Polityka Ochrony Danych

Fundacja Panda Team im. Michałka Tarachowicza

os. Bolesława Śmiałego 38/26

60-682 Poznań

Data wejścia w życie: 3.12.2021

1. Postanowienia ogólne

Polityka ochrony danych odnosi się do danych osobowych przetwarzanych
przez Fundację Panda Team im. Michałka Tarachowicza z siedzibą os. Bolesława Śmiałego 38/26 60-682 Poznań (dalej jako „Fundacja") na podstawie przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U.UE.L.2016.119.1).

W niniejszej Polityce ustanowione zostają procedury wewnętrzne chroniące dane osób fizycznych, przetwarzane w Fundacji.

Polityka ochrony danych w szczególności określa:

a) obowiązki Administratora danych;

b) tryb nadawania upoważnień do przetwarzania danych osobowych;

c) zasady realizacji praw osób, których dane dotyczą;

a) instrukcję postępowania w sytuacji wystąpienia incydentu bezpieczeństwa/naruszenia ochrony danych osobowych;

b) środki techniczne oraz organizacyjne służące ochronie danych osobowych przed ich naruszeniem.

2. Administrator danych

Administrator danych jest odpowiedzialny za przestrzeganie zasad, o których mowa w RODO oraz musi być w stanie wykazać ich przestrzeganie („rozliczalność").

Administrator danych realizuje obowiązki wynikające z przepisów o ochronie danych osobowych, w szczególności:

a) uwzględniając 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, wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku; środki te są w razie potrzeby poddawane przeglądom i na bieżąco uaktualniane;

b) spełnia obowiązki informacyjne, o których mowa w art. 13 i 14 RODO;

c) zapewnia realizację praw, których dane dotyczą w myśl przepisów rozdziału III RODO;

d) przestrzega obowiązków związanych z wystąpieniem naruszenia ochrony danych określonych w art. 33 i 34 RODO;

e) prowadzi w formie elektronicznej rejestr czynności przetwarzania/rejestr kategorii czynności przetwarzania, o których mowa w art. 30 RODO;

f) upoważnia pracowników do przetwarzania danych osobowych w zakresie zgodnym z ich obowiązkami służbowymi oraz wyłącznie na polecenie AD, a także zobowiązuje ich do zachowania
w tajemnicy przetwarzanych danych osobowych oraz zastosowanych środków technicznych

i organizacyjnych zapewniających odpowiedni poziom bezpieczeństwa danych w trakcie trwania zatrudnienia oraz po jego ustaniu, a także do zapewnienia bezpieczeństwa danych osobowych;

g) zawiera, gdy to konieczne, umowy powierzenia przetwarzania danych osobowych na zasadach określonych w art. 28 RODO;

h) analizuje zasadność wyznaczenia Inspektora ochrony danych oraz w razie potrzeby go wyznacza;

i) dokonuje oceny ryzyka naruszenia praw lub wolności osób fizycznych przed przystąpieniem do przetwarzania danych osobowych lub w przypadku planowanej zmiany zakresu i sposób przetwarzania, a w razie konieczności również oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, o której mowa w art. 35 RODO;

j) uwzględnia zasadę prywatności, w fazie projektowania (privacy by design) oraz domyślnej ochrony danych (privacy by default);

k) zapewnia pracownikom wprowadzające oraz cykliczne szkolenia z zakresu przepisów o ochronie danych osobowych oraz środków zapewniających bezpieczeństwo przetwarzania danych osobowych (co najmniej raz na 2 lata);

l) przeprowadza przynajmniej raz do roku przegląd, a w razie potrzeby również aktualizację wprowadzonych regulacji wewnętrznych oraz zastosowanych środków technicznych i organizacyjnych.

3. Inspektor ochrony danych

Na Administratorze danych spoczywa obowiązek analizy czy przetwarzanie danych osobowych w Fundacji powoduje konieczność wyznaczenia Inspektora ochrony danych, w myśl art. 37 ust. 1 RODO.

