POLITYKA OCHRONY DANYCH OSOBOWYCH

Pracodawców RP Wielkopolska

Obowiązuje od dnia 01.06.2018

I. POSTANOWIENIA OGÓLNE

§1

1. Polityka ochrony danych osobowych określona w niniejszym dokumencie, zwana dalej **"Polityką"**, została opracowana w celu zapewnienia zgodności przetwarzania danych osobowych w Pracodawcach RP Wielkopolska **(zwanej dalej PRPW) oraz zapewnieniu zgodności działania administratora tych danych** z wymogami rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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, s. 1) oraz innymi obowiązującymi przepisami prawa. Polityka zawiera wymogi i zasady ochrony danych osobowych przez PRPW**.**
2. Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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, s. 1).
3. Sposób przetwarzania danych osobowych w PRPW oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych ujęte zostają zbiorczo w Polityce oraz w Instrukcji zarządzania systemem informatycznym, która określa warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zwanej dalej "**Instrukcją".** Wzór instrukcji stanowi załącznik nr 9 do Polityki będący jej integralną częścią.
4. Wdrożenie, aktualizacja i przestrzeganie niniejszej Polityki należy do Dyrektora PRPW.
5. Nadzór nad przestrzeganiem Polityki i kontrola przestrzegania Polityki należy do Dyrektora PRPW.
6. Za stosowanie niniejszej Polityki odpowiedzialne są wszystkie osoby zatrudnione w PRPW bez względu na podstawę prawną zatrudnienia.

II. DEFINICJE

§2

Określenia użyte w Polityce Bezpieczeństwa oznaczają:

a) **administrator danych osobowych (Administrator) - Pracodawcy RP Wielkopolska,**
b) **dane osobowe** - oznaczają 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, adres, numer telefonu, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej,
c) **przetwarzanie danych osobowych** - 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,
d) **RODO** - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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, s. 1),

e) **system informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych w PRPW,
f) **ograniczenie przetwarzania** - oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania,
g) **odbiorca** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania,
h) **naruszenie ochrony danych osobowych** - oznacza 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,
i) **dokumenty** - wszelkie nie elektroniczne nośniki informacji zawierające dane osobowe,
j) **polityka** - oznacza niniejszy dokument.

III. OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH

§3

1. Obszarem przetwarzania danych osobowych przez PRPW**, zwanym dalej "Obszarem przetwarzania",** są wydzielone pomieszczenia biurowe oraz części pomieszczeń znajdujące się w siedzibie Administratora przy ul. Św. Marcin 24/402, Poznań. Do pomieszczeń, o których mowa w zdaniu poprzedzającym zalicza się w szczególności:

a) pomieszczenia biurowe, w których zlokalizowane są stacje robocze lub serwery służące do przetwarzania danych osobowych,
b) pomieszczenia, w których przechowuje się dokumenty źródłowe oraz wydruki z systemu informatycznego zawierające dane osobowe,
c) pomieszczenia, w których przechowywane są sprawne i uszkodzone urządzenia, elektroniczne nośniki informacji oraz kopie zapasowe zawierające dane osobowe,
d) pomieszczenie przeznaczone na archiwum, w którym przechowywane są dokumenty zawierające dane osobowe,
e) sekretariat,
f) gabinety Prezesa oraz Dyrektora.

Wykaz podmiotów, którym Administrator powierzył przetwarzanie danych osobowych, wraz ze wskazaniem obszaru przetwarzania danych wskazany został w załączniku nr 1 do Polityki będącym jej integralną częścią.

IV. ZAKRES STOSOWANIA

§4

1. Politykę stosuje się do wszelkich danych osobowych przetwarzanych w PRPW zarówno w formie dokumentacji tradycyjnej i elektronicznej, do danych osobowych przetwarzanych w Systemie informatycznym jak i do Systemu informatycznego.

2. W PRPW przetwarzane są następujące dane osobowe , w tym:
a) Dane przetwarzane w związku z zatrudnieniem, w tym dane kandydatów do pracy, pracowników, współpracowników, zleceniobiorców.
b) Dane dostawców usług oraz osób świadczących usługi, w tym dane dostawców, usługodawców, dane osób wspierających działania PRPW w formie np. praktyk, staży, itp.
c) Dane klientów:
   i. dane klientów, które przetwarzane są w celu wystawienia rachunku, faktury i prowadzenia rozliczeń finansowych,
   ii. dane obecnych i byłych klientów – w zakresie ograniczonym do danych niezbędnych do identyfikacji oraz wskazania charakteru współpracy przetwarzane w celu bieżącej organizacji,
   iii. dane potencjalnych klientów – w podstawowym zakresie niezbędnym do prowadzenia planowania rozwoju działalności oraz analiz rynku.
3. Polityka i Instrukcja obowiązuje wszystkie osoby zatrudnione w PRPW bez względu na podstawę prawną zatrudnienia.
4. Polityka i Instrukcja dotyczy Obszaru przetwarzania i obowiązuje na Obszarze przetwarzania.
5. Informacje niejawne nie są objęte zakresem Polityki.

V. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

§5

[Informacje ogólne]

1. Za bezpieczeństwo danych osobowych odpowiedzialni są wszystkie organy PRPW, a także każda osoba zatrudniona w PRPW, niezależnie od formy zatrudnienia, w zakresie zajmowanego stanowiska i posiadanych informacji.
2. W umowach zawieranych przez PRPW winny znajdować się postanowienia zobowiązujące podmioty zewnętrzne do ochrony danych osobowych udostępnionych przez PRPW.

