POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

Stowarzyszenie Na Rzecz Osób Niepełnosprawnych „Równy Start" w Poznaniu, ul. Św. Rocha 13, 61- 142 Poznań

POSTANOWIENIA OGÓLNE

DEKLARACJA I ZASTOSOWANIE

1. Stowarzyszenie Na Rzecz Osób Niepełnosprawnych „Równy Start" w Poznaniu, ul. Św. Rocha 13, 61- 142 Poznań (dalej: **„STOWARZYSZENIE"**) – jako Administrator danych osobowych - ma świadomość znaczenia przetwarzanych informacji dla realizacji celów instytucji i potrzeby ochrony informacji, ze szczególnym uwzględnieniem ochrony danych osobowych, poprzez budowę systemu zarządzania bezpieczeństwem informacji.
2. Niniejszy dokument (dalej: **„POLITYKA"**) określa zasady bezpieczeństwa przetwarzania danych osobowych jakie powinny być przestrzegane i stosowane w STOWARZYSZENIU, przez osoby, którzy przetwarzają dane osobowe.
3. Procedury i dokumenty związane z POLITYKĄ będą weryfikowane i dostosowywane w celu zapewnienia odpowiedniego poziomu bezpieczeństwa. Przeglądy dokumentacji odbywają się **nie rzadziej niż raz w roku.**
4. POLITYKA określa środki techniczne i organizacyjne zastosowane przez STOWARZYSZENIE dla zapewnienia ochrony danych oraz tryb postępowania w przypadku stwierdzenia naruszenia zabezpieczenia danych albo w sytuacji podejrzenia o takim naruszeniu.
5. POLITYKA została opracowana z uwzględnieniem metod i środków ochrony danych, których skuteczność w czasie ich zastosowania jest powszechnie uznawana. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania charakteru poufnego wraz z zachowaniem ich integralności i rozliczalności, ze szczególnym uwzględnieniem obowiązujących przepisów prawa dotyczących ochrony danych osobowych.
6. Niniejsza POLITYKA obowiązuje Administratora, a także wszystkich podmiotów występujących w ramach STOWARZYSZENIA, bez względu na podstawę prawną nawiązanej współpracy.
7. Każda z osób, o których mowa w pkt 1 powyżej, ma obowiązek zapoznania się z treścią POLITYKI.
8. POLITYKA dotyczy wyposażenia, systemów, urządzeń przetwarzających informacje w formie elektronicznej, papierowej lub jakiejkolwiek innej.
9. Nieprzestrzeganie postanowień zawartych w dokumentacji bezpieczeństwa informacji może skutkować sankcjami w pełnym zakresie dopuszczonym przez

stosunek prawny pomiędzy STOWARZYSZENIEM a naruszającym oraz obowiązujące przepisy prawa.

10. W celu skutecznego zapoznania pracowników i współpracowników z zasadami zawartymi w niniejszej POLITYCE wprowadza się zestaw reguł stanowiący wyciąg najistotniejszych zapisów zawartych w POLITYCE.

DEFINICJE

Ilekroć w POLITYCE jest mowa o:

1) **Administratorze danych osobowych** (dalej: **„Administrator"**) - rozumie się przez to Stowarzyszenie Na Rzecz Osób Niepełnosprawnych „Równy Start" w Poznaniu, ul. Św. Rocha 13, 61- 142 Poznań.
2) **Specjaliście ds. ochrony danych osobowych** (dalej: **„Specjalista"**) – rozumie się przez to osobę nadzorującą przestrzeganie zasad ochrony przetwarzanych danych osobowych i innych informacji prawem chronionych. Nadzoruje on stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych, a w szczególności zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów oraz zmianą, utratą, uszkodzeniem, lub zniszczeniem, a także przeprowadzi kontrole w zakresie określonym regulacjami wewnętrznymi Administratora.
3) **Aktywach** – wszystko co ma wartość dla organizacji (wartość materialna: np. komputery, bazy danych itp. oraz wartość niematerialna: dobre imię, rozpoznawalność i wizerunek organizacji itp.)
4) **Zbiorze danych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
5) **Kartotece** – rozumie się przez to zewidencjonowany, usystematyzowany zbiór wykazów, skoroszytów, wydruków komputerowych i innej dokumentacji gromadzonej w formie papierowej, zawierającej dane osobowe.
6) **Przetwarzaniu danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

7) **Systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

8) **Bezpieczeństwie danych** – zachowanie poufności, integralności i dostępności informacji; dodatkowo, mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

9) **Usuwanie danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.

