POLITYKA OCHRONY DANYCH OSOBOWYCH
W PODMIOCIE Restaurators Sp. z o.o.

Wstęp

Niniejsza Polityka Ochrony Danych Osobowych wskazuje wytyczne oraz określa zasady zabezpieczenia danych osobowych podczas ich przetwarzania, zapewniając zgodność przetwarzania danych osobowych z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) z 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 (dalej: RODO).

Definicje

Przez użyte w Polityce Ochrony Danych Osobowych określenia należy rozumieć:

1. **Polityka Ochrony Danych Osobowych (Polityka ODO)** - dokumentacja Ochrony Danych Osobowych obowiązująca w Restaurators Sp. z o.o.
2. **Administrator (ADO)** - podmiot, który samodzielnie lub wspólnie z innymi podmiotami ustala cele i sposoby przetwarzania danych osobowych.
3. **Administrator Systemów Informatycznych (ASI)** - osoba sprawująca nadzór nad prawidłową pracą systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień.
4. **Kategoria danych** - dane zwykłe lub dane szczególnych kategorii.
5. **Dane Osobowe** - wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, umożliwiające taką identyfikację.
6. **Przetwarzanie danych osobowych** - wykonywanie jakichkolwiek operacji na danych osobowych, w tym: zbieranie, utrwalanie, przechowywanie, opracowywanie, udostępnianie, zmienianie, usuwanie.
7. **Rejestr Czynności Przetwarzania** - jest to rejestr zawierający zespół powiązanych ze sobą operacji na danych, wykonywanych przez jedną lub kilka osób, które można określić w sposób zbiorczy, w związku z celem, w jakim te czynności są podejmowane.
8. **Rejestr Kategorii Czynności Przetwarzania** - jest to rejestr zawierający zespół powiązanych ze sobą operacji na danych, wykonywanych przez Procesora na rzecz Administratora powierzającego mu zadania zawiązane z przetwarzaniem danych osobowych w swoim imieniu i na swoją rzecz.
9. **Procesor/ Podprocesor/ Podmiot Przetwarzający -** odbiorca danych realizujący zadania związane z przetwarzaniem danych w imieniu i na rzecz Administratora.
10. **Odbiorca Danych** - osoba fizyczna lub prawna, organ publiczny lub inny podmiot, któremu ujawnia się dane osobowe.
11. **Organ nadzorczy** - jest to niezależny organ publiczny powołany w celu ochrony podstawowych praw i wolności osób w związku z przetwarzaniem danych osobowych.
12. **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.
13. **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych.
14. **Zabezpieczenie systemu informatycznego** – wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych należących do Administratora, a także ich utratą.
15. **Użytkownik systemu informatycznego** - osoba posiadająca uprawnienia do pracy w systemie informatycznym.

16. **Identyfikator użytkownika** systemu informatycznego – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę uprawnioną do przetwarzania danych osobowych w systemie informatycznym.
17. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
18. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości użytkownika.
19. **Sieć lokalna** – połączenie systemów informatycznych Administratora wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych.
20. **Nośnik komputerowy (wymienny)** – elektroniczny nośnik danych służący do zapisu i przechowywania informacji.

Postanowienia ogólne

1. Polityka ODO dotyczy wszystkich danych osobowych przetwarzanych przez Restaurators Sp. z o.o., niezależnie od formy ich przetwarzania.
2. Polityka ODO przechowywana jest w wersji papierowej w siedzibie Administratora.
3. Polityka ODO jest udostępniana do wglądu osobom posiadającym upoważnienie do przetwarzania danych osobowych.
4. Polityka ODO obowiązuje wszystkich, którzy w Restaurators Sp. z o.o. przetwarzają dane osobowe, niezależnie od formy współpracy z Administratorem.
5. Polityka jest dokumentem wewnętrznym Administratora o charakterze poufnym.
6. Dla skutecznej realizacji Polityki ODO, Administrator zapewnia:
    a. środki techniczne i rozwiązania organizacyjne odpowiednie do zagrożeń i kategorii danych objętych ochroną;
    b. kontrolę i nadzór nad przetwarzaniem danych osobowych;
    c. monitorowanie zastosowanych środków ochrony.
7. ADO zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem danych osobowych są zgodne z niniejszą Polityką ODO oraz odpowiednimi przepisami prawa.

