lub pracownika w skazanego przez Dyrektora Placówki w wersji elektronicznej. RCPD stanowi dokument powiązany z PBDO. Rejestr czynności przetwarzania danych dostępny jest u IOD lub w sekretariacie Dyrekcji. Rejestr jest udostępniany pracownikom na każde żądanie. W przypadku aktualizacji rejestru jest on udostępniany wszystkim pracownikom do wiadomości. RCPD nie podlega udostępnieniu w trybie dostępu do informacji publicznej.

Procesy wskazane w rejestrze czynności przetwarzania danych mogą być w każdym czasie zmieniane, a zakres przetwarzanych w nich danych w zależności od celu i obowiązujących zasad, rozszerzany lub ograniczany przez Administratora danych, o czym poinformuje przez uprawnione osoby wszystkich pracowników/ współpracowników Placówce.
Wprowadzenie zmian do Rejestru czynności przetwarzania danych dokonuje IOD – z własnej inicjatywy lub na wniosek Administratora danych. Zgłoszenia zmian lub ich propozycji może dokonać każdy Pracownik. Zgłoszone zmiany lub ich propozycje konsultowane są z IOD, jeżeli zostaną zaakceptowane przez IOD oraz Dyrektora Placówki są wprowadzane do Rejestru czynności przetwarzania danych.

9. Rejestrowanie czynności przetwarzania danych

W Placówce, zgodnie z art. 30 ust. 1 RODO prowadzony jest Rejestr czynności przetwarzania danych osobowych, za które odpowiada Administrator danych. Rejestr zawiera m.in. dane ADO i IOD, cele przetwarzania, opis kategorii osób, których dane dotyczą, opis kategorii danych, kategorie odbiorców danych, planowane terminy usunięcia danych, ogólny opis środków technicznych i organizacyjnych zastosowanych w celu zapewnienia bezpieczeństwa danych. Pełny zakres informacji zawartej w rejestrze dostępny jest u IOD lub w Sekretariacie Dyrekcji. Dane do rejestru czynności przetwarzania danych w przypadku wprowadzania nowych procesów lub aktualizacji istniejących zgłaszają pracownicy do IOD, celem weryfikacji zgodności procesu z przepisami dotyczącymi przetwarzania danych. IOD po pozytywnej ocenie procesu w kontekście danych osobowych zgłasza ten fakt Dyrektorowi Placówki celem uzyskania akceptacji. Po akceptacji, IOD lub wyznaczona w tym celu osoba

wprowadza do rejestru nowy proces lub aktualizuje dotychczasowy i przekazuje odpowiedni komunikat pracownikom w tym zakresie.

Z uwagi na fakt, że placówka może być również podmiotem przetwarzającym dane w rozumieniu art. 28 RODO zobowiązana jest do prowadzenia rejestru kategorii czynności przetwarzania danych zgodnie z art. 30 ust. 2 RODO.

Oba rejestry nadzorowane są przez IOD lub działającą w jego imieniu osobę. Rejestry stanowią odpowiednio **załącznik nr 6** i **załącznik nr 7.**

10. Zapoznanie się z zasadami ochrony danych osobowych

Administrator Danych zapewnia, by wszystkie osoby przed rozpoczęciem pracy z Danymi osobowymi zostały zapoznane z przepisami o ich ochronie oraz z wewnętrznymi regulacjami. Zapoznanie może mieć formę zorganizowanego szkolenia dla większej liczby osób lub samokształcenia kierowanego bezpośrednio do osoby przez przesłanie odpowiedniego zestawu materiałów informacyjnych i uzyskania potwierdzenia o zapoznaniu się z ich treścią.

Administrator danych, poprzez wyznaczonego pracownika lub Inspektora ochrony danych, przeprowadza szkolenia lub udostępnia materiały do samokształcenia.

Szkolenie/samokształcenie zostaje zakończone podpisaniem oświadczenia o wzięciu udziału w szkoleniu/samokształceniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych zasad ochrony danych osobowych. Wzór oświadczenia stanowi ***załącznik nr 8***.