10) **Użytkowniku** – rozumie się przez to osobę upoważnioną przez Administratora do przetwarzania informacji i danych osobowych.

11) **Komórce organizacyjnej** – rozumie się przez to każdą wydzieloną organizacyjnie i funkcjonalnie komórkę wewnętrzną, zgodnie z podziałem organizacyjnym przeprowadzonym przez Administratora.

12) **Pomieszczeniach** – rozumie się przez to budynki i pomieszczenia określone przez Administratora danych, tworzące obszar, w którym przetwarzane są dane osobowe i inne informacje prawem chronione.

13) **Incydencie** – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji. Wzór raportu z naruszenia ochrony danych oraz rejestru naruszeń stanowią załącznik do niniejszej Polityki.

ZASADY OCHRONY DANYCH OSOBOWYCH

Bezpieczeństwo przetwarzania danych osobowych opiera się na następujących niezaprzeczalnych zasadach ochrony informacji oraz danych:

1) **Zasada zgodności z prawem, rzetelności i przejrzystości**. Dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dal osoby, której dane dotyczą.

2) **Zasada ograniczenia celu**. Dane osobowe muszą być zbierane w konkretnych, wyraźnie i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

3) **Zasada minimalizacji danych**. Dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.
4) **Zasada prawidłowości**. Dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.
5) **Zasada ograniczenia przechowywania**. Dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.
6) **Zasada integralności i poufności**. Dane osobowe muszą być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i poufność, w tym ochronę przed:
    a) niedozwolonym lub niezgodnym z prawem przetwarzaniem – czyli nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu,
    b) przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.
7) **Zasada znajomości wymagań Polityki Bezpieczeństwa**. Każdy pracownik powinien zostać zapoznany z regułami oraz z kompletnymi i aktualnymi procedurami ochrony informacji i podpisać stosowne oświadczenie o zapoznaniu się z zasadami obowiązującej polityki.
8) **Zasada uprawnionego dostępu.** Każdy pracownik stosuje się do obowiązujących zasad ochrony informacji, spełnia kryteria dopuszczenia do informacji.
9) **Zasada przywilejów koniecznych**. Każdy pracownik posiada prawa dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań.
10) **Zasada wiedzy koniecznej**. Każdy pracownik posiada wiedzę o systemie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań.
11) **Zasada usług koniecznych**. Systemy informacyjne świadczą tylko te usługi, które są konieczne do realizacji zadań biznesowych i operacyjnych.

12) **Zasada asekuracji**. Każdy mechanizm zabezpieczający musi być ubezpieczony drugim, (podobnym). Jako mechanizmy zabezpieczeń dopuszczalne jest stosowanie zarówno zabezpieczeń technicznych, jak i organizacyjnych.
13) **Zasada świadomości zbiorowej**. Wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych i aktywnie uczestniczą w tym procesie.
14) **Zasada indywidualnej odpowiedzialności**. Za bezpieczeństwo poszczególnych elementów odpowiadają konkretne osoby.
15) **Zasada obecności koniecznej**. Prawo przebywania w określonych miejscach mają tylko osoby do tego upoważnione.
16) **Zasada stałej gotowości**. System jest przygotowany na wszelkie zagrożenia. Niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających.
17) **Zasada najsłabszego ogniwa**. Poziom bezpieczeństwa wyznacza najsłabszy (najmniej zabezpieczony) element. Elementy takie są wyznaczane na podstawie analizy ryzyka.
18) **Zasada kompletności**. Skuteczne zabezpieczenie jest tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ogniwa ogólnie pojętego procesu przetwarzania informacji.
19) **Zasada ewolucji**. Każdy system musi ciągle dostosowywać mechanizmy wewnętrzne do zmieniających się warunków zewnętrznych.
20) **Zasada odpowiedniości**. Używane mechanizmy muszą być adekwatne do sytuacji.
21) **Zasada świadomej konwersacji**. Nie zawsze i wszędzie trzeba mówić, co się wie, ale zawsze i wszędzie trzeba wiedzieć, co, gdzie i do kogo się mówi.
22) **Zasada rozliczalności**. Administrator jest odpowiedzialny za przestrzeganie powyższych zasad. Musi on być także w stanie wykazać ich przestrzeganie.

