Estedentica Magdalena Jaszczak - Małkowska

NIP 1131538864

REGON 290899330

POLITYKA OCHRONY DANYCH OSOBOWYCH

Wersja:	0.1
Data wersji:	23.04.2018
Utworzony przez:	Baraniewski & Kawa Kancelaria Adwokacka, Spółka Jawna
Zatwierdzony przez:	Właściciela Firmy

Historia zmian

Data	Wersja	Wprowadzona przez	Opis zmiany
23.04.2018	0.1	Baraniewski & Kawa Kancelaria Adwokacka, Spółka Jawna	Wprowadzenie danych Firmy i osób odpowiedzialnych za ochronę danych osobowych w Firmie oraz lokalizacji przechowywania danych oraz osób odpowiedzialnych za ich ochronę

Spis treści

ul. Śniadeckich 10 • 00-656 Warszawa
+ 48 22 400 11 28 • + 48 606 137 033
biuro@baraniewski.pl

ul. Śniadeckich 10 • 00-656 Warszawa
+ 48 22 400 11 28 • + 48 606 137 033
biuro@baraniewski.pl

1. Cel, zakres i użytkownicy

Estedentica, w dalszej części dokumentu zwana “Firmą”, dąży do przestrzegania obowiązujących przepisów ustaw i rozporządzeń związanych z ochroną Danych Osobowych w krajach, w których Firma prowadzi działalność. Niniejsza Polityka określa podstawowe zasady, na podstawie których Firma przetwarza dane osobowe konsumentów, klientów, dostawców, partnerów biznesowych, pracowników i innych osób fizycznych, a także opisuje obowiązki oddziałów i pracowników w zakresie przetwarzania danych osobowych.

Użytkownikami niniejszego dokumentu są wszyscy pracownicy, zatrudnieni na stałe lub tymczasowo, oraz wszyscy wykonawcy pracujący na rzecz Firmy.

2. Dokumenty referencyjne

- RODO 2016/679 (Rozporządzenie (EU) 2016/679 Parlamentu Europejskiego i Rady 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)
- Projekt ustawy o Ochronie Danych Osobowych
- Polityka Ochrony Danych Osobowych Pracowników
- Polityka Zatrzymywania Danych
- Wytyczne dotyczące Rejestru Danych i Czynności Przetwarzania
- Wniosek Osoby, które Dane Dotyczą, o Udostępnienie Danych
- Wytyczne dotyczące Oceny Skutków w Zakresie Ochrony Danych
- Procedura Transgranicznego Przekazywania Danych Osobowych
- Polityka Bezpieczeństwa Informatycznego
- Polityka Kontroli Dostępu
- Polityka BYOD
- Polityka w zakresie urządzeń przenośnych i telepracy
- Polityka czystego biurka i czystego ekranu
- Procedura Zawiadomienia o Naruszeniu

3. Definicje

Poniższe definicje terminów zastosowanych w niniejszych dokumencie pochodzą z Artykułu 4 Ogólnego Rozporządzenia o Ochronie Danych Unii Europejskiej:

Dane Osobowe: Wszelkie 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.

ul. Śniadeckich 10 • 00-656 Warszawa
+ 48 22 400 11 28 • + 48 606 137 033
biuro@baraniewski.pl

Wrażliwe Dane Osobowe: Dane osobowe, które z racji swego charakteru są szczególnie wrażliwe w świetle podstawowych praw i wolności, wymagają szczególnej ochrony, gdyż kontekst ich przetwarzania może powodować poważne ryzyko dla podstawowych praw i wolności. Do takich danych osobowych zaliczają się dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby.

Administrator Danych: Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

Podmiot Przetwarzający Dane: Osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora.

Przetwarzanie: Operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka 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.

Anonimizacja: Nieodwracalnepozbawianie danych osobowych elementów pozwalających na identyfikację, przez co osoba nie może zostać zidentyfikowana przy rozsądnym nakładzie czasu, środków i za pomocą technologii przez administratora lub inną osobę. Zasady przetwarzania danych osobowych nie mają zastosowania do danych zanonimizowanych, ponieważ nie są to w dalszym ciągu dane osobowe.

Pseudonimizacja: Przetworzenie danych osobowych w taki sposób, by nie można ich było 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. Pseudonimizacjazmniejsza możliwość (lecz nie eliminuje jej całkowicie)przypisania danych osobowych osobie, której dane dotyczą. Ze względu na to, że spseudonimizowane dane są w dalszym ciągu danymi osobowymi, przetwarzanie spseudonimizowanych danych musi odbywać się zgodnie z zasadami Przetwarzania Danych Osobowych.

