Członkostwo i składka Spa Club przystań Hotel & Spa

Członkinią Spa Club Przystań Hotel & Sp może zostać osoba, która spełni poniższe warunki:

- zostanie rekomendowana przez obecną Członkinię
- opłaci składkę członkowską

Dlaczego warto zostać Członkinią Spa Club Przystań Hotel & Spa

- w przypadku wydarzeń, organizowanych przez Przystań Hotel & Spa, których koszty w całości pokrywane są przez Partnerów Przystań Hotel&Spa Członkini nie ponosi kosztów uczestnictwa,
- Członkini Spa Club Przystań Hotel &Spa ma pierwszeństwo w uczestnictwie w wydarzeniach organizowanych przez Przystań Hotel & SPa (spotkaniach, warsztatach, itp.) jako uczestniczka
- Członkini Spa Club Przystań Hotel &Spa ma możliwość uczestnictwa w projektach medialnych Przystań Hotel & Spa i jej wydarzeniach
- Członkini Spa Club Przystań Hotel &Spa otrzymuje wszelkie przywileje kwartalne organizowane lub sponsorowane przez Przystań Hotel & Spa takie jak:
  treningi , prezenty i gifty do testowania,
- Członkini Spa Club Przystań Hotel &Spa otrzymuje wszelkie przywileje takie jak :
  - karta rabatowa obowiązująca w Restauracji Port
  - karta lojalnościowa w Spa Przystań Hotel & Spa wraz z nagrodami

Zasady opłacania składek członkowskich:

Składka członkowska wynosi PLN 125, 00 miesięcznie i może być opłacona:

- kwartalnie – PLN 375
- półrocznie – PLN 712,5 (z rabatem 5%)
- rocznie – PLN 1350 (z rabatem 10%)

Polityka Bezpieczeństwa Przetwarzania Danych Osobowych

1. Cel i źródła wymagań polityki bezpieczeństwa

Niniejszy dokument określa zasady bezpieczeństwa przetwarzania danych osobowych jakie powinny być przestrzegane i stosowane w Spa Club Przystań Hotel &Spa otrzymuje wszelkie przywileje , realizującej zadania związane z promocją przedsiębiorczości kobiet i wpieraniem kobiet, z siedzibą w Olsztynie, zwanej dalej Areon Sp z o o , przez osoby, które przetwarzają dane osobowe.

Stosowanie zasad określonych w niniejszym dokumencie ma na celu zapewnienie prawidłowej ochrony danych osobowych przetwarzanych przez Areon Sp z o o wynikającej z 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 oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) zwanym dalej RODO, oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

Polityka bezpieczeństwa w razie konieczności jest modyfikowana (np. wymogami prawa) lub wydawane są do niej stosowne załączniki na podstawie zarządzeń i/lub decyzji Administratora.

2. Zakres stosowania

Politykę stosuje w celu zabezpieczenia danych osobowych przetwarzanych tradycyjnie w wersji papierowej, na stacjonarnych i przenośnych elektronicznych nośnikach informacji (pen-drive, dyski zewnętrzne, płyty CD itp.) oraz w systemie informatycznym. W zakresie podmiotowym, POLITYKA obowiązuje wszystkie osoby współpracujące z Areon Spa z oo mające dostęp w jakiejkolwiek formie do danych osobowych. Powyższy zapis stosuje się także do osób niezatrudnionych bezpośrednio Areon Sp z o o, mające jednak dostęp w jakiejkolwiek formie do danych osobowych.