Administrator danych zapewnia by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.

Administrator danych wspiera IOD w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.

Administrator danych zapewnia, aby IOD nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez Administratora danych za wypełnianie swoich zadań.

IOD bezpośrednio podlega Administratorowi danych.

Osoby, których dane dotyczą, mogą kontaktować się z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw.

IOD zobowiązany jest do zachowania w poufności informacji dotyczących wykonywania swoich zadań.

Zakres zadań IOD określa RODO.

4. Podstawy prawne przetwarzania

Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy - i w takim zakresie, w jakim - spełniony jest co najmniej jeden z warunków określonych w art. 6,9,10 RODO.

Jeżeli przetwarzanie danych osobowych w myśl przepisów RODO odbywa się na podstawie zgody, Administrator danych musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych. Zgoda winna być:

- dobrowolna, konkretna, świadoma i jednoznaczna;

- zrozumiała i łatwo dostępna;

- odwoływalna w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

Treść przykładowej zgody stanowi załącznik nr 1 do Polityki ochrony danych.

5. Upoważnienie do przetwarzania danych osobowych

Pracownicy przetwarzają dane osobowe wyłącznie na polecenie Administratora danych, zgodnie z zakresem upoważnienia i w celu realizacji obowiązków służbowych.

Do przetwarzania danych osobowych w imieniu Administratora danych mogą być dopuszczone wyłącznie osoby posiadające imienne upoważnienie do przetwarzania danych osobowych wydane przez Administratora danych.

Każda osoba działająca z upoważnienia Administratora danych i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie Administratora danych, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego

Wzór upoważnienia stanowi załącznik nr 2 do Polityki ochrony danych.

Jeden egzemplarz upoważnienia otrzymuje pracownik, drugi jest przekazywany do akt osobowych pracownika, a trzeci jest dołączany do rejestru upoważnień.

Odwołanie lub zmiana upoważnienia do przetwarzania danych osobowych pracownikowi odbywa się w formie przewidzianej powyżej.

Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych w Fundacji stanowi załącznik nr 3 do Polityki ochrony danych.

Do podstawowych obowiązków pracowników upoważnionych do przetwarzania danych osobowych należy zwłaszcza:

a) przestrzeganie przepisów o ochronie danych osobowych;

b) zachowanie szczególnej staranności przy przetwarzaniu danych osobowych w celu ochrony interesów osób, których dane dotyczą;

c) zabezpieczanie danych osobowych przed ich naruszeniem;

d) podporządkowanie się poleceniom Administratora danych w zakresie ochrony danych osobowych;

e) niezwłoczne zgłaszanie Administratorowi danych incydentów bezpieczeństwa/naruszeń ochrony danych osobowych;

f) zachowania w tajemnicy przetwarzanych danych osobowych oraz sposobów ich zabezpieczania;

g) stosowania określonych przez Administratora danych procedur, środków technicznych, organizacyjnych mających na celu ochronę danych osobowych;

h) udział w szkoleniach dotyczących ochrony danych osobowych.

6. Rejestry

Administrator danych prowadzi w formie elektronicznej, na podstawie przepisów RODO, rejestr czynności przetwarzania danych osobowych, za które odpowiada, a w razie potrzeby również rejestr kategorii czynności przetwarzania dokonywanych w imieniu administratora danych.

Rejestry są prowadzone w formie elektronicznej.

Zakres rejestrów określają przepisy RODO.

7. Obowiązek informacyjny

Zasady spełnienia obowiązku informacyjnego określają przepisy o ochronie danych osobowych.

Wzory klauzul informacyjnych, z uwzględnieniem celu przetwarzania, opracowuje Administrator danych, który jest zobowiązany do ich przekazania pracownikom upoważnionym do przetwarzania danych osobowych ze wskazaniem formy, w jakiej obowiązek informacyjny winien zostać spełniony. Pracownicy są zobowiązani do ich stosowania w toku podejmowanych czynności służbowych, z uwzględnieniem obowiązujących przepisów.

