ROZANI OPAKOWANIA

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH W ROZANI

Spis treści

WZÓR OPAKOWANIA

Informacje ogólne

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych w ROZANI.
Dokument opisuje zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.
W szczególności zwraca uwagę na zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ww. rozporządzenia oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
Dokument, wskazuje sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych i przeznaczony jest dla osób zatrudnionych i upoważnionych do przetwarzaniu tych danych.
Polityka bezpieczeństwa została opracowana na podstawie postanowień 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.

ROZANI OPAKOWANIA

Definicje

Użyte w niniejszym dokumencie określenia oznaczają:

1. „**rozporządzenie**" oznacza 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. „**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, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
3. „**przetwarzanie**" 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;
4. „**ograniczenie przetwarzania**" oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
5. „**usuwanie danych**" oznacza zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
6. „**poufność danych**" oznacza właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom;
7. „**profilowanie**" oznacza dowolną formę zautomatyzowanego przetwarzania danych osobo-wych, 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;
8. „**pseudonimizacja**" oznacza 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;

9. „**zbiór danych**" oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
10. „**administrator**" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;
11. „**podmiot przetwarzający**" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
12. „**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;
13. „**strona trzecia**" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;
14. „**zgoda**" osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
15. „**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;
16. „**przedstawiciel**" oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający na mocy art. 27 do reprezentowania administratora lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z niniejszego rozporządzenia;
17. „**przedsiębiorca**" oznacza osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą;
18. „**organ nadzorczy**" oznacza niezależny organ publiczny ustanowiony przez państwo człon-kowskie zgodnie z art. 51;
19. „**państwo trzecie**" oznacza Państwo nienależące do Europejskiego Obszaru Gospodarczego;

20. „**identyfikator**" oznacza ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
21. „**hasło**" oznacza ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w Systemie informatycznym;
22. „**uwierzytelnianie**" oznacza działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
23. „**system zarządzania bazą danych**" oznacza system oprogramowania zawierający mechanizmy zapewniające spójność i bezpieczeństwo danych, sprawny dostęp do danych, środki programistyczne służące do przetwarzania danych, jednoczesny dostęp do danych dla wielu użytkowników, środki pozwalające na regulację dostępu do danych, środki pozwalające na odtworzenie zawartości bazy danych po awarii,
24. „**system informatyczny**" oznacza zbiór powiązanych ze sobą elementów: serwerów z systemami operacyjnymi, systemu zarządzania bazą danych, baz danych, oprogramowania (programów użytkowych), urządzeń końcowych (komputerów, terminali, urządzeń przenośnych, drukarek) oraz urządzeń służących do komunikacji między sprzętowymi elementami systemu,
25. „**zabezpieczenie danych w systemie informatycznym**" oznacza wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
26. „**środki techniczne i organizacyjne**" oznacza środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych;
27. „**sieć telekomunikacyjna**" oznacza sieć telekomunikacyjna w rozumieniu art. 2 pkt. 23 ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z późn. zm.)
28. „**internet**" oznacza sieć publiczna w rozumieniu art. 2 pkt. 22 ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne;
29. „**teletransmisja**" oznacza przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;

OPRACOWANIA

Administrator danych

Administrator danych osobowych realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:

1. wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie danych osobo-wych odbywało się zgodnie z Rozporządzeniem i aby móc to wykazać. Środki te są podejmowane uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia. W razie potrzeby poddawane są także przeglądom i uaktualniane.
2. wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania (ilość zbieranych danych osobowych, zakres ich przetwarzania, okres ich przechowywania oraz ich dostępność). W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.
3. wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą. Środki te są uwzględniane przy określaniu sposobów przetwarzania oraz w czasie samego przetwarzania 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 zagrożenia wynikające z przetwarzania.
4. Prowadzi ewidencję osób upoważnionych do przetwarzania
5. Prowadzi ewidencję zawartych umów powierzenia przetwarzania
6. Prowadzi rejestr naruszeń
7. Prowadzi rejestr czynności przetwarzania[2]
8. Prowadzi rejestr kategorii czynności przetwarzania[3]
9. Wyznacza Inspektora Ochrony Danych (IOD)[4]

