POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

opracowała: Natalia Jagodzińska

zatwierdziła: Mariola Ciesielska

data: 25.05.2018 r.

Spis treści

Rozdział 1 Wstęp

Celem niniejszego opracowania jest wprowadzenie ochrony przed wszelakiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub w odniesieniu do zasobów informacji oraz danych osobowych na zgodność z rozporządzeniem 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 (w skrócie RODO) poprzez odpowiednie określenie wartości zasobów informacji, zrozumienie ich wrażliwości oraz wskazanie zagrożenia, które mogą narazić te zasoby na ryzyko.

Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

1. poufność danych - rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
2. integralność danych - rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
3. rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
4. integralność systemu rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.
5. dostępność rozumianą jako właściwość zapewniającą, że informacje/dane osobowe są dostępne uprawnionym osobom.
6. dostępność systemu rozumianą jako możliwość korzystania z systemu w określony sposób przez uprawnione osoby.

Ilekroć w dokumencie jest mowa o:

1) **rozporządzeniu** – rozumie się przez to rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
2) **danych osobowych** – rozumie się przez to 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;
3) **zbiorze danych** – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

4) **przetwarzaniu danych** – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich 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;
5) **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, polityk, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
6) **zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
7) **usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
8) **administratorze danych** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;
9) **zgodzie osoby, której dane dotyczą** – oznacza to dobrowolne, konkretne, świadome i jednoznaczne okazanie woli osoby, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwalając w ten sposób na przetwarzanie dotyczących jej danych osobowych;
10) **odbiorcy danych** – rozumie się przez to 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;
11) **państwie trzecim** – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego;
12) **środkach technicznych i organizacyjnych** – należy przez to rozumieć środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych;
13) **ograniczeniu przetwarzania** – należy przez to rozumieć oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
14) **profilowaniu** – oznacza to dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej

osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

15) **pseudonimizacji** – oznacza to przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
16) **podmiocie przetwarzającym** – oznacza to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora – Procesor.
17) **naruszeniu ochrony danych osobowych** – oznacza to 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

Rozdział 2 Administrator danych

Administrator danych uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

Administrator danych ze względu na charakter prowadzonej działalności nie jest zobligowany do wyznaczenia Inspektora Ochrony Danych.

Administrator identyfikuje procesy przetwarzania danych osobowych oraz sporządza inwentaryzację zasobów dla tychże procesów opracowując *F 01 PBD Lista procesów przetwarzania* oraz *F 02 PBD Inwentaryzacja zasobów*.

W ramach realizacji działania należy zidentyfikować i zinwentaryzować:

- procesy, w których przetwarzane są dane osobowe;
- zasoby wykorzystywane do realizacji zidentyfikowanych procesów, w szczególności systemy IT;
- podmioty, którym powierzono przetwarzanie dane (procesorzy);
- odbiorców danych, którym ujawnia się dane osobowe, niezależnie od tego, czy są stroną trzecią;
- cele przetwarzania danych osobowych w ramach każdego z zidentyfikowanych procesów;
- operacje przetwarzania w ramach każdego z zidentyfikowanych procesów;
- czas przetwarzania danych osobowych w ramach każdego z zidentyfikowanych procesów;
- właścicieli zidentyfikowanych procesów i zasobów.

Rozdział 3 Środki techniczne i organizacyjne

W celu ochrony danych spełniono wymogi, o których mowa w rozporządzeniu, w szczególności:

a) przeprowadzono analizę ryzyka w stosunku do zasobów biorących udział w poszczególnych procesach zgodnie *F 05 PBD Analiza ryzyka*,
b) zawarto umowy powierzenia przetwarzania;
c) została opracowana i wdrożona niniejsza polityka bezpieczeństwa.

W celu ochrony danych osobowych stosuje się następujące środki ochrony fizycznej danych osobowych:

a) zbiory danych osobowych przechowywane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi, a wejście do budynku, w którym się one znajdują zabezpieczona zamkiem na klucz, do którego dostęp mają wyłącznie osoby upoważnione;
b) pomieszczenia, w których przetwarzane są zbiory danych osobowych, zabezpieczone są przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy;
c) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone przez zastosowanie niszczarek dokumentów.

W celu ochrony danych osobowych stosuje się następujące środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej:

a) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
b) zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych;
c) zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł;
d) zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej;
e) zastosowano środki ochrony przed szkodliwym oprogramowaniem, takim jak np. robaki, wirusy, konie trojańskie, rootkity;
f) użyto system Firewall do ochrony dostępu do sieci komputerowej;

W celu ochrony danych osobowych stosuje się następujące środki ochrony w ramach narzędzi programowych i baz danych:

a) dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
b) zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych;
c) zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe;
d) zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

W celu ochrony danych osobowych stosuje się następujące środki organizacyjne:

a) właściciel odbył szkolenie w zakresie przepisów dotyczących ochrony danych osobowych oraz systemu informatycznego;
b) właściciel zobowiązuje się do przestrzegania zasad poufności i do zachowania danych w tajemnicy;

c) monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane;

Inne zabezpieczenia zostały wyszczególnione w *F 09 PBD Wykaz zabezpieczeń*.