Wzory klauzul informacyjnych podlegają cyklicznemu przeglądowi oraz aktualizacji.

8. Prawa osób, których dane dotyczą

Realizacja praw osób, których dotyczą odbywa się na zasadach określonych w przepisach o ochronie danych osobowych.

Każdy przypadek zgłoszenia przez osobę, której dane dotyczą, woli skorzystania z praw przewidzianych w RODO, Administrator danych rozpatruje indywidualnie.

Pracownicy mają obowiązek niezwłocznego przekazywania do Administratora danych wniosków o realizację praw osób, których dane dotyczą.

Prawo do realizacji uprawnień wynikających z RODO, nie może niekorzystnie wpływać na prawa i wolności innych osób.

Realizacja praw osób, których dane dotyczą następuje na podstawie uprzednio złożonego wniosku w dowolnej formie.

Wszelkie wnioski o realizację praw osób, których dane dotyczą wraz z informacją o sposobie ich rozstrzygnięcia są odnotowywane w rejestrze, którego wzór stanowi załącznik nr 4 do Polityki ochrony danych.

9. Podmiot przetwarzający

Jeżeli przetwarzanie ma być dokonywane w imieniu Administratora danych, korzysta on wyłącznie
z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

Skorzystanie z usług podmiotu przetwarzającego jest poprzedzone zawarciem umowy powierzenia przetwarzania danych osobowych, zgodnie z wymaganiami zawartymi w art. 28 RODO.

Za opracowanie projektu umowy powierzenia przetwarzania danych osobowych, odpowiada Administrator danych.

Wzór rejestru zawartych umów powierzenia przetwarzania danych stanowi załącznik nr 5 do Polityki ochrony danych.

10. Zarządzanie ryzykiem

Administrator danych, przed rozpoczęciem przetwarzania danych osobowych w nowym procesie, przeprowadza analizę ryzyka oraz uwzględnia prawa i wolności osób, których dane dotyczą, na każdym kluczowym etapie jego projektowania i wdrażania nowego procesu przetwarzania danych osobowych.

Analiza ryzyka jest przeprowadzana również w przypadku istotnej zmiany w tym zakresie np. zmiany dostawcy usług, zmiany sposobu przetwarzania danych, rozszerzenia zakresu geograficznego, wymiany zasobów biorących udział w procesie.

Analiza ryzyka jest poddawana przeglądowi nie rzadziej niż raz w roku oraz w razie potrzeby aktualizowana.

Analizę ryzyka przeprowadza się zwłaszcza z uwzględnieniem:

1) prawdopodobieństwa wystąpienia określonego zdarzenia będącego naruszeniem, oraz

2) powagi tego zdarzenia, tj. wielkości szkody, jakie zdarzenie to może spowodować w odniesieniu do osoby, której dane dotyczą.

W wyniku oszacowania ryzyka stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko, z którym wiąże się obowiązek przeprowadzania oceny skutków dla ochrony danych (DPIA), o której mowa w przepisach RODO.

Na podstawie wyników przeprowadzonej analizy ryzyka, Administrator danych wdraża sposoby postępowania z ryzykiem.

Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator danych przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych (DPIA). Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

Ocena ryzyka jest dokumentowana w formie elektronicznej.

11. Środki organizacyjne i techniczne ochrony przetwarzanych danych osobowych

Dane osobowe w Fundacji są przetwarzane w formie:

a) tradycyjnej – papierowej;

b) informatycznej – na nośnikach danych (przenośne komputery - laptopy).