SZKOLENIA

Środki techniczne i organizacyjne

Administrator danych spełnia wymogi dotyczące ochrony danych osobowych zawartych w rozporządzeniu.
Podjęte działania:

1. Wykonana przed opracowaniem polityki bezpieczeństwa i aktualizowana cyklicznie (nie rzadziej niż raz na rok) ocena skutków dla ochrony danych osobowych dla procesów, które z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, zgodnie z załącznikiem nr 2.
2. Wykonana przed opracowaniem polityki bezpieczeństwa i aktualizowana cyklicznie (nie rzadziej niż raz na rok) analiza ryzyka i plan postepowania z ryzykiem w odniesieniu do każdego z zasobów biorących udział w procesów w firmie, zgodnie z załącznikiem nr 1.
3. Ograniczenie dostępu do danych osobowych tylko do osób, które zostały przeszkolone i nadane zostały uprawnienia czego potwierdzeniem jest ewidencji osób upoważnionych do przetwarzania z załącznika 8.
4. Przetwarzania danych poza administratorem dopuszczone są jedynie podmioty przetwarzające spełniające wymogi rozporządzenia z którymi zawarto stosowne umowy zawarte w ewidencji w załączniku nr 10.
5. Opracowano i wdrożono politykę bezpieczeństwa danych osobowych.

Dla zapewnienia poufności, integralności, rozliczalności przetwarzanych danych stosuje się następujące środki:

Środki organizacyjne

1. Dopuszczenie do przetwarzania danych jedynie osób poprzez upoważnienie nadane przez administratora danych
2. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych
3. Przeszkolenie osób zatrudnionych przy przetwarzaniu danych z zakresu
    - przepisów dotyczących ochrony danych osobowych
    - zabezpieczeń systemów informatycznych
4. Zobowiązanie osób zatrudnionych przy przetwarzaniu danych osobowych do zachowania ich w tajemnicy poprzez podpisanie stosownych oświadczeń
5. Ustawianie ekranów komputerowych tak, by osoby niepowołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia

6. Przechowywanie kopii zapasowych zbiorów danych osobowych odbywa się w innym po-mieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco
7. Opuszczanie stanowiska pracy dopiero po aktywizowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób
8. Niepozostawianie bez kontroli dokumentów, nośników danych i sprzętu w hotelach i innych miejscach publicznych oraz w samochodach
9. Kasowanie po wykorzystaniu danych na dyskach przenośnych;
10. Niezapisywanie hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku i niepozostawianie w miejscu widocznym
11. Niszczenie w niszczarce lub chowania do szaf w pomieszczeniach zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy
12. Niepozostawianie osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych
13. Chowanie do szaf w zamykanych na klucz pomieszczeniach wszelkich akt zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;
14. Umieszczanie kluczy do pomieszczeń w ustalonym, przeznaczonym do tego miejscu po zakończeniu dnia pracy;
15. Zniszczenie fizycznie uszkodzonych nośników przed ich wyrzuceniem
16. Nie wykorzystywanie powtórnie, do sporządzania brudnopisów pism, jednostronnie zadrukowanych kart, jeśli zawierają one dane chronione. Zaleca się natomiast dwustronne drukowanie brudnopisów pism i sporządzanie dwustronnych dokumentów;
17. Niszczenie w niszczarce wydruków zawierające dane osobowe po wykorzystaniu. Czynność ta należy wykonywać należy codziennie przed zakończeniem pracy. O ile to możliwe, nie należy przechowywać takich wydruków w czasie dnia na biurku ani też wynosić poza siedzibę administratora danych.