Dane osobowe przetwarzane przez administratora

Dane osobowe, stanowiące część zbioru danych lub mających stanowić część zbioru danych mogą być przetwarzane przez Administratora w sposób całkowicie lub częściowo zautomatyzowany lub inny niż zautomatyzowany.

Osoby odpowiedzialne za ochronę danych osobowych w organizacji

Administrator systemów informatycznych (ASI)

1. ADO wyznacza Administratora Systemów Informatycznych (ASI).
2. Do głównych zadań ASI należą:
    a. wdrożenie zdefiniowanych zabezpieczeń elektronicznych zbiorów danych osobowych i aplikacji, za pomocą których są przetwarzane dane osobowe i przedłożenie ich do oceny IOD;
    b. wdrożenie zabezpieczeń adekwatnych do ryzyka przetwarzania oraz konsultowanie tych zabezpieczeń z Administratorem;
    c. bieżące monitorowanie zabezpieczeń podległych mu systemów;
    d. bieżąca aktualizacja systemów, zabezpieczeń oraz aplikacji, celem zapewnienia bezpieczeństwa systemów informatycznych i aplikacji, za pomocą których przetwarzane są dane osobowe;
    e. tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemie informatycznym;
    f. organizacja procesu tworzenia kopii zapasowych oprogramowania, konfiguracji oprogramowania, systemów, konfiguracji systemów oraz innych danych, kluczowych

dla zapewnienia optymalnego bezpieczeństwa systemów i przetwarzanych w nich danych;
g. przeglądy oraz konserwacja sprzętu informatycznego wykorzystywanego do przetwarzania danych osobowych;
h. nadawanie oraz odbieranie uprawnień do systemów oraz aplikacji zgodnie z upoważnieniami do przetwarzania danych osobowych nadanymi przez ADO.

Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem

1. Wszystkie osoby posiadające upoważnienie do przetwarzania danych osobowych w podmiocie zobowiązane są do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami prawa i zgodnie z niniejszą Polityką ODO, a także innymi dokumentami wewnętrznymi i procedurami, związanymi z przetwarzaniem danych osobowych.
2. Wszystkie dane osobowe są przetwarzane z poszanowaniem zasad przetwarzania przewidzianych przez przepisy prawa:
    a. w każdym wypadku występuje chociaż jedna z przewidzianych przepisami prawa podstawa prawna dla przetwarzania danych;
    b. dane przetwarzane są rzetelnie i w sposób przejrzysty;
    c. dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
    d. dane osobowe są przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu przetwarzania danych;
    e. dane osobowe są prawidłowe i w razie potrzeby uaktualniane;
    f. czas przechowywania danych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane bądź do okresu wskazanego odrębnymi przepisami prawa;
    g. wobec osoby, której dane dotyczą, wykonywany jest obowiązek informacyjny, zgodnie z treścią art. 13 i 14 RODO;
    h. dane są zabezpieczone przed naruszeniami zasad ich ochrony.
3. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony danych osobowych uważa się w szczególności:
    a. naruszenie bezpieczeństwa systemów informatycznych, w których przetwarzane są dane osobowe;
    b. udostępnianie lub umożliwienie udostępniania danych osobom lub podmiotom do tego nieupoważnionym;
    c. zaniechanie, choćby nieumyślne, dopełnienia obowiązku zapewnienia danym osobowym należytej ochrony;
    d. niedopełnienie obowiązku zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
    e. przetwarzanie danych osobowych niezgodnie z celem ich zbierania;
    f. spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie danych osobowych;
    g. naruszenie praw osób, których dane są przetwarzane.
4. W przypadku stwierdzenia okoliczności naruszenia zasad ochrony danych osobowych, każda osoba przetwarzająca dane osobowe zobowiązana jest do niezwłocznego powiadomienia ADO na dedykowany adres mailowy rodo@pierogarnie.com i do podjęcia wszystkich niezbędnych kroków, mających na celu ograniczenie skutków naruszenia.
5. Do obowiązków ADO w zakresie zatrudniania, zakończenia lub zmiany warunków zatrudnienia pracowników lub współpracowników należy dopilnowanie, by:
    a. pracownicy lub współpracownicy zostali odpowiednio przeszkoleni z zasad ochrony danych osobowych, obowiązujących w podmiocie na danym stanowisku pracy;
    b. każdy z pracowników lub współpracowników przetwarzających dane osobowe posiadał stosowne upoważnienie do przetwarzania danych;

c. każdy pracownik lub współpracownik zobowiązał się do zachowania w tajemnicy danych osobowych przetwarzanych w podmiocie oraz sposobów ich zabezpieczeń.

