POLITYKA BEZPIECZEŃSTWA INFORMACJI

W FIRMIE

IMILK

Wersja:	01/2018
Data wersji:	30.11.2018 r.
Utworzony przez:	
Zatwierdzony przez:	
Poziom poufności:	1

Listopad 2018

Spis treści

1. Postanowienia ogólne

Realizując obowiązki wynikające z przepisów dotyczących ochrony danych osobowych, firma IMILK Sylwia Margasińska (dalej: **„IMILK”**) zmierza do spełnienia wymagań chroniących prywatność i godność każdego klienta oraz kontrahenta firmy.

Sposób przetwarzania danych osobowych w firmie **IMILK** oraz środki techniczne i organizacyjne, zapewniające ochronę przetwarzanych danych osobowych, ujęte zostały zbiorczo w niniejszym dokumencie określającym **Politykę Bezpieczeństwa Informacji (PBI).** PBI należy rozumieć jako zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji, zarówno wewnątrz jak i na zewnątrz organizacji. Zwraca ona uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Celem opracowania Polityki Bezpieczeństwa Informacji jest określenie zasad ochrony danych osobowych przetwarzanych w firmie **IMILK**, a co za tym idzie organizacyjne, fizyczne i logiczne zabezpieczenia posiadanych danych osobowych. Utrzymanie bezpieczeństwa przetwarzanych przez **IMILK** danych osobowych oraz informacji rozumiane jest jako zapewnienie ich poufności, integralności i dostępności oraz rozliczalności, na jak najwyższym, możliwym do uzyskania w danym czasie, poziomie. Pośrednim celem PBI jest systematyczne edukowanie użytkowników systemu ochrony danych osobowych. Jednocześnie deklaruje zaangażowanie właściciela do Zarządzania Bezpieczeństwem Informacji.

Polityka Bezpieczeństwa Informacji zapewnia:

- **poufność** – informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom i procesom;
- **integralność** – dane nie zostają zmienione lub zniszczone w sposób nieautoryzowany;
- **dostępność** – istnieje możliwość wykorzystania ich na żądanie, w założonym czasie, przez autoryzowany podmiot;

- **rozliczalność** – możliwość jednoznacznego przypisania działań poszczególnym osobom;
- **autentyczność** – zapewnienie, że tożsamość podmiotu lub zasobu jest zgodna z zadeklarowaną;
- **niezaprzeczalność** – uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne;
- **niezawodność** – zamierzone zachowania i skutki są spójne.

Wszystkie podmioty zewnętrzne, którym udostępniane są dane, zobowiązane są przestrzegać Zasad Bezpieczeństwa Informacji określonych w Polityce Bezpieczeństwa Informacji, a także współpracować we wdrażaniu oraz doskonaleniu procedur ochrony informacji poprzez m.in. zgłaszanie uwag i opiniowanie zastosowanych rozwiązań.

Odpowiedzialność za realizację ochrony danych ponoszą wszyscy użytkownicy w proporcjonalnie nadanych uprawnieniach.

Polityka Bezpieczeństwa Informacji została opracowana na podstawie:

- 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);
- Normy PN-EN ISO/IEC 27001 dotyczącej zarządzania bezpieczeństwem informacji;
- Normy PN-ISO/IEC 17799 dotyczącej praktycznych zasad zarządzania bezpieczeństwem informacji;
- Normy PN-EN ISO/IEC 27002 dotyczącej praktycznych zasad zabezpieczania informacji;
- Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 r. poz. 1000);

2. Definicje

Użyte w niniejszej dokumentacji przetwarzania danych osobowych definicje i pojęcia są wspólne dla wszystkich pozostałych dokumentów, które zostały przyjęte przez Administratora w zakresie ochrony danych osobowych.

Tabela 1. Zbiór definicji i pojęć używanych w dokumencie

Administrator Danych	Organ, jednostka organizacyjna, podmiot lub osoba, która decyduje o celach i środkach przetwarzania danych osobowych. W niniejszej dokumentacji przez Administratora Danych rozumie się **IMILK.**
Bezpieczeństwo danych osobowych	Zachowanie poufności, integralności i dostępności danych osobowych oraz odporności systemów i usług przetwarzania.
Dane osobowe (lub „dane")	Wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby.
Dostępność	Właściwość bycia dostępnym i użytecznym na zadanie autoryzowanego podmiotu [źródło ISO/IEC 27000].
Działanie korygujące	Działanie w celu wyeliminowania przyczyny wykrytej niezgodności lub innej niepożądanej sytuacji [źródło: ISO 9000].
Działanie zapobiegawcze	Działanie w celu wyeliminowania przyczyny potencjalnej niezgodności lub innej potencjalnej sytuacji niepożądanej [źródło: ISO 9000].
Urząd Ochrony Danych Osobowych (UODO)	Organ ochrony danych osobowych.
Grupa zasobów	Zbiór zasobów rozpatrywanych wspólnie ze względu na podobny charakter i funkcjonalność.