11. Podejście oparte na ryzyku

Administrator danych, podejmując działania zmierzające do wdrożenia odpowiednich środków technicznych i organizacyjnych, ma obowiązek wprowadzenia takich rozwiązań, które spełniać będą wymogi realizacji zasad RODO, w tym celu realizuje odpowiednią procedurę analizy ryzyka.

Realizując podejście oparte na ryzyku Administrator danych:

1) rozważa, jakie konkretnie środki ma zastosować,
2) poddaje przyjęte środki, w zależności od potrzeb, przeglądom,
3) dokonuje aktualizacji przyjętych środków,
4) w zależności od potrzeb, wdraża odpowiednie polityki ochrony danych,
5) w zależności od potrzeb, stosuje zatwierdzone kodeksy postępowania lub mechanizmy certyfikacji.

Szczegółowe zasady, analiza oraz szacowanie ryzyka związanego z istniejącymi lub potencjalnymi zagrożeniami dla zasobów i aktywów informacyjnych wykorzystywanych do przetwarzania informacji, w tym danych osobowych określa „Procedura zarządzania ryzykiem dla aktywów informacyjnych oraz ryzykiem dla prywatności" stanowiąca odrębny dokument.

12. Środki organizacyjne i techniczne zastosowane w placówce w celu zapewnienia bezpieczeństwa i ochrony danych

Zgodnie z art.24 RODO Administrator danych wdraża odpowiednie środki techniczne i organizacyjne w celu zapewnienia, że przetwarzanie będzie odbywało się zgodnie z prawem. Stosowanie środków musi uwzględniać charakter, zakres, kontekst i cele przetwarzania danych, a także ryzyko naruszenia praw lub wolności osób, których dane dotyczą. Zastosowane środki muszą zostać wdrożone w sposób umożliwiający ich wykazanie, w razie potrzeb poddawane są przeglądom i aktualizacji. Minimalny standard bezpieczeństwa stanowią:

Środki organizacyjne zastosowane w placówce mające na celu zapewnienie bezpieczeństwa i ochrony Danych osobowych to przede wszystkim:

1. Wdrożenie i stosowanie zapisów niniejszej Polityki Bezpieczeństwa Danych Osobowych,
2. Wyznaczenie Inspektora ochrony danych,
3. Wyznaczenie Administratora Systemu Informatycznego,
4. Ciągłe podnoszenie świadomości wszystkich pracowników i współpracowników w obszarze ochrony danych osobowych,
5. Organizowanie szkoleń z obszaru ochrony danych osobowych dla wszystkich osób mających dostęp do przetwarzania Danych osobowych,
6. Prowadzenie i aktualizowanie Rejestru czynności przetwarzania Danych osobowych,
7. Prowadzenie i aktualizowanie Rejestru kategorii czynności przetwarzania Danych osobowych
8. Przestrzeganie zasad „czystego biurka" i „czystego ekranu" (***załącznik nr 9***)
9. Powierzenie przetwarzania Danych osobowych w drodze umowy podmiotowi przetwarzającemu,
10. Nadawanie upoważnień do przetwarzania danych osobowych w celu zapewnienia, że dostęp do danych mają jedynie osoby uprawnione, w określonym zakresie, czasie i celu, jedynie na polecenie administratora
11. Prowadzenie ewidencji osób upoważnionych.

Środki informatyczno-techniczne zastosowane w placówce mające na celu zapewnienie bezpieczeństwa i ochrony Danych osobowych to przede wszystkim:

1. Zapewnienie rozliczalności we wszystkich systemach teleinformatycznych poprzez ustalony system nadawania/zmiany/odbioru uprawnień w systemie teleinformatycznym,
2. Stosowanie fizycznej kontroli dostępu do szaf i pomieszczeń, w których przechowywane są dane osobowe,
3. Ochrona przed szkodliwym oprogramowaniem (programy antywirusowe),
4. Nadawanie identyfikatorów i haseł,
5. Kontrola dostępu,
6. Stosowanie zabezpieczeń nośników danych, sprzętu komputerowego, aplikacji, sieci
7. System Firewall do ochrony dostępu do sieci komputerowej;
8. Wygaszacze ekranów na stanowiskach, na których przetwarzane są Dane osobowe;
9. Urządzenia chroniące system informatyczny przed awarią zasilania lub zakłóceniami w sieci zasilającej.