3. Bezpieczeństwo przetwarzania danych osobowych

Przez bezpieczeństwo przetwarzania danych osobowych rozumie się zapewnienie:

- poufności – właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom,
- integralności – właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
- rozliczalności- właściwości zapewniającej, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

4. Definicje

Na podstawie art. 4. RODO stosuje się następujące definicje na potrzeby polityki i w dziedzinie ochrony danych osobowych:

- „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,
- „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,
- „ograniczenie przetwarzania” – oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania,
- „profilowanie” – oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, 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,

- „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,
- „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,
- „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,
- „podmiot przetwarzający" – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora,
- „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,
- „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,
- „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,
- „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,
- „dane genetyczne" – oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej,

- „dane biometryczne” – oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne,
- „dane dotyczące zdrowia” – oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia,
- „przedsiębiorca”- oznacza osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą,
- „grupa przedsiębiorstw” – oznacza przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa przez nie kontrolowane,
- „organ nadzorczy” – oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51 RODO,
- „transgraniczne przetwarzanie” oznacza:
  a) przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności jednostek organizacyjnych w więcej, niż jednym państwie członkowskim administratora lub podmiotu przetwarzającego w Unii posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim; albo
  b) przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego w Unii, ale które znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim;

Administrator Danych Osobowych (ADO) – podmiot decydujący o celach i środkach przetwarzania danych osobowych, w przypadku niniejszej Polityki funkcję ADO Areon Sp zo o . Inspektor danych osobowych (IOD) – jeśli został powołany – posiada statut w podmiocie określony w art. 37 RODO i zasadach wskazanych w art. 38 i 39 RODO.

5. Odpowiedzialność

Obowiązki Administratora Danych Osobowych:

- podejmowanie odpowiednich i niezbędnych kroków mających na celu zapewnienie prawidłowej ochrony danych osobowych na podstawie art 24 i 32 RODO.

Zadania Inspektora Ochrony Danych:

- nadzorowanie przestrzegania zasad ochrony danych osobowych, między innymi rozporządzenia RODO w porozumieniu i współpracy z Administratorem Danych Osobowych (ADO) na postawie art. 37-39,
- nadzór nad wdrożeniem stosowanych środków organizacyjnych, technicznych i fizycznych w celu ochrony przetwarzania danych osobowych.

Osoby upoważnione do przetwarzania danych osobowych:

- do obowiązków osób upoważnionych do przetwarzania danych osobowych należy znajomość i stosowanie w możliwie największym zakresie wszelkich dostępnych środków ochrony

danych osobowych, w szczególności zasad określonych w art.29 RODO to jest, każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.

Do obowiązków należy również:

- zapoznanie się z regulacjami wewnętrznymi dotyczącymi ochrony danych osobowych w Areon Sp zo o w szczególności z Polityką danych osobowych,
- przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa oraz przyjętymi regulacjami,
- przetwarzanie danych osobowych wyłącznie za pomocą autoryzowanych urządzeń służbowych,
- udzielanie wyczerpujących wyjaśnień Administratorowi ochrony danych osobowych w toku prowadzonego przez niego sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
- zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczania, do których uzyskały dostęp w trakcie zatrudnienia, również po ustaniu zatrudnienia,
- informowania o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe Administratora ochrony danych osobowych.

6. Zarządzanie bezpieczeństwem danych osobowych

Podstawowe zasady:

- za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba przetwarzająca te dane w zakresie zgodnym z obowiązkami służbowymi oraz rolą sprawowaną w procesie przetwarzania danych,
- każda z osób mająca styczność z danymi osobowymi jest zobowiązana do ochrony danych osobowych oraz przetwarzania ich w granicach udzielonego jej upoważnienia,
- należy zapewnić poufność, integralność i rozliczalność przetwarzanych danych osobowych,
- należy stosować adekwatny do zmieniających się warunków i technologii poziom bezpieczeństwa przetwarzania danych osobowych.

Procedury postępowania z danymi osobowymi:

- dostęp do danych osobowych powinien być przyznawany zgodnie z zasadą wiedzy koniecznej,
- dane osobowe powinny być chronione przed nieuprawnionym dostępem i modyfikacją.