Incydent związany z bezpieczeństwem danych osobowych	Pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem danych osobowych, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych, w tym zgodności z RODO i zagrażają bezpieczeństwu danych osobowych.
Integralność	Właściwość polegająca na zapewnieniu dokładności i kompletności zasobów [źródło: ISO/IEC 27000].
Osoba fizyczna możliwa do zidentyfikowania	Osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności poprzez powołanie się na numer identyfikacyjny lub specyficzny czynnik/czynniki określające jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.
Osoba upoważniona	Osoba, która otrzymała od Administratora upoważnienie do przetwarzania danych.
Podatność	Słabość zasobu lub zabezpieczenia, która może być wykorzystana przez zagrożenie [źródło: ISO/IEC 27000].
Poufność	Właściwość polegająca na tym, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom [źródło: ISO/IEC 27000].
Przetwarzanie danych	Jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te operacje, które wykonuje się w systemach informatycznych.
RODO	Rozporządzenie 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
Skuteczność	Stopień, w jakim zaplanowane działania są realizowane, a zaplanowane rezultaty osiągnięte [źródło: ISO 9000].
Skutek	Negatywna zmiana w odniesieniu do poziomu osiągania zgodności z RODO.
Upoważnienie	Oświadczenie nadawane przez Administratora wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane we wskazanym zakresie.
Właściciel zasobu	Osoba lub podmiot, który ma zatwierdzoną kierowniczą odpowiedzialność w organizacji za nadzorowanie produkcji, rozwój, utrzymanie, korzystanie i bezpieczeństwo zasobów. Pojęcie to nie oznacza, że osoba ta rzeczywiście posiada jakiekolwiek prawa własności do zasobu.
Zabezpieczenie	Środki służące zarządzaniu ryzykiem, łącznie z politykami, procedurami, zaleceniami, praktyką lub strukturami organizacyjnymi, które mogą mieć naturę administracyjną, techniczną, zarządczą lub prawną [źródło: ISO/IEC 27000].
Zbiór danych	Każdy posiadający strukturę zestaw danych, o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
Zasoby	Wszystko, co ma wartość dla każdego, kto zajmuje się przetwarzaniem informacji umożliwiających identyfikację osoby fizycznej [źródło: ISO/IEC 29134:2017].
Zagrożenie	Potencjalna przyczyna niepożądanego incydentu, który może wywołać naruszenie praw lub wolności osób fizycznych. Skoordynowane działania kierowania i zarządzania

	organizacją z uwzględnieniem ryzyka [źródło: PKN-ISO Guide 73].
Zdarzenie	Wystąpienie szczególnego zbioru okoliczności [źródło: PKN-ISO Guide 73].
Zdarzenie związane z bezpieczeństwem danych osobowych	Określony stan systemu, usługi lub sieci, który wskazuje na możliwe naruszenie bezpieczeństwa danych osobowych, błąd zabezpieczenia lub nieznana dotychczas sytuacje, która może być związana z bezpieczeństwem danych osobowych.

Źródło: Opracowanie własne

3. Ogólne Rozporządzenie o Ochronie Danych Osobowych (RODO)

Parlament Europejski i Rada przyjęły Rozporządzenie 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), zwane w skrócie RODO. W polskim porządku prawnym jest ono stosowane bezpośrednio, od dnia 25 maja 2018 r., bez konieczności implementowania go ustawą.

Po wejściu w życie RODO przetwarzanie danych osobowych odbywa się w nowym otoczeniu prawnym. Celem niniejszego wprowadzenia jest jak najbardziej przystępne i syntetyczne objaśnienie zmian w dziedzinie ochrony danych osobowych, w taki sposób, aby każdy posiadł podstawową wiedzę o tym, w jaki sposób wprowadzić i przestrzegać zasad RODO.