§6

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie nadane przez Administratora. Administrator upoważniając osoby do przetwarzania danych osobowych zachowuje zasadę, że dostęp do danych osobowych będą miały tylko te osoby, którym jest to niezbędne do relacji powierzonych im zadań, oraz tylko w takim zakresie, jaki jest konieczny do realizacji powierzonych zadań. Każda z osób upoważnionych do przetwarzania danych osobowych zostanie, przed dopuszczeniem do przetwarzania danych osobowych, przeszkolona z wymagań ochrony danych osobowych, oraz poinformowana o konsekwencjach prawnych jakie jej grożą za naruszenie tych zasad.

§ 7

[obowiązki Administratora]

1. Zakres uprawnień i obowiązków Administratora wskazany został w RODO. Do uprawnień i obowiązków Administratora należy m. in.:
   a) stały nadzór nad treścią Polityki i Instrukcji, a także ich aktualizacja i zmiany,
   b) kontrolowanie zgodności przetwarzania danych osobowych z obowiązującymi przepisami prawa,

c) udział w kontrolach prowadzonych przez upoważnione podmioty,
d) udzielanie odpowiedzi na zapytania kierowane do Administratora przez podmioty zewnętrzne, dotyczące administrowanych zbiorów danych osobowych,
e) nadawanie poszczególnym pracownikom upoważnień do przetwarzania danych osobowych oraz przeprowadzanie dla nich szkoleń z zakresu ochrony danych,
f) nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w Systemie informatycznym,
g) prowadzenie aktualnej ewidencji osób upoważnionych do przetwarzania danych osobowych we wszystkich zbiorach,
h) nadzór nad fizycznym zabezpieczeniem Obszarów przetwarzania,
i) monitorowanie działania i skuteczności zabezpieczeń wdrożonych w celu ochrony danych osobowych,
j) nadzór nad obiegiem oraz przechowywaniem Dokumentów,
k) nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w Systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,
l) podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,
m) identyfikacja i monitorowanie zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych i tradycyjnych,
n) regularne testowanie, mierzenie i ocena skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych w PRPW.

2. W zakresie administrowania Systemem informatycznym do obowiązków Administratora należy m.in.:
a) bieżący monitoring i zapewnienie ciągłości działania Systemu informatycznego oraz baz danych,
b) bieżący monitoring nad oprogramowaniem wykorzystywanym do przetwarzania danych osobowych w Systemie informatycznym oraz zapewnienie by oprogramowanie to było legalne i zapewniało adekwatny poziom bezpieczeństwa danych w nim przetwarzanych,
c) bieżący monitoring i identyfikacja zagrożeń dla przetwarzania danych osobowych w Systemie informatycznym,
d) bieżący monitoring Systemu informatycznego w celu zapewnienia realizacji zasady minimalizmu i zapewnienia prywatności danych (privacy by design),
e) bieżący monitoring Systemu informatycznego w celu zapewnienia by domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania (privacy by default),
f) nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
g) utworzenie procedur tworzenia i przechowywania kopii zapasowych zbiorów danych osobowych oraz programów i narzędzi służących do ich przetwarzania,
h) zapewnienie zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
i) zapewnienie adekwatnych zabezpieczeń antywirusowych i antydostępowych oraz ich bieżąca aktualizacja.

§8

[osoby upoważnione do przetwarzania danych osobowych]

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie nadane przez Administratora.
2. Administrator upoważnia osoby do przetwarzania danych osobowych, którym jest to niezbędne

do relacji powierzonych im zadań, oraz tylko w takim zakresie, jaki jest konieczne do ich realizacji.

3. Każda z osób upoważnionych do przetwarzania danych osobowych w PRPW przed dopuszczeniem do ich przetwarzania:
    a) jest zapoznawana z treścią Polityki i Instrukcji, oraz przepisami dotyczącymi ochrony danych osobowych, w tym z RODO,
    b) jest przeszkalana z wymagań ochrony danych osobowych, a także poinformowana o konsekwencjach prawnych jakie jej grożą za naruszenie tych zasad,
    c) jest informowana o zakresie odpowiedzialności w zakresie ochrony danych osobowych oraz związanymi z tym obowiązkami,
    d) podpsuje pisemne oświadczenie o zobowiązaniu do przestrzegania postanowień Polityki i Instrukcji, a w szczególności do zachowania w poufności wszystkich informacji dotyczących danych osobowych przetwarzanych w PRPW oraz sposobach ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia. Wzór oświadczenia o którym mowa w zdaniu poprzedzającym stanowi załącznik nr 2 do Polityki, będący jego integralną częścią.
4. Ochrona zasobów danych osobowych przetwarzanych przez PRPW jako całości przed ich nieuprawnionym użyciem lub zniszczeniem jest jednym z podstawowych obowiązków Pracowników.
5. Upoważnienie do przetwarzania danych osobowych w PRPW nadaje Administrator z własnej inicjatywy lub na wniosek przełożonego osoby, której upoważnienie ma zostać nadane. Administrator może upoważnić w formie pisemnej inne osoby do nadawania upoważnienia do przetwarzania danych osobowych w PRPW.
6. Wniosek o nadanie uprawnień do przetwarzania danych osobowych, o którym mowa w ust. 5 niniejszego paragrafu zawiera w szczególności:
    a) imię i nazwisko użytkownika,
    b) stanowisko zajmowane przez użytkownika,
    c) nazwę zbioru danych osobowych oraz nazwę systemu informatycznego, do którego użytkownik będzie miał dostęp,
    d) zakres upoważnienia do przetwarzania danych osobowych, obejmujący także wskazanie operacji przetwarzania objętych upoważnieniem,
    e) datę, z jaką upoważnienie ma być wydane,
    f) okres ważności upoważnienia.
7. Upoważnienie do przetwarzania danych osobowych udzielane jest w formie pisemnej, przed przystąpieniem do przetwarzania danych osobowych, w dwóch egzemplarzach, po jednym dla osoby upoważnionej i PRPW. Upoważnienie, o którym mowa w zdaniu poprzedzającym składa się do akt osobowych osoby upoważnionej. Wraz z udzieleniem upoważnienia do przetwarzania danych osobowych Administrator nadaje identyfikator w Systemie informatycznym zwany dalej „Identyfikatorem".
8. Użytkownik niebędący zatrudnionym na podstawie stosunku pracy otrzymuje oryginał upoważnienia i kwituje jego odbiór na piśmie. Kopia upoważnienia przechowywana jest w sekretariacie PRPW.
9. Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 3 do Polityki będący jego integralną częścią.
10. Uprawnienie do przetwarzania danych osobowych nadawane będzie w zakresie niezbędnym do realizacji celu przetwarzania danych osobowych przez PRPW.
11. Administrator jest zobowiązany do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych w PRPW. Wzór ewidencji, o której mowa w zdaniu poprzedzającym stanowi załącznik nr 4 do Polityki, będący jej integralną częścią. Ewidencja, o której mowa w zdaniu poprzedzającym zawiera co najmniej:
    a) imię i nazwisko osoby upoważnionej,

b) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,
c) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym,
d) oznaczenie zbioru danych osobowych.

12. Administrator może cofnąć upoważnienie w każdym czasie bez podania przyczyny / w razie naruszenia przez osobę upoważnioną przepisów RODO / Polityki w zakresie bezpieczeństwa danych osobowych / jeżeli upoważnienie danej osoby do przetwarzania danych nie jest niezbędne dla realizacji celu przetwarzania.

VI. UMOWY O POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

§ 9

1. Administrator może powierzyć przetwarzanie danych osobowych w jego imieniu innym podmiotom.
2. Powierzenie przetwarzania danych osobowych, o którym mowa w ust. 1 następuje w drodze umowy zawartej w formie pisemnej.
3. Umowa o której mowa w ust. 2 niniejszego paragrafu spełnia wymagania wskazane w RODO. Wzór umowy powierzenia przetwarzania danych osobowych stanowi załącznik nr 5 do Polityki będący jej integralną częścią.

VII. ZASADY BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

§ 10.

1. Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze, indywidualną odpowiedzialność ponosi przede wszystkim każdy Użytkownik mający dostęp do danych.
2. W toku przetwarzania danych osobowych osoba przetwarzająca te dane jest osobiście odpowiedzialna za bezpieczeństwo powierzonych mu danych.
3. Osoby mające dostęp do danych osobowych nie mogą ich ujawniać zarówno w Obszarze przetwarzania, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
4. Przed przystąpieniem do przetwarzania danych osobowych osoba przetwarzająca dane sprawdza, czy posiadane i przetwarzane przez niego dane osobowe były należycie zabezpieczone, oraz czy zabezpieczenia te nie były naruszone.
5. Zabronione jest przechowywanie na biurku lub w pobliżu komputera lub innego urządzenia, w którym przetwarzane są dane osobowe napojów lub jedzenia. Za zgodą administratora dopuszczalne jest przechowywanie napojów w pojemnikach minimalizujących ryzyko zalania, zniszczenia lub uszkodzenia danych osobowych.
6. Bezwzględnie zakazane jest spożywanie posiłków lub napojów przy biurku, stole lub innym podobnym urządzeniu, na którym znajdują się oryginały nośników danych osobowych.
7. Bezwzględnie zakazane jest wnoszenie jakichkolwiek napojów lub jedzenia do archiwum, serwerowni lub innych miejsc gdzie przechowywane są dane osobowe lub ich nośniki.
8. W toku przetwarzania danych osobowych osoba przetwarzająca dane osobowe dane powinna dbać o ich należyte zabezpieczenie przed możliwością wglądu, bądź zmiany przez osoby do tego nieupoważnione
9. W Obszarze przetwarzania osoby przetwarzające dane osobowe zobowiązane są do nie pozostawiania, po godzinach pracy lub w trakcie nieobecności, wykorzystywanych przez siebie Dokumentów lub innych nośników zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację obowiązku odpowiedzialny jest każda osoba przetwarzająca

dane osobowe w stosunku do Dokumentów, lub wszelkich innych nośników zawierających dane, przez siebie wykorzystywanych lub mu powierzonych.