Podstawowe środki organizacyjne ochrony przetwarzanych danych osobowych:

1) wiedzy koniecznej (ograniczonego dostępu do informacji) – pracownicy posiadają dostęp tylko do tych informacji, które są konieczne do realizacji powierzonych im zadań;

2) indywidualnej odpowiedzialności – za utrzymanie odpowiedniego poziomu bezpieczeństwa danych osobowych odpowiadają konkretne osoby, w zakresie nałożonych obowiązków i nadanych uprawnień;

3) niewygody uzasadnionej – bezpieczeństwo danych osobowych co do zasady opiera się na ograniczeniach oraz jest niewygodne;

4) czystego biurka i czystego ekranu:

a) pod nieobecność pracownika na stanowisku pracy dokumenty winny być zabezpieczone przed dostępem osób nieupoważnionych w meblach biurowych, w przeznaczonych do tego pomieszczeniach itp.,

b) na czas nieobecności pracownika dostęp do komputera jest blokowany, a po zakończeniu pracy komputer jest wyłączany, chyba że dany komputer musi pracować w trybie ciągłym; w czasie obecności pracownika monitor powinien być tak ustawiony, aby nie pozwalał na zapoznawanie się z wyświetlanymi treściami przez osoby postronne, nieupoważnione;

5) dyskrecji (ograniczonego zaufania i odpowiedzialnej konwersacji) – wszelkie informacje służbowe mogą być przekazywane wyłącznie w celu wykonywania zadań w zakresie do tego niezbędnym oraz osobom uprawnionym do pozyskania tych informacji;

6) obecności koniecznej – prawo przebywania w określonych miejscach (istotnych dla bezpieczeństwa danych osobowych) mogą mieć tylko osoby upoważnione; przebywanie osób nieupoważnionych w tych miejscach jest możliwe wyłącznie w obecności osób upoważnionych;

7) zamykania pomieszczeń – niedopuszczalne jest pozostawienie pod nieobecność pracownika niezabezpieczonego pomieszczenia służbowego, zarówno w godzinach pracy, jak i po jej zakończeniu; na zakończenie dnia pracy ostatnia wychodząca z pomieszczenia osoba jest zobowiązana zamknąć wszystkie okna i drzwi oraz zabezpieczyć klucze do pomieszczenia;

8) nadzorowania dokumentów – po godzinach pracy wszystkie dokumenty zawierające dane osobowe należy przechowywać w miejscach zabezpieczonych przed dostępem osób nieuprawnionych;

9) zachowania prywatności kont w systemach – każdy użytkownik zobowiązany jest do pracy w systemach informatycznych na przypisanych lub udostępnionych mu kontach; zabronione jest udostępnianie własnych kont osobom trzecim;

10) poufności informacji uwierzytelniających – każdy użytkownik zobowiązany jest do zachowania poufności udostępnionych mu haseł, kodów dostępu, w szczególności do systemów informatycznych;

11) legalnego oprogramowania – na stacjach roboczych zainstalowane jest wyłącznie legalne oprogramowanie; oprogramowanie powinno posiadać możliwość automatycznej aktualizacji bez dodatkowych działań ze strony użytkownika;

12) automatyzacji kopii zapasowych – procesy tworzenia kopii zapasowych powinny być odpowiednio zaplanowane z uwzględnieniem wymogów prawnych i potrzeb Fundacji, jak również powinny być zautomatyzowane oraz niemożliwe do przerwania;

13) ochrony nośników danych – nośniki dane użytkowane dla celów służbowych wynoszone poza pomieszczenia użytkowane przez Fundację powinny być odpowiednio zabezpieczone w czasie transportu i przechowywania, co najmniej poprzez szyfrowanie; nie dopuszcza się użytkowania przez pracowników nieautoryzowanych zewnętrznych pamięci danych (np. pendrive, drukarki itd.);

14) przetwarzania w siedzibie Fundacji - przetwarzanie danych osobowych zarówno w formie papierowej jak i elektronicznej poza siedzibą Fundacji winno mieć charakter wyjątkowy; jest ono możliwe wyłącznie gdy służy wyłącznie celom służbowym i nie da się zrealizować tego celu w inny sposób, odbywa się za pomocą przypisanego pracownikowi narzędzia służbowego jakim jest komputer przenośny; w formie zapewniającej odpowiedni poziom bezpieczeństwa danych osobowych; jest ograniczone czasowo i trwa do czasu ustania celu jakim jest realizacja konkretnego zadania służbowego;