Transgraniczne Przetwarzanie Danych Osobowych: Przetwarzanie danych osobowych, które odbywa się 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 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.

Organ Nadzorczy: Niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z Art. 51 RODO.

ul. Śniadeckich 10 • 00-656 Warszawa
+ 48 22 400 11 28 • + 48 606 137 033
biuro@baraniewski.pl

Wiodący Organ Nadzorczy: Organ nadzorczy, na którym spoczywa główna odpowiedzialność za przeprowadzenie czynności transgranicznego przetwarzania danych, na przykład w sytuacji, gdy osoba, której dane dotyczą, wnosi skargę na przetwarzanie danych osobowych tej osoby; jest między innymi odpowiedzialny za przyjmowanie zawiadomień o naruszeniu ochrony danych osobowych, o czynnościach przetwarzania obarczonych ryzykiem i posiada pełne upoważnienie w zakresie swoich obowiązków do podjęcia czynności zapewniających przestrzeganie przepisów RODO.

Każdy „**lokalny organ nadzorczy**" będzie nadal sprawował kontrolę nad swoim terytorium i monitorował wszelkie podejmowane lokalnie czynności przetwarzania danych osobowych, które wpływają na osoby, których dane dotyczą, lub które są przeprowadzane przez administratora lub podmiot przetwarzający z UE lub spoza UE, gdy przetwarzanie dotyczy osób zamieszkujących jego terytorium. Do jego zadań i uprawnień należy przeprowadzanie dochodzenia, wdrażanie środków administracyjnych, nakładanie kar, zwiększanie wiedzy społeczeństwa o ryzyku, zasadach, bezpieczeństwie i prawach związanych z przetwarzaniem danych osobowych, a także uzyskanie dostępu do wszelkich pomieszczeń należących do administratora i podmiotu przetwarzającego, w tym do wszelkich urządzeń i środków służących do przetwarzania danych.

„Główna jednostka organizacyjna, jeśli chodzi o administratora"posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim – miejsce, w którym znajduje się jego centralna administracja w Unii, a jeżeli decyzje co do celów i sposobów przetwarzania danych osobowych zapadają w innej jednostce organizacyjnej tego administratora w Unii i ta jednostka organizacyjna ma prawo nakazać wykonanie takich decyzji, to za główną jednostkę organizacyjną uznaje się jednostkę organizacyjną, w której zapadają takie decyzje.

„Główna jednostka organizacyjna, jeśli chodzi o podmiot przetwarzający"posiadający jednostki organizacyjne w więcej niż jednym państwie członkowskim – miejsce, w którym znajduje się jego centralna administracja w Unii lub, w przypadku gdy podmiot przetwarzający nie ma centralnej administracji w Unii – jednostkę organizacyjną podmiotu przetwarzającego w Unii, w której odbywają się główne czynności przetwarzania w ramach działalności jednostki organizacyjnej podmiotu przetwarzającego, w zakresie w jakim podmiot przetwarzający podlega szczególnym obowiązkom na mocy niniejszego rozporządzenia.

Grupa przedsiębiorstw: Spółka dominująca wraz z jej podmiotami zależnymi.

4. Podstawowe zasady dotyczące przetwarzania danych osobowych

Zasady ochrony danych osobowych określają podstawowe obowiązki organizacji zajmujących się przetwarzaniem danych osobowych. Zgodnie z Art. 5 ust. 2 RODO „*administrator jest odpowiedzialny za przestrzeganie przepisów i musi być w stanie wykazać ich przestrzeganie*".

4.1. Zgodność z prawem,rzetelność i przejrzystość

Dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.

ul. Śniadeckich 10 • 00-656 Warszawa
+ 48 22 400 11 28 • + 48 606 137 033
biuro@baraniewski.pl

4.2. Ograniczenie celu

Dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

4.3. Minimalizacja danych

Dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. W miarę możliwości Firma musi zastosować anonimizację lub pseudonimizację podczas przetwarzania danych osobowych w celu zmniejszenia ryzyka naruszenia praw osób, których dane dotyczą.

4.4. Prawidłowość

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.

4.5. Ograniczenie przechowywania

Dane osobowe muszą być przechowywane przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.

