Polityka Bezpieczeństwa

przetwarzania danych osobowych

w Greysoft sp zo.o. z siedzibą w Warszawie

Spis treści

Cel wprowadzenia Polityki Bezpieczeństwa

Celem Polityki Bezpieczeństwa jest zapewnienie ochrony danych osobowych przetwarzanych przez Greysoft Sp. z o.o. zwanej Spółką przed wszelakiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.

Polityka określa zasady przetwarzania danych osobowych oraz ich zabezpieczania, jako zestaw praw, reguł i zaleceń, regulujących sposób ich zarządzania, ochrony i dystrybucji wewnątrz Spółki oraz w kontaktach z otoczeniem.

Zakres stosowania Polityki Bezpieczeństwa

Każdy pracownik Spółki który przetwarza dane osobowe ma obowiązek zapoznać się z zasadami i procedurami ochrony danych zawartych w tym dokumencie oraz stosować je w codziennej pracy.

Definicje

Administrator Danych (AD) - Greysoftsp. z o.o.

Administrator Systemu – osoba odpowiedzialna za funkcjonowanie systemów informatycznych u Administratora Danych

Rozporządzenie – Rozporządzenie Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 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)

przetwarzanie danych osobowych - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

zbiór danych osobowych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie.

zbiór nieinformatyczny – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie, prowadzony poza systemem informatycznym, w szczególności w formie kartoteki, skorowidza, księgi, wykazu lub innego zbioru ewidencyjnego.

Deklaracja Zarządu Spółki

Zarząd Spółki zobowiązuje się do podjęcia odpowiednich kroków, mających na celu zapewnienie prawidłowej ochrony danych osobowych, w szczególności do zapewnienia, że przez cały okres ich przetwarzania, dane będą:

a) Przetwarzane zgodnie z prawem,

b) Zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,

c) Merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,

d) Przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania,

e) Zabezpieczone środkami technicznymi i organizacyjnymi, które zapewniają rozliczalność, integralność oraz poufność danych,

f) Przy przetwarzaniu danych osobowych w systemach informatycznych Spółki należy stosować wysoki poziom bezpieczeństwa.

Informacje o dokumentacji z zakresu ochrony danych osobowych

1. Niniejsza Polityka oraz dokumenty z nią powiązane powinny być aktualizowane wraz ze zmieniającymi się przepisami prawa o ochronie danych osobowych oraz zmianami faktycznymi w ramach Spółki, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.
2. Przegląd Polityki ma na celu stwierdzenie, czy postanowienia Polityki odpowiadają aktualnej i planowanej działalności Spółki oraz stanowi prawnemu aktualnemu w momencie dokonywania przeglądu.
3. Zmiany niniejszej Polityki wymagają przeglądu innych dokumentów obowiązujących w Spółce dotyczących ochrony danych osobowych.
4. Wszelkie znaczące zmiany Polityki powinny być zatwierdzane przez Administratora Danych.

Odpowiedzialność Zarządu Spółki

1. Zarząd Spółki jest odpowiedzialny za przetwarzanie i ochronę danych osobowych zgodnie z przepisami prawa, w tym wprowadzenie do stosowania procedur postępowania zapewniających prawidłowe przetwarzanie danych osobowych, rozumiane jako ochronę danych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.
2. Do kompetencji Zarządu Spółki należy w szczególności:

a) wyznaczanie Właścicieli zasobów danych osobowych,

b) określenie celów i strategii ochrony danych osobowych,

c) podział zadań i obowiązków związanych z organizacją ochrony danych osobowych.

3. Do obowiązków Zarządu Spółki należy:
    a) Zapewnienie szkoleń dla pracowników w zakresie przepisów o ochronie danych osobowych oraz zagrożeń związanych z ich przetwarzaniem,
    b) Przyjmowanie i zatwierdzanie niezbędnych, wymaganych przez przepisy prawa dokumentów regulujących ochronę danych osobowych w Spółce,
    c) Zapewnienie środków finansowych na ochronę fizyczną pomieszczeń, w których przetwarzane są dane osobowe,
    d) Zapewnienie środków finansowych niezbędnych do ochrony danych osobowych przetwarzanych w systemach informatycznych oraz w zbiorach nieinformatycznych,
    e) Zapewnienie środków finansowych na merytoryczne przygotowanie osób odpowiedzialnych za nadzór nad ochroną danych osobowych,