6. Pracownicy lub współpracownicy zobowiązani są do:
    a. ścisłego przestrzegania zakresu nadanego upoważnienia do przetwarzania danych osobowych;
    b. przetwarzania i ochrony danych osobowych zgodnie z przepisami prawa;
    c. zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
    d. bezzwłocznego zgłaszania incydentów związanych z naruszeniem bezpieczeństwa danych osobowych oraz zgłaszania podejrzenia naruszenia bezpieczeństwa danych osobowych, a także niewłaściwym funkcjonowaniem systemu informatycznego na dedykowany adres mailowy rodo@pierogarnie.com
    e. niezwłocznego poinformowania ADO o potencjalnym dostępie do danych osobowych, w sytuacji, gdy pracownikowi nie zostało nadane upoważnienie do przetwarzania danych osobowych.

Obszar przetwarzania danych osobowych

1. Do obszaru przetwarzania zalicza się wszelkie budynki lub pomieszczenia, w których Administrator prowadzi swoją działalność i przetwarzane są dane osobowe.
2. Samodzielne przebywanie osoby w obszarach przetwarzania danych możliwe jest wyłącznie w sytuacji posiadania upoważnienia do przetwarzania danych osobowych.

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych

1. ADO zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych.
2. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych.
3. Środki obejmują w szczególności:
    a. ograniczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe, jedynie do osób posiadających zgody na przebywanie w obszarach przetwarzania bądź odpowiednio upoważnionych. Inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do przetwarzania danych jedynie w towarzystwie osoby upoważnionej lub posiadającej zgodę;
    b. zamykanie pomieszczeń tworzących obszar przetwarzania danych osobowych na czas nieobecności pracowników, w sposób uniemożliwiający dostęp do nich osobom trzecim;
    c. wykorzystanie zamykanych szafek i sejfów do zabezpieczenia dokumentów;
    d. Wykorzystanie niszczarki, bądź korzystanie z usług zewnętrznych podmiotów specjalizujących się w utylizacji dokumentów dla skutecznego usuwania dokumentów zawierających dane osobowe;
    e. ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz;
    f. wykonywanie regularnych kopii zapasowych danych osobowych przetwarzanych w systemach informatycznych;
    g. ochronę sprzętu komputerowego należącego do ADO przed złośliwym oprogramowaniem oraz ingerencją osób niepowołanych;
    h. zabezpieczenie dostępu do urządzeń przetwarzających dane przy wykorzystaniu unikatowych identyfikatorów użytkowników systemów informatycznych i haseł dostępu;
    i. wykorzystanie mechanizmów szyfrowania danych przy ich transmisji.

Naruszenia zasad ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych ADO dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.
2. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, ADO zgłasza fakt naruszenia zasad ochrony danych organowi nadzorczemu bez zbędnej zwłoki, nie później niż w terminie 72 godzin od stwierdzenia naruszenia.
3. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, ADO zawiadamia o incydencie także osoby, których dane dotyczą.

Powierzenie przetwarzania danych osobowych

1. ADO może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej prawem dozwolonej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO.
2. Przed powierzeniem przetwarzania danych osobowych ADO w miarę możliwości uzyskuje informacje o dotychczasowych praktykach procesora dotyczących zabezpieczenia danych osobowych.

Przekazywanie danych do państwa trzeciego

Przekazywanie danych osobowych do państwa poza Europejskim Obszarem Gospodarczym (EOG) jest możliwe wyłącznie jeżeli firma znajduje się na liście Data Privacy Framework.

Procedury przetwarzania danych osobowych

1. W celu prawidłowej realizacji postanowień niniejszej Polityki ODO, ADO wprowadza procedury regulujące i zapewniające prawidłowe przetwarzanie danych osobowych.
2. Wykaz obowiązujących procedur stanowi załącznik 1 do niniejszej Polityki ODO.
3. Procedury dotyczą procesów przetwarzania danych zarówno przy wykorzystaniu systemów informatycznych, jak i w formie tradycyjnej.
4. Wszystkie osoby, które uzyskają dostęp do danych osobowych bądź do obszarów przetwarzania danych zobowiązane są do przestrzegania procedur.

ZAŁĄCZNIK 1 DO POLITYKI OCHRONY DANYCH OSOBOWYCH

WYKAZ PROCEDUR

LP	Nazwa procedury
1	
2	
3	
4	