ZAKRES ZASTOSOWANIA

1. Zasady określone w niniejszej POLITYCE mają zastosowanie do całego systemu przetwarzania danych, a w szczególności do:
   1) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz będących w formie papierowej w których przetwarzane są lub będą dane osobowe,
   2) informacji będących własnością Administratora lub jednostek obsługiwanych, o ile zostały przekazane na podstawie umów lub porozumień,

3) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach zabezpieczenia danych osobowych oraz innych dokumentów zawierających dane osobowe,
4) wszystkich nośników papierowych, magnetycznych lub optycznych, na których są lub będą znajdować się dane osobowe podlegające ochronie,
5) wszystkich lokalizacjach – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
6) wszystkich pracowników w rozumieniu przepisów kodeksu pracy, konsultantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

2. We wszystkich umowach, które mogą dotyczyć przetwarzania danych w jednostce, należy uwzględnić zapisy zobowiązujące drugą stronę do przestrzegania odpowiednich zapisów niniejszej POLITYKI.
3. Administrator prowadzi wykaz podmiotów zewnętrznych, z którymi realizacja umów/porozumień/zamówień lub aneksów do nich zobowiązuje lub umożliwia zleceniobiorcy/wykonawcy dostęp do informacji zawierających dane osobowe. Wzór wykazu stanowi załącznik do niniejszej POLITYKI.

OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH

I.

Podział zagrożeń:

1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona, nie dochodzi do naruszenia poufności danych;
2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych;
3) zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

II.

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są informacje, to głównie:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy,
3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
6) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych,
7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
8) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
9) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony informacji - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu itp.,
11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. bocznej furtki itp.,
12) podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane,

13) rażąco naruszono dyscyplinę w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych itp.).

III.

Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych, tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.

PRZEDSIĘWZIĘCIA ZABEZPIECZAJĄCE PRZED NARUSZENIEM OCHRONY DANYCH

I.

1. Każdy użytkownik – przed dopuszczeniem do przetwarzania informacji podlega przeszkoleniu z przepisów w zakresie ochrony informacji oraz wynikających z nich zadań i obowiązków.
2. Wszyscy użytkownicy podlegają okresowym szkoleniom.
3. Za organizację szkoleń odpowiedzialny jest Specjalista.

II.

1. Do zapewnienia bezpieczeństwa danych i informacji zastosowano następujące środki organizacyjne:

a) Dostęp do danych osobowych mogą mieć tylko i wyłącznie pracownicy posiadający pisemne, imienne upoważnienia nadane przez Administratora,

b) Każdy z pracowników powinien zachować szczególną ostrożność przy przenoszeniu wszelkich nośników z danymi,

c) Należy chronić dane przed wszelkim dostępem do nich osób nieupoważnionych,

d) Pomieszczenia, w których są przetwarzane dane osobowe, powinny być zamykane na klucz,

e) Dostęp do kluczy posiadają tylko upoważnieni pracownicy,

f) Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy. W wypadku gdy jest wymagany poza godzinami pracy – możliwy jest tylko na podstawie zezwolenia Administratora,

g) Dostęp do pomieszczeń, w których są przetwarzane dane osobowe, mogą mieć tylko upoważnieni pracownicy,

h) W przypadku pomieszczeń, do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności,

i) Szafy, w których przechowywane są dane, powinny być zamykane na klucz,

j) Klucze do tych szaf posiadają tylko upoważnieni pracownicy,

k) Szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych, a następnie powinny być zamykane,

l) Dane w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych, a następnie muszą być chowane do szaf,

2. Do zapewnienia bezpieczeństwa danych i informacji zastosowano następujące środki techniczne:

a) Dostęp do komputerów, na których są przetwarzane dane, mają tylko upoważnieni pracownicy,

b) Monitory komputerów, na których przetwarzane są dane, są tak ustawione, aby osoby nieupoważnione nie miały wglądu w dane,

c) Po zakończeniu pracy komputery przenośne (np. typu notebook) zawierające dane osobowe powinny być zabezpieczone w zamykanych na klucz szafach,

d) W wypadku potrzeby wyniesienia komputera przenośnego (np. typu notebook) zawierającego dane osobowe lub inne informacje chronione, komputer taki musi być odpowiednio dodatkowo zabezpieczony, a dane zaszyfrowane,

e) Nie należy udostępniać osobom nieupoważnionym tych komputerów,

f) W przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami należy dokonać tego z zachowaniem szczególnej ostrożności,

g) Nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie), aby nie zostały na nich dane osobowe,

h) W wypadku niemożliwości skasowania danych z nośnika (płyta CD-ROM) należy taką płytę zniszczyć fizycznie,

i) W przypadku wykorzystania do przenoszenia dysków dane należy kasować z tych dysków,

j) Niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną,

k) Sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz.

l) Błędne lub nieaktualne wydruki i wersje papierowe zawierające dane osobowe lub inne informacje chronione niszczone są za pomocą niszczarki lub w inny mechaniczny sposób uniemożliwiający powtórne ich odtworzenie.