Konsekwencje naruszenia ochrony danych osobowych

1. Naruszenie ochrony danych osobowych przez pracownika, może skutkować postawieniem mu zarzutu popełnienia, jednego z przestępstw określonych w Rozdziale 8 Ustawy lub przestępstwa określonego w art. 266 Kodeksu Karnego. W takim przypadku zgodnie z przepisem art. 66 Kodeksu Pracy umowa o pracę z pracownikiem tymczasowo aresztowanym wygasa z upływem 3 miesięcy nieobecności pracownika w pracy z powodu tymczasowego aresztowania, chyba że pracodawca rozwiąże wcześniej bez wypowiedzenia umowę o pracę z winy pracownika.
2. Zgodnie z art. 100 § 2 pkt 5 Kodeksu Pracy, pracownik jest obowiązany przestrzegać tajemnicy określonej w odrębnych przepisach. Dane osobowe, którym Spółka nadaje charakter poufny mają charakter takiej tajemnicy, a jej ujawnienie w zależności od zakresu ujawnionych danych osobowych oraz nastawienia pracownika dopuszczającego się nieuprawnionego ujawnienia danych, może mieć charakter naruszenia lub ciężkiego naruszenia obowiązków pracowniczych.
3. Pracownik dopuszczający się nieuprawnionego ujawnienia lub wykorzystania danych osobowych w sposób sprzeczny z ich przeznaczeniem (np. wykorzystania danych osobowych do celów prywatnych) czy też ich przetwarzania w sposób niezgodny z przyjętymi w Spółce procedurami może zostać ukarany karą upomnienia lub karą nagany.
4. W razie ciężkiego naruszenia obowiązku zachowania danych osobowych w tajemnicy lub przetwarzania ich w sposób rażąco sprzeczny z przyjętymi zasadami i procedurami, Spółka może rozwiązać bez wypowiedzenia umowę o pracę z winy pracownika.
5. Sankcje dotyczące ujawnienia poufnych danych osobowych stosuje się analogicznie do ujawnienia przez pracownika informacji dotyczących zabezpieczenia danych osobowych w Spółce.

Obowiązek informacyjny

Pracownicy zbierający dane osobowe, w szczególności na formularzach, umowach, drukach (zarówno papierowych jak i elektronicznych) odpowiadają za umieszczenie na nich klauzuli informującej o przetwarzaniu danych osobowych. Treść klauzuli podlega uzgodnieniu z Administratorem Danych lub osobą przez niego wyznaczoną.

Szkolenia z zakresu ochrony danych osobowych

1. Przed rozpoczęciem przetwarzania danych osobowych pracownik powinien zostać przeszkolony. Zakres szkolenia powinien obejmować zaznajomienie pracownika z przepisami o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi i instrukcjami obowiązującymi u Administratora Danych.
2. Za przeprowadzenie szkolenia odpowiada bezpośredni przełożony pracownika.
3. Szkolenia powinny być powtarzane okresowo lub na żądanie, gdy zaistnieje taka potrzeba.
4. Szczegółowy zakres szkolenia ustala Administrator Danych lub osoba przez niego wyznaczona.

Dopuszczenie osób do przetwarzania danych osobowych

1. Przetwarzanie danych osobowych jest możliwe wyłącznie po uzyskaniu przez pracownika formalnego upoważnienia do przetwarzania danych osobowych wystawianego przez Administratora Danych. W tym celu przełożony pracownika przed dopuszczeniem pracownika do pracy przy przetwarzaniu danych osobowych:
    a) Zapoznaje pracownika z przepisami dotyczącymi ochrony danych osobowych oraz uregulowaniami wewnętrznymi obowiązującymi w tym zakresie w Spółce,
    b) Przyjmuje od pracownika podpisane oświadczenie o zachowaniu danych osobowych i sposobów ich zabezpieczania w tajemnicy, przetwarzania danych osobowych zgodnie z przepisami oraz oświadczenia o znajomości niniejszego dokumentu, a także o znajomości „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych", którego wzór stanowi Załącznik nr 1 niniejszej Polityki,
    c) Wnioskuje do Administratora Danych lub osoby przez niego wyznaczonej o formalne upoważnienie pracownika do przetwarzania danych osobowych sporządzane wg wzoru niniejszej Polityki stanowiącego Załącznik nr 2 niniejszej Polityki.
5. Oświadczenia i upoważnienia, o których mowa w ust. 1 przechowuje się w aktach osobowych pracownika.
6. Przełożony pracownika jest zobowiązany niezwłocznie po ustaniu potrzeby przetwarzania danych osobowych przez pracownika, złożyć rezygnację do Administratora Danych lub osoby przez niego wyznaczonej Informacji dotyczącą jego dostępu do danych osobowych.
7. Osoby upoważnione do przetwarzania danych osobowych powinny być wpisywane do ewidencji. Zakres danych podlegających ewidencjonowaniu określa Administrator Danych. Wzór karty z ewidencji stanowi Załącznik nr 3 niniejszej Polityki.