Upoważnienie do przetwarzania danych osobowych:

- do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez ADO,

- upoważnienia są wydawane indywidualnie przed rozpoczęciem przetwarzania danych osobowych,
- do przetwarzania danych osobowych może zostać dopuszczona wyłącznie osoba, która została przeszkolona przez ADO z przepisów dotyczących ochrony danych osobowych i podpisała oświadczenie, stanowiące załącznik nr 1 do Polityki,
- na podstawie podpisanego oświadczenia wydawane jest Upoważnienie do przetwarzania danych osobowych, stanowiącego załącznik nr 2 do Polityki,
- odwołanie Upoważnienia do przetwarzania danych osobowych następuje na podstawie dokumentu, stanowiącego załącznik nr 3 do Polityki,
- upoważnienia, o których mowa powyżej, przechowywane są w aktach osobowych pracownika i obowiązują do czasu ustania stosunku pracy lub cofnięcia upoważnienia do przetwarzania danych osobowych,
- ze względu na charakter prowadzonej działalności dokumenty dotyczące upoważnień, tj. załączniki nr 1-3, stanowią wzory, do wykorzystania w przyszłości.

Ewidencja osób upoważnionych.
Jeśli, poza ADO, inne osoby będą przetwarzały dane, na podstawie wydanych upoważnień, ADO zobowiązany jest do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych, (załącznik nr 4 do Polityki). Ewidencja zawiera w szczególności:

- imię i nazwisko osoby upoważnionej do przetwarzania danych osobowych,
- zakres upoważnienia do przetwarzania danych osobowych,
- identyfikator, jeżeli osoba upoważniona została zarejestrowana w systemie informatycznym, służącym do przetwarzania danych osobowych – jeśli konieczne,
- datę nadania i ustania uprawnień.

Zachowanie danych osobowych w tajemnicy:

- każda z osób, mająca styczność z danymi osobowymi, jest zobowiązana do zachowania w tajemnicy danych osobowych, do których ma lub będzie miała dostęp, w związku z wykonywaniem obowiązków pracowniczych, w ramach zadań służbowych lub zleconych,
- sposoby zabezpieczania danych osobowych, stosowane w FUNDACJI BUSINESS BOUTIQUE, stanowią tajemnicę pracodawcy oraz tajemnicę przedsiębiorstwa – w rozumieniu art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji,
- postępowanie sprzeczne z powyższymi zobowiązaniami jest ciężkim naruszeniem obowiązków pracowniczych z wszystkimi wynikającymi stąd konsekwencjami, z rozwiązaniem stosunku pracy włącznie (za naruszenie przepisów karnych ustawy o ochronie danych osobowych/ przepisów prawa cywilnego w przypadku umów cywilnoprawnych).

Zgodność:

- niniejsza Polityka jest aktualizowana wraz ze zmieniającymi się przepisami prawnymi, dotyczącymi ochronny danych osobowych oraz zmianami faktycznymi, w ramach FUNDACJI BUSINESS BOUTIQUE, które mogą powodować, iż zasady ochrony danych osobowych, określone w obowiązujących dokumentach, będą nieaktualne lub nieadekwatne,

- zmiany niniejszej Polityki wymagają przeglądu innych dokumentów dotyczących ochrony danych osobowych obowiązujących w FUNDACJI BUSINESS BOUTIQUE.

7. Zarządzanie usługami zewnętrznymi

Bezpieczeństwo usług zewnętrznych:

- należy zapewnić, aby usługi zewnętrzne były prowadzone wyłącznie zgodnie z wymaganiami bezpieczeństwa przetwarzania danych osobowych, obowiązującymi w Areon Sp zo o , wymaganiami umowy oraz wymaganiami prawa,
- wymagania bezpieczeństwa przetwarzania danych osobowych, zakres usług oraz poziom ich dostarczania należy określić w umowie świadczenia usług oraz, jeśli ma to zastosowanie, w odrębnej umowie powierzenia,
- należy zapewnić, aby użytkownicy, nie będący pracownikami Areon Spa zo o , posiadali Upoważnienie do przetwarzania danych osobowych, nadanych przez ADO i stosowali te same zasady bezpieczeństwa przetwarzania danych osobowych, co użytkownicy będący pracownikami,
- podmiot przetwarzający (zarządzający usługami zewnętrznymi), w przypadku stwierdzenia naruszenia ochrony danych osobowych, jest zobowiązany niezwłocznie (do 24 godzin) zgłosić ten fakt Administratorowi Danych osobowych.