RODO SPARKOWANIA

Środki techniczne

1. System informatyczny wykorzystywany do przetwarzania danych osobowych:
    - rejestruje zmiany dokonywane w zbiorach danych osobowych
    - reguluje zakres uprawnień do przetwarzania poszczególnych zbiorów dla każdego z pracowników
    - wymaga uwierzytelnienia z wykorzystaniem identyfikatora i hasła/karty procesoro-wej/danych biometrycznych
    - wymusza okresowa zmianę hasła dostępowego
    - wykorzystuje szyfrowanie w trakcie przesyłania danych
    - automatycznie blokuje dostęp w przypadku dłuższej nieaktywności użytkownika
2. Na komputerach gdzie przetwarzane są dane osobowe zastosowano:
    - zabezpieczenie przed nieautoryzowanym dostępem (wymagane hasło)
    - aktywowano automatyczne wygaszacze włączane pod dłuższej nieaktywności użytkownika wymagające ponownego podania hasła dostępowego
    - zastosowano system Firewall w celu ochrony przed atakami
    - zainstalowano oraz aktywowano automatyczna aktualizację programu antywirusowego

Środki ochrony fizycznej

(Wśród wymienionych należy wybrać zastosowane środki ochrony fizycznej)

1. Specyfikacja pomieszczenia, w którym przetwarzany jest zbiór danych osobowych:
    - zabezpieczenie drzwiami zwykłymi
    - poza godzinami pracy pomieszczenie zamykane na klucz
    - nadzór ochrony
    - zabezpieczone jest przed skutkami pożaru za pomocą wolnostojącej gaśnicy
2. Zbiór danych osobowych w formie papierowej przechowywany jest w szafie zwykłej, w po-mieszczeniu zamykanym na klucz
3. Kopie zapasowe/archiwalne zbiorów danych osobowych w formie papierowej przechowywane są w szafie zwykłej szafie zwykłej, w pomieszczeniu zamykanym na klucz
4. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek.

WZÓR OPAKOWANIA

Analiza oraz postępowanie z ryzykiem

1. Administrator dokonuje cyklicznej (nie rzadziej niż raz do koku) analizy ryzyka dla zasobów biorących udział w przetwarzaniu danych.
2. Prawdopodobieństwo i powaga ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określać poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko oszacuje na podstawie obiektywnej oceny zgodnie z arkuszem Analizy ryzyka i planu postępowania z ryzykiem stanowiącym załącznik nr 1.
3. W wyniku przeprowadzonej analizy administrator stwierdza, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko.
4. Na podstawie wyników przeprowadzonej analizy ryzyka administrator podejmuje decyzje o sposobie postępowania z ryzykiem i określa plan postępowania z ryzykiem mający na celu jego zminimalizowanie.

Ocena skutków dla ochrony danych

1. Administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, jeżeli dany rodzaj przetwarzania ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę. Przed wykonaniem oceny administrator weryfikuje, czy dany typ przetwarzania znajduje się na liście rodzajów przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków dla ochrony danych, publikowanych przez organ nadzorczy.
2. Administrator dokonuje cyklicznej (nie rzadziej niż raz do koku) weryfikacji oceny skutków dla ochrony danych dla procesów, w których wcześniejsza weryfikacja wykazała duże prawdopodobieństwo wystąpienia wysokiego naruszenia praw lub wolności osób fizycznych. Ponadto ocena skutków jest wykonywana, gdy w operacji przetwarzania dochodzi do istotnej zmiany, kiedy np. została wprowadzona do użytku nowa technologia, dane osobowe są wykorzystywane w innym celu lub też administrator danych zdecydował o rozpoczęciu transferu tych danych do państwa trzeciego.
3. Ocena skutków dla ochrony danych (ang. Data Protection Impact Assessment, DPIA) jest dokonywana zgodnie z wytycznymi rozporządzenia i zawiera co najmniej:

- systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
- ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
- ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1; oraz
- środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

Szablon oceny skutków dla ochrony danych DPIA opracowany na podstawie rozporządzenia oraz wytycznych opublikowanych w art. 29 grupy roboczej UE z dnia 4 kwietnia 2017 r stanowi załącznik nr 2 niniejszej polityki bezpieczeństwa