We wprowadzeniu zostaną zasygnalizowane następujące kwestie:

- zgód na przetwarzanie danych osobowych;
- obowiązku informacyjnego;
- nowych praw podmiotów danych;
- rejestru czynności przetwarzania danych;

- zgłaszania naruszeń ochrony danych osobowych;
- powierzania przetwarzania danych;
- kodeksów i certyfikatów zgodności przetwarzania danych.

W świetle zmian wprowadzanych przez RODO, przedsiębiorcy (czyli administratorzy danych) w pierwszej kolejności powinni dokonać audytu zbiorów danych osobowych i podstaw prawnych stosowanych w ich organizacjach do przetwarzania danych.

Z uwagi na to, że jedną z najczęściej stosowanych podstaw przetwarzania danych jest zgoda osoby, której dane dotyczą (czyli podmiotu danych), RODO szczególnie odnośni się do kształtu zgody i jej założeń, które przechodzą ewolucje.

Zgodnie z RODO zgoda osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome, jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych w formie ustnej, pisemnej lub elektronicznej. Może to polegać na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej, na wyborze ustawień technicznych do korzystania z usług społeczeństwa informacyjnego lub też na innym oświadczeniu, bądź zachowaniu, które w danym kontekście jasno wskazuje, że podmiot danych zaakceptował proponowane przetwarzanie jej danych osobowych. Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie powinny być traktowane jako wyrażenie zgody.

Dla osób fizycznych przetwarzanie ich danych osobowych powinno być jasne, przejrzyste i rzetelne. Celem realizacji wymienionych przymiotów legalnego przetwarzania danych podmiot powinien posiadać wiedzę w przedmiocie tego, kto i po co przetwarza jego dane osobowe. Jednym z narzędzi zapewniających legalność przetwarzania jest obowiązek informacyjny, tj. zakres informacji, które administrator danych powinien przekazać podmiotowi danych w związku z przetwarzaniem jego danych osobowych.

Zgodnie z RODO, Administrator danych w przypadku pozyskiwania informacji od osoby, której one dotyczą, jest zobowiązany do podania:

- swojej tożsamości, pełnej nazwy i danych kontaktowych;
- danych kontaktowych Inspektora Ochrony Danych (IOD), jeżeli został powołany;
- celu i podstawy przetwarzania danych osobowych;
- prawnie uzasadnionego interesu/-ów administratora danych (jeżeli takowy istnieje);
- informacji o odbiorcach danych osobowych lub o kategoriach odbiorców;
- informacji o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
- okresu przechowywania danych;
- informacji o prawach podmiotu (dostęp do danych, ich przenoszenie, sprzeciw, sprostowanie, usunięcie etc.);
- informacji o prawie do cofnięcia zgody;
- informacji o prawie do wniesienia skargi do organu nadzorczego;
- informacji, czy podanie danych to wymóg ustawowy lub umowny lub warunek zawarcia umowy oraz konsekwencji niepodania danych;
- informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu (w tym o zasadach podejmowania, znaczeniach i konsekwencjach).

Regulacje RODO wprowadzają instytucję Inspektora Ochrony Danych, dalej zwanego także IOD, którego powołanie w określonych sytuacjach jest obowiązkowe dla administratora danych.

IOD powinien podlegać jedynie najwyższemu kierownictwu przedsiębiorstwa (np. zarządowi). Nie musi być on pracownikiem administratora danych, funkcja ta może zostać powierzona osobie zewnętrznej na podstawie umowy o świadczenie usług (outsourcing).

W ramach swojej działalności IOD powinien być m.in. właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych w przedsiębiorstwie, wspierany przez administratora w wypełnianiu zadań, poprzez zapewnienie mu zasobów niezbędnych do wykonania tych zadań, np. powołania

odpowiedniego zespołu wsparcia IOD oraz dostęp do danych osobowych i operacji przetwarzania, nie powinien również otrzymywać instrukcji od administratora danych.