Powierzanie przetwarzania danych osobowych:

- powierzenie przetwarzania danych osobowych może mieć miejsce wyłącznie na podstawie pisemnej umowy – Umowy Powierzenia danych osobowych (stanowiąca załącznik nr 7 do Polityki), określającej w szczególności zakres i cel przetwarzania danych,
- umowa musi określać również zakres odpowiedzialności podmiotu, któremu powierzono przetwarzanie danych z tytułu niewykonania lub nienależytego wykonania umowy,
- powierzenie przetwarzania danych osobowych musi uwzględniać wymogi określone w art. 28 RODO. W szczególności podmiot zewnętrzny, któremu ma zostać powierzone przetwarzanie danych osobowych, jest obowiązany przed rozpoczęciem przetwarzania danych do podjęcia środków organizacyjno-technicznych określonych w art 32-36 RODO,
- w umowach stanowiących podstawę powierzenia przetwarzania danych, eksploatacji systemu informatycznego lub części infrastruktury należy umieścić zobowiązanie podmiotu zewnętrznego do, przestrzegania niniejszej Polityki oraz zastosowania odpowiednich środków technicznych i organizacyjnych, zapewniających bezpieczeństwo i odpowiedni poziom ochrony danych,
- powierzenie przetwarzania danych nie oznacza zwolnienia z odpowiedzialności Areon Sp z o o za, zgodne z prawem, przetwarzanie powierzonych danych, co wymaga, w umowach stanowiących podstawę powierzenia przetwarzania danych, umieszczenia prawa Areon Sp zo o do kontroli wykonania przedmiotu umowy, w siedzibie pomiotu zewnętrznego, m.in. w zakresie przestrzegania Polityki obowiązujących regulacji wewnętrznych, umów i właściwych przepisów prawa.

Udostępnianie danych osobowych:

- dane osobowe mogą być udostępniane wyłącznie podmiotom uprawnionym do ich otrzymania, na mocy przepisów prawa oraz osobom, których dotyczą,
- udostępnianie danych osobowych może nastąpić wyłącznie za zgodą ADO,
- informacje zawierające dane osobowe powinny być przekazywane uprawnionym podmiotom lub osobom bezpiecznym sposobem, określonym wymogiem prawnym lub umową,
- udostępniając dane osobowe innym podmiotom, należy odnotować informacje o udostępnieniu bezpośrednio w systemie informatycznym, z którego udostępniono dane lub w inny zatwierdzony sposób. Odnotować należy: informacje o odbiorcy danych, dacie i zakresie udostępnionych danych osobowych, celu i czasie przetwarzania,
- udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.

8. Bezpieczeństwo fizyczne obszarów przetwarzania

Obszar przetwarzania.
Dane osobowe mogą być przetwarzane wyłącznie w obszarach przetwarzania danych osobowych, na które składają się pomieszczenia biurowe oraz innych pomieszczeń, gdzie Areon Sp z o o prowadzi działalność. Do takich pomieszczeń, zalicza się w szczególności:

- pomieszczenia biurowe, w których zlokalizowane są stacje robocze lub serwery służące do przetwarzania danych osobowych,
- pomieszczenia, w których przechowuje się dokumenty źródłowe oraz wydruki z systemu informatycznego zawierające dane osobowe,
- pomieszczenia, w których przechowywane są sprawne i uszkodzone urządzenia, elektroniczne, wszelkie inne nośniki informacji oraz kopie zapasowe zawierające dane osobowe,
- dopuszczalne jest przetwarzania danych osobowych poza pomieszczeniami biurowymi oraz częścią pomieszczeń, gdzie Areon Sp zo o prowadzi działalność, jeśli jest to uzasadnione charakterem czynności oraz każdorazowo zostało potwierdzone przez Administratora Danych, bądź postanowieniami umowy oraz pod warunkiem właściwego zabezpieczenia przetwarzanych danych osobowych.

Wykaz zawierający obszar przetwarzania danych stanowi załącznik nr 8.

Pomieszczenia, w których przetwarzane są dane osobowe, są zamykane podczas nieobecności osób upoważnionych do przetwarzania danych osobowych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.