DOSTĘP DO INFORMACJI I DANYCH OSOBOWYCH

1. Przetwarzanie, w tym udostępnianie danych osobowych, jest prawnie dopuszczalne, jeżeli jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.
2. W przypadku udostępnienia informacji w celach innych niż włączenie do zbioru Administrator udostępnia posiadane informacje osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
3. Dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
4. Podmiot występujący o udostępnienie informacji powinien wskazać podstawę prawną upoważniającą go do otrzymania tych danych albo uzasadnioną potrzebę żądania ich udostępnienia. Tylko w takiej sytuacji można dokonać oceny, czy w określonym przypadku udostępnienie danych jest prawnie dopuszczalne i czy nie będzie ono stanowić naruszenia zasad ochrony informacji.
5. Przetwarzanie, w tym udostępnianie informacji w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą, oraz następuje w celu badań naukowych, dydaktycznych, historycznych oraz statystycznych, z zachowaniem praw i wolności osób, których dane dotyczą i po zanonimizowaniu danych osobowych.
6. Udostępnienie informacji może nastąpić jedynie za zgodą Administratora lub Specjalisty i powinno być odpowiednio udokumentowane.

Porozumienia i kontakty ze stronami zewnętrznymi

1. W przypadku zawierania umów z podmiotami zewnętrznymi mającymi wpływ na funkcjonowanie kluczowych elementów systemu zarządzania bezpieczeństwem informacji zalecane jest zawarcie umowy powierzenia i określenie w niej następujących wymagań bezpieczeństwa:
    1) zakres i cel czynności oraz danych mających być przedmiotem współpracy z firmą zewnętrzną,
    2) zakresy odpowiedzialności w przypadku utraty lub ujawnienia danych,
    3) własność informacji i oprogramowania oraz obowiązki w zakresie ochrony danych osobowych,
    4) specjalne zabezpieczenia, które mogą być wymagane do ochrony informacji szczególnie chronionych, takich jak dane finansowe czy też identyfikatory i hasła dostępu,

5) warunki dostępu do informacji, zobowiązanie do zachowania w tajemnicy czynnika uwierzytelniającego,
6) Definicji informacji, które mają być chronione (np. informacji poufnych).
7) spodziewanego czasu trwania umowy, łącznie z przypadkami, w których obowiązek zachowania poufności może być bezterminowy,
8) wymaganych działań w momencie zakończenia umowy,
9) zasad zwrotu lub niszczenia informacji przy zakończeniu umowy,
10) działań podejmowanych w przypadku naruszenia warunków umowy,
11) ustaleń dotyczących licencji, własności kodu i prawa do własności intelektualnej,
12) zasad testowania przed instalacją w celu wykrycia kodu złośliwego i koni trojańskich.

2. Specjalista prowadzi wykaz podmiotów zewnętrznych.

POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH

I.
Działania korygujące i zapobiegawcze

1. **Działania korygujące** podejmowane są w przypadku wykrycia niezgodności w działalności bądź nieprawidłowego działania procesu. Przesłanką do podjęcia działań korygujących mogą być wyniki audytów, zgłoszenia niezgodności, zdarzenia i incydenty związane z bezpieczeństwem informacji, zapisy, wyniki badania zadowolenia klientów, analiza reklamacji klientów.
2. **Działania zapobiegawcze** mają na celu zapobiec wystąpieniu potencjalnych niezgodności.
3. Podejmowanie działań korygujących oraz zapobiegawczych powinno być dokumentowane w odpowiednich rejestrach działań korygujących i zapobiegawczych. Za prowadzenie rejestru działań zapobiegawczych i korygujących odpowiedzialny jest Specjalista.
4. Specjalista przedkłada Administratorowi cykliczny plan kontroli zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

II.
Stwierdzenie naruszenia

1. W przypadku stwierdzenia naruszenia:
   a) zabezpieczenia systemu informatycznego,
   b) technicznego stanu urządzeń,
   c) zawartości zbioru danych osobowych,
   d) ujawnienia metody pracy lub sposobu działania programu,
   e) jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
   f) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.)

