Fundacja Underground

Polityka ochrony danych osobowych

Celem Polityki ochrony danych osobowych, zwanej dalej Polityką, jest wprowadzenie i utrzymanie wymaganej przez przepisy rozporządzenia Parlamentu Europejskiego i Rady 2016/679 z dnia 27 kwietnia 2016 r. oraz ustawy o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000) właściwej ochrony danych osobowych w związku z przetwarzaniem danych osobowych w Fundacji Underground.

Niniejsza Polityka dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, aktach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych. Dotyczy istniejących oraz przetwarzanych w przyszłości zbiorów danych osobowych. Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych, jak i innych, np. wolontariuszy, praktykantów, stażystów.

Określenia użyte w Polityce ochrony danych osobowych oznaczają:

1. administrator danych osobowych (ADO) – Fundacja Underground,
2. administrator systemów informatycznych (ASI) – osoba zobowiązana do zarządzania systemami informatycznymi wykorzystywanymi do przetwarzania danych osobowych,
3. dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
4. przetwarzanie danych osobowych – gromadzenie, utrwalanie, przechowywanie, opracowywanie, modyfikowanie, udostępnianie i usuwanie danych osobowych, zwłaszcza w systemach informatycznych,
5. użytkownik – osoba upoważniona do przetwarzania danych osobowych,
6. system informatyczny – system (urządzenia, narzędzia, programy), w którym przetwarzane są dane osobowe,
7. kierownik zakładu – prezes zarządu Fundacji Underground,
8. zabezpieczenie systemu informatycznego – należy przez to rozumieć wdrożenie stosowanych środków administracyjnych, technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych a także ich utratą,
9. RODO – 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,
10. ustawa o ochronie danych osobowych – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000).

1. Zasady przetwarzania danych osobowych

1.1.

Administrator danych osobowych:

- zbiera dane osobowe w konkretnych, wyraźnych i prawnie uzasadnionych celach;
- przetwarza dane osobowe:
    - zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,
    - adekwatnie, stosownie oraz w sposób ograniczony do tego, co niezbędne do celów, w których są przetwarzane,
    - prawidłowo, w razie potrzeby je uaktualniając,
    - w sposób zapewniający odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych;
- przechowuje dane osobowe w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane.

1.2.

W celu realizacji tych zasad administrator danych przetwarza dane legalnie, na podstawie przesłanek opisanych w art. 6 RODO. Pobiera dane osobowe adekwatnie do celów przetwarzania i przetwarza je przez określony czas. Wobec osób, których dane przetwarza wypełnia obowiązki informacyjne określone w art. 13 RODO lub w art. 14 RODO (gdy informacje pobierane są w sposób inny niż od osoby, której dane dotyczą) oraz wskazuje przysługujące im uprawnienia takie jak prawo do:

- dostępu do danych,
- sprostowania danych,
- usunięcia danych (prawo do bycia zapomnianym),
- przenoszenia,
- sprzeciwu wobec przetwarzania,
- ograniczenia przetwarzania,
- wniesienia skargi do organu nadzorczego,
- sprzeciwu wobec bycia profilowanym.

Administrator danych zapewnia ochronę danych w przypadku korzystania z usług podmiotów zewnętrznych w postaci zawierania stosownych umów powierzenia oraz korzystając z usług podmiotów przetwarzających realizujących obowiązki wynikające z RODO. W razie wystąpienia incydentu technicznego lub fizycznego administrator danych zapewnia zdolność do szybkiego przywrócenia dostępności do danych osobowych i dostępu do nich.

1.3.

Potwierdzenie spełniania obowiązków informacyjnych przez administratora danych stanowią klauzule informacyjne przekazywane osobom, których dane są przetwarzane.

2. Upoważnienia do przetwarzania danych

Administrator danych zapewnia aby dostęp do danych osobowych w Fundacji Underground miały tylko osoby legitymujące się nadanym przez ADO upoważnieniem. Upoważnienia określają do jakich operacji użytkownicy są uprawnieni, tj. tworzenia, usuwania, wglądu, przekazywania danych, w jakich systemach oraz na jaki czas. Administrator danych prowadzi ewidencję osób upoważnionych. Upoważnienia do

przetwarzania danych osobowych mogą być nadawane na wniosek bezpośredniego przełożonego użytkownika systemu.