Osoby upoważnione zobowiązane są do zamykania na klucz wszelkich pomieszczeń wchodzących w skład obszarów, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w pomieszczeniu, jak i po jej zakończeniu. Wydruki i nośniki elektroniczne zawierające dane osobowe należy zabezpieczyć przed dostępem do nich osób nieupoważnionych. Niepotrzebne wydruki lub inne dokumenty należy niszczyć za pomocą niszczarek.

Przebywanie wewnątrz obszarów przetwarzania danych osobowych osób nieuprawnionych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych.

Ewidencja osób upoważnionych do przetwarzania danych osobowych stanowi załącznik nr 4 do Polityki.

Instrukcja alarmowa:

- instrukcja definiuje sposób reakcji w przypadku zagrożenia i naruszenia bezpieczeństwa danych osobowych oraz opisuje sposób reagowania na nie. Celem instrukcji jest minimalizacja skutków wystąpienia powyższych incydentów bezpieczeństwa, ograniczenie ryzyka ich powstania zagrożeń i występowania w przyszłości,
- każdy pracownik w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych zobowiązany jest poinformować ADO,
- do typowych zagrożeń bezpieczeństwa danych osobowych należą:

1. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
2. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
3. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek),
4. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników dotyczących korespondencji e-mail, lub np. korzystanie w miejscu pracy z poczty prywatnej i/lub portali społecznościowych, dokonywania zakupów przez internet itp.,
5. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
6. zdarzenia losowe wewnętrzne (awarie sprzętu: serwera, komputerów, twardych dysków, awarii oprogramowania, pomyłki personelu: informatyków, użytkowników, utrata/zagubienie danych),
7. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania),
8. inne niekategoryzowane mogące wystąpić podczas przetwarzania danych osobowych, lub mające na te przetwarzanie wpływ.

- przeprowadza się ocenę skutków ryzyka ochrony danych, aby ocenić konkretne prawdopodobieństwo i powagę mogącego wystąpić wysokiego ryzyka, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz źródła ryzyka,
- ocena skutków w szczególności obejmuje planowane środki, zabezpieczenia i mechanizmy mające minimalizować to ryzyko, zapewniać ochronę danych osobowych oraz wykazać przestrzeganie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679,
- ocenę ryzyka przeprowadza się nie rzadziej niż co 3 lata o czym stanowi załącznik nr 9.
- w przypadku stwierdzenia wystąpienia zagrożenia ADO prowadzi postępowanie wyjaśniające, w toku którego:

1. ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,

2. inicjuje ewentualne działania dyscyplinarne,
3. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości,
4. dokumentuje prowadzone postępowania.

- w przypadku stwierdzenia naruszenia ADO prowadzi postępowanie wyjaśniające, w toku którego:

1. ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,
2. zabezpiecza ewentualne dowody,
3. ustala osoby odpowiedzialne za naruszenie,
4. podejmuje działania naprawcze po stwierdzeniu jakie mogły powstać ewentualne szkody dla podmiotów danych,
5. w ciągu 72 godzin powiadamia jeśli to konieczne organ nadzorczy dla spraw ochrony danych osobowych i /lub podmioty danych osobowych. Jeśli ADO uzna, że nie ma takiej konieczności sporządza odpowiednią notatkę, która jest przedstawiana w przypadku kontroli organu nadzorczego,
6. inicjuje działania dyscyplinarne,
7. wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,
8. dokumentuje prowadzone postępowania.

Procedura działań korygujących i zapobiegawczych:

- celem procedury jest uporządkowanie i przedstawienie czynności związanych z inicjowaniem oraz realizacją działań korygujących i zapobiegawczych wynikających z zaistnienia incydentów bezpieczeństwa lub zagrożeń systemu ochrony danych osobowych,
- procedura działań korygujących i zapobiegawczych obejmuje wszystkie czynności i procesy, w których zagrożenia lub naruszenia bezpieczeństwa mogą wpłynąć na zgodność z wymaganiami art 32-34 RODO, jak również na poprawne funkcjonowanie systemu ochrony danych osobowych,
- osobą odpowiedzialną za nadzór nad procedurą Areon sp z o o jest ADO.