   każda osoba zatrudniona przy przetwarzaniu danych jest obowiązana niezwłocznie powiadomić o tym fakcie Administratora lub Specjalistę.
2. Do czasu przybycia na miejsce naruszenia ochrony danych Administratora lub Specjalisty należy:
   a) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,
   b) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
   c) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
   d) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
   e) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej,
   f) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku.
3. Po przybyciu na miejsce naruszenia Specjalisty lub osoba go zastępująca:
   a) zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metody dalszego postępowania, mając na uwadze ewentualne zagrożenia dla prawidłowości pracy,

b) może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
c) rozważa celowość i potrzebę powiadamia o zaistniałym naruszeniu Administratora danych,
d) nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, z zewnętrznymi specjalistami.

4. Specjalista dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który powinien zawierać w szczególności:
   a) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
   b) określenie czasu i miejsca naruszenia i powiadomienia,
   c) określenie okoliczności towarzyszących i rodzaju naruszenia,
   d) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
   e) wstępną ocenę przyczyn wystąpienia naruszenia,
   f) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.
5. Sporządzony raport Specjalista niezwłocznie przekazuje Administratorowi.
6. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Specjalista zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.

III.
Analiza przyczyn i skutków naruszeń

1. Zaistniałe naruszenie może stać się przedmiotem szczegółowej, zespołowej analizy prowadzonej przez Administratora, Specjalisty, Informatyka oraz osób wyznaczonych przez Administratora danych.
2. Analiza powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych, wnioski co do ewentualnych przedsięwzięć proceduralnych, organizacyjnych, kadrowych i technicznych, które powinny zapobiec podobnym naruszeniom w przyszłości.
3. W przypadku naruszenia ochrony danych osobowych skutkującym ryzykiem naruszenia praw lub wolności osób fizycznych administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu

naruszenia – zgłasza je organowi nadzorczemu. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Wzór zgłoszenia naruszenia do organu nadzorczego stanowi załącznik do niniejszej Polityki.

GRUPY INFORMACJI PODLEGAJĄCE OCHRONIE

1. Grupa informacji **dotycząca działalności:**
   1) dane osobowe klientów
   2) dane osobowe kontrahentów
   3) informacje dotyczące współpracy i rozliczeń z podmiotami współpracującymi
   4) skargi, zażalenia, reklamacje
2. Grupa informacji **dotycząca pracowników:**
   1) dane osobowe pracowników
   2) dane osobowe rodzin pracowników
   3) dane osoby - kandydata do zatrudniania
   4) informacje dot. obsługi kadrowo-płacowej pracownika (wynagrodzenia, ewidencja czasu pracy, informacja a urlopach)
3. Grupa informacji **dotycząca infrastruktury fizycznej i teleinformatycznej:**
   1) informacje dotyczące zarządzania zasobami (plany i rozmieszczenia i ilość zasobów – środki trwałe, informacja o nieruchomościach)
   2) dane na temat postępowania w sytuacji krytycznej (ewakuacja)
   3) informacje dotyczące stanu infrastruktury
   4) dane o zabezpieczeniach systemu informatycznego
   5) dane o zabezpieczeniach infrastruktury fizycznej
   6) informacje dotyczące systemów zarządzania
   7) dokumentacja techniczna infrastruktury
4. Grupa informacji **dotycząca finansów organizacji:**
   1) informacje finansowe
   2) dane z kontroli i audytów
   3) informacje dotyczące kontrahentów
5. Specjalista prowadzi wykaz zbiorów danych.
6. W Wykazie zbiorów zawarty jest opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między oraz wykaz

programów i systemów komputerowych wykorzystywanych do przetwarzania danych w tych zbiorach.

7. Opis struktury baz danych oraz sposób przepływu danych pomiędzy poszczególnymi systemami jest w posiadaniu Administratora, a także u dostawców i autorów oprogramowania służącego do przetwarzania danych.