Środki ochrony fizycznej:

1. Zapewnienie ochrony fizycznej w postaci zawartych umów z zewnętrznymi agencjami,

2. Zabezpieczenie pomieszczeń stanowiących obszar przetwarzania Danych osobowych drzwiami zamykanymi na klucz, kartę dostępu lub kod,
3. Zapewnienie dostępu do niszczarki służącej do niszczenia zbędnych, bieżących dokumentów,
4. Zapewnienie szaf/mebli zamykanych na klucz,
5. Umożliwienie przebywania w obszarze przetwarzania danych osobowych osobom nieuprawnionym jedynie za zgodą Administratora danych lub w obecności Osób upoważnionych.

Wskazane powyżej środki techniczne i organizacyjne wskazują minimalny standard. Dla niektórych procesów systemów lub kategorii danych należy stosować indywidualnie zabezpieczenia odpowiadający stwierdzonemu ryzyku.

W każdym przypadku, w którym przetwarza się dane osobowe stosuje się takie rozwiązania, aby przetwarzanym Danym osobowym w stosownym przypadku zapewnić poufność, integralność, dostępność, a systemy wykorzystywane do przetwarzania gwarantowały odporność na zagrożenia. W razie incydentów stosowane są procedury zmierzające do niezwłocznego i szybkiego przywrócenia ich pracy, a tym samym dostępności przetwarzanych Danych osobowych.

Administrator danych, podejmując działania zmierzające do wdrożenia odpowiednich środków technicznych i organizacyjnych, ma obowiązek wprowadzenia takich rozwiązań, które spełniać będą wymogi realizacji zasad RODO, w tym celu realizuje odpowiednią procedurę analizy ryzyka.

Realizując podejście oparte na ryzyku Administrator danych:

1) rozważa, jakie konkretnie środki ma zastosować,
2) poddaje przyjęte środki, w zależności od potrzeb, przeglądom,
3) dokonuje aktualizacji przyjętych środków,
4) w zależności od potrzeb, wdraża odpowiednie polityki ochrony danych,
5) w zależności od potrzeb, stosuje zatwierdzone kodeksy postępowania lub mechanizmy certyfikacji.

Zasady regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania Danych osobowych w systemach teleinformatycznych określają odrębne dokumenty.

13. Zasady obowiązujące przy zbieraniu nowych danych osobowych

W przypadku planowanego zbierania nowych Danych osobowych osoba, która zamierza zbierać nowy rodzaj Danych osobowych lub stworzyć nowy proces związany z Przetwarzaniem Danych osobowych zobowiązana jest poinformować o tym Dyrektora, który informuje IOD, a następnie po pozytywnej weryfikacji przedstawia proces lub zbiór danych Dyrektorowi celem ostatecznej akceptacji. Przed rozpoczęciem takich działań, osoba zgłaszająca proces powinna podać jednocześnie informacje w zakresie:

1. od kogo będą zbierane Dane osobowe;
2. zakresu Danych osobowych jakie będą zbierane;
3. celu zbierania Danych osobowych;
4. udostępnianiu lub Powierzaniu przetwarzania danych na zewnątrz;
5. formy fizycznej zbioru Danych osobowych (papierowa czy informatyczna).

IOD ocenia zgłoszenie pod względem zgodności z przepisami dotyczącymi przetwarzania danych, w tym celowości, legalności, czasowości i adekwatności zbieranych danych oraz rekomenduje zasadność takiego przetwarzania lub wnosi swoje zastrzeżenia. Rekomendacje lub zastrzeżenia kieruje do osoby zgłaszającej i do wiadomości Administratora danych.

Dane osobowe przetwarzane w placówce mogą być uzyskiwane w granicach dozwolonych przepisami prawa.
Dane osobowe muszą być:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);
b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu”);
c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);
d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);
e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania”);
f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).

Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność”).

14. Ocena skutków dla ochrony danych

W przypadku gdy dany rodzaj przetwarzania danych ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może spowodować wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, w szczególności gdy przetwarzanie może skutkować uszczerbkiem fizycznym, szkodami majątkowymi i niemajątkowymi Administrator jeszcze przed rozpoczęciem przetwarzania dokonuje oceny skutków dla ochrony danych osobowych. Ocena skutków dotyczy przede wszystkim planowanego przetwarzania z użyciem nowych technologii.

W placówce ocena skutków musi być dokonywana w konsultacji z Inspektorem ochrony danych.

Dokonując oceny skutków dla ochrony danych, Administrator danych konsultuje się z Inspektorem ochrony danych.

Ocena skutków dla ochrony danych, jest wymagana w szczególności w przypadku:

1. planowanego przetwarzania Danych osobowych z użyciem nowych technologii;
2. systematycznej, kompleksowej oceny 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;
3. przetwarzania na dużą skalę (przetwarzanie znacznej ilości danych osobowych na szczeblu regionalnym, krajowym lub ponadnarodowym, które może wpłynąć na dużą liczbę osób) szczególnych kategorii danych osobowych, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa;
4. systematycznego monitorowania (optycznego lub elektronicznego) na dużą skalę miejsc dostępnych publicznie (w tym sieci publicznej),
5. w przypadkach wskazywanych przez Prezesa Urzędu Ochrony Danych publikowanych na stronie urzędu.

Ocena zawiera co najmniej:

1. systematyczny opis planowanych operacji przetwarzania i celów przetwarzania;
2. ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
3. ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
4. środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę Danych osobowych i wykazać przestrzeganie prawa powszechnie obowiązującego.

W razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z operacji przetwarzania, Administrator danych dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych.
Wyniki oceny należy uwzględnić przy określaniu odpowiednich środków, które należy zastosować, by wykazać, że przetwarzanie Danych osobowych odbywa się zgodnie z RODO.

Jeżeli ocena skutków dla ochrony danych wykaże, że operacje przetwarzania powodują wysokie ryzyko, którego Administrator danych nie może zminimalizować odpowiednimi środkami z punktu widzenia dostępnej technologii i kosztów wdrożenia, przed przetwarzaniem należy skonsultować się z Prezesem Urzędu Ochrony Danych Osobowych.

Administrator danych lub IOD może zlecić wykonanie oceny skutków dla ochrony danych podmiotowi, który świadczy takie usługi w ramach profesjonalnej działalności gospodarczej i legitymuje się stosowną wiedzą i doświadczeniem.

W placówce ocenę skutków dla ochrony danych wykonuje się z wykorzystaniem narzędzia udostępnionego przez CNIL oraz rekomendowanego przez Prezesa UODO – aplikacja o nazwie PIA. Administrator danych po konsultacji z IOD może zadecydować o odrębnej metodzie oceny skutków dla ochrony danych.

15. Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

Administrator danych uwzględnia ochronę praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych jeszcze przed przystąpieniem do faktycznego przetwarzania danych – już na najwcześniejszym etapie w fazie projektowania, tj. opracowywania, wybierania aplikacji, programów i usług.
Wybór produktu uwzględnia kwestie związane z ochroną danych, które będą w nim przetwarzane, uwzględniając przede wszystkim zasadę minimalizacji danych (przetwarzamy tylko te dane, które są niezbędne do osiągniecia celu przetwarzania), a także ich pseudonimizację („szyfrowanie" danych w celu uniemożliwienia identyfikacji osoby). Stosowanie zasady domyślnej ochrony danych ma na celu zapewnienie, że przetwarzane są tylko te dane osobowe, które są niezbędne dla osiągnięcia konkretnego celu przetwarzania. Domyślna ochrona danych odnosi się do ilości zbieranych danych, zakresu ich przetwarzania, okresu przechowywania oraz ich dostępności.
Zasada uwzględniania ochrony danych osobowych w fazie projektowania oraz zasada domyślnej ochrony danych brana jest pod uwagę m.in. przy realizacji zamówień i w przetargach publicznych. Polityka domyślnej ochrony danych i ochrony danych w fazie projektowania stanowi ***załącznik nr 10*** do niniejszej polityki.