Wymiana informacji dotyczących ochrony danych osobowych

Pracownicy oraz współpracownicy Spółki w celu ochrony wymienianych informacji dotyczących danych osobowych powinni podczas przetwarzania uwzględniać zasady bezpieczeństwa ustalone przez Administratora Danych.

Retencja danych

Zgodnie z art. 5 Rozporządzenia dane osobowe należy przechowywać w okresie nie dłuższym, niż jest to niezbędne do celów przetwarzania. Okresy przetwarzania oraz kryteria na podstawie których wyznaczane są te okresy znajdują się w polityce retencji danych osobowych stanowiącej załącznik nr 5 niniejszej Polityki.

Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Zabezpieczenia organizacyjne
    a) Została opracowana i wdrożona Polityka Bezpieczeństwa,
    b) Została opracowana i wdrożona Instrukcja Zarządzania Systemem Informatycznym,
    c) Do przetwarzania danych osobowych zostali dopuszczeni wyłącznie pracownicy posiadający upoważnienia nadane przez Administratora Danych,
    d) Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych,
    e) Osoby zatrudnione przy przetwarzaniu danych osobowych zostały zaznajomione z przepisami dotyczącymi ochrony tych danych oraz z zasadami zabezpieczeń systemu informatycznego,
    f) Osoby zatrudnione przy przetwarzaniu danych osobowych zostały zobowiązane do zachowania ich w tajemnicy,
    g) Przetwarzanie danych osobowych prowadzonej jest w warunkach zabezpieczających je przed dostępem osób niepowołanych,
    h) Przebywanie osób nieuprawnionych w pomieszczeniach, w których przetwarzane są dane osobowe jest dopuszczalne jedynie w obecności osoby zatrudnionej przy przetwarzaniu tych danych i w warunkach zapewniających bezpieczeństwo danych,
    i) Stosuje się pisemne umowy powierzenia przetwarzania danych osobowych dla współpracy ze stronami przetwarzającymi dane osobowe, których administratorem jest Spółka. Umowy powierzenie są rejestrowane w Rejestrze umów powierzenia stanowiącym załącznik nr 4 niniejszej Polityki.
2. W celu ochrony danych osobowych stosuje się następujące zabezpieczenia fizyczne:
    a) Serwery są zlokalizowane w pomieszczeniach biurowych. W pomieszczeniach tych mogą znajdować się wyłącznie osoby upoważnione przez Administratora Danych.
    b) Urządzenia systemu informatycznego Administratora Danych są zasilane za pośrednictwem UPS.
3. Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej:

a) Administrator danych wykorzystuje zaporę sieciową w celu separacji sieci lokalnej od sieci publicznej.

b) Korzystanie z zasobów sieci wewnętrznej możliwe jest tylko po podaniu nazwy użytkownika i hasła.

c) Administrator danych stosuje zabezpieczenie oprogramowaniem antywirusowym, by zminimalizować ryzyko ingerencji przez złośliwe wirusy w Systemy Informatyczne i Dane Osobowe