BEZPIECZEŃSTWO OSOBOWE

Etap naboru pracownika / współpracownika

1. Do przetwarzania danych osobowych i do dostępu do innych informacji chronionych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora. Administrator może wydać pełnomocnictwo do nadawania upoważnień.
2. Zakres upoważnienia może również być określony w umowie o pracę lub współpracę.
3. Osoba upoważniona zobowiązana jest podpisać oświadczenie lub umowę, która dokładnie określa odpowiedzialność w zakresie bezpieczeństwa informacji. Role i zakresy odpowiedzialności powinny uwzględniać:
   1) działania zgodne z POLITYKĄ,
   2) ochronę aktywów przed nieuprawnionym dostępem, ujawnieniem, modyfikacją lub zniszczeniem,
   3) wykonywanie działań związanych z bezpieczeństwem informacji,
   4) odpowiedzialność pracownika za jego działania lub niepodejmowanie działań,
   5) raportowanie zdarzeń związanych z bezpieczeństwem informacji,
   6) zapisy o zachowaniu poufności i nieujawnianiu informacji,
   7) prawa i obowiązki w odniesieniu do praw autorskich i ochrony danych osobowych;
   8) obowiązek klasyfikacji informacji i zarządzania aktywami organizacji związanymi z systemami informacyjnymi i usługami,
   9) odpowiedzialność w zakresie przetwarzania informacji otrzymywanej z zewnątrz,
   10) odpowiedzialność organizacji w zakresie przetwarzania danych osobowych,
   11) odpowiedzialność rozszerzoną, np. praca w domu, po godzinach pracy,
   12) konsekwencje nieprzestrzegania procedur bezpieczeństwa.

4. Wszyscy kandydaci do pracy, wykonawcy oraz podwykonawcy powinni podlegać weryfikacji, zgodnie z przepisami prawnymi i regulacjami wewnętrznymi, adekwatnie do wymagań biznesowych, klasyfikacji udostępnionych informacji oraz zidentyfikowanego ryzyka. Weryfikacja nie może naruszać prywatności, ochrony danych osobowych ani regulacji prawnych dotyczących zatrudnienia i może obejmować:
    1) dostępność referencji osobistych i świadectw pracy,
    2) sprawdzenie przedstawionego życiorysu,
    3) potwierdzenie deklarowanego wykształcenia i kwalifikacji zawodowych,
    4) niezależne potwierdzenie tożsamości, np. paszport.

Zatrudnienie / współpraca

1. Pracownicy, wykonawcy i podwykonawcy powinni być świadomi swoich obowiązków i odpowiedzialności prawnej oraz zagrożeń związanych z bezpieczeństwem informacji. W tym celu należy zapewnić wszystkim zatrudnionym właściwy poziom świadomości poprzez kształcenie i szkolenie z zakresu bezpieczeństwa informacji, ze szczególnym uwzględnieniem procedur bezpieczeństwa. Dokumentują to: lista obecności ze szkoleń, oświadczenia pracowników, umowy o poufności, posiadane zaświadczenia, dyplomy lub certyfikaty.
2. W przypadku naruszenia zasad bezpieczeństwa jest uruchomiana odpowiednia procedura postępowania dyscyplinarnego, która powinna być poprzedzona potwierdzeniem naruszenia zasad bezpieczeństwa i zgromadzeniem materiału dowodowego.
3. Postępowanie dyscyplinarne powinno uwzględniać: rodzaj i wagę naruszenia zasad bezpieczeństwa, wpływ na procesy biznesowe, przypadek incydentalny, czy jest to kolejne naruszenie oraz jakość odbytego przeszkolenia.
4. W przypadku pracy mobilnej i na odległość z wykorzystaniem urządzeń przenośnych zastosowano odpowiednie, dodatkowe środki bezpieczeństwa.
5. Przekazywanie sprzętu i urządzeń służących do przetwarzania danych odbywa się na podstawie protokołów przekazania sprzętu.

Zakończenie zatrudnienia / współpracy

1. Odchodzenie z organizacji lub zmiana stanowiska pracy wiąże się ze zwrotem posiadanego przez pracownika sprzętu i odebraniem lub zmianą praw dostępu.

2. Odebranie lub ograniczenie praw dostępu jest poprzedzone analizą ryzyka uwzględniającą następujące uwarunkowania:
   1) ustalenie inicjatora (pracownik, wykonawca czy kierownictwo instytucji) i przyczyn zakończenia lub zmiany zatrudnienia,
   2) aktualny zakres czynności pracownika, wykonawcy lub podwykonawcy,
   3) wartość aktualnie dostępnych aktywów.