Rozdział 4 Analiza ryzyka i plan postępowania z ryzykiem

Zarządzanie ryzykiem w ochronie danych osobowych jest procesem ciągłym, monitorującym adekwatność oraz skuteczność stosowanych zabezpieczeń organizacyjnych i technicznych, w celu utrzymania ryzyka na akceptowalnym poziomie. Analizę ryzyka dla zasobów biorących udział w procesach przeprowadza samodzielnie z wykorzystaniem *F 05 PBD Analiza ryzyka* osoba odpowiedzialna za proces wskazana przez administratora danych.
Analiza ryzyka jest przeprowadzana nie rzadziej niż raz w roku i stanowi podstawę do aktualizacji sposobu postępowania z ryzykiem. Na podstawie wyników przeprowadzonej analizy ryzyka, wskazane przez administratora danych osoby odpowiedzialne za proces lub administrator danych samodzielnie wdrażają sposoby postępowania z ryzykiem.
W ramach postępowania z ryzykiem należy dokonać wyboru wariantu postępowania z ryzykiem np.:

a) minimalizacja ryzyka - wdrożenie odpowiednich zabezpieczeń organizacyjnych i technicznych mających na celu minimalizację ryzyka do poziomu akceptowalnego oraz zapewnianie zgodności z RODO;
b) unikanie ryzyka - rezygnacja z realizacji działań lub warunków, które powodują powstanie określonych ryzyk;
c) transfer ryzyka - przeniesienie ryzyka na inny podmiot, który może skutecznie zarządzać ryzykiem;
d) akceptacja ryzyka - podjęcie przez administratora danych decyzji o zachowaniu ryzyka bez podejmowania dalszych działań. Decyzję tą administrator danych może podjąć tylko w przypadku wydania pozytywnej opinii przez organ nadzorujący przetwarzania danych osobowych.

W wyniku postępowania z ryzykiem właściciel procesu opracowuje plan postępowania z ryzykiem, który uwzględnia:

a) dane wejściowe do utworzenia planu postępowania z ryzykiem – informacje o kontekście przetwarzania danych, zidentyfikowanych ryzykach związanych z zapewnieniem adekwatnej niezbędności i proporcjonalności przetwarzania danych oraz zidentyfikowanych wysokich ryzykach dotyczących naruszenia praw lub wolności osób fizycznych;
b) wariant postępowania z ryzykiem - informacje, jaki wariant obsługi dla niezbędności i proporcjonalności przetwarzania oraz wysokich ryzykach naruszenia praw lub wolności osób fizycznych został przyjęty wraz z uzasadnieniem (w przypadku przyjęcia innego sposobu obsługi niż minimalizacja ryzyka);
c) opis planu działania – opis działań, jakie zostaną podjęte w celu minimalizacji ryzyka;
d) oczekiwany efekt – opis mechanizmów organizacyjnych lub/i technologicznych, jakie powstaną po realizacji planu postępowania;

e) mierniki oceny skuteczności realizacji planu postępowania – należy określić wskaźniki, na podstawie których będzie możliwość oceny skuteczności mechanizmów organizacyjnych lub/i technologicznych mających na celu minimalizację zidentyfikowanego ryzyka do poziomu akceptowalnego;

f) odpowiedzialność za realizację – informacja, kto (z imienia i nazwiska) będzie odpowiedzialny za realizację wskazanego planu postępowania;

g) termin realizacji – informacja, kiedy planowane jest zakończenie wdrożenia mechanizmów organizacyjnych lub/i technologicznych mających na celu minimalizację zidentyfikowanego ryzyka.

Każdorazowo administrator danych wybiera sposób postępowania z ryzykiem i określa, które ryzyka i w jakiej kolejności będą rozpatrywane jako pierwsze. Administrator danych nie może zlekceważyć krytycznych ryzyk, zgodnie z *F 05 PBD Analiza ryzyka.* W proces informowania o ryzyku i konsultacjach zaangażowane są wszystkie strony zainteresowane na każdym etapie procesu zarządzania ryzykiem ochrony danych osobowych.