16. Obowiązek informacyjny

Przy przetwarzaniu danych osobowych Administrator musi pamiętać o spełnieniu tzw. obowiązku informacyjnego względem osoby, której dane dotyczą.

Osobom fizycznym należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem. W szczególności, konkretne cele przetwarzania danych osobowych powinny być wyraźne, uzasadnione i określone w momencie ich zbierania.

Placówka spełnia niniejszy obowiązek poprzez zamieszczenie informacji:

a) w stopce wiadomości elektronicznej,
b) dodanie odpowiedniej klauzuli w stosowanych formularzach,
c) stosowanie odpowiedniej klauzuli w zawieranych umowach,
d) stosowanie odpowiednich klauzul w procesie realizacji zamówień publicznych,
e) stosowanie odpowiedniej klauzuli w procesie rekrutacyjnym
f) informując w regulaminie wykorzystania plików „cookies"
g) odpowiednie oznaczenie monitoringu.

17. Bezpieczeństwo teleinformatyczne

Dane osobowe przetwarzane przez placówkę w systemach teleinformatycznych podlegają ochronie zapewniającej bezpieczeństwo m.in. przed nieuprawnionym dostępem, ujawnieniem, nieautoryzowaną modyfikacją, usunięciem lub ich zmianą, tj. podlegają ochronie zapewniającej ich poufność, integralność i dostępność.

Komputery (w tym laptopy) posiadają aktualne oprogramowanie antywirusowe.

Dostęp do komputerów (w tym laptopów), w których przetwarzane są Dane osobowe oraz przechowywane są informacje mające znaczenie dla Placówki uwierzytelniany jest hasłem. Hasła użytkowników do systemów podlegają następującym zasadom:

1. składają się z minimum 8 znaków,
2. muszą spełniać warunek złożoności polegający na występowaniu w nich: wielkiej i małej litery oraz cyfry lub znaku specjalnego (np. !@#),
3. muszą być zmieniane minimum co 30 dni,
4. kolejne hasła muszą różnić się od poprzedniego,
5. należy przechowywać je w sposób gwarantujący ich poufność. Zabronione jest pozostawianie zapisanych haseł w widocznych, dostępnych dla nieupoważnionych osób miejscach (np. przyklejanie „żółtych karteczek" z zapisanym hasłem do monitora, chowanie ich pod klawiaturą itp.) oraz udostępnianie haseł innym osobom. Zabrania się tworzenia haseł na podstawie:
   a) cech i numerów osobistych (np. dat urodzenia, imiona itp.),
   b) sekwencji klawiszy klawiatury (np. qwerty, 123456789),
   c) identyfikatora użytkownika,
   d) innych haseł łatwych do odgadnięcia.

W celu zapewnienia bezpieczeństwa Danym osobowym przetwarzanym w systemach teleinformatycznych Pracownicy (użytkownicy) zobowiązani są do stosowania poniższych zasad:

1. Rozpoczynając pracę z systemem należy sprawdzić ogólny stan używanego sprzętu oraz ocenić jakość pracy urządzenia (wydajność, niestandardowe komunikaty itp.),
2. Uwierzytelnianie użytkownika odbywa się zgodnie z komunikatami uruchamianego systemu. Użytkownik loguje się do systemu używając swojego identyfikatora i hasła.
3. Pracując z systemem informatycznym, użytkownik zobowiązany jest do zachowania bezpieczeństwa tego procesu. Podczas pracy należy pamiętać o następujących czynnościach:

a) ustawieniu monitorów w sposób uniemożliwiający osobom trzecim dostęp do wyświetlanych informacji,

b) blokowaniu dostępu do systemu operacyjnego poprzez naciśnięcie przycisków Ctrl+Alt+Delete oraz kliknięcie w „Zablokuj komputer" dla Windows lub skrótem klawiszowym: Logo Windows + L,