15) bezpiecznej współpracy z podmiotami zewnętrznymi – gdy wymaga tego przedmiot lub specyfika umowy z podmiotami zewnętrznymi zawiera się umowę powierzenia przetwarzania danych osobowych spełniającą wymogi przepisów RODO;

16) doskonalenia – dobór środków bezpieczeństwa jest dostosowywany do zmieniających się warunków wewnętrznych i zewnętrznych;

17) czystego kosza – dokumenty papierowe zawierające dane osobowe są niszczone w sposób uniemożliwiający ich odczytanie; niedopuszczalne jest wyrzucanie dokumentów zawierających dane osobowe do zwykłego kosza; w celu zniszczenia takich dokumentów należy korzystać z udostępnionych niszczarek; niszczenie elektronicznych nośników danych odbywa się poprzez zlecenie tego wykwalifikowanej firmie zewnętrznej;

18) praktyka odbioru wydruków z drukarki – wszelkie wydruki zawierające dane osobowe zabierane są natychmiast z drukarki po zakończeniu drukowania; za każdym razem należy sprawdzić czy wszystkie strony zostały wydrukowane i czy nie pozostał jakiś wydruk na drukarce; w przypadku wykonywania kserokopii należy zawsze pamiętać o zabraniu dokumentu, z którego wykonywano kserokopię z tzw. szyby ksera.

Podstawowe środki techniczne ochrony przetwarzanych danych osobowych:

- każdemu z użytkowników systemu informatycznego ustala się identyfikator i hasło dostępu, jak również uprawnienia do poszczególnych funkcji systemu informatycznego określone według zakresu obowiązków pracownika;

- przed rozpoczęciem pracy użytkownik zobowiązany jest do sprawdzenia stanu stacji komputerowej; w szczególności uszkodzeń lub ingerencji osób trzecich;

- rozpoczynając pracę na komputerze użytkownik wprowadza wszystkie wymagane identyfikatory i hasła w sposób uniemożliwiający ich ujawnienie innym osobom;

- w przypadku przerwy w korzystaniu z systemu informatycznego użytkownik zobowiązany jest zawiesić pracę w systemie poprzez zablokowanie konta użytkownika, wylogowanie się z systemu informatycznego lub w inny sposób zablokowanie stacji roboczej;

- w przypadku braku aktywności użytkownika w systemie informatycznym trwającej dłużej niż 15 minut automatycznie włącza się wygaszacz ekranowy; ponowny dostęp do systemu informatycznego następuje po poprawnym uwierzytelnieniu;

- hasło do komputera musi składać się z co najmniej 11 znaków, zawierać duże i małe litery, cyfry i co najmniej jeden znak specjalny; konto użytkownika jest blokowane w przypadku trzech nieudanych prób dostępu; hasło i login nie może być zapisywane lub przechowywane w miejscu dostępnym dla osób niepowołanych; hasło dostępu zmienia się raz na miesiąc; użytkownik zmienia hasło w przypadku kompromitacji hasła;

- nośniki informatyczne zawierające dane osobowe, a przeznaczone do likwidacji, naprawy lub przekazania podmiotowi nieuprawnionemu do otrzymania danych, przed oddaniem są pozbawiane zapisu;

- zabrania się wykorzystywania systemów informatycznych do celów niezgodnych z przeznaczeniem;

- zabrania się dokonywania przez pracowników samodzielnej kopii danych osobowych;

- kopie bezpieczeństwa wykonuje się regularnie w celu zachowania ich aktualności; kopie bezpieczeństwa przechowuje się poza siedzibą Fundacji w zabezpieczonych lokalizacjach;