Rozdział 5 Współpraca z podmiotami zewnętrznymi

PROCESOR - PODMIOT PRZETWARZAJĄCY - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora. Podmiot przetwarzający – procesor:

- jest zobowiązany do prowadzenia rejestru kategorii czynności przetwarzania;
- ma domyślny zakaz podpowierzania danych innym podmiotom (zatrudnienia innego podmiotu przetwarzającego - podprocesora) bez pisemnej zgody administratora;
- jest w pełni odpowiedzialny za działania zatrudnionego innego podmiotu przetwarzającego – podprocesora;
- nie może zmieniać celu przetwarzania danych zebranych przez administratora – jeśli zmieni cel przetwarzania automatycznie będzie za nie odpowiadał jako administrator;
- na żądanie organu nadzorczego współpracuje z nim w ramach wykonywanych przez niego zadań.

Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo UE lub prawo państwa członkowskiego.
Każdorazowe skorzystanie z usług podmiotu przetwarzającego jest poprzedzone zawarciem umowy powierzenia przetwarzania danych osobowych. Umowa powierzenia powinna zapewniać w szczególności, że podmiot przetwarzający:

- przetwarza dane tylko i wyłącznie na udokumentowane polecenie administratora,
- pomaga administratorowi wywiązać się z jego obowiązków,
- zapewnia, by osoby przetwarzające dane zachowały je w tajemnicy,
- po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa dane lub oddaje je administratorowi,
- przestrzega warunków korzystania z innego podmiotu przetwarzającego,
- udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków, umożliwia przeprowadzenie audytu.

Podwykonawcy realizujący zadania związane z dostępem do aktywów będących własnością organizacji/lub Klienta (realizacja usług, BHP, obsługa prawna, doradztwo w zakresie systemów zarządzania) zobowiązują się do stosowania zasad poufności poprzez podpisanie umowy „Umowa poufności - outsourcing", „Umowa powierzenia przetwarzania danych osobowych"/„Umowa powierzenia usługi IT".

Rozdział 6 Zarządzanie incydentami

Incydent jest to pojedyncze zdarzenie lub seria zdarzeń, związanych z bezpieczeństwem informacji niejawnych, które zagrażają ich poufności, dostępności lub integralności. Należy zauważyć, że incydent dotyczy zarówno poufności, jak i integralności i dostępności. Nie tylko ujawnienie informacji jest incydentem, ale z definicji wynika, że może być także modyfikacja informacji oraz brak dostępności informacji. Dodać trzeba, że incydent dotyczy nie tylko informacji, ale szeroko rozumianych zasobów systemu teleinformatycznego, takich jak: osoby, usługi, oprogramowanie, dane, sprzęt i inne elementy mające wpływ na bezpieczeństwo informacji.

PODZIAŁ ZDARZEŃ:
I) Zdarzenia losowe zewnętrzne (np.: klęski żywiołowe, przerwy w zasilaniu) - ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej, ciągłość pracy systemów zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
2) Zdarzenia losowe wewnętrzne (np.: niezamierzone pomyłki operatorów, administratorów, awarie sprzętowe, błędy w oprogramowaniu) - może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
3) Zdarzenia zamierzone, świadome i celowe - stanowią najpoważniejsze zagrożenie naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zdarzenia te możemy podzielić na:

- nieuprawniony dostęp do danych z zewnątrz (włamanie do systemu),
- nieuprawniony dostęp do danych z sieci wewnętrznej,
- nieuprawniony transfer danych,
- pogorszenie funkcjonowania sprzętu i oprogramowania (np.: działanie wirusów),
- bezpośrednie zagrożenie materialnych składników systemu (np.: kradzież sprzętu).

PRZYKŁADY ZDARZEŃ, które mogą być zakwalifikowane jako uzasadnione podejrzenie naruszenia bezpieczeństwa informacji:

- sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na infrastrukturę teleinformatyczną jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja osób zewnętrznych itp.;
- niewłaściwe parametry środowiska jak zbyt wysoka temperatura lub nadmierna wilgotność (w szczególności dotyczy to serwerowni);
- awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie systemu, a w tym sam fakt brak nadzoru;

- pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;
- jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikacje w systemie;
- nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie;
- stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
- nastąpiła niedopuszczalna manipulacja danymi w systemie;
- ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą elementy systemu zabezpieczeń.
- praca w systemie lub w sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych, np.: praca w systemie lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.
- ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp. dla dokumentów papierowych: oryginał jest bezpiecznie przechowywany wraz z informacją, kto znalazł dokument, gdzie, kiedy i kto by był świadkiem tego zdarzenia; każde śledztwo może wykazać, że oryginał nie został naruszony.