4.6. Integralność i poufność

Uwzględniając stan wiedzy technicznej i inne dostępne środki bezpieczeństwa, koszty wdrożenia, prawdopodobieństwo i wagę zagrożenia danych osobowych, Firma musi zastosować odpowiednie środki techniczne lub organizacyjne w celu przetwarzania danych osobowych w sposób zapewniający odpowiednie ich bezpieczeństwo, w tym ochronę przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, zmianą, nieupoważnionym dostępem lub ujawnieniem.

4.7. Rozliczalność

Administratorzy są odpowiedzialni za przestrzeganie powyższych zasad i muszą być w stanie wykazać ich przestrzeganie.

5. Włączenie ochrony danych do działalności gospodarczej

Aby organizacja była w stanie wykazać przestrzeganie zasad ochrony danych, musi ona włączyć ochronę danych do swojej działalności gospodarczej.

5.1. Zawiadamianie osób, których dane dotyczą

(Zobacz ustęp na temat Wytycznych dotyczących Rzetelnego Przetwarzania.)

ul. Śniadeckich 10 • 00-656 Warszawa
+ 48 22 400 11 28 • + 48 606 137 033
biuro@baraniewski.pl

5.2. Decyzja i zgoda osoby, której dane dotyczą

(Zobacz ustęp na temat Wytycznych dotyczących Rzetelnego Przetwarzania.)

5.3. Gromadzenie

Firma musi dążyć do zebrania jak najmniejszej ilości danych osobowych. Jeśli dane osobowe są gromadzone od strony trzeciej, Pracownik Recepcji musi zapewnić, że dane osobowe będą gromadzone zgodnie z prawem.

5.4. Wykorzystanie, zatrzymanie i usuwanie

Cele, metody, ograniczenie przechowywania i okres zatrzymania danych osobowych muszą zgadzać się z informacjami zawartymi w Oświadczeniu o Ochronie Prywatności. Firma musi utrzymać integralność, poufność i aktualność danych osobowych zgodnie z celem przetwarzania. Należy wdrożyć odpowiednie środki bezpieczeństwa, aby zapewnić ochronę danych osobowych przed kradzieżą, niewłaściwym użyciem, nadużyciem czy naruszeniem. Pracownicy Recepcji są odpowiedzialni za zgodność z wymogami określonymi w niniejszym ustępie.

5.5. Ujawnienie danych stronom trzecim

W przypadku, gdy Firma zleca przetwarzanie danych osobowych w swoim imieniu zewnętrznemu dostawcy lub partnerowi biznesowemu, Dyrektor Zarządzający musi zapewnić, że taki podmiot przetwarzający wprowadzi środki bezpieczeństwa w celu zabezpieczenia danych osobowych, które odpowiadają związanemu z tym ryzyku. W tym celu należy skorzystać z Kwestionariusza Przestrzegania RODO przez Podmiot Przetwarzający.

Firma musi umownie zobowiązać dostawcę lub partnera biznesowego do zapewnienia takiego samego poziomu ochrony danych. Dostawca lub partner biznesowy mają prawo do przetwarzania danych osobowych jedynie w celu spełnienia zobowiązań umownych na rzecz Firmy lub na polecenie Firmy, lecz nie w innych celach. W przypadku, gdy Firma przetwarza dane osobowe razem z niezależną stroną trzecią, Firma musi wyraźnie określić swoje obowiązki oraz obowiązki strony trzeciej w odpowiedniej umowie lub innym prawnie wiążącym dokumencie, takim jak Umowa Powierzenia Dostawcy Przetwarzania Danych Osobowych.

5.6. Transgraniczne przekazywanie danych osobowych

Przed przekazaniem danych osobowych poza Europejski Obszar Gospodarczy (EOG) należy wdrożyć odpowiednie zabezpieczenia, w tym podpisać Umowę Przekazania Danych zgodnie z wymogiem Unii Europejskiej i uzyskać upoważnienie od odpowiedniego Organu właściwego w sprawach ochrony danych, jeśli istnieje taki wymóg. Podmiot otrzymujący dane osobowe musi przestrzegać zasad przetwarzania danych osobowych określonych w Procedurze Transgranicznego Przekazania Danych Osobowych.

ul. Śniadeckich 10 • 00-656 Warszawa
+ 48 22 400 11 28 • + 48 606 137 033
biuro@baraniewski.pl

5.7. Prawo dostępu osób, których dane dotyczą

Działając w charakterze administratora danych, Dyrektor Zarządzający jest odpowiedzialny za zapewnienie osobom, których dane dotyczą, rozsądnego mechanizmu dostępu do ich danych osobowych, i musi umożliwić im aktualizację, sprostowanie, usunięcie lub przesłanie ich Danych Osobowych, jeśli jest to stosowne lub wymagane przez prawo. Mechanizm dostępu zostanie bardziej szczegółowo opisany we Wniosku Osoby, której Dane Dotyczą, o Udostępnienie Danych.

5.8. Przenoszenie danych

Osoby, których dane dotyczą, mają prawo do otrzymania, na żądanie, kopii dostarczonych danych w ustrukturyzowanym formacie i do przekazania tych danych innemu administratorowi nieodpłatnie. Dyrektor Zarządzający jest odpowiedzialny za zapewnienie, że takie żądania zostaną rozpatrzone w ciągu jednego miesiąca, że nie są nadmierne i nie wpływają na prawa związane z danymi osobowymi innych osób fizycznych.

5.9. Prawo do bycia zapomnianym

Osoby, których dane dotyczą, mają prawo żądania od administratora usunięcia dotyczących ich danych osobowych. Jeśli Firma działa w charakterze Administratora, Dyrektor Zarządzający musi podjąć niezbędne działania (w tym zastosować środki techniczne), żeby zawiadomić strony trzecie korzystające z tych danych lub je przetwarzające o konieczności dostosowania się do żądania.

6. Wytyczne dotyczące rzetelnego przetwarzania

Dane osobowe mogą być przetwarzane tylko w przypadku wyraźnego upoważnienia Dyrektora Zarządzającego.

Firma musi zdecydować, czy należy przeprowadzić Ocenę Skutków w Zakresie Ochrony Danych dla każdej czynności przetwarzania danych zgodnie z Wytycznymi dotyczącymi Oceny Skutków w Zakresie Ochrony Danych.

6.1. Zawiadomienie osób, których dane dotyczą

W momencie zbierania danych osobowych lub przed ich zebraniem w celu dowolnego rodzaju czynności przetwarzania, w tym między innymi sprzedaży produktów, usług lub przeprowadzenia działań marketingowych, Dyrektor Zarządzający jest odpowiedzialny za właściwe poinformowanie osób, których dane dotyczą, o: rodzajach zbieranych danych osobowych, celach przetwarzania, metodach przetwarzania, prawach osób, których dane dotyczą, związanych z ich danymi osobowymi, okresie zatrzymania, możliwej międzynarodowej wymianie danych, o tym, czy dane zostaną przekazane stronom trzecim, a także środkach bezpieczeństwa Firmy stosowanych w celu ochrony danych osobowych. Informacje te zostaną zawarte w Oświadczeniu o Ochronie Prywatności.

Jeśli firma prowadzi wiele czynności przetwarzania danych, należy sporządzić różne oświadczenia, które zostaną dostosowane do rodzaju czynności przetwarzania i kategorii zbieranych danych oso-

ul. Śniadeckich 10 • 00-656 Warszawa
+ 48 22 400 11 28 • + 48 606 137 033
biuro@baraniewski.pl

bowych –na przykład jedno Oświadczenie może zostać przygotowane do celów mailingowych, a inne do celów wysyłkowych.

W przypadku, gdy dane osobowe są udostępniane stronom trzecim, Dyrektor Zarządzający musi zapewnić, by osoby, których dane dotyczą, zostały poinformowane o tym fakcie za pośrednictwem Oświadczenia o Ochronie Prywatności.

Jeśli dane osobowe są przekazywane do kraju trzeciego zgodnie z Polityką Transgranicznego Przekazywania Danych Osobowych, w Oświadczeniu o Ochronie Prywatności musi znaleźć się o tym informacja, a także jasne określenie tego, jakim krajom i jakim podmiotom przekazywane są dane osobowe.

W przypadku zbierania wrażliwych danych osobowych, Dyrektor Zarządzający lub, w przypadku jego wyznaczenia, Inspektor Ochrony Danych musi upewnić się, że Oświadczenie o Ochronie Prywatności zawiera wyraźną informację o celu gromadzenia wrażliwych danych osobowych.

6.2. Uzyskanie zgody

W przypadku, gdy dane osobowe są przetwarzane na podstawie zgody osoby, której dane dotyczą, lub w oparciu o inne, zgodne z prawem podstawy, Dyrektor Zarządzający jest odpowiedzialny za prowadzenie rejestru takich zgód. Dyrektor Zarządzający jest odpowiedzialny za zapewnienie osobom, których dane dotyczą, możliwości wyrażenia zgody i musi poinformować takie osoby oraz zapewnić, że ich zgoda (w przypadku, gdy stanowi ona zgodną z prawem podstawę przetwarzania) może zostać wycofana w dowolnym czasie.

W przypadku zbierania danych osobowych od dziecka poniżej 16 roku życia, Dyrektor Zarządzający musi zapewnić, by przed zebraniem uzyskana została zgoda rodzicielska za pośrednictwem Formularza Zgody Rodzicielskiej.

W przypadku żądań skorygowania, poprawy lub zniszczenia wpisów danych osobowych Dyrektor Zarządzający musi zapewnić, by żądania te zostały rozpatrzone w rozsądnym terminie. Dyrektor Zarządzający musi również prowadzić rejestr takich żądań.

Dane osobowe mogą być przetwarzane jedynie w celu, w którym zostały pierwotnie zebrane. W przypadku, gdy Firma zamierza przetwarzać zebrane dane osobowe w innym celu, musi ona uzyskać zgodę osób, których dane dotyczą, w jasnej i zwięzłej formie pisemnej. Prośba musi zawierać informacje o pierwotnym celu, w którym zebrane zostały dane, oraz nowym, dodatkowym celu (celach). Ponadto prośba musi zawierać powód zmiany celu (celów). Dyrektor Zarządzający jest odpowiedzialny za przestrzeganie zasad wymienionych w niniejszym akapicie.

Obecnie i w przyszłości Dyrektor Zarządzający musi zapewnić, że metody gromadzenia są zgodne z obowiązującym prawem, dobrą praktyką i normami branżowymi.

Dyrektor Zarządzający jest odpowiedzialny za stworzenie i prowadzenie Rejestru Oświadczeń o Ochronie Prywatności.

ul. Śniadeckich 10 • 00-656 Warszawa
+ 48 22 400 11 28 • + 48 606 137 033
biuro@baraniewski.pl

7. Organizacja i obowiązki

Odpowiedzialność za zapewnienie właściwego przetwarzania danych osobowych spoczywa na wszystkich osobach, które pracują dla Firmy lub z Firmą i mają dostęp do danych osobowych przetwarzanych przez Firmę.

Za kluczowe obszary przetwarzania danych osobowych odpowiadają jednostki o następujących funkcjach w organizacji:

Dyrektor Zarządzający podejmuje decyzje na temat ogólnych strategii Firmy w zakresie ochrony danych osobowych i zatwierdza te strategie.

Dyrektor Zarządzający jest odpowiedzialny za zarządzanie programem ochrony danych osobowych oraz opracowaniem i promowaniem polityk kompleksowej ochrony danych osobowych.

Dyrektor Zarządzający monitoruje i analizuje przepisy ustaw i zmiany w rozporządzeniach dotyczących danych osobowych, opracowuje wymogi w zakresie zgodności i wspiera działy biznesowe w realizacji celów związanych z danymi osobowymi.

Dyrektor Zarządzający jest odpowiedzialny za:

- Zapewnienie, by wszystkie systemy, usługi i urządzenia wykorzystywane do przechowywania danych spełniały dopuszczalne normy bezpieczeństwa.
- Przeprowadzanie regularnych kontroli i analiz, aby zagwarantować, że sprzęt komputerowy i oprogramowanie służące do zapewnienia bezpieczeństwa funkcjonują poprawnie.

Dyrektor Zarządzający jest odpowiedzialny za:

- Zatwierdzanie wszelkich oświadczeń na temat ochrony danych załączonych do korespondencji, na przykład wiadomości e-mail i listów.
- Odpowiadanie na wszelkie zapytania odnośnie do ochrony danych wystosowane przez dziennikarzy lub serwisy medialne takie jak gazety.
- W razie konieczności, współpracę z Właścicielem w celu zapewnienia, by działania marketingowe były zgodne z zasadami ochrony danych.

Dyrektor Zarządzający jest odpowiedzialny za:

- Zwiększanie wiedzy wszystkich pracowników na temat ochrony danych osobowych użytkownika.
- Organizowanie szkoleń na temat ochrony danych osobowych dla pracowników zajmujących się danymi osobowymi.
- Kompleksową ochronę danych osobowych pracowników. Dyrektor Zarządzający musi zapewnić, by dane osobowe pracowników były przetwarzane według uzasadnionych celów biznesowych pracodawcy i zgodnie z zasadą konieczności.

Dyrektor Zarządzający jest odpowiedzialny za zobowiązanie dostawców do spełnienia obowiązków związanych z ochroną danych osobowych, zwiększenie wiedzy dostawców na temat ochrony danych osobowych oraz przekazanie wymogów dotyczących danych osobowych wszystkim stronom trzecim,

ul. Śniadeckich 10 • 00-656 Warszawa
+ 48 22 400 11 28 • + 48 606 137 033
biuro@baraniewski.pl

z których usług korzysta dostawca. Odpowiedni Pracownik musi zapewnić, by Firma zastrzegała sobie prawo do przeprowadzenia audytu u dostawców.

8. Wytyczne dotyczące wyznaczenia wiodącego organu nadzorczego

8.1. Konieczność wyznaczenia wiodącego organu nadzorczego

Ustanowienie Wiodącego Organu Nadzorczego jest konieczne tylko wtedy, gdy Firma prowadzi transgraniczne przetwarzanie danych osobowych.

Transgraniczne przetwarzanie danych osobowych ma miejsce wtedy, gdy:

a) *przetwarzanie danych osobowych jest prowadzone przez podmioty zależne Firmy, których siedziba znajduje się w innych państwach członkowskich;*

lub

b) *przetwarzanie danych osobowych odbywa się w pojedynczej jednostce organizacyjnej Firmy w Unii Europejskiej, ale znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim.*

Jeśli Firma posiada jednostki organizacyjne wyłącznie w jedynym państwie członkowskim, a jej czynności przetwarzania wpływają tylko na osoby, których dane dotyczą, w tym państwie członkowskim, nie jest konieczne wyznaczanie wiodącego organu nadzorczego. Jedynym właściwym organem będzie Organ Nadzorczy w kraju, w którym Firma została należycie utworzona.

8.2. Główna jednostka organizacyjna i wiodący organ nadzorczy

8.2.1. Główna jednostka organizacyjna dla administratora danych

Dyrektor Zarządzający musi wskazać główną jednostkę organizacyjną, aby możliwe było wyznaczenie wiodącego organu nadzorczego.

Jeśli siedziba Firmy znajduje się w państwie członkowskim UE i Firma podejmuje decyzje związane z czynnościami transgranicznego przetwarzania w siedzibie swojej centralnej administracji, wyznaczony zostanie jeden wiodący organ nadzorczy w zakresie czynności przetwarzania danych osobowych prowadzonych przez Firmę.

W przypadku, gdy Firma posiada wiele jednostek organizacyjnych, które działają niezależnie od siebie i podejmują decyzje na temat celów i metod przetwarzania danych osobowych, Dyrektor Zarządzający musi potwierdzić, że istnieje więcej niż jeden wiodący organ nadzorczy.

8.2.2. Główna jednostka organizacyjna dla podmiotu przetwarzającego dane

W przypadku, gdy Firma działa w charakterze podmiotu przetwarzającego dane, główną jednostką organizacyjną będzie siedziba centralnej administracji. Jeśli siedziba centralnej administracji nie znaj-

ul. Śniadeckich 10 • 00-656 Warszawa
+ 48 22 400 11 28 • + 48 606 137 033
biuro@baraniewski.pl

duje się na terytorium UE, główną jednostką organizacyjną będzie jednostka organizacyjna na terenie UE, w której odbywają się główne czynności przetwarzania.

8.2.3. Główna jednostka organizacyjna dla Firm spoza UE dla administratorów i podmiotów przetwarzających

Jeśli główna jednostka organizacyjna Firmy nie znajduje się w UE, a jej podmioty zależne znajdują się na terenie UE, właściwym organem nadzorczym jest lokalny organ nadzorczy.

Jeśli ani główna jednostka organizacyjna Firmy, ani je podmioty zależne nie znajduje się w UE, Firma musi wyznaczyć przedstawiciela w UE, a właściwym organem nadzorczym będzie lokalny organ nadzorczy, w którym swoją siedzibę ma przedstawiciel.

9. Reagowanie na przypadki naruszenia ochrony danych osobowych

W przypadku, gdy Firma wykryje naruszenie ochrony danych osobowych lub będzie podejrzewać wystąpienie takiego naruszenia, Dyrektor Zarządzający jest zobowiązany do niezwłocznego przeprowadzenia wewnętrznego dochodzenia i podjęcia właściwych środków naprawczych zgodnie z Polityką w zakresie Naruszenia Ochrony Danych. Jeśli istnieje ryzyko naruszenia praw i wolności osób, których dane dotyczą, Firma musi niezwłocznie, a jeśli to możliwe, w ciągu 72 godzin zawiadomić odpowiednie organy ochrony danych.

10.Audyt i rozliczalność

Dyrektor Zarządzający jest odpowiedzialny za przeprowadzenie audytu w celu oceny stopnia wdrożenia niniejszej Polityki przez działy biznesowe.

Pracownik, który nie przestrzega niniejszej Polityki, będzie podlegał postępowaniu dyscyplinarnemu, ponadto, jeśli swoim postępowaniem narusza przepisy ustaw i rozporządzeń, może zostać pociągnięty do odpowiedzialności cywilnej lub karnej.

11.Przepisy kolizyjne

Celem niniejszej Polityki jest zgodność z przepisami ustaw i rozporządzeń obowiązujących w miejscu, w którym znajduje się jednostka organizacyjna, i w państwach, w których Estedentica prowadzi działalność. W przypadku jakichkolwiek sprzeczności między niniejszą Polityką a obowiązującymi przepisami ustaw i rozporządzeń moc rozstrzygającą będą miały przepisy ustaw i rozporządzeń.

ul. Śniadeckich 10 • 00-656 Warszawa
+ 48 22 400 11 28 • + 48 606 137 033
biuro@baraniewski.pl

12.Zarządzanie dokumentacją przechowywaną na podstawie niniejszego dokumentu

Nazwa dokumentu	Lokalizacja przechowywania	Osoba odpowiedzialna za przechowywanie	Kontrola ochrony folderu	Okres zatrzymania
Formularz Zgody Osoby, której Dane Dotyczą	Serwer wewnętrzny/Rodo/Ogólny/ Formularz Zgody Osoby, której Dane Dotyczą	Pracownik Recepcji	Jedynie upoważnione osoby mają dostęp do formularzy	10 lat
Formularz Wycofania Zgody Osoby, której Dane Dotyczą	Serwer wewnętrzny/Rodo /Ogólny/Formularz Wycofania Zgody Osoby, której Dane Dotyczą	Pracownik Recepcji	Jedynie upoważnione osoby mają dostęp do formularzy	10 lat
Formularz Zgody Rodzicielskiej	Serwer wewnętrzny/Rodo /Ogólny/Formularz Zgody Rodzicielskiej	Pracownik Recepcji	Jedynie upoważnione osoby mają dostęp do formularzy	10 lat
Formularz Wycofania Zgody Rodzicielskiej	Serwer wewnętrzny/Rodo /Ogólny/Formularz Wycofania Zgody Rodzicielskiej	Pracownik Recepcji	Jedynie upoważnione osoby mają dostęp do formularzy	10 lat
Umowy Powierzenia Dostawcy Przetwarzania Danych Osobowych	Serwer wewnętrzny/Rodo /Ogólny/Umowy Powierzenia Dostawcy Przetwarzania Danych Osobowych	Dyrektor Zarządzający	Jedynie upoważnione osoby mają dostęp do formularzy	5 lat po wygaśnięciu umowy
Rejestr Oświadczeń o Ochronie Prywatności	Serwer wewnętrzny/Rodo /Ogólny/Rejestr Oświadczeń o Ochronie Prywatności	Dyrektor Zarządzający	Jedynie upoważnione osoby mają dostęp do formularzy	Na stałe

ul. Śniadeckich 10 • 00-656 Warszawa
+ 48 22 400 11 28 • + 48 606 137 033
biuro@baraniewski.pl

13.Ważność dokumentu i zarządzanie dokumentem

Dokument obowiązuje od dnia 25.05.2018 r.

Dysponentem dokumentu jest Dyrektor Zarządzający, który jest zobowiązany do sprawdzenia dokumentu i, w razie konieczności, jego aktualizacji przynajmniej raz w roku.

Dyrektor Zarządzający
Krzysztof Małkowski

_____

[podpis]

ul. Śniadeckich 10 • 00-656 Warszawa
+ 48 22 400 11 28 • + 48 606 137 033
biuro@baraniewski.pl