10. Wszelkie Dokumenty przechowywane są w zamykanych na klucz szafach lub pomieszczeniach, znajdujących się w Obszarze przetwarzania.
11. Po zakończeniu pracy osoby przetwarzające dane osobowe zobowiązane są odłożyć Dokumenty lub inne nośniki, do szaf lub pomieszczeń wskazanych w ust. 10 niniejszego paragrafu. Zabronione jest pozostawianie Dokumentów lub innych nośników zawierających dane osobowe na stanowisku służbowym po zakończeniu pracy.
12. Dane osobowe i ich nośniki przechowywane są wyłącznie w czasie, jaki jest niezbędny do realizacji celu przetwarzania, a po zrealizowaniu celu przetwarzania wyłącznie w czasie w jakim PRPW jest zobowiązana do ich przechowywania na podstawie obowiązujących przepisów prawa. Po upływie tego okresu PRPW niezwłocznie usunie dane osobowe zawarte w Dokumentach i innych nośnikach w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.
13. Zbędne brudnopisy, błędne lub zbędne kopie materiałów zawierających dane osobowe powinny być natychmiast niszczone w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek. Niszczenie materiałów, o których mowa w zdaniu poprzedzającym może odbywać się również poprzez ich umieszczenie w specjalnie przeznaczonych do tego pojemnikach wskazanych przez Administratora.
14. Zabronione jest wynoszenie jakichkolwiek Dokumentów lub innych nośników zawierających dane osobowe poza Obszar przetwarzania chyba, że związane jest to z wykonywaniem czynności służbowych lub świadczeniem usług przez PRPW, a Dokumenty lub inne nośniki, po wykonaniu czynności służbowych lub po zakończeniu świadczenia usług przez PRPW, powrócą do Obszaru przetwarzania. Za bezpieczeństwo i zwrot Dokumentów lub innych nośników odpowiada osoba wynosząca je z Obszaru przetwarzania.
15. Bezpowrotne wydanie danych osobowych lub nośników je zawierających z Obszaru przetwarzania, w tym w szczególności zwrot właścicielom Dokumentów lub ich części dokonywane jest wyłącznie przez Administratora lub upoważnioną przez niego osobę. Wydanie, o którym mowa w zdaniu poprzedzającym stwierdzane jest protokołem, w którym zamieszcza się w szczególności:
    a) informacje o rodzaju i oznaczeniu Dokumentów bądź ich części wydawanej właścicielom,
    b) oznaczenie podmiotu na rzecz którego są one wydawane,
    c) własnoręczne podpisy wydającego i odbierającego.
16. Przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne wyłącznie za zgodą Administratora lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
17. Użytkownicy zobowiązani są do zamykania na klucz wszelkich pomieszczeń wchodzących w skład Obszaru przetwarzania w czasie ich chwilowej nieobecności w tych pomieszczeniach jak i po zakończeniu pracy. Klucze do pomieszczeń wskazanych w zdaniu poprzedzającym nie mogą być pozostawione w zamku w drzwiach. Użytkownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia posiadanych kluczy przed nieuprawnionym dostępem.
18. Archiwizację dokumentów zawierających dane osobowe prowadzi się w sposób wskazany w ust. 10 niniejszego paragrafu lub w innych przeznaczonych do tego miejscach prowadzonych przez podmioty zajmujące się świadczeniem usług archiwizacyjnych.
19. Szczegółowy opis zasad bezpieczeństwa przetwarzania danych w Systemie informatycznym, w tym zasady nadawania upoważnień zawarte są w Instrukcji.
20. Administrator wyznacza pomieszczenie w Obszarze przetwarzania przeznaczone na archiwum i serwerownie oraz pomieszczenia rezerwowe, które w razie nagłej potrzeby będą mogły być wykorzystane do tych samych celów.

VIII. INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH ORAZ INCYDENTÓW

§ 11

1. Incydent oznacza zdarzenie mogące prowadzić do naruszenia ochrony danych osobowych. W szczególności występuje ono, gdy:
   a) stwierdzono naruszenie zabezpieczenia Systemu informatycznego,
   b) stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej, stan Dokumentów, pomieszczeń, szaf, okien lub drzwi w Obszarze przetwarzania lub inne zaobserwowane symptomy mogą wskazywać na naruszenie zabezpieczeń danych osobowych.
2. Każda osoba, która poweźmie wiadomość o naruszeniu ochrony danych osobowych lub o incydencie lub podejrzewa naruszenie ochrony danych osobowych, bądź posiada informacje mogące mieć wpływ na bezpieczeństwo danych osobowych, zwana dalej **"Osobą zgłaszającą"**, jest zobowiązana fakt ten niezwłocznie zgłosić Administratorowi.
3. Niezależnie od obowiązku określonego w ust. 2 Osoba zgłaszająca do czasu otrzymania odmiennych poleceń od Administratora lub osób przez niego upoważnionych zobowiązana jest do:
   a) niezwłocznego podjęcia czynności niezbędnych dla powstrzymania niepożądanych następstw naruszenia, incydentu lub możliwości naruszenia ochrony danych osobowych a następnie ustalić przyczyny, lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe,
   b) powstrzymania się od wykonywania jakichkolwiek czynności, które mogą uniemożliwić lub utrudnić udokumentowanie i analizę zgłoszonego naruszenia, incydentu lub możliwości naruszenia ochrony danych osobowych,
   c) dokonania wstępnego zabezpieczenia i udokumentowania zaistniałego naruszenia danych ochrony osobowych,
   d) pozostania w miejscu ujawnienia naruszenia lub możliwości naruszenia ochrony danych osobowych do czasu przybycia Administratora lub osoby upoważnionej przez Administratora.
4. Niezwłocznie po otrzymaniu zgłoszenia naruszenia, incydentu lub możliwości naruszenia ochrony danych osobowych Administrator lub osoba przez niego upoważniona zapoznaje się z zaistniałą sytuacją oraz:
   a) zapisuje wszelkie informacje i okoliczności związane z danym zdarzeniem, a w szczególności dokładny czasu uzyskania informacji o incydencie lub naruszeniu ochrony danych osobowych lub samodzielnym wykryciu tego faktu,
   b) wysłuchuje relacji Osoby zgłaszającej z zaistniałego zdarzenia,
   c) żąda wyjaśnień każdej innej osoby, która może posiadać informacje związane z zaistniałym zdarzeniem,
   d) generuje i drukuje wszystkie dokumenty i raporty, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i podpisania,
   e) przystępuje do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń, metody dostępu osoby niepowołanej do danych itp.,
   f) podejmuje odpowiednie działania w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych osobowych, a w tym celu może m.in.:
      i. odłączyć urządzenia i segmentów Systemu informatycznego, które mogły umożliwić dostęp do bazy danych osobie niepowołanej,
      ii. doprowadzić do wylogowania z Systemu informatycznego osobę podejrzaną o naruszenie ochrony danych, oraz pozbawić ją dostępu do baz danych,
      iii. zmienić hasła dostępu do konta użytkownika w Systemie informatycznym poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby uzyskania takiego dostępu,

g) dokonuje szczegółowej analizy stanu Systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych,
h) przywraca normalne działanie Systemu informatycznego, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, podejmuje decyzję co do odtworzenia jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności mających na celu uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną, tą samą drogą,
i) dokumentuje dany przypadek naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze w zakresie pozwalającym organowi nadzorczemu weryfikowanie przestrzegania art. 33 RODO.

5. Po przywróceniu normalnego działania Systemu informatycznego i prawidłowego stanu bazy danych osobowych Administrator lub osoba przez niego upoważniona przeprowadza szczegółową analizę zaistniałego przypadku naruszenia ochrony danych osobowych w celu określenia jego przyczyn, oraz podejmuje działania mające na celu zapobiegnięcie podobnych zdarzeń w przyszłości (działania naprawcze).
6. Działania naprawcze, o których mowa w ust. 5 niniejszego paragrafu mogę polegać w szczególności na:
    a) przeprowadzeniu ponownego szkolenia wszystkich osób przetwarzających dane osobowe w PRPW, jeśli przyczyną naruszenia ochrony danych osobowych był błąd takiej osoby,
    b) zastosowaniu dodatkowego zabezpieczenia antywirusowego i organizacyjnego jeśli przyczyną naruszenia ochrony danych osobowych było działanie złośliwego oprogramowania,
    c) pociągnięciu osoby, która dopuściła się naruszenia ochrony danych osobowych do odpowiedzialności dyscyplinarnej i zastosowaniu w tym celu środków wynikających z kodeksu pracy lub innych obowiązujących przepisów, jeśli przyczyną naruszenia ochrony danych osobowych było zaniedbanie ze strony osoby przetwarzającej dane osobowe w Izbie,
    d) podjęcie odpowiednich kroków pranych jeśli przyczyną naruszenia ochrony danych osobowych było działanie osoby, która nie jest zatrudniona w PRPW na podstawie jakiegokolwiek tytułu prawnego.
7. W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, zgłasza je właściwemu organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
8. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Zawiadomienie, o którym mowa w zdaniu poprzedzającym sporządzane jest jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki i zawiera:
    a) imię i nazwisko oraz dane kontaktowe inspektora ochrony danych (jeżeli jest wyznaczony) lub oznaczenie upoważnionego pracownika Izby, od którego można uzyskać więcej informacji;
    b) opis możliwych konsekwencji naruszenia ochrony danych osobowych;
    c) opis środków zastosowanych lub proponowanych przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

IX. ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

§12

1. W PRPW stosowane są w szczególności następujące kategorie środków zabezpieczeń danych osobowych:
    a) zabezpieczenia fizyczne:
        i. całodobowy monitoring siedziby PRPW,
        ii. alarm antywłamaniowy,
        iii. pomieszczenia zamykane na klucz;
        iv. szafy z zamkami.
    b) zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej:
        i. przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach w Obszarze przetwarzania,
        ii. przetwarzanie danych osobowych następuje przez wyznaczone do tego celu i upoważnione osoby,
        iii. dokumenty zawierające dane osobowe, które są zbędne do osiągnięcia celu przetwarzania, a które nie podlegają archiwizacji na podstawie obowiązujących przepisów prawa, są niezwłocznie niszczone w sposób uniemożliwiający ich odczytanie, w tym ustalenie tożsamości osoby, której dane dotyczą,
        iv. serwerownia i archiwum zlokalizowana jest w pomieszczeniu pozbawionym instalacji wodnych a nośniki danych osobowych nie są składowane w pobliżu okien lub kaloryferów.
    c) zabezpieczenia informatyczne,
    d) zabezpieczenia organizacyjne:
2. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora.

§13

1. W ramach zabezpieczenia danych osobowych ochronie podlegają:
    a) sprzęt komputerowy - serwer, komputery osobiste, drukarki i inne urządzenia zewnętrzne,
    b) oprogramowanie - kody źródłowe, programy użytkowe, systemy operacyjne, narzędzia wspomagające i programy komunikacyjne,
        i. dane zapisane na dyskach oraz dane podlegające przetwarzaniu w systemie,
        ii. hasła użytkowników,
        iii. pliki dziennych operacji systemowych i baz danych, kopie zapasowe i archiwa,
    c) dokumentacja zawierająca dane systemu, opisująca jego zastosowanie, przetwarzane informacje, itp.,
    d) Dokumenty.
2. Zasady korzystania z poczty elektronicznej oraz internetu wskazane zostały w Instrukcji.
3. Zasady szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego wskazane zostały w Instrukcji.

X. KONTROLA PRZETWARZANIA I STANU BEZPIECZEŃSTWA DANYCH OSOBOWYCH

§ 14

4. Nadzór i kontrolę nad ochroną danych osobowych przetwarzanych w PRPW sprawuje w imieniu PRPW, Dyrektor PRPW.
5. Czynności kontrolne przeprowadzane są nie rzadziej niż raz na kwartał.
6. Z czynności kontrolnych sporządzany jest protokół, w którym dokonuje się dokładnego opisu zakresu kontroli i przeprowadzonych czynności. Wzór protokołu, o którym mowa w zdaniu poprzedzającym stanowi załącznik nr 6 do Polityki, będący jej integralną częścią.

7. Protokół podpisywany jest przez osoby wykonujące czynności kontrolne. Dołącza się go do dokumentacji przechowywanej przez PRPW.

XI. OBOWIĄZEK INFORMCYJNY

§ 15

1. PRPW zapewnia wypełnienie wszystkich obowiązków informacyjnych przewidzianych w RODO względem osób, których dotyczą przetwarzane przez PRPW dane osobowe, w tym w szczególności obowiązki wskazane w art. 13 i 14 RODO.
2. Obowiązek informacyjny, o którym mowa w ust. 1 niniejszego paragrafu realizowany jest w sposób umożliwiający rzeczywiste zapoznanie się z nim osoby, której dane osobowe dotyczą oraz w miejscu łatwo dostępnym dla tych osób.
3. PRPW informuje osobę o prawie sprzeciwu, o którym mowa w art. 21 RODO, najpóźniej przy okazji pierwszej komunikacji z tą osobą.
4. PRPW bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.
5. Wszelkie komunikaty kierowane do dzieci formułowane są w sposób prosty i dla nich zrozumiały.

XII. TRYB POSTĘPOWANIA W PRZYPADKU WNIOSKU OSOBY, KTÓREJ DANE DOTYCZĄ O UDZIELENIE INFORMACJI I REALIZACJA ŻĄDAŃ TEJ OSOBY

§ 16

1. Administrator bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem na podstawie art. 15–22. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania Administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia.
2. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.
3. Administrator prowadzi ewidencję żądań, o których mowa w ust.1, w której wskazuje się datę wpływu żądania, osobą, której dane dotyczą, datę pism kierowanych do osoby, której dane dotyczą.
4. Administrator może w przypadkach wskazanych w RODO odmówić podjęcia działań związanych z żądaniem osoby, której dane dotyczą.

§ 17

[Prawo do informacji]

1. PRPW udziela osobie o to wnioskującej potwierdzenia czy przetwarzane są jej dane osobowe. Jeżeli PRPW nie przetwarza danych osoby wnioskującej informuje ją o tym.
2. Jeżeli dane osobowe osoby żądającej są przetwarzane, ma ona prawo do informacji wskazanych w art. 15 RODO.
3. W przypadku odmowy rozpatrzenia wniosku, o którym mowa w ust. 1, i informuje się osobę o przysługujących jej w związku z tym prawach.
4. Na żądanie osoby, której dane dotyczą dostarcza się tej osobie nieodpłatnie kopie jej danych

osobowych podlegających przetwarzaniu. PRPW odnotowuje wydanie pierwszej kopii danych osobowych.
5. PRPW może wprowadzić odpłatność za wydawanie kopi danych osobowych w przypadkach wskazanych w RODO.

§ 18
[Sprostowanie i uzupełnienie danych].

1. Osoba, której dane dotyczą, ma prawo żądania od Administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe.
2. W przypadku sprostowania danych PRPW informuje osobę, której dane dotyczą, o odbiorcach danych, jeżeli osoba, której dane dotyczą, tego zażąda.
3. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
4. W celu poparcia żądania, o którym mowa w ust. 3 niniejszego paragrafu, osoba, której dane dotyczą może składać PRPW oświadczenie lub udzielić dodatkowych informacji lub wyjaśnień. Oświadczenie, informacje lub wyjaśnienia, o którym mowa w zdaniu poprzedzającym mogą być udzielane w dowolnej formie, w tym w formie elektronicznej.
5. PRPW może nie uwzględnić żądania, o którym mowa w ust. 3 niniejszego paragrafu jeżeli uzupełnienie danych osobowych byłoby niezgodne z celami przetwarzania danych, w szczególności jeżeli żądanie dotyczy danych, które ze względu na zasadę minimalizacji nie są Administratorowi niezbędne do osiągnięcia celu przetwarzania danych.
6. PRPW odmawia sprostowania lub uzupełnienia danych osobowych, o których mowa w ust. 1 i 3 niniejszego paragrafie, jeżeli w wyniku ich uwzględnienia dane osobowe byłyby w dalszym ciągu nieprawidłowe lub niekompletne.
7. PRPW może odmówić sprostowania lub uzupełnienia danych osobowych, o których mowa w ust. 1 i 3 niniejszego paragrafu jeżeli stosownie do zasady rozliczalności wskazanej w art. 5 ust. 2 RODO, jest w stanie wykazać, że przetwarzane dane osobowe są prawidłowe.

§ 19

[**Prawo usunięcia danych, 'prawo bycia zapomnianym']**

1. Na żądanie osoby, której dane dotyczą PRPW niezwłocznie usuwa dane tej osobowe, gdy:
   a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane,
   b) osoba, której dane dotyczą cofnęła zgodę na ich przetwarzanie i nie ma innej podstawy prawnej przetwarzania,
   c) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,
   d) dane osobowe były przetwarzane niezgodnie z prawem,
   e) konieczność usunięcia danych osobowych wynika z obowiązku prawnego,
   f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1. RODO, tj. w przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku, które ukończyło 16 lat, na podstawie zgody tego dziecka a w przypadku dzieci, które nie ukończyły 16 lat, w przypadkach, gdy zgodę na przetwarzanie danych osobowych w związku ze świadczeniem takich usług wyraziła lub zaaprobowała osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody.
2. Jeżeli dane osobowe podlegające usunięciu zostały upublicznione przez PRPW, PRPW podejmuje rozsądne działania, by poinformować administratorów przetwarzających te dane osobowe, że

osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje, z zastrzeżeniem ust. 3 niniejszego paragrafu.

3. Na wyraźne żądanie osoby, której dane dotyczą, PRPW nie informuje pozostałych administratorów o usunięciu danych osobowych tej osoby, stosownie do treści art. 17 ust. 2 RODO.
4. W przypadku usunięcia danych PRPW informuje osobę o odbiorcach danych, na żądanie tej osoby.
5. PRPW zapewniając efektywną realizację prawa określonego w niniejszym paragrafie, mając na względnie przestrzeganie wszystkich zasad ochrony i bezpieczeństwa danych osobowych, weryfikuje jednocześnie występowanie przesłanek, o których mowa w art. 17 ust. 3 RODO, wyłączających możliwość skorzystania z tego prawa.

§ 20

[Ograniczenie przetwarzania]

1. Osoba, której dane dotyczą, ma prawo żądania od PRPW ograniczenia przetwarzania w następujących przypadkach:
    a) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający Administratorowi sprawdzić prawidłowość tych danych,
    b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
    c) PRPW nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
    d) osoba, której dane dotyczą, wniosła na mocy art. 21 ust. 1 RODO sprzeciw wobec przetwarzania związany z jej szczególną sytuacją – do czasu stwierdzenia, czy prawnie uzasadnione podstawy występujące po stronie PRPW są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.
2. W przypadku ograniczenia przetwarzania danych osobowych PRPW może przetwarzać te dane, z wyjątkiem przechowywania, wyłącznie:
    a) za zgodą osoby, której dane dotyczą, lub
    b) w celu ustalenia, dochodzenia lub obrony roszczeń, lub
    c) w celu ochrony praw innej osoby fizycznej lub prawnej, lub
    d) z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.
3. Przed uchyleniem ograniczenia przetwarzania PRPW informuje o tym osobę, której dane dotyczą, która żądała ograniczenia na mocy ust. 1 niniejszego paragrafu.
4. W przypadku ograniczenia przetwarzania danych PRPW informuje osobę, której dane dotyczą, o odbiorcach danych, jeżeli osoba, której dane dotyczą, tego zażąda.

§ 21

[Prawo do przenoszenie danych].

1. Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła PRPW, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony PRPW, jeżeli:
    a) przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą lub na podstawie umowy zawartej z PRPW, oraz
    b) przetwarzanie odbywa się w sposób zautomatyzowany.

2. W ramach realizacji uprawnienia do przenoszenia danych, o którym mowa w ust. 1 niniejszego paragrafu, osoba, której dane dotyczą może żądać, by PRPW przesłała jej dane osobowe bezpośrednio innemu administratorowi, o ile jest to techniczne możliwe.
3. Poprzez dane dostarczone PRPW przez osobę, której dane dotyczą, rozumie się dane aktywnie i świadomie przekazywane przez osobę, której dane dotyczą (np. imię, nazwisko, nazwa użytkownika, adres pocztowy itp.),
4. PRPW zapewni sprawną realizację uprawnienia wskazanego w ust. 1 niniejszego paragrafu, w szczególności poprzez jego nieodpłatność, chyba że zachodzą okoliczności wskazane w art. 12 ust. 5 zd. 2 RODO, a także zapewni przenoszenie danych bez zbędnej zwłoki oraz ograniczenie procedur identyfikacyjnych osoby zgłaszającej żądanie wskazane w ust. 1 niniejszego paragrafu do niezbędnego minimum.

§ 22

[Prawo do sprzeciwu]

1. Jeżeli osoba, której dane dotyczą, wniesie sprzeciw związany z jej szczególną sytuacją, względem przetwarzania jej danych osobowych przez Izbę, w tym profilowania, w oparciu o uzasadniony interes PRPW lub o powierzone PRPW zadanie w interesie publicznym, PRPW uwzględni sprzeciw.
2. PRPW może nie uwzględnić sprzeciwu, o którym mowa w ust. 1 niniejszego paragrafu, jeżeli po stronie PRPW zachodzą ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby której dane dotyczą, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.
3. W przypadku wniesienia przez osobę, której dane dotyczą sprzeciwu wobec przetwarzania dotyczących jej danych osobowych na potrzeby marketingu bezpośredniego Izby, w tym profilowania, PRPW uwzględni sprzeciw i zaprzestanie przetwarzania danych osobowych tej osoby w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.
4. PRPW umożliwia wniesienie sprzeciwu o którym mowa w ust. 1 i 3 niniejszego paragrafu drogą elektroniczną.