- na każdej stacji komputerowej na której przetwarzane są dane osobowe stosuje się aktywną ochronę antywirusową, działającą w czasie rzeczywistym; aktualizacja programu antywirusowego przeprowadzana jest codziennie, automatycznie bez udziału użytkownika;

- w celu ochrony dostępu do danych komputera z sieci publicznej wykorzystuje się rozwiązania typu Firewall;

- stosowane zabezpieczenia systemu informatycznego są regularnie testowane oraz w razie potrzeby ulepszane;

- prace dotyczące przeglądów, konserwacji i napraw wymagające zaangażowania autoryzowanych firm zewnętrznych, są wykonywane pod nadzorem Administratora danych, bez możliwości dostępu do danych osobowych.

12. Naruszenia ochrony danych osobowych

Administrator danych określił poniżej katalog zdefiniowanych incydentów bezpieczeństwa.

a) Do typowych zagrożeń bezpieczeństwa danych osobowych zaliczamy:

- niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;

- niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą lub utratą danych osobowych;

- nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, brak ochrony haseł, niezamykanie pomieszczeń, szaf, biurek, okien, wyrzucanie niezniszczonych/niezanonimizowanych dokumentów zawierających dane osobowe).

b) Do typowych incydentów bezpieczeństwa danych osobowych należą:

- zdarzenia losowe zewnętrzne (pożar, powódź, utrata zasilania, utrata łączności);zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki użytkowników, utrata lub zagubienie danych);

- umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów, działanie wirusów i innego szkodliwego oprogramowania).

Rodzaje zagrożeń naruszających ochronę danych osobowych:

Zagrożenia losowe:

a) zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu) - ich wystąpienie może prowadzić do utraty integralności danych, ich zniszczenia lub uszkodzenia infrastruktury technicznej systemu. Ciągłość systemu zostaje zakłócona, jednak nie dochodzi do naruszenia poufności danych;

b) zagrożenia wewnętrzne (np. niezamierzone pomyłki użytkowników, awarie sprzętowe, błędy oprogramowania) – w wyniku ich wystąpienia może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych;

Zagrożenia zamierzone: świadome i celowe naruszenia poufności danych – w wyniku ich wystąpienia zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy. W ramach tej kategorii wyróżnia się:

c) nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu);

d) nieuprawniony dostęp do systemu z jego wnętrza;

e) nieuprawnione przekazanie danych,

f) bezpośrednie zagrożenie materialnych składników systemu (np. kradzież sprzętu, dokumentów).

Okoliczności zakwalifikowane jako incydent bezpieczeństwa, w którym przetwarzane są dane osobowe, to w szczególności:

a) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu (np. pożar, zalanie pomieszczeń, katastrofa budowlana, napad czy działania terrorystyczne, niewłaściwa ingerencja ekipy remontowej);

b) niewłaściwe parametry środowiska, nadmierna wilgotność, skrajnie niekorzystna temperatura, oddziaływanie pola elektromagnetycznego, wibracje pochodzące od pracujących agregatów czy urządzeń przemysłowych;

c) awarie sprzętu lub oprogramowania, które wyraźnie wskazują na naruszenia ochrony danych osobowych;

d) pojawienie się komunikatu alarmowego od części systemu, która zapewnia ochronę zasobów systemu lub inny komunikat o podobnym znaczeniu;

e) pogorszenie jakości danych w systemie informatycznym lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;

f) naruszenie lub próba naruszenia integralności systemu informatycznego lub bazy danych osobowych w tym systemie;

g) modyfikacja danych osobowych lub zmiana w strukturze danych bez odpowiedniego upoważnienia;

h) ujawnienie osobom nieuprawnionym danych osobowych lub objętych tajemnicą procedur ochrony lub przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń;

i) praca w systemie informatycznym, wskazująca nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych (praca na stanowisku osoby, która formalnie nie była dopuszczona do obsługi komputera, sygnał o uporczywym nieautoryzowanym logowaniu);

j) podmienienie lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub skasowanie bądź skopiowanie niedozwolonych danych osobowych;

k) rażące naruszenie obowiązków w zakresie przestrzegania procedur bezpieczeństwa informacji, jak np. niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce lub kserokopiarce, niezamknięcia pomieszczenia z komputerem, niewykonanie w określonym terminie kopii zapasowych;

i) stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych, znajdujących się na dyskach, pamięciach flash, oraz wydrukach komputerowych w formie niezabezpieczonej (otwarte szafy, biurka, regały, urządzenia archiwalne i inne).