Domyślna ochrona danych osobowych

1. Przed rozpoczęciem nowego procesu oraz na etapie projektowania nowego produktu/usługi administrator przeprowadza ocenę skutków dla ochrony danych osobowych 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 zagrożenia wynikające z przetwarzania.
2. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Szczególnie odnosi się to do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.
3. Administrator cyklicznie (nie rzadziej niż raz na rok) przeprowadza ocenę skutków dla ochrony danych osobowych oraz analizę ryzyka i plan postępowania z ryzykiem dla wszystkich procesów oraz wszystkich produktów/usług w firmie

Współpraca z podmiotami przetwarzającymi

1. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy powierzenia przetwarzania danych osobowych zgodnie z załącznikiem nr 9.
2. Podmioty przetwarzające dokonujące przetwarzania w imieniu administratora muszą za-pewnić wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi Rozporządzenia i chroniło prawa osób, których dane dotyczą.
3. Administrator danych weryfikuje zgodność podmiotu przetwarzającego z Rozporządzeniem przed podpisaniem umowy oraz cyklicznie nie rzadziej niż raz do koku.

Pozyskiwanie danych osobowych

1. W przypadku pozyskiwania danych bezpośrednio od osoby, której dane dotyczą, administrator przekazuje informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania zgodnie z załącznikiem 12 część A.
2. W przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą, administrator przekazuje informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania zgodnie z załącznikiem 12 część B.
3. Przekazanie informacji następuje:
    - w rozsądnym terminie po pozyskaniu danych osobowych (najpóźniej w ciągu miesiąca),
    - najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą, jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą,
    - najpóźniej przy ich pierwszym ujawnieniu jeżeli planuje się ujawnić dane osobowe innemu odbiorcy.
4. W przypadku przetwarzania danych osobowych w celu innym niż cel, w którym te dane zostały pozyskane, przed dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w rozporządzeniu.

Zarządzanie incydentami

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych administrator w sposób niezwłoczny dokonuje zabezpieczenia danych, dokumentuje okoliczności oraz weryfikuje, czy naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych
2. W przypadku gdy naruszenie ochrony danych osobowych może powodować ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55 rozporządzenia.
3. W przypadku gdy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, których dane dotyczą, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu
4. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.
5. Po każdym wystąpieniu naruszenia ochrony danych osobowych, administrator dokonuje weryfikacji zagrożeń oraz zabezpieczeń procesu, w którym doszło do incydentu oraz podejmuje działania zaradcze mające na celu uniemożliwienie lub zminimalizowanie prawdopodobieństwa jego ponownego wystąpienia.

Realizacja praw osób, których dane dotyczą

1. Administrator zgodnie z rozporządzeniem niezwłocznie realizuje prawa osób, których dane dotyczą:
    - prawo do dostępu do danych
    - prawo do sprostowania danych
    - prawo do usunięcia danych („prawo do bycia zapomnianym”)
    - prawo do ograniczenia przetwarzania
    - prawo do przenoszenia danych
    - prawo do informacji o odbiorcach, którym administrator ujawnił dane osobowe
    - prawo do sprzeciwu wobec przetwarzania jej danych osobowych
    - prawo do nie podlegania decyzjom, które opierają się wyłącznie na zautomatyzowanym przetwarzaniu
2. Administrator rozpatruje każde zgłoszenie osoby, której dane dotyczą i rozpatruje je indywidualnie zgodnie z protokołem z załącznika nr 15.

3. Administrator odmawia realizacji praw osób, których dane dotyczą w przypadku nie zaistnienia przesłanek opisanych w rozporządzeniu. Każdorazowo odmowa musi być uzasadniona podstawa prawą z rozporządzenia.
4. Administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

Postanowienia końcowe

1. Wszystkie osoby upoważnione do przetwarzania danych osobowych zobowiązane są do stosowania postanowień zawartych w niniejszej Polityce bezpieczeństwa.
2. W sprawach nieuregulowanych w niniejszej Polityce bezpieczeństwa mają zastosowanie przepisy rozporządzenia.
3. Niniejsza Polityka bezpieczeństwa danych osobowych obowiązuje od dnia zatwierdzenia jej przez administratora danych.

ROZA PAKOWANIA

Spis załączników do dokumentu Polityki bezpieczeństwa

RODO PAKOWANIA PL