§ 23

[Zautomatyzowane podejmowanie decyzji w tym profilowanie]

1. PRPW może przetwarzać dane w sposób zautomatyzowany, w tym w szczególności profilować dane, i wyłącznie na tej podstawie podejmować względem osoby decyzje wywołujące wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływające wyłącznie jeżeli decyzja ta jest niezbędna do zawarcia lub wykonania umowy między osobą, które dane dotyczą a PRPW lub decyzja opiera się na wyraźnej zgodzie osoby, której dane dotyczą.
2. PRPW zapewnia osobie, która podlega decyzji wydanej w przypadku wskazanym w ust. 1 niniejszego paragrafu, prawo do:
    a) uzyskania interwencji ludzkiej ze strony Izby,
    b) wyrażenia własnego stanowiska,
    c) zakwestionowania tej decyzji.
3. Realizacja uprawnień, o których mowa w ust. 2 niniejszego paragrafu, może nastąpić w dowolnej formie, w szczególności w formie elektronicznej.

§ 24

[Prywatność]

1. PRPW chroni prywatność osób, których dane dotyczą na każdym etapie procesu przetwarzania danych osobowych, począwszy od fazy projektowania przedsięwzięcia łączącego się z przetwarzaniem danych osobowych, poprzez jego realizację aż do jego zakończenia. W tym celu PRPW zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania stosuje adekwatne środki zapewniające realizację zasad przetwarzania danych wskazanych w art. 5 RODO (privacy by design).
2. PRPW wdrożyła środki techniczne i organizacyjne w celu osiągnięcia minimalizacji danych (privacy by default). Zasada minimalizacji uwzględniana jest w odniesieniu do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności.
3. PRPW weryfikuje, przynajmniej raz w roku, zakres i ilość pozyskiwanych danych osobowych, oraz ilość i zakres przetwarzanych danych by ilość pozyskanych oraz zakres ich przetwarzanych był adekwatny do celu przetwarzania.
4. PRPW wprowadza organizacyjne i fizyczne środki zabezpieczające dostęp do danych osobowych oraz stale kontroluje dostęp do tych danych w celu zapewnienia by dostępu do danych nie miały osoby nieuprawnione.
5. PRPW monitoruje przydatność danych osobowych dla celów przetwarzania w celu realizacji zasady wskazanej w art. 5 ust. 1 lit e) RODO.

§ 25

[Analiza ryzyka i ocena skutków przetwarzania]

1. PRPW przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych jeżeli planowany rodzaj przetwarzania z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.
2. W celu dokonania oceny skutków, o której mowa w ust. 1 niniejszego paragrafu PRPW dokonuje analizy ryzyka.
3. PRPW dokonała identyfikacji procesów przetwarzania danych osobowych a także dokonała identyfikacji swoich aktywów rozumianych jako środki materialne i niematerialne (zasoby ludzkie, systemy informatyczne, sprzęt, programy komputerowe) mające wpływ na przetwarzanie danych osobowych oraz zidentyfikowała przetwarzane przez siebie dane osobowe, które ujęte zostały w wykazie zbiorów danych osobowych, którego wzór stanowi załącznik numer 7 do Polityki będący jej integralną częścią.
4. PRPW dokonało analizy ryzyka w sposób wskazany w załączniku numer 8 będącym jej integralną częścią.
5. W celu możliwości przypisania odpowiedzialności konkretnemu właścicielowi aktywów PRPW ustaliło jakie osoby odpowiedzialne są za konkretne procesy przetwarzania konkretnych danych osobowych (właścicieli aktywów).
6. PRPW zidentyfikowało cel przetwarzania danych oraz odpowiednią do tego celu podstawę prawną przetwarzania danych.
7. PRPW zidentyfikowało źródła i sposób pozyskiwania danych oraz przepływy danych w czasie ich przetwarzania.

XIII. POSTANOWIENIA KOŃCOWE

§ 26

1. Zmiany niniejszej Polityki mogą być dokonywane jedynie przez Administratora.

2. Wszelkie zmiany niniejszej Polityki wymagają zachowania formy pisemnej.
3. Zasady bezpieczeństwa dotyczące danych osobowych przetwarzanych w Systemie informatycznym lub zapisanych na elektronicznych nośnikach określone zostały szczegółowo w Instrukcji. Polityka Bezpieczeństwa ma zastosowanie do danych osobowych przetwarzanych w Systemie informatycznym lub zapisanych na elektronicznych nośnikach w zakresie w jakim dane zagadnienia nie zostały uregulowane w Instrukcji.

Załączniki:

1. Załącznik nr 1 – wykaz podmiotów, którym administrator powierzył przetwarzanie danych osobowych,
2. załącznik nr 2 - wzór oświadczenia o zobowiązaniu do przestrzegania postanowień Polityki i Instrukcji, oraz do zachowania w poufności wszystkich informacji dotyczących danych osobowych przetwarzanych w PRPW oraz sposobach ich zabezpieczenia,
3. załącznik nr 3 - wzór upoważnienia do przetwarzania danych osobowych w PRPW dla osób zatrudnionych na podstawie umowy o pracę,
4. załącznik nr 4 - wzór ewidencji osób upoważnionych do przetwarzania danych osobowych w Izbie,
5. załącznik nr 5 - wzór umowy powierzenia przetwarzania danych osobowych,
6. załącznik nr 6 - wzór protokołu z czynności kontrolnych,
7. załącznik nr 7 - wzór wykazu zbiorów danych osobowych przetwarzanych przez PRPW,
8. załącznik nr 8 - sposób analizy ryzyka.
9. załącznik nr 9 - Instrukcja

Poznań, dnia 01.06.2018

.....