Ogólne zasady bezpieczeństwa osobowego

1. Każdy pracownik przy wykonywaniu swoich obowiązków służbowych jest zobowiązany do przestrzegania postanowień niniejszej POLITYKI oraz postanowień innych części dokumentacji bezpieczeństwa informacji, a także poleceń dotyczących bezpieczeństwa otrzymywanych od Specjalisty oraz Administratora.
2. Specjalista i przełożeni zobowiązani są do nadzoru nad przestrzeganiem postanowień niniejszej POLITYKI.
3. Każdy z pracowników jest zobowiązany do uczestniczenia w organizowanych okresowych szkoleniach z zakresu bezpieczeństwa informacji. Specjalista oraz Administrator są zobowiązani do utrzymywania i podnoszenia poziomu wiedzy dotyczącej bezpieczeństwa informacji.
4. Każdy pracownik jest zobowiązany do podjęcia bezpośrednich działań dla zapobiegania incydentom lub minimalizowania skutków incydentów w miarę swoich możliwości i kompetencji, w razie potrzeby zawiadamiając Specjalistę lub przełożonych. W razie potrzeby o zgłoszeniu incydentu Policji decyduje Administrator.

Zasady przyznawania dostępu

1. Przyznawanie zakresu uprawnień powinno być w ścisłym związku z zakresem obowiązków danego pracownika.
2. Zarządzanie dostępem na etapie nadawania, zmiany i cofania praw dostępu pracowników w obszarze przetwarzania danych oraz do systemów teleinformatycznych powinno się odbywać na wniosek bezpośredniego przełożonego Użytkownika.
3. Na wniosek przełożonego lub specjalisty ds. kadrowych upoważnionemu użytkownikowi Administrator zakłada konto w systemie z adekwatnym poziomem uprawnień.

4. W zarządzaniu dostępem obowiązuje zasada, że dostęp użytkownika powinien opierać na spełnieniu zasady rozliczalności oraz zasady niezaprzeczalności. W przypadku systemów informatycznych obowiązują następujące wymagania:
   1) wymóg jednoznacznej identyfikacji pracownika - tj. w systemach informatycznych każdy użytkownik pracuje wyłącznie na swoim indywidualnym koncie, nie są stosowane konta anonimowe lub współdzielone poza wyjątkami, gdzie z przyczyn technicznych nie ma innej możliwości,
   2) wymóg uwierzytelnienia pracownika przy korzystaniu z systemu informatycznego,
   3) autoryzacji przyznania praw dostępu do systemów informatycznych,
   4) zasady przywilejów, wiedzy i usług koniecznych.

BEZPIECZEŃSTWO TELEINFORMATYCZNE

Autoryzacja i dopuszczalne wykorzystanie zasobów

1. Przy ochronie zasobów kluczowe jest stosowanie podstawowej zasady bezpieczeństwa, że nie jest dozwolone wykorzystywanie zasobów w sposób inny, niż jawnie dozwolony.
2. Do wykonywania obowiązków służbowych związanych z przetwarzaniem informacji dozwolone jest używanie systemów, urządzeń i oprogramowania dopuszczonych do użytku zgodnie z wymogami POLITYKI.
3. Pracownicy są uprawnieni do korzystania z zasobów teleinformatycznych niezbędnych do wykonywania ich obowiązków. Za określenie takich zasobów dla każdego pracownika i wnioskowanie o przyznanie dostępu odpowiedzialny jest bezpośredni przełożony pracownika.
4. Zakazane jest użytkowanie na terenie obszaru przetwarzania danych lub przy wykonywaniu obowiązków służbowych poza obszarem przetwarzania danych innych niż dopuszczone urządzeń, systemów i oprogramowania bez zgody Administratora.
5. Zakazane jest bez zgody Administratora:
   1) użytkowanie urządzeń skutkujących połączeniem systemów Administratora danych z sieciami teleinformatycznymi innych podmiotów, w tym publicznymi sieciami teleinformatycznymi,
   2) użytkowanie urządzeń lub oprogramowania mających na celu zakłócenie działania innych systemów, urządzeń lub oprogramowania,

3) użytkowanie urządzeń lub oprogramowania do testowania bezpieczeństwa lub wykrywania podatności,
4) użytkowanie urządzeń lub oprogramowania mogących naruszyć bezpieczeństwo innych systemów lub urządzeń,
5) wprowadzanie zmian konfiguracji urządzeń, systemów lub oprogramowania.