Zgodnie z brzmieniem rozporządzenia, od 25 maja 2018 r. podmioty danych są wyposażone w takie uprawnienia, jak:

- prawo do bycia zapomnianym – podmiot danych ma prawo zażądać od administratora niezwłocznego usunięcia jego danych osobowych, jeżeli zajdzie jedna z enumeratywnie wymienionych okoliczności z art. 17 ust. 1 pkt. a-f RODO;
- prawo do sprostowania danych – podmiot ma prawo żądać od administratora danych niezwłocznego sprostowania dotyczących jego danych osobowych, które są nieprawidłowe. Instytucja ta obecna jest już w polskich przepisach;
- prawo do ograniczenia przetwarzania – osoba, której dane dotyczą, ma prawo żądania od administratora danych ograniczenia przetwarzania jej danych osobowych w przypadkach wymienionych w art. 18 ust. 1 pkt. a-d RODO;
- prawo do przenoszenia danych – osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe. Przeniesienie danych jest możliwe, jeżeli przetwarzanie odbywa się na podstawie zgody lub wykonania umowy lub odbywa się w sposób zautomatyzowany (np. *scoring* kredytowy);
- prawo do niepodlegania przez konkretną osobę fizyczną decyzjom wywołującym wobec niej skutki prawne lub podobnie wpływającym na nią w inny istotny sposób, a opartym na przetwarzaniu jej danych wyłącznie w sposób zautomatyzowany (za pomocą systemów informatycznych), w tym za pomocą profilowania danych. Przepis ten przewiduje również wyjątki od tej zasady, m.in. gdy takie przetwarzanie danych opiera się na wyraźnie udzielonej zgodzie przez osobę, której one dotyczą.

Co do zasady, realizacja wspomnianych praw przysługujących podmiotowi danych powinna być bezpłatna. Jednak jeśli żądania osoby, której dane dotyczą, wymagają od administratora dużych nakładów finansowych i czasowych, są ewidentnie nieuzasadnione, lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może pobrać opłatę, adekwatną do trudności przedsięwzięcia związanego z żądaniem. Administrator powinien zapewnić podmiotom danych możliwość skorzystania ze swoich praw również drogą elektroniczną, szczególnie kiedy przetwarzanie danych odbywa się elektronicznie.

Administrator danych bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania, powinien odnieść się do wniosku osoby, której dane dotyczą w zakresie realizacji przysługujących jej praw. Jeżeli administrator nie spełni żądania podmiotu danych, powinien podać tego przyczyny.

Celem ułatwienia administratorom wypełniania obowiązków związanych z przetwarzaniem danych osobowych, i jednoczesnym ograniczeniem biurokracji w tej materii, RODO wprowadza zupełnie nowe rozwiązanie, które zastępuje obowiązek rejestracji zbiorów danych – rejestr czynności przetwarzania danych osobowych.

Obowiązek posiadania takiego rejestru spoczywa zarówno na administratorze danych, jak i na podmiocie, któremu powierzono przetwarzanie danych.

Rejestr może być prowadzony w formie pisemnej lub elektronicznej. Administrator lub podmiot przetwarzający dane ma obowiązek udostępnić rejestr na każde żądanie organu nadzorczego. Organ nadzorczy dokonuje kontroli tych rejestrów w celu monitorowania operacji przetwarzania.

Obowiązek posiadania rejestru dotyczy podmiotów zatrudniających powyżej 250 osób.

RODO przewiduje również obowiązek zgłaszania naruszeń ochrony danych osobowych do organu nadzorczego. O naruszeniu administrator powinien poinformować organ niezwłocznie, nie później niż 72 godziny od wykrycia naruszenia.

Zgłoszenie musi zawierać informacje wskazane w art. 33 ust. 3 pkt. 2-d RODO, czyli m.in. charakter naruszenia, wskazywać kategorię i przybliżoną liczbę osób, których dotyczy

naruszenie, możliwe konsekwencje. Jeżeli naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki powinien również zawiadomić o naruszeniu osobę, której dane dotyczą.

Z uwagi na nieprzerwanie rozwijający się segment usług outsourcingowych i coraz powszechniejsze korzystanie z tych usług przez administratorów danych, konieczne stało się bardziej precyzyjne uregulowanie współpracy pomiędzy administratorem danych osobowych, a podmiotem, na rzecz którego dochodzi do powierzenia przetwarzania danych.

Regulacje RODO wymieniają obligatoryjne elementy umowy o powierzenie przetwarzania danych, która zgodnie z nowymi przepisami powinna zawierać: przedmiot powierzenia, czas powierzenia, charakter powierzenia, cel powierzenia, rodzaj danych osobowych podlegających powierzeniu, kategorie osób, których powierzane dane dotyczą, obowiązki i prawa administratora (prawo dokonywania kontroli warunków przetwarzania danych osobowych/obowiązek cyklicznego sprawdzania merytorycznej poprawności powierzanych danych osobowych), obowiązki procesora (m.in. zobowiązanie do zachowania poufności w zakresie przetwarzanych danych, podjęcie środków bezpieczeństwa w stosunku do przetwarzanych danych, legalne korzystanie z usług innego podmiotu przetwarzającego).

4. Polityka bezpieczeństwa informacji

Polityka Bezpieczeństwa Informacji w firmie **IMILK** przedstawiona jest w formie dokumentu, opublikowanego i dostępnego dla wszystkich wykonawców lub podwykonawców firmy. Dokument ten podlega ciągłej aktualizacji i udoskonalaniu, w celu dostosowania go do zmieniających się warunków działalności firma.

PBI została przygotowana w celu:

- ograniczenia możliwości nieautoryzowanego udostępnienia danych osobowych przetwarzanych przez kontrahentów;

- ograniczenia naruszeń przepisów prawa oraz innych regulacji;
- zapobiegania obniżenia reputacji IMILK;
- ograniczenia strat finansowych.

Polityka Bezpieczeństwa Informacji firmy, w odniesieniu do ochrony danych osobowych, zakłada:

- zbieranie danych osobowych w jasno określonych celach;
- przetwarzanie danych osobowych, które jest zgodne tylko z wcześniej ustalonymi celami;
- przechowywanie danych osobowych przez określony czas, przeznaczony na realizację poszczególnych zadań;
- przedstawienie danych osobowych w sposób sformalizowany, umożliwiający łatwą identyfikację;
- przetwarzanie danych osobowych w sposób zgodny z obowiązującymi przepisami prawa.

5. Odpowiedzialności i uprawnienia

Za bezpieczeństwo przetwarzanych danych osobowych odpowiedzialny jest firma IMILK, zwana dalej Administratorem Danych Osobowych (ADO). Odpowiedzialność Administratora Danych Osobowych została wskazana w Rozporządzeniu oraz ustawie o ochronie danych osobowych, wraz z aktami wykonawczymi do niej. Nie mniej, poniżej, zgodnie z RODO, wskazuje się na podstawowe obowiązki Administratora Danych Osobowych:

- zapewnienie przetwarzania zgodnego z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
- zbieranie danych osobowych w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;

- zapewnienie adekwatności, stosowności oraz ograniczenie przetwarzania tylko do niezbędnych celów wskazanych w PBI;
- zapewnienie prawidłowości przetwarzania danych osobowych i, w razie potrzeby, ich uaktualniania;
- zapewnienie przechowywania danych osobowych w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane;
- zapewnienie przetwarzania danych osobowych w sposób gwarantujący odpowiedni poziom bezpieczeństwa, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych;
- deklaracja pełnego zaangażowania w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych, a także prawidłowego zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych;
- nadzór jakie dane, kiedy i przez kogo zostały do zbiorów Administratora wprowadzone, bądź z tych zbiorów usunięte oraz komu są przekazywane;
- bieżące dostosowywanie systemów informatycznych służących do przetwarzania danych i wszelkie systemy zabezpieczeń przetwarzania danych osobowych do wymogów określonych w rozporządzeniu.

Obowiązkiem Administratora jest zapewnienie:

- środków technicznych i organizacyjnych niezbędnych dla zapewnienia bezpiecznego przetwarzania danych w pomieszczeniach do tego przeznaczonych;
- systemu i sprzętu informatycznego umożliwiającego bezpieczne przetwarzanie danych;

- że do przetwarzania danych osobowych zostały dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych;
- zapoznania z przepisami o ochronie danych osobowych każdej osoby upoważnionej do przetwarzania danych osobowych;
- prowadzenia ewidencji osób upoważnionych;
- należytego i terminowego udzielenia informacji na wniosek osób, których dane są przetwarzane i które zwróciły się z wnioskiem o udzielenie informacji w trybie art. 33 Ustawy;
- kontroli nad tym jakie dane, kiedy i przez kogo zostały do zbiorów Administratora wprowadzone, ze zbiorów usunięte oraz komu i przez kogo przekazane.

W razie wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, Administrator jest zobowiązany, bez zbędnej zwłoki, do uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru.

Dodatkowo, ADO zobligowany jest, zgodnie z RODO, w razie jakichkolwiek wątpliwości do wykazania przestrzegania powyższych obowiązków.