3. Analiza ryzyka

Administrator danych prowadzi analizę ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń. Analiza prowadzona jest w przypadku zaistnienia zagrożenia. Analiza ryzyka prowadzona jest dla całego zbioru danych.

4. Wykaz zabezpieczeń

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, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

5. Rejestr czynności przetwarzania

Administrator danych nie prowadzi rejestru czynności przetwarzania.

6. Procedura postępowania z incydentami

Administrator danych wprowadza do stosowania procedurę postępowania z incydentami naruszenia ochrony danych osobowych. Celem tej procedury jest wypełnienie obowiązku wynikającego z art. 33 RODO. Procedura określa sposób definiowania incydentów zagrażających bezpieczeństwu danych osobowych oraz sposób reagowania na nie, a także procedurę wprowadzenia działań naprawczych. Każda osoba upoważniona do przetwarzania danych osobowych ma obowiązek poinformowania o możliwości wystąpienia incydentu lub o jego wystąpieniu. Taka informacja powinna być przekazana bezpośredniemu przełożonemu.

Powiadomienia wymagają:

- niewłaściwe zabezpieczenie sprzętu elektronicznego, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych, udostępnienie haseł osobom postronnym,
- niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
- nieprzestrzeganie zasad ochrony danych osobowych przez pracowników,
- ślady na drzwiach, oknach i szafach wskazujące na próbę włamania,
- dokumentacja zawierająca dane osobowe niszczona bez użycia niszczarki,
- otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
- obecność osób postronnych w jednostce,
- złe ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe,
- wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz jednostki bez upoważnienia administratora danych,
- awarie serwera, komputerów, twardych dysków, oprogramowania,
- udostępnienie danych osobowych osobom nieupoważnionym,

- telefoniczne próby wyłudzenia danych osobowych,
- kradzież, zagubienie komputerów lub CD, twardych dysków, pen-drive z danymi osobowymi,
- maile nakłaniające do ujawnienia identyfikatora lub hasła,
- zainfekowanie komputerów wirusem,
- zdarzenia losowe (pożar obiektu, zalanie wodą),
- włamanie do systemu informatycznego lub pomieszczeń,
- kradzież danych/sprzętu,
- świadome zniszczenie dokumentów.

Należy również powiadomić administratora systemów informatycznych. Ponadto należy udokumentować wystąpienie incydentu, jego skutki oraz podjęte działania naprawcze i zaradcze. W przypadku gdy incydent skutkuje naruszeniem praw lub wolności osób fizycznych, administrator danych zgłasza je w ciągu 72 godzin Prezesowi Urzędu Ochrony Danych Osobowych oraz gdy istnieje taki wymóg, powiadamia o tym fakcie osoby, których incydent dotyczył.

7. Regulamin ochrony danych osobowych i szkolenia wewnętrzne

Administrator danych wprowadza w Fundacji Underground Regulamin ochrony danych osobowych w celu zapewnienia osobom przetwarzającym dane osobowe pełny zakres wiedzy na temat zasad przetwarzania danych osobowych w jednostce oraz obciążających je obowiązków z tym związanych. Osoby zapoznane z Regulaminem zobowiązane są potwierdzić fakt zapoznania się z tym dokumentem oraz zdeklarować stosowanie się do jego zasad. Każda osoba przed zatrudnieniem powinna zostać zapoznana z Regulaminem. Administrator danych zapewnia również przeszkolenie pracowników z zakresu stosowania przepisów dotyczących ochrony danych osobowych, a obecność pracowników należy potwierdzić pisemnie.

8. Umowy powierzenia przetwarzania danych osobowych

W przypadku zlecania przetwarzania danych osobowych podmiotom zewnętrznym administrator danych zobowiązany jest zawrzeć umowę powierzenia. W jednostce prowadzony jest rejestr umów powierzenia przetwarzania danych osobowych.

9. Czynności kontrolne

Nadzór i kontrolę nad ochroną danych osobowych sprawuje kierownik zakładu.

Czynności kontrolne przeprowadzane są raz do roku.

Z czynności kontrolnych sporządza się protokół, w którym dokonuje się opisu zakresu kontroli i przeprowadzonych czynności, a także zalecenia i działania naprawcze. Protokół podpisywany jest przez osoby wykonujące czynności kontrolne.

10. Odpowiedzialność osób upoważnionych do przetwarzania danych

Niezastosowanie się do prowadzonej przez administratora danych Polityki ochrony danych osobowych, której założenia określa niniejszy dokument, i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych.