Polityka ochrony danych osobowych

instytut-witelon.pl

treninginterpersonalny.pl

DANE ADMINISTRATORA DANYCH:

Instytut Witelon Tomasz Waleczko

30-430 Kraków, ul. Podhalańska 18c/2

Telefon: 507087795

e-mail: biuro@instytut-witelon.pl

JAKI JEST CEL PRZETWARZANIA DANYCH?

Korzystając z naszych usług przekazują Państwo niektóre informacje- imię, nazwisko, mail, nr telefonu, dane psychometryczne, odpowiedzi w testach). Przekazanie tych danych jest dobrowolne i służy ulepszaniu usług i ich prawidłowemu wykonaniu. Dane podlegają ochronie opisanej w niniejsze polutyce.

Dane, które zbieramy i przechowujemy służą realizacji naszych usług (imię, nazwisko, mail, nr telefonu, dane psychometryczne):

- szkolenia: przygotowanie zaświadczeń, list obecności,
- testy i konsultacje: tworzenie zbiorczych raportów, indywidualizacja raportów i rozwiązań, dopasowanie konsultacji do klienta, statystyki

PROFILOWANIE

Dane są przetwarzane w chronionych programami systemach i nie są przekazywane nieupoważnionym przez Adm. Danych osobom trzecim. Dane te pomagają w tworzeniu profili i dostosowaniu programu usług do potrzeb klienta.

UPRAWNIENIA KLIENTÓW W ZAKRESIE PRZETWARZANIA DANYCH

W tym punkcie skorzystano z polityki opisanej przez politykbezpieczenstwa.pl

1. **Prawo dostępu- do 7 dni od zgłoszenia udostępnimy dane osoby**
2. **Prawo do sprostowanie danych- do 7 dni od zgłoszenia mamy obowiązek poprawić dane**
3. **Prawo do bycia zapomnianym- do 7 dni od zgłoszenia, mamy obowiązek usunąć dane**

Przesłanki usunięcia danych to między innymi:

- brak podstawy prawnej do przetwarzania danych (np. cofnięcie zgody na ich wykorzystywanie);
- zebrane dane nie są już potrzebne do celów, w których zostały one zgromadzone;
- dane zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego;
- wniesienie sprzeciwu przez osobę, której dane dotyczą (więcej o prawie sprzeciwu w dalszej części tekstu);
- dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator.

Istnieją również sytuacje, które sprawiają, że osoby, których dane dotyczą nie mogą skorzystać z prawa do usunięcia danych osobowych. Mowa tu o przypadkach, kiedy przetwarzanie jest niezbędne:

- w celu korzystania z prawa do wolności wypowiedzi i informacji;
- do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- w celu profilaktyki zdrowotnej (np. medycyna pracy, czy zapewnienie opieki zdrowotnej) ;
- do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych;
- do ustalenia, dochodzenia lub obrony roszczeń.

4. **Prawo do ograniczenia przetwarzania danych**

RODO przewiduje także możliwość wniesienia o ograniczenie przetwarzania danych. Okoliczności, w jakich osoba, której dane dotyczą może z tego prawa skorzystać wymienione są w art. 18 RODO:

- kiedy zgromadzone dane są nieprawidłowe — ograniczenie ich przetwarzania następuje do momentu, kiedy zostaną one poprawione;

- w momencie, kiedy nie ma podstawy prawnej do przetwarzania danych;
- kiedy nie są one potrzebne administratorowi danych osobowych, jednak potrzebuje ich osoba, do której one należą;
- w przypadku kiedy osoba, której dane dotyczą zgłosiła sprzeciw wobec przetwarzania danych — ograniczenie obowiązuje do momentu ustalenia, czy sprzeciw ten jest podstawny.

5. Prawo do przenoszenia danych

W artykule 20 RODO wprowadzone zostało kolejne prawo osób, których dane dotyczą — prawo do ich przenoszenia pomiędzy różnymi podmiotami (administratorami). Jeśli prośba taka zostanie wystosowana, administrator ma obowiązek przekazać osobie komplet zgromadzonych danych na jej temat w formie, która będzie możliwa do odczytania. Osoba, której dane dotyczą może później bez przeszkód przekazać te informacje innemu administratorowi.