Postępowanie w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych

1. Poniższe postanowienia mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych przetwarzanych w systemach informatycznych, jak i w zbiorach nieinformatycznych.
2. Przed przystąpieniem do pracy pracownicy zobowiązani są dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, w tym zwrócić szczególną uwagę, czy nie zaszły okoliczności wskazujące na naruszenie lub próby naruszenia ochrony danych osobowych.
3. Za okoliczności, które uznaje się za naruszenie lub podejrzenie naruszenia ochrony systemu przetwarzającego dane osobowe, uważa się w szczególności:
    a) Nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują,
    b) Nieuprawnione naruszenie lub próby naruszenia poufności, integralności i rozliczalności danych i systemu,
    c) Niezamierzoną zmianę lub utratę danych zapisanych na kopiach zapasowych,
    d) Nieuprawniony dostęp do danych osobowych (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu),
    e) Udostępnienie osobom nieupoważnionym danych osobowych lub ich części,
    f) Inny stan systemu informatycznego lub pomieszczeń, niż pozostawiony przez użytkownika po zakończeniu pracy,
    g) Wydarzenia losowe, obniżające poziom ochrony systemu (np. brak zasilania lub pożar),
    h) Kradzież sprzętu informatycznego lub nośników zewnętrznych zawierających dane osobowe (np. wydruków komputerowych, dyskietek, płyt CD-ROM, dysków twardych, pamięci zewnętrznych, itp.).
4. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych pracownicy zobowiązani są do bezzwłocznego powiadomienia o tym fakcie przełożonego.
5. Do czasu rozpoczęcia procedury sprawdzającej zgłaszający:
    a) Powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów,

b) Zabezpiecza elementy systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osobom nieupoważnionym,

c) Podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych,

d) Wykonuje polecenia Administratora Systemu.

6. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych osoba wyznaczona przez Administratora Danych z pomocą Administratora Systemu, po przybyciu na miejsce:

   a) Ocenia zastałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane osobowe oraz stan urządzeń, a także szacuje wielkość negatywnych następstw incydentu,

   b) Wysłuchuje relacji osoby, która dokonała powiadomienia oraz innych osób związanych z incydentem,

   c) Podejmuje decyzje o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych.

7. Osoba wskazana przez Administratora Danych sporządza raport z przebiegu zdarzenia, w którym powinny się znaleźć w szczególności informacje o:

   a) dacie i godzinie powiadomienia,

   b) godzinie pojawienia się w pomieszczeniach, w których przetwarzane są dane,

   c) sytuacji, jaką zastał,

   d) podjętych działaniach i ich uzasadnieniu,

   e) stanie systemu po podjęciu działań naprawczych,

   f) wnioskach w sprawie ograniczenia możliwości ponownego wystąpienia naruszenia ochrony danych osobowych.

8. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik może kontynuować pracę dopiero po zakończeniu czynności opisanych powyżej i zgodzie udzielonej przez przełożonego lub Administratora Systemu.

9. W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej w Spółce dyscypliny pracy, Osoba wyznaczona przez Administratora Danych wyjaśnia wszystkie okoliczności incydentu i podejmuje stosowne działania wobec osób, które dopuściły się wskazanego naruszenia.

10. Po zakończeniu czynności naprawczych system powinien utrzymać poziom ochrony nie niższy niż przed wystąpieniem incydentu związanego z naruszeniem ochrony danych osobowych.

Zasady ochrony danych osobowych w zbiorach nieinformatycznych

1) Zbiory nieinformatyczne powinny być odpowiednio zabezpieczone przed nieuprawnionym dostępem i zniszczeniem.

2) Dokumenty i wydruki, zawierające dane osobowe, należy przechowywać w zamykanych pomieszczeniach, do których dostęp mają jedynie uprawnione osoby.

3) Na czas nieużytkowania, dokumenty i wydruki zawierające dane osobowe powinny być zamykane w szafach biurowych lub zamykanych szufladach.

4) Wydruki robocze, błędne lub zdezaktualizowane powinny być niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie lub zanonimizowanie.

5) Dla udokumentowania czynności dokonywanych w celu likwidacji zbiorów archiwalnych, powinny być stosowane odpowiednie przepisy obowiązujące w Spółce.

Postanowienia końcowe

1) Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w niniejszej Polityce może być podstawą rozwiązania stosunku pracy bez wypowiedzenia z osobą, która dopuściła się naruszenia.

W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy Rozporządzenia Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 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) Spis załączników

Załącznik nr 1 – Oświadczenie pracownika zatrudnionego przy przetwarzaniu danych osobowych w zbiorach danych przetwarzanych przez Greysoft Sp. z o.o.,

Załącznik nr 2 – Upoważnienie do przetwarzania danych osobowych,

Załącznik nr 3 – Ewidencja osób upoważnionych do przetwarzania danych osobowych,

Załącznik nr 4 – Rejestr umów powierzenia danych osobowych,

Załącznik nr 5 – Polityka Retencji danych osobowych,