Opis czynności:

- ADO jest odpowiedzialny za analizę zagrożeń lub naruszeń bezpieczeństwa ochrony danych osobowych. Typowymi źródłami informacji o incydentach, zagrożeniach lub lub naruszeniach są: zgłoszenia od pracowników, wiedza ADO, wyniki kontroli,
- w przypadku gdy ADO, stwierdzi konieczność podjęcia działań korygujących lub zapobiegawczych, określa źródło powstania zagrożeń lub naruszeń, zakres działań korygujących lub zapobiegawczych, termin realizacji, osobę odpowiedzialną,

- ADO jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych. ADO może skorzystać z zewnętrznego Inspektora ochrony danych stanowiącego w tym przypadku, rolę konsultacyjno-doradczą w celu zapewnienia wymogów RODO i innych przepisów dotyczących ochrony danych osobowych,
- po przeprowadzeniu działań korygujących lub zapobiegawczych ADO, jest zobowiązany do oceny efektywności ich zastosowania,
- sposób postępowania określa w przypadku wystąpienia naruszenia przedstawia załącznik nr 10 (Zasady postępowania przy zgłaszaniu naruszenia ochrony danych osobowych organowi nadzorczemu i osobom, których dane dotyczą).

Kontrola systemu ochrony danych osobowych:

- ADO może wprowadzić we własnym zakresie procedury w celu ustalenia porządku i czynności związanych z kontrolą stanu bezpieczeństwa danych osobowych,
- procedura obejmuje wówczas wszystkie procesy organizacji, gdzie przestrzeganie zasad ochrony danych osobowych jest wymagane,
- kontrolę stanu ochrony danych osobowych przeprowadza ADO,
- kontroli podlegają: systemy informatyczne przetwarzające dane osobowe, zabezpieczenia fizyczne, zabezpieczenia organizacyjne, bezpieczeństwo osobowe oraz zgodność stanu faktycznego z wymaganiami ustawy i aktów wykonawczych,
- kontrola powinna odbyć się co najmniej raz w roku a sprawdzenie winno uwzględniać zakres oraz czas wykonania sprawdzeń.

9. Rejestr czynności przetwarzania danych osobowych

Rejestr czynności przetwarzania stanowi załącznik nr 6 do Polityki. Rejestr ten jest aktualizowany na bieżąco. Dane osobowe gromadzone w rejestrach są przetwarzane w systemach informatycznych oraz w kartotekach ewidencyjnych, które są zlokalizowane w pomieszczeniach lub części pomieszczeń należących do obszaru przetwarzania danych osobowych.
Sposób przepływu danych pomiędzy systemami:

- obieg dokumentów zawierających dane osobowe, pomiędzy komórkami organizacyjnymi firmy, winien odbywać się w sposób zapewniający pełną ochronę przed ujawnieniem zawartych w tych dokumentach danych (informacji),
- przekazywanie informacji (danych) w systemie informatycznym poza sieć lokalną firmy, powinno odbywać się w sposób szyfrowany.

10. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia wymogów przetwarzania danych

Ochrona pomieszczeń wykorzystanych do przetwarzania danych osobowych:

- budynki i wszystkie pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone są przed dostępem osób nieuprawnionych,
- dokumentacja papierowa po godzinach pracy jest przechowywana w zamkniętych pomieszczeniach,

- przebywanie osób nieuprawnionych w obszarze przetwarzania danych osobowych jest dopuszczalne w obecności osoby upoważnionej do przetwarzania danych osobowych.

Przedsięwzięcia w zakresie zabezpieczenia sprzętu komputerowego:

- dla zapewnienia ciągłości działania systemów informatycznych służących do przetwarzania danych osobowych stosuje się w nich sprzęt oraz oprogramowanie wyprodukowane przez renomowanych producentów oraz zabezpiecza się sprzęt przed awarią zasilania lub zakłóceniami w sieci zasilającej,
- zbiory danych osobowych oraz programy służące do przetwarzania danych osobowych są zabezpieczane przed przypadkową utratą oraz celowym zniszczeniem poprzez wykonywanie kopii zapasowych,
- kopie zapasowe są usuwane niezwłocznie po ustaniu ich użyteczności.