6. Prawo do sprzeciwu oraz do niepodleganiu decyzji opartych na zautomatyzowanym przetwarzaniu

Na podstawie przepisu znajdującego się w artykule 21 RODO, osoby, których dane dotyczą mają prawo nie zgodzić się na to, aby ich dane były wykorzystywane do celów „podejmowania decyzji opartych na zautomatyzowanym przetwarzaniu"" – np. profilowania, które powodują skutek prawny dla osoby. Administrator w takim przypadku nie ma prawa do przetwarzania danych, pod warunkiem, że nie będą istniały inne ważne podstawy prawne do przetwarzania danych osobowych.

Wyjątek stanowi sytuacja, kiedy to przeprowadzenie profilowania jest wymagane w celu prawidłowego zawarcia bądź wykonania umowy – wtedy osoba, której dane dotyczą nie ma prawa do sprzeciwu wobec takiego przetwarzania

GDZIE ZWRÓCIĆ SIĘ PO WIĘCEJ INFORMACJI?

TOMASZ WALECZKO; biuro@instytut-witelon.pl;507087795

WSTĘP

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Instytut Witelon Tomasz Waleczko w celu spełnienia wymagań

Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO). Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

Instytut Witelon Tomasz Waleczko odnosi się do rozwiązań, opublikowanych na stronach internetowych www.instytut-witelon.pl oraz www.treninginterpersonalny.pl
które pozwalają użytkownikom na wzięcie udziału w:

- szkoleniach i kursach edukacyjnych,
- treningu interpersonalnym,
- badaniach ewaluacyjnych

oraz na korzystanie z usług psychologicznych (diagnoza).

DEFINICJE

Administrator (danych) – osoba prawna pod nazwą Instytut Witelon Tomasz Waleczko, która samodzielnie lub wspólnie z innymi osobami prawnymi określa cele i sposoby przetwarzania danych osobowych.
RODO – rozporządzenie parlamentu europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016)
Dane osobowe - wszelkie informacje związane z osobą fizyczną, przystępującą do korzystania z usług udostępnionych na stronach internetowych www.instytut-witelon.pl oraz www.treninginterpersonalny.pl
Przetwarzanie danych osobowych – operacje lub czynności, których przedmiotem są dane osobowe osoby fizycznej. Przetwarzanie może oznaczać takie procesy jak zbieranie, rejestrowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, wykorzystanie, ujawnianie, rozpowszechnianie lub udostępnianie w inny sposób, ograniczenie, usunięcie lub zniszczenie danych osobowych.

Ograniczenie przetwarzania – operacja polegająca na wyborze poszczególnych danych osobowych, których przyszłe przetwarzanie zostanie ograniczone.

Zgoda osoby, której dane dotyczą - oznacza dowolne, świadome i jednoznaczne wskazanie osoby fizycznej, której dane dotyczą, która za pośrednictwem oświadczenia lub innego wyraźnego działania potwierdzającego, wyrazi zgodę na przetwarzanie swoich danych osobowych dotyczących danego działania. Zgoda osoby fizycznej musi być udokumentowana w taki sposób, aby można ją było później udowodnić.

Podmiot danych - każda osoba fizyczna, której dane osobowe będą przetwarzane.

Odbiorca danych osobowych - osoba fizyczna lub prawna lub inny podmiot, któremu dane osobowe zostaną ujawnione na potrzeby konkretnego działania.

Podmiot przetwarzający (**Procesor)** - osoba fizyczna lub prawna przetwarzająca udostępnione dane osobowe na podstawie odrębnej umowy i w imieniu Administratora.