Biorąc pod uwagę standardy bezpieczeństwa teleinformatycznego podstawowe zagrożenia dla danych osobowych przetwarzanych w systemach informatycznych to utrata: poufności, dostępności, integralności, oraz rozliczalności.

Poufność - to zapewnienie, aby tylko uprawniona osoba posiadała dostęp do danych osobowych w zakresie wymaganym realizowanymi zadaniami. W związku z tym zagrożenia w zakresie poufności obejmują:

a) nieuprawniony dostęp do obszarów i pomieszczeń, w których zlokalizowane są zasoby systemu informatycznego służącego do przetwarzania danych osobowych;

b) ujawnienie haseł dostępu do systemu informatycznego;

c) nieuprawnione udostępnienie informacji przez osobę uzyskującą dostęp do danych osobowych systemu informatycznego;

d) nieuprawnione przeniesienie informacji na nośnik danych;

e) utrata nośnika danych zawierającego dane osobowe;

f) podszycie przez nieuprawnioną osobę pod posiadającego uprawnienia użytkownika systemu informatycznego;

Dostępność - to zapewnienie, aby użytkownik systemu informatycznego posiadał możliwość pracy na stanowisku komputerowym zgodnie z założonymi wymaganiami ochrony danych osobowych. Zagrożenia oraz procedury postępowania w tym zakresie obejmują przypadki postępowania w takich przypadkach jak:

a) brak możliwości przetwarzania danych osobowych spowodowany brakiem dostępu do pomieszczeń, w których zainstalowane są zasoby systemu informatycznego;

b) awaria sprzętu lub systemu informatycznego;

c) zakłócenia w zasilaniu systemu informatycznego;

d) brak dostępu do haseł systemu informatycznego;

e) klęska żywiołowa;

Integralność - to zapewnienie, aby wszelkie operacje wykonywane na danych osobowych przetwarzanych w systemie informatycznym były skutkiem świadomych i zaplanowanych działań użytkowników systemu. Zagrożenia oraz procedury postępowania w tym zakresie obejmują przypadki postępowania w takich przypadkach jak:

a) brak kontroli nad operacjami wykonywanymi na danych osobowych przez użytkowników systemów informatycznych;

b) nieuprawnione przetwarzanie danych osobowych;

c) nieuprawniony dostęp do danych osobowych;

d) błędy sprzętu i systemu informatycznego;

Rozliczalność – to zapewnienie aby czynności wykonywane przez użytkowników systemów informatycznych były rejestrowane w celu uniemożliwienia wyparcia się przez osoby wykonujące czynności na danych osobowych. Zagrożenia oraz procedury postępowania w tym zakresie obejmują przypadki postępowania w takich przypadkach jak:

a) brak kontroli nad czynnościami wykonywanymi w systemie informatycznym służącym do przetwarzania danych osobowych;

b) nieaktualne listy osób uprawnionych do przetwarzania danych osobowych w systemie informatycznym;

c) brak poufności haseł dostępu do systemu informatycznego;

d) brak ochrony fizycznej krytycznych elementów systemów informatycznych;

e) braki w dokumentacji eksploatacyjnej systemu, w tym dokumentowania zmian systemu.

Autentyczność – zapewnieniu, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji);

Niezaprzeczalność – braku możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie;

Niezawodność – zapewnieniu spójności oraz zamierzonych zachowań i skutków;

Przestrzeganie powyższych atrybutów bezpieczeństwa danych osobowych zapewnia ochronę przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, zmianą, utratą, uszkodzeniem lub zniszczeniem oraz przetwarzaniem niezgodnym z zapisami prawa.