Przedsięwzięcia w zakresie teletransmisji danych:

- w celu ochrony systemów informatycznych służących do przetwarzania danych osobowych przed zagrożeniami pochodzącymi z Internetu stosuje się zabezpieczenia chroniące przed nieuprawnionym dostępem.

Przedsięwzięcia w zakresie środków ochrony, w ramach oprogramowania systemów:

- w celu zapewnienia rozliczalności operacji dokonywanych przez użytkowników systemu informatycznego, w systemie tym dla każdego użytkownika rejestrowany jest odrębny identyfikator i hasło,
- w przypadku, gdy do uwierzytelnienia użytkowników używa się identyfikatora i hasła, które winno być na tyle bezpiecznie i tak przechowywane aby nie stanowiło zagrożenia do wystąpienia incydentu doprowadzającego do naruszenia ochrony danych osobowych,
- dobrą praktyką jest, aby hasło składało się z co najmniej 4-8 znaków, zawierać przynajmniej jedną małą, jedną dużą literę, oraz znak specjalny lub ciąg liter lub znaków trudny do zidentyfikowania przez osobę nieupoważnioną,
- hasła służące do uwierzytelnienia w systemach informatycznych służących do przetwarzania danych osobowych winny być zmieniane co najmniej kilka razy w roku.

Przedsięwzięcia w zakresie środków ochrony w ramach narzędzi baz danych i innych narzędzi programowych:

- w celu ochrony zbiorów danych osobowych prowadzonych w systemach informatycznych przed nieuprawnionym dostępem stosuje się mechanizmy kontroli dostępu do tych danych,
- system zapewnia automatyczne odnotowywanie w systemie informacji o identyfikatorze użytkownika, które wprowadził dane osobowe oraz dacie pierwszego wprowadzenia danych do systemu,
- zaleca się stosowanie oprogramowania umożliwiającego trwałe usunięcie danych osobowych z urządzeń, dysków, lub innych elektronicznych nośników informacji, które przeznaczone są do naprawy, przekazania lub likwidacji przez osobę nieuprawnioną.

Przedsięwzięcia w zakresie środków ochrony w ramach systemu użytkowego:

- w celu ochrony danych osobowych przetwarzanych na stacjach roboczych na czas krótkotrwałego opuszczenia stanowiska pracy przez użytkownika systemu, zaleca się stosować mechanizm blokady stacji roboczej zabezpieczony hasłem,
- stosuje się oprogramowania antywirusowe z automatyczną aktualizacją w celu ochrony systemu przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
- kontrola antywirusowa jest przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie jak i do celów instalacyjnych.

Przedsięwzięcia w zakresie środków organizacyjnych:

- prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych,
- dostęp do danych osobowych możliwy jest po uzyskaniu formalnego upoważnienia do przetwarzania danych osobowych wydanego przez upoważnione osoby,
- monitoruje się wdrożone zabezpieczenia systemu informatycznego.

Lista oprogramowań służących do przetwarzania danych osobowych stanowi załącznik nr 5 do Polityki.

Sposób przepływu danych znajduje się w dokumentacji technicznej eksploatowanego Oprogramowania użytkowego przechowywanej na Komputerach lub w postaci papierowej jeśli była dołączana do licencji.

11. Postanowienia końcowe

W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy:

- 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 oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
- Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych. Ustawa o ochronie danych osobowych stanowi akt uzupełniający do RODO.

Pracownicy i współpracownicy FUNDACJI BUSINESS BOUTIQUE zobowiązani są do stosowania, przy przetwarzaniu danych osobowych, postanowień zawartych w niniejszej Polityce. W wypadku odrębnych, od zawartych w niniejszej Polityce, uregulowań, występujących w innych procedurach, obowiązujących w FUNDACJI BUSINESS BOUTIQUE, użytkownicy mają obowiązek stosowania zapisów dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.