4. Zakończenie pracy z systemem odbywa się poprzez:

a) wylogowanie się z używanych aplikacji,

b) zamknięcie otwartych dokumentów i ewentualne zapisanie zmian,

c) wykonanie kopii bezpieczeństwa wykonywanej pracy (według potrzeby, dotyczy w szczególności danych przechowywanych lokalnie),

d) zamknięciu systemu operacyjnego (należy zaczekać na jego całkowite wyłączenie).

e) wyłączenie monitora

5. Po zamknięciu systemu należy sprawdzić, czy nie pozostawiono bez nadzoru elektronicznych lub papierowych nośników informacji zawierających dane osobowe lub informacje chronione.

6. Użytkownik w pełnym zakresie odpowiada za powierzony mu sprzęt komputerowy i wykonywane czynności.

Szczegółowe zasady dotyczące bezpieczeństwa sprzętu i obszaru teleinformatycznego opisane zostały w „Instrukcji zarządzania systemem informatycznym" (***załącznik nr 11***).

18. Prawa osób, których dane dotyczą

Każda osoba, której dane dotyczą posiada następujące prawa:

1. Prawo dostępu do swoich danych oraz uzyskania na ich temat informacji (art.15 RODO),
2. Prawo do sprostowania danych (art.16 RODO),
3. Prawo do usunięcia danych („prawo do bycia zapomnianym") (art17 RODO),
4. Prawo do ograniczenia przetwarzania (art.18 RODO),
5. Prawo do przenoszenia danych (art.20 RODO),
6. Prawo do sprzeciwu wobec przetwarzania danych, w tym profilowania, o ile takie jest dokonywane (art. 21,22 RODO).

Egzekwowanie powyższych praw nie może niekorzystnie wpływać na prawa i wolności innych osób, jak również korzystanie z poszczególnych może wywoływać inne określone skutki prawne, w zależności od celu ich przetwarzania (np. prawo do usunięcia danych w przypadku cofnięcia zgody na ich przetwarzanie w kontekście zatrudnienia oznacza brak możliwości realizacji przez ADO określonego celu wobec osoby jakim jest zatrudnienie).

O posiadanych prawach osoby są informowane przed przystąpieniem zbierania danych – informacje zamieszczone są na stronie internetowej Instytutu bądź przekazywane w inny sposób osobom, których dane dotyczą.

Sposób egzekwowania poszczególnych praw w przypadku złożenia wniosku przez osobę, której dane dotyczą został opisany w procedurze (***załącznik nr 12***).

19. Umowy powierzenia przetwarzania danych osobowych

Niektóre procesy przetwarzania danych osobowych w placówce wymuszają konieczność powierzenia przetwarzania danych osobowych innym podmiotom. Do najczęstszych procesów należą prowadzenie kadr i rozliczeń finansowo księgowych przez Dzielnicowe Biura Finansowania Oświaty, usługi informatyczne lub utrzymywane i dostarczane oprogramowanie np. do rekrutacji. Powierzenie odbywa się w drodze odrębnych umów powierzenia. Przetwarzanie danych i sposoby ich zabezpieczenia muszą być zgodne z zapisami RODO oraz krajowymi przepisami w obszarze ochrony

danych. Informacje dotyczące zawartych umów powierzenia zostały zamieszczone w rejestrze czynności przetwarzania.

W przypadku dokonywania zlecenia podmiotowi zewnętrznemu świadczenia usług, z którymi wiąże się przekazanie danych osobowych lub w wyniku, którego podmiot zewnętrzny będzie miał dostęp do danych osobowych, których Administratorem danych jest Placówka, umowę powierzenia przetwarzania danych osobowych należy zawrzeć w formie pisemnej.

20. Nadzór zgodności przetwarzania danych osobowych

Inspektor ochrony danych osobowych przeprowadza sprawdzenia i audyty w trybie:
1) Sprawdzenia/audytu planowego,
2) Sprawdzenia/audytu doraźnego.