5.1. Kontrola dostępu

Każdemu z kontrahentów firmy, podczas podpisywania umowy, nadawane jest prawo dostępu do pewnego zakresu informacji, czy danych osobowych.

Każdy z partnerów biznesowych informowany jest również, podczas udzielania mu dostępu do danych osobowych, o sankcjach, które będą egzekwowane w przypadku nieautoryzowanego ich udostępnienia.

6. Przetwarzanie danych

Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:

- osoba, której dane dotyczą wyrazi na to zgodę, chyba, że chodzi o usunięcie dotyczących jej danych;
- jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa;
- jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą;
- jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego;
- jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez Administratora albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Za prawnie uzasadniony cel Administratora uznaje się w szczególności dochodzenie roszczeń z tytułu prowadzonej działalności oraz marketing bezpośredni własnych produktów lub usług, przy czym przy podejmowaniu działań marketingowych za pomocą środków komunikacji elektronicznej należy stosować przepisy ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2013 r. poz. 1422) oraz ustawy z dnia 16 lipca 2004 r. prawo telekomunikacyjne (Dz.U. z 2014 r. poz. 243), które przewidują dalej idącą ochronę.

Zgoda na przetwarzanie danych osobowych:

- nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści;
- może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania;
- może zostać odwołana w każdym czasie. W przypadku odwołania zgody na przetwarzanie danych osobowych Administrator zobowiązany jest usunąć

wszystkie dane osobowe osoby, która zgodę cofnęła, chyba, że istnieje inne podstawa prawna upoważniająca Administratora do dalszego przetwarzania tych danych dla innych celów, niż wskazany w cofniętej zgodzie;

- powinna być odebrana w postaci możliwej do późniejszego udowodnienia (np. pisemnie w ramach systemu informatycznego po zastosowaniu metody dwustopniowego uwiarygodniania, jako nagranie przeprowadzonej rozmowy telefonicznej – po poinformowaniu rozmówcy o prowadzonej rejestracji).

7. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

Administrator zobowiązuje się zachować w tajemnicy dane osobowe, do których posiada dostęp, sposoby zabezpieczania danych, jak również wszelkie informacje, które powziął w czasie przetwarzania danych, zarówno w sposób zamierzony, jak i przypadkowy. Obowiązek zachowania danych w tajemnicy jest bezterminowy.

Podczas przetwarzania danych Administrator zachowuje szczególną ostrożność i podejmuje wszelkie możliwe środki umożliwiające zabezpieczenie oraz ochronę danych przed nieuprawnionym dostępem, modyfikacją, zniszczeniem lub ujawnieniem.

Podczas przesyłania dokumentów zawierających dane za pomocą środków komunikacji elektronicznej, dochowuje się należytej staranności, w szczególności upewnia się, czy przesyłane za pomocą poczty elektronicznej dokumenty trafiły do właściwego odbiorcy.

W przypadku przesyłania, za pomocą środków komunikacji elektronicznej, zestawień, spisów, czy innych dokumentów zawierających dane osobowe, przesyłany dokument należy zaszyfrować, a hasło przesłać w miarę możliwości innym środkiem komunikacji.

Wszelkie dokumenty zawierające dane osobowe przechowywane są w szafach lub pomieszczeniach zamykanych na klucz.

Po zakończeniu pracy z danymi osobowymi stanowisko jest porządkowane, zabezpieczane są dokumenty i nośniki elektroniczne z danymi w specjalnie do tego przeznaczonych szafach lub pomieszczeniach. Niszczenie dokumentów zawierających dane odbywa się jedynie za pomocą niszczarki gwarantującej odpowiedni stopień rozdrobnienia. Alternatywnym rozwiązaniem do celów niszczenia dokumentacji jest zatrudnienie wykwalifikowanej firmy zewnętrznej, zajmującej się profesjonalną utylizacją dokumentów. Wymogiem jest zawarcie z nią umowy o powierzeniu przetwarzania danych osobowych. Każdy dokument zawierający dane, a nieużyteczny niszczy się niezwłocznie. Podczas korzystania z urządzeń wielofunkcyjnych, należy zachować szczególną ostrożność. Dokumenty kopiowane, bądź skanowane wyjmowane są z urządzenia wielofunkcyjnego niezwłocznie po ich użyciu. Dotyczy to również dokumentów powstałych na skutek kopiowania, bądź skanowania.

8. Praca zdalna

Użytkownicy sprzętu mobilnego ponoszą całkowitą odpowiedzialność za powierzony do użytkowania sprzęt oraz powinni stosować się do poniższych zasad:

- zabrania się pozostawiania bez opieki w miejscach publicznych sprzętu elektronicznego czy dokumentów;
- komputery przenośne należy przewozić jako bagaż podręczny i, w miarę możliwości, je maskować;
- zaleca się zachowanie ostrożności podczas używania urządzeń do przetwarzania mobilnego w miejscach publicznych, salach spotkań i innych niechronionych miejscach poza siedzibą organizacji;
- zaleca się, aby urządzenia przetwarzania mobilnego wyposażyć w fizyczne zabezpieczenia przed kradzieżą, zwłaszcza gdy są pozostawiane, np. w samochodach i innych środkach transportu, pokojach hotelowych, centrach konferencyjnych i salach spotkań;
- zabrania się spożywania posiłków i picia podczas pracy z powierzonym sprzętem;

- połączenia w sieciach bezprzewodowych publicznych są zabronione;

W celu zabezpieczenia sprzętu podczas podróży zaleca się:

- pilnowanie bagażu zawierającego sprzęt elektroniczny w pociągu oraz samolocie;
- nie pozostawianie sprzętu w samochodzie w widocznych miejscach;
- korzystanie z automatycznej blokady zamków w trakcie użytkowania pojazdu służbowego;
- umieszczanie sprzętu przed transportem w specjalnie dedykowanym futerale ochronnym.

9. Procedura postępowania z incydentami ochrony danych osobowych, kontakt z organami władzy

Celem Procedury Postępowania w Przypadku Naruszenia Danych jest określenie zadań pracowników w zakresie:

- ochrony wszystkich informacji przed ich modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem, a także utratą oraz ochroną zasobów technicznych;
- prawidłowego reagowania pracowników przy przetwarzaniu danych, w przypadku stwierdzenia ich naruszenia (zwłaszcza naruszenia ochrony danych osobowych) lub naruszenia zabezpieczeń systemu informatycznego;
- ograniczenia ryzyka powstania zagrożeń oraz minimalizacji skutków wystąpienia zagrożeń.

W przypadku naruszenia ochrony danych osobowych należy zgodnie z Rozporządzeniem 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), zgłosić to naruszenie właściwemu

organowi nadzorczemu, a także w uzasadnionych przypadkach, wszystkim osobom, których to naruszenie dotyczy.

W przypadku naruszenia ochrony danych osobowych, bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Urzędowi Ochrony Danych Osobowych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu, po upływie 72 godzin, dołącza się wyjaśnienie przyczyn opóźnienia. Wzór zgłoszenia – Załącznik nr 1.

Zgłoszenie to musi zawierać co najmniej:

- opis charakteru naruszenia ochrony danych osobowych, w tym, w miarę możliwości, wykaz kategorii i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- imię i nazwisko oraz dane kontaktowe punktu kontaktowego, od którego można uzyskać więcej informacji;
- opis możliwych konsekwencji naruszenia ochrony danych osobowych;
- opis środków zastosowanych lub proponowanych przez Administratora, w celu zaradzenia naruszeniu ochrony danych osobowych, w tym, w stosownych przypadkach, środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.

Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszych zapisów.

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, bez zbędnej zwłoki zawiadamia się również osobę, której dane dotyczą, o takim naruszeniu. Zawiadomienie powinno jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej następujące informacje i środki:

- imię i nazwisko oraz dane kontaktowe punktu kontaktowego, od którego można uzyskać więcej informacji;
- opis możliwych konsekwencji naruszenia ochrony danych osobowych;
- opis środków zastosowanych lub proponowanych przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym, w stosownych przypadkach, środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Zawiadomienie nie jest wymagane, w następujących przypadkach:

- Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
- Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w pkt. 1;
- wymagałoby ono niewspółmiernie dużego wysiłku.

W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

10. Postanowienia końcowe

W sprawach nieuregulowanych w niniejszej Polityce Bezpieczeństwa mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy ustawy.

11. Ważność oraz zarządzanie niniejszym dokumentem

Stwierdza się ważność niniejszego dokumentu na dzień ..... r.

Właścicielem niniejszego dokumentu jest Administrator Danych Osobowych, który jest odpowiedzialny za weryfikację oraz w razie konieczności aktualizację.

……

Właściciel