Inspektor Ochrony Danych (IOD) – osoba, która na podstawie formalnego wskazania została wyznaczona przez Administratora do prowadzenia następujących czynności: informowanie, konsultacje i doradztwa Administratorowi lub Podmiotowi przetwarzającemu lub pozostałym pracownikom w temacie obowiązującego przepisów dotyczących ochrony danych osobowych, informacji i rozwiązań zawartych w niniejszym dokumencie. IOD ma również obowiązek monitorowania prawidłowego przestrzegania zapisów niniejszego dokumentu oraz funkcjonowania jako osoba kontaktowa dla osób fizycznych, których dane osobowe są przetwarzane.

Naruszenie ochrony danych osobowych - przypadkowy lub niezgodny z prawem incydent, który doprowadził do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu osób trzecich do gromadzonych danych osobowych.

§ 1

1. Administratorem danych osobowych jest Instytut Witelon Tomasz Waleczko, ul. Podhalańska 18c/2 30-430 Kraków, Polska.
2. W przypadku zapytań związanych z przetwarzaniem danych osobowych przez Administratora, realizacji wszelkich praw przynależnych każdemu użytkownikowi, osobą odpowiedzialną jest Inspektor Ochrony Danych (IOD)- Tomasz Waleczko, z którym należy się kontaktować za pomocą adresu mailowego biuro@instytut-witelon.pl

3. W celu realizacji danej usługi Administrator przetwarza dane osobowe, których podanie jest niezbędne do wzięcia udziału w szkoleniach i kursach edukacyjnych, treningu interpersonalnym, badaniach ewaluacyjnych oraz korzystanie z usług psychologicznych (diagnoza), w tym także w celu obsługi ewentualnych reklamacji, rozwiązywania problemów technicznych.
4. Administrator zachowuje prawo do przetwarzania danych osobowych także w sytuacjach wynikających z przepisów obowiązującego prawa lub w celu zapewnienia bezpieczeństwa oferowanych usług, podnoszenia ich jakości lub wprowadzenia zmian technicznych.
5. Administrator zobowiązuje się także do przetwarzania danych osobowych w celach podatkowych zgodnie z obowiązującymi przepisami prawa.
6. Przy korzystaniu z usług dostępnych na stronach internetowych Administratora podanie danych osobowych jest dobrowolne, jednakże może być warunkiem niezbędnym do zawarcia umowy. W przypadku odmowy podania niezbędnych danych osobowych Instytut Witelon Tomasz Waleczko ma prawo do odmowy wykonania usługi.

§ 2

1. Zbierane dane osobowe wykorzystywane będą na własny użytek Administratora. W ramach swojej działalności Administrator ma prawo gromadzić i przetwarzać dane osobowe osób fizycznych chcących skorzystać z oferowanych usług. Administrator zobowiązany jest do przestrzegania wszystkich obowiązujących przepisów prawa oraz pozostałych regulacji dotyczących ochrony danych osobowych. W szczególności Administrator zobowiązany jest do:
   a) umożliwienia dostępu, zmiany, poprawienia lub usunięcia Informacji kontaktowych Klienta;
   b) zastosowania wszelkich uzasadnionych i dostępnych środków technicznych i organizacyjnych w celu zachowania poufności i integralności przetwarzanych danych osobowych Klienta oraz w celu zapobieżenia nieuprawnionemu ujawnieniu, dostępowi lub ich wykorzystaniu;
   c) nieprzekazywania danych osobowych Klienta osobom trzecim bez wyraźnej zgody osoby, której te dane dotyczą. Zaznacza się, że przetwarzane dane osobowe mogą być udostępnione instytucjom i organom państwowym, które są do tego upoważnione na podstawie powszechnie obowiązujących przepisów prawa.

§ 3

1. Na pisemny wniosek Klienta, po zakończeniu korzystania z usług lub w przypadku wygaśnięcia umowy lub jej wcześniejszego rozwiązania, Administrator przekaże Klientowi kopię wszystkich, możliwych do uzyskania danych osobowych i efektów korzystania z oferowanych usług. Administrator ma jednak prawo do tworzenia ogólnych danych statystycznych na podstawie zanonimizowanych danych osobowych i efektów korzystania z oferowanych usług dotyczących Klienta. Te anonimowe dane statystyczne będą własnością Administratora i mogą być przez niego wykorzystane po zakończeniu umowy.
2. Klient ma prawo żądania dostępu do swoich danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, a także prawo do wniesienia sprzeciwu wobec przetwarzania oraz prawo do przenoszenia danych.