Sprawdzenia i audyty planowe wykonywane są według planu opracowanego przez IOD.
Audyty i sprawdzenia doraźne są przeprowadzane niezwłocznie po powzięciu wiadomości przez Inspektora ochrony danych o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia.
IOD zawiadamia Administratora danych o rozpoczęciu audytu doraźnego. Osoba odpowiedzialna za przetwarzanie danych osobowych, której dotyczy audyt, bierze w nim udział lub umożliwia IOD przeprowadzenie czynności w toku sprawdzenia.
Po zakończeniu sprawdzenia Inspektor Ochrony Danych przygotowuje raport.
W przypadku stwierdzenia naruszania zasad ochrony danych osobowych IOD wydaje pouczenie lub instrukcję dla osoby naruszającej zasady ochrony danych osobowych oraz zawiadamia Dyrektora placówki o stwierdzonym naruszeniu.

21. Zgłaszanie naruszeń ochrony danych osobowych

W przypadku naruszenia ochrony danych osobowych, które skutkuje bądź może skutkować ryzykiem naruszenia praw i wolności osób, zgodnie z art. 33 RODO ADO bez zbędnej zwłoki, nie później jednak niż w terminie 72 godzin po stwierdzeniu naruszenia, zgłasza ten fakt organowi nadzorczemu. Naruszenia są dokumentowane, dokumentację dotyczącą naruszeń prowadzi i przechowuje ADO.

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych są one bez zbędnej zwłoki zawiadamiane o zaistnieniu takiego naruszenia (art. 34 RODO).

Szczegóły dotyczące zgłaszania naruszeń ochrony danych oraz postepowania z incydentami określa „Procedura postepowania z incydentami i naruszeniami" stanowiąca odrębny dokument.

22. Konsekwencje naruszenia Polityki Bezpieczeństwa Danych osobowych

Naruszenie przepisów o ochronie danych osobowych skutkuje nałożeniem:
1) administracyjnej kary pieniężnej art. 83 ust. 1 – 5 RODO;

2) sankcjami z tytułu naruszenia zasad Kodeksu Karego, Kodeksu Administracyjnego, Kodeksu Cywilnego, Kodeksu Pracy za nieprzestrzeganie postanowień dokumentacji oraz brak nadzoru nad bezpieczeństwem informacji, ujawnienie informacji osobie nieuprawnione;
3) odpowiedzialności cywilnej za naruszenie przepisów o ochronie danych osobowych;
4) odpowiedzialności karne i administracyjne kary pieniężne za naruszenie przepisów o ochronie danych osobowych;

23. Przegląd systemu ochrony danych osobowych

W celu utrzymania odpowiedniego, wysokiego poziomu bezpieczeństwa danych osobowych w placówce dokonuje się w miarę potrzeb przeglądów PBDO i sprawdzeń, szczególnie w sytuacji:

1) przekazania do eksploatacji nowego, kluczowego systemu informatycznego,
2) znaczących zmian organizacyjnych w funkcjonowaniu Placówki,
3) zmian w obowiązującym prawie.

Wykaz załączników

Załącznik nr 1 – Regulamin organizacji przetwarzania danych osobowych

Załącznik nr 2 – Wzór upoważnienia do przetwarzania danych osobowych

Załącznik nr 3 – Wzór oświadczenia o zachowaniu danych w poufności

Załącznik nr 4 – Procedura nadawania upoważnień do przetwarzania danych

Załącznik nr 5 – Ewidencja osób upoważnionych do przetwarzania danych osobowych

Załącznik nr 6 – Rejestr czynności przetwarzania danych osobowych

Załącznik nr 7 – Rejestr umów powierzenia i kategorii przetwarzania

Załącznik nr 8 – Wzór oświadczenia o uczestnictwie w szkoleniu/ samokształceniu

Załącznik nr 9 – Polityka „czystego biurka” i „czystego ekranu”

Załącznik nr 10 – Polityka domyślnej ochrony danych i ochrony danych w fazie projektowania

Załącznik nr 11 – Instrukcja zarządzania systemem informatycznym

Załącznik nr 12 – Procedura realizacji żądań osób których dane dotyczą