6. Zakazane jest bez zgody Specjalisty wykorzystywanie urządzeń do niejawnego przekazywania lub rejestracji danych dotyczących informacji chronionych, w tym głosu i obrazu, tj.: magnetofonów, dyktafonów, aparatów fotograficznych, kamer, telefonów komórkowych z opcją rejestrowania dźwięku i obrazu, rejestratorów ruchu sieciowego, rejestratorów pracy klawiatur itp.
7. Powyższy zakaz nie dotyczy sytuacji, gdy rejestrowane są dane pochodzące z systemu testowego, a działania pracownika nie prowadzą, i w sposób oczywisty nie mogą prowadzić, do odczytywania jakichkolwiek poufnych informacji, do których pracownik nie ma dostępu.
8. Wykorzystanie należących do Administratora urządzeń, systemów i oprogramowania oraz innych zasobów do prywatnych celów pracowników jest dozwolone jedynie na uzasadniony wniosek pracownika i za zgodą Specjalisty.
9. Zasoby Administratora powinny być przechowywane w taki sposób, aby zapobiec możliwości ich kradzieży lub uszkodzenia przez osoby postronne oraz przypadkowe uszkodzenia przez osoby lub czynniki środowiskowe.
10. Wynoszenie aktywów (zasobów i informacji) poza obszar przetwarzania danych możliwe jest za zgodą Specjalisty lub Administratora poza przypadkami, gdy jest to ujęte w planie praw dostępu.
11. Zakazane jest przesyłanie informacji podlegających ochronie na prywatne adresy poczty elektronicznej oraz prowadzenie korespondencji służbowej z wykorzystaniem prywatnego adresu e-mail użytkownika.
12. Zakazane jest używanie prywatnych nośników zewnętrznych (np. typu pendrive) i tworzenie nieautoryzowanych kopii z baz danych.
13. Pracownicy zobowiązani są stosować zasadę czystego biurka - wszystkie dokumenty i materiały powinny być po zakończeniu pracy chowane w przeznaczonych do tego szafkach, szufladach itp. W przypadku braku dostatecznej ilości dostępnego miejsca dokumenty i materiały powinny być pozostawiane na biurku uporządkowane.
14. Pracownicy są zobowiązani do ochrony zasobów będących własnością innych podmiotów, a powierzonych lub oddanych do dyspozycji Administratorowi lub udostępnionych pracownikom na czas wykonywania przez nich czynności

służbowych w takim samym stopniu jak w przypadku zasobów będących własnością Administratora.

POSTANOWIENIA KOŃCOWE

1. Do stosowania zasad określonych przez dokumenty POLITYKI zobowiązani są wszyscy pracownicy w rozumieniu przepisów Kodeksu pracy, konsultanci, współpracownicy, zleceniobiorcy, stażyści i inne osoby mające dostęp do informacji podlegającej ochronie.
2. Z treścią niniejszego dokumentu powinni zapoznać się wszyscy pracownicy i inne osoby mające dostęp do informacji przetwarzanej w jednostce, przed przystąpieniem do przetwarzania danych.
3. Niniejszy dokument może być przedstawiany podmiotom i jednostkom współpracującym, z którymi współpraca może skutkować możliwością dostępu do informacji chronionych.
4. Wobec osoby, która w przypadku naruszenia bezpieczeństwa informacji lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne lub porządkowe.
5. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która wobec naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym Specjalistę.
6. W przypadku naruszenia postanowień POLITYKI pracownik, który dopuścił się takiego naruszenia lub przyczynił do niego (umyślnie lub nieumyślnie), może zostać ukarany zgodnie z obowiązującym regulaminem pracy, obowiązującymi przepisami prawa z zakresu ochrony informacji, a w skrajnych przypadkach pociągnięty do odpowiedzialności karnej.
7. Umyślne lub nieumyślne naruszenie postanowień POLITYKI niestosowanie się do poleceń służbowych w tym zakresie może być potraktowane jako naruszenie obowiązków pracowniczych.
8. POLITYKA jest dokumentem wewnętrznym i nie może być udostępniana osobom postronnym w żadnej formie.

9. Użytkownicy są zobowiązani zapoznać się z treścią POLITYKI.
10. Użytkownik zobowiązany jest złożyć oświadczenie o tym, iż został zaznajomiony z zasadami i przepisami o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych, z niniejszą POLITYKĄ, a także zobowiązać się do ich przestrzegania.
11. Oświadczenia przechowywane są w aktach osobowych.
12. W sprawach nieuregulowanych w niniejszej POLITYCE mają zastosowanie aktualnie obowiązujące przepisy prawa w zakresie ochrony informacji.
13. Użytkownicy zobowiązani są do bezwzględnego stosowania postanowień zawartych w niniejszej POLITYCE. W wypadku odrębnych od zawartych w niniejszej POLITYCE uregulowań występujących w innych procedurach obowiązujących u Administratora danych użytkownicy mają obowiązek stosowania unormowań dalej idących, których stosowanie zapewni wyższy poziom ochrony informacji.