Każdy kto przetwarza dane osobowe na polecenie Administratora danych jest odpowiedzialny za bezpieczeństwo tych danych.

Incydenty bezpieczeństwa nie zakwalifikowane jako naruszenie ochrony danych osobowych ewidencjonuje się w rejestrze incydentów, którego wzór stanowi załącznik nr 6 do Polityki ochrony danych.

W przypadku stwierdzenia naruszenia ochrony danych osobowych, Administrator danych osobiście
lub upoważniona przez niego osoba, nie później niż w terminie 72 godzin po stwierdzeniu

naruszenia – zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Oceny czy naruszenie wymaga notyfikacji dokonuje Administrator danych. Przy analizie konieczności dokonania zgłoszenia naruszenia ochrony danych należy wziąć
w szczególności pod uwagę okoliczności naruszenia, w tym fakt, czy dane osobowe były zabezpieczone odpowiednimi technicznymi środkami ochrony skutecznie ograniczającymi prawdopodobieństwo oszustwa dotyczącego tożsamości lub innych form nadużycia oraz uwzględnić prawnie uzasadnione interesy organów ścigania, jeżeli przedwczesne ujawnienie mogłoby niepotrzebnie utrudnić badanie okoliczności naruszenia ochrony danych osobowych.

Zgłoszenia naruszenia ochrony danych dokonuje się zgodnie z trybem określonym przez organ nadzorczy.

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych Administrator danych osobiście lub przez upoważnioną przez niego osobę, bez zbędnej zwłoki zawiadamia osoby, których dane dotyczą, jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Oceny prawdopodobieństwa naruszenia praw lub wolności osób fizycznych oraz doboru sposobu zawiadomienia osób, których dane dotyczą, dokonuje Administrator danych.

Wszelkie naruszenia ochrony danych osobowych odnotowuje się w formie rejestru naruszeń, którego wzór stanowi załącznik nr 7 do Polityki Ochrony Danych.

Każdy zaistniały incydent bezpieczeństwa musi stać się przedmiotem szczegółowej analizy, która powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych wniosków co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, aby w przyszłości zapobiec podobnym naruszeniom w przyszłości.

13. Odpowiedzialność za nieprzestrzeganie zasad ochrony danych osobowych

Nieprzestrzeganie przepisów o ochronie danych osobowych oraz zasad określonych w niniejszej Polityce może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych i stanowić podstawę do wszczęcia postępowania dyscyplinarnego lub porządkowego na zasadach określonych
w przepisach szczególnych.

W zakresie określonym powyżej, pracownicy podlegają również odpowiednio odpowiedzialności, o której mowa w przepisach RODO oraz innych przepisach prawa powszechnie obowiązującego.

Wobec osób winnych dopuszczenia do uchybień, oprócz postępowania dyscyplinarnego, może być wszczęte inne postępowanie przewidziane prawem np. możliwość wniesienia wobec tej osoby sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

WYKAZ ZAŁĄCZNIKÓW:

Załącznik nr 1 – Zgoda na przetwarzanie danych osobowych

Załącznik nr 2 - Upoważnienie do przetwarzania danych osobowych wydane na podstawie przepisów RODO

Załącznik 3 –Ewidencja osób upoważnionych na podstawie przepisów RODO

Załącznik 4 – Rejestr realizacji praw osób, których dane dotyczą na podstawie przepisów RODO

Załącznik nr 5 – Ewidencja umów powierzenia przetwarzania danych osobowych zawartych na postawie przepisów RODO

Załącznik nr 6 – Rejestr incydentów bezpieczeństwa niezakwalifikowanych jako naruszenie ochrony danych osobowych

Załącznik nr 7 – Rejestr naruszeń ochrony danych osobowych.