§ 4

1. Zgodnie z określoną w art. 35 RODO procedurą przeprowadzenia analizy ryzyka, za jej wykonanie odpowiada Administrator. Analiza ryzyka powinna być przeprowadzona i zatwierdzona przy współudziale Inspektora Ochrony Danych.
2. Pierwszym etapem w procesie analizy ryzyka jest poprawne zidentyfikowanie zbieranych i przetwarzanych danych osobowych, które należy zabezpieczyć.
3. Opis zbiorów zbieranych i przetwarzanych danych osobowych będzie obejmować takie informacje, jak:
    a. nazwę zbioru, np. trening interpersonalny
    b. opis celów przetwarzania
    c. charakter i zakres danych osobowych
4. Administrator zobowiązuje się do spełnienia obowiązków prawnych wobec danych w zbiorach dla poszczególnych kategorii osób, a w szczególności:
    a) dane są legalnie przetwarzane (na podstawie art. 6, 9)
    b) dane są adekwatne w stosunku do celów przetwarzania
    c) dane są przetwarzane przez określony czas (retencja danych)

d) wobec osób powierzających dane osobowe zastosowany został obowiązek informacyjny (art. 12, 13 i 14) wraz ze wskazaniem ich prawa dostępu do danych, przenoszenia, zmiany, usunięcia, ograniczenia przetwarzania, odwołania zgody
e) opracowane zostały klauzule informacyjne.

5. Wszystkie działania dotyczące analizy ryzyka mają na celu odpowiednie zabezpieczenie danych osobowych, adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu osób trzecich do danych osobowych.

§ 5

1. Administrator ma prawo do nadawania i anulowania upoważnień do przetwarzania danych osobowych w zbiorach w postaci papierowej i elektronicznej.
2. Osoba upoważniona przez Administratora musi przetwarzać dane wyłącznie na jego polecenie administratora lub na podstawie przepisów prawa
3. Upoważnienia określają zakres operacji przeprowadzanych na zbiorach danych osobowych, np. tworzenie, usuwanie, wgląd, przekazywanie i są nadawane w formie udokumentowanego na piśmie zakresu obowiązków.
4. Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli, audytów, wykonania czynności służbowych, udokumentowanego polecenia administratora w postaci umowy powierzenia.
5. Administrator lub Inspektor Ochrony Danych prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych.
6. Po zapoznaniu się z zasadami ochrony danych osobowych, upoważnione osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania.

§ 6

1. Każda osoba upoważniona przed dopuszczeniem do pracy ze zbiorami danych osobowych musi zostać przeszkolona i zapoznana z przepisami RODO.
2. Za przeprowadzenie szkolenia odpowiada Inspektor Ochrony Danych Osobowych.

3. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych wskazane jest udokumentowanie odbycia tego szkolenia.
4. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania.

§ 7

1. W celu minimalizacji skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenia ryzyka powstania zagrożeń i występowania incydentów w przyszłości, Administrator ustanowił procedurę postępowania.
2. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu Inspektora Ochrony Danych.
3. Do typowych podatności bezpieczeństwa danych osobowych należą:
    a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
    b) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych
    c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników.
4. Do typowych incydentów bezpieczeństwa danych osobowych należą:
    a) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
    b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych)
    c) 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)
5. W przypadku stwierdzenia wystąpienia incydentu, Inspektor Danych Osobowych prowadzi postępowanie wyjaśniające w toku, którego:
    a) ustala zakres i przyczyny incydentu oraz jego ewentualne skutki
    b) inicjuje ewentualne działania dyscyplinarne
    c) działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu

d) rekomenduje działania prewencyjne zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia

6. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.
7. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych
8. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – Administrator zgłasza je organowi nadzorczemu.
9. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
10. Zgodnie z art. 32 RODO, Administrator jest zobowiązany do zapewnienia szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.