W każdym przypadku naruszenia ochrony danych osobowych administrator danych weryfikuje, czy naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Administrator danych w przypadku stwierdzenia takiej nieprawidłowości, zawiadamia niezwłocznie organ nadzorczy, jednak nie później niż w **ciągu 72 godzin** od stwierdzenia nieprawidłowości.
Administrator ocenia poziom istotności incydentu dla spółki kierując się następującymi kryteriami:
• wpływ incydentu na ciągłość działania podmiotu;
• krytyczność systemów dotkniętych skutkami incydentu bezpieczeństwa;
• wrażliwość informacji, których poufność, integralność czy dostępność naruszono (na przykład czy naruszono bezpieczeństwo informacji prawnie chronionej - np.: danych osobowych, informacji niejawnych);
• rozległość wpływu incydentu na działanie systemów (nie działa jeden komputer, cała sieć itp.);
• rozmiar szkód powstałych skutkiem incydentu;
• koszt usunięcia i naprawy skutków incydentu bezpieczeństwa;
• szacowany czas przywrócenia ciągłości działania dotkniętego incydentem bezpieczeństwa systemu;
• zasoby wymagane do przywrócenia ciągłości działania systemu (personel, wsparcie firm zewnętrznych, wymagane dodatkowe czy zamienne urządzenia oraz oprogramowanie, czas odtwarzania systemów z kopii zapasowych, itp.)

Administrator danych zawiadamia osoby, których dane dotyczą, w przypadku wystąpienia wobec nich naruszeń skutkujących ryzykiem naruszenia ich praw lub wolności, chyba że zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka wystąpienia ww. naruszenia.
Administrator danych dokumentuje incydenty, które skutkują naruszeniem praw i wolności osób fizycznych zgodnie z *F 07 PBD Zgłoszenie Incydentu, F 08 PBD Rejestr Incydentów.*

Administrator danych inicjuje działania naprawcze zmierzające do zniwelowania szkód wyrządzonych przez incydent, wyciąga wnioski z każdego incydentu i określa, jeśli to możliwe, działania korygujące w celu uniknięcia ponownego wystąpienia incydentu.
Administrator danych na bieżąco dokumentuje swoje działania na każdym z etapów procesu zarządzania incydentem w formie zapisów w rejestrze. Obsługa incydentu kończy się zapisem w formie wniosków co do działań na przyszłość odnotowanych w rejestrze incydentów.

Rozdział 7 Zasady realizacji praw osób

Każdy przypadek zgłoszenia przez osobę, której dane dotyczą, woli skorzystania z praw przewidzianych w rozporządzeniu administrator danych rozpatruje indywidualnie.
Administrator danych niezwłocznie realizuje następujące prawa osób, których dane dotyczą:

a) prawo dostępu do danych,
b) prawo do sprostowania danych,
c) prawo do usunięcia danych,
d) prawo do przenoszenia danych,
e) prawo do sprzeciwu wobec przetwarzania danych,
f) prawo do niepodlegania decyzjom oparty wyłącznie na profilowaniu.

W przypadku realizacji prawa do sprostowania, usunięcia i ograniczenia przetwarzania danych administrator danych niezwłocznie informuje odbiorców danych, którym udostępnił on przedmiotowe dane, chyba że jest to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.
Administrator danych odmawia realizacji praw osób, których dane dotyczą, jeżeli możliwość taka wynika z przepisów rozporządzenia, jednak każda odmowa realizacji praw osób, których dane dotyczą, wymaga uzasadnienia z podaniem podstawy prawnej wynikającej z rozporządzenia.

Rozdział 8 Odbieranie zgód oraz informowanie osób

W każdym przypadku pobierania danych bezpośrednio od osoby, której dane dotyczą, administrator danych informuje osobę, której dane dotyczą, zgodnie z *F 06 PBD Klauzula informacyjna.*. W każdym przypadku pobierania danych z innych źródeł niż osoba, której dane dotyczą, administrator danych informuje osobę, której dane dotyczą, niezwłocznie, jednak nie później niż przy pierwszym kontakcie z osobą, której dane dotyczą.

Rozdział 9 Postanowienia końcowe

Dokument niniejszy obowiązuje od dnia jego zatwierdzenia przez administratora danych.

Załączniki

- *F 01 PBD Lista procesów przetwarzania danych osobowych*
- *F 02 PBD Inwentaryzacja zasobów*
- *F 03 PBD Ocena zgodności procesów przetwarzania danych osobowych*
- *F 04 PBD Lista podmiotów przetwarzających dane*
- *F 05 PBD Analiza ryzyka*

- *F 06 PBD Klauzula informacyjna*
- *F 07 PBD Zgłoszenie Incydentu*
- *F 08 PBD Rejestr Incydentów*
- *F 09 PBD Wykaz zabezpieczeń*

Dokumenty związane:

- *Umowa o zachowaniu poufności- outsourcing*
- *Umowa powierzenia przetwarzania danych osobowych*
- *Umowa powierzenia usługi IT*