POLITYKA BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

Szymon Zalarski IT Solutions

ul. Orzechowa 35

32-500 Chrzanów

NIP: 6282288416

Data wprowadzenia:	30.04.2024 r.
Daty aktualizacji:	
Opracowanie:	Piotr Tarasek PT SCC – doradztwo prawne i gospodarcze

INFORMACJE OGÓLNE

CEL POLITYKI BEZPIECEŃSTWA OCHRONY DANYCH OSOBOWYCH

Polityka Bezpieczeństwa Ochrony Danych Osobowych została opracowana i wdrożona w strukturze Administratora Danych prowadzącego działalność pod firmą Szymon Zalarski IT Solutions w celu zapewnienia zgodności przetwarzania danych osobowych z wymogami obowiązujących w tym zakresie polskich i wspólnotowych aktów prawnych, w szczególności:

1. 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);

2. Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2018 r., poz. 1000 ze zm.);

3. Ustawy z dnia 16 lipca 2004 roku – prawo telekomunikacyjne (Dz. U. z 2004 r. nr 171, poz. 1800);

Polityka Bezpieczeństwa Ochrony Danych Osobowych ma zastosowanie do wszystkich czynności związanych z przetwarzaniem danych osobowych w ramach organizacji funkcjonowania firmy Administratora Danych, w tym do jego pracowników i zleceniobiorców, którzy w zakresie swoich obowiązków służbowych przetwarzają dane osobowe, jak również innych osób, które z upoważnienia Administratora Danych uzyskały dostęp do danych osobowych na zasadach powierzenia.

Każda z tych osób została/zostanie zapoznana z najważniejszymi procedurami bezpieczeństwa danych opisanymi w niniejszej Polityce Bezpieczeństwa Ochrony Danych Osobowych i zobowiązana do ich przestrzegania w zakresie wynikającym z przydzielonych zadań.

Osoby, o których mowa złożyły/złożą oświadczenie o zapoznaniu się z procedurami bezpieczeństwa danych oraz zobowiązały/zobowiążą się do ich stosowania. Wszelkie wątpliwości dotyczące sposobu interpretacji zapisów niniejszej Polityki, powinny być rozstrzygane na korzyść zapewnienia najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą.

TERMINOLOGIA

1. **Administrator Danych (ADO**) – Szymon Zalarski;
2. **Administrator Systemów Informatycznych (ASI)** – osoba wyznaczona przez Administratora Danych, koordynująca działania związane z zapewnieniem bezpieczeństwa systemów informatycznych, w tym odpowiadająca za nadzór nad zabezpieczeniem danych osobowych przetwarzanych w systemach informatycznych wykorzystywanych przez Administratora Danych;
3. **dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, gdzie poprzez możliwą do zidentyfikowania osobę fizyczną rozumie się osobę, 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 (za RODO);
4. **DPIA** – ocena skutków dla ochrony danych osobowych (data protection impact assessment);
5. **Inspektor Ochrony Danych Osobowych (IODO)** – osoba wyznaczona przez Administratora Danych, koordynująca procesy związane z przestrzeganiem zasad ochrony danych osobowych w ramach procesów przetwarzania danych osobowych zachodzących w strukturze Administratora Danych;
6. **organ nadzorczy** – niezależny organ publiczny powołany w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii Europejskiej, powołany w każdym państwie członkowskim Unii, którego podstawowym zadaniem jest monitorowanie stosowania przepisów rozporządzenia RODO;
7. **podmiot przetwarzający** –osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora Danych;
8. **Polityka** – niniejsza Polityka Bezpieczeństwa Ochrony Danych Osobowych;
9. **pracownik** - osoba świadcząca pracę na rzecz Administratora Danych na podstawie umowy o pracę;
10. **zleceniobiorca** - osobą wykonująca powierzone jej zlecenie przez ADO na podstawie umowy cywilnoprawnej;

11. **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;
12. **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 (ogólne rozporządzenie o ochronie danych).

ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH ORAZ ZAKRES ZASTOSOWANIA

Polityka Bezpieczeństwa Ochrony Danych Osobowych opisuje zasady i procedury przetwarzania danych osobowych. Jest to zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych wewnątrz struktury Administratora Danych.

Polityka odnosi się całościowo do kwestii zabezpieczenia danych osobowych, tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych. Politykę stosuje się do wszelkich czynności, stanowiących w myśl RODO oraz ustaw krajowych przetwarzanie danych osobowych. Bez względu na źródło pochodzenia danych osobowych, ich zakres, cel zebrania, sposób przetwarzania lub czas przetwarzania, stosowane są zasady ujęte w niniejszej Polityce. Rygorowi Polityki podlegają także dane powierzone Administratorowi Danych do przetwarzania na podstawie umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego oraz dane osobowe, które zostały Administratorowi Danych udostępnione. Dokument powstał aby szczegółowo określić środki techniczne i organizacyjne, procedury i zasady, które zapewnią ochronę przetwarzanych danych osobowych przed potencjalnym zagrożeniem.

1. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

1.1. STRUKTURA ORGANIZACJI OCHRONY DANYCH OSOBOWYCH

Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami RODO, wskazanych ustaw, Polityki oraz procedur wewnętrznych z zakresu ochrony danych osobowych wdrożonych w strukturze Administratora Danych, odpowiadają:

1. Administrator Danych,

2. Inspektor Ochrony Danych,

3. Administrator Systemów Informatycznych,

4. Osoby upoważnione do przetwarzania danych osobowych na podstawie szczegółowych upoważnień wydawanych w określony w strukturze organizacyjnej firmy sposób.

1.2. ADMINISTRATOR DANYCH

Administrator Danych wyznacza:

• IODO;

• Administratora Systemów Informatycznych.

Administrator Danych jest odpowiedzialny za:

• zapewnienie odpowiednich środków organizacyjnych w celu realizacji i wykazania przetwarzania danych osobowych zgodnie z określonymi w RODO zasadami przetwarzania danych osobowych;

• wdrożenie odpowiednich procedur ochrony danych osobowych;

• jeśli uzna to za konieczne, stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji, jako element dla stwierdzenia przestrzegania przez Administratora Danych ciążących na nim obowiązków;

• zapewnienie środków umożliwiających prawidłową realizację praw osób, których dane dotyczą;

• współpracę z organem nadzorczym w ramach wykonywania przez niego swoich zadań;

• wdrożenie odpowiednich środków organizacyjnych aby zapewnić stopień bezpieczeństwa odpowiadający istniejącemu ryzyku naruszenia praw lub wolności osób, których dane dotyczą;

• zgłaszanie naruszenia ochrony danych osobowych właściwemu organowi nadzorczemu, a w przypadku, gdy zajdą ku temu odpowiednie przesłanki, również osobie, której dane dotyczą;

• dokumentowanie wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia, jego skutków oraz podjętych działań zaradczych;

• zapewnienie legalności przekazywania danych osobowych do podmiotów trzecich. W stosunku do IODO ADO zobowiązuje się do:

• zapewnienia, że jest on właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych;

• wspierania IODO w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.

Administrator Danych nadzoruje działania IODO oraz ASI oraz wydaje im zalecenia, co do sposobu wykonywania obowiązków wynikających z Polityki. Administrator Danych każdorazowo wyraża zgodę oraz ostateczną akceptację na kluczowe z perspektywy organizacji działania IODO oraz ASI, w które zaangażowane są podmioty trzecie. Do zaakceptowania tych działań, wystarczająca jest zgoda wyrażona w formie wiadomości e-mail.

1.3.INSPEKTOR OCHRONY DANYCH OSOBOWYCH

Funkcję IODO pełni osoba wyznaczona przez Administratora Danych na podstawie zawartej z nią umowy cywilnoprawnej. IODO jest wyznaczany przez Administratora Danych na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia swoich zadań.

Do zadań IODO należy:

• informowanie o obowiązkach wynikających z RODO oraz innych właściwych przepisów Wspólnotowych lub państw członkowskich o ochronie danych osobowych oraz doradzanie w tym zakresie;

• monitorowanie przestrzegania RODO oraz innych właściwych przepisów Wspólnotowych lub państw członkowskich o ochronie danych osobowych;

• monitorowanie przestrzegania wdrożonych procedur ochrony danych osobowych;

• realizacja działań zwiększających świadomość pracowników Administratora Danych w zakresie obowiązków wynikających z RODO lub przyjętych procedur;

• przeprowadzanie audytów w zakresie przestrzegania RODO i wdrożonych procedur ochrony danych osobowych;

• udzielanie na żądanie zaleceń, co do oceny skutków dla ochrony danych osobowych oraz monitorowanie jej wykonania.

1.4.ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

Funkcję ASI pełni osoba wyznaczona przez Administratora Danych.

Do zadań ASI należy:

• prowadzenie rejestru nadanych uprawnień do systemów informatycznych;

• nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów;

• podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń;

• identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych;

• inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych.

2. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

Każda osoba, która uzyskała upoważnienie do przetwarzania danych, zobowiązana jest do ich ochrony w sposób zgodny z przepisami RODO oraz określonych w niniejszym dokumencie ustaw. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu stosunku pracy oraz stosunku cywilnoprawnego. Naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy skutkuje poniesieniem odpowiedzialności karnej na podstawie przepisów wskazanych w dokumencie oraz stanowi ciężkie naruszenie obowiązków pracowniczych może być podstawą rozwiązania stosunku pracy w trybie art. 52 Ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (tekst jedn. Dz.U. z 2018 r., poz. 108 ze zm.), bądź rozwiązania stosunku cywilnoprawnego. Zasada rozliczalności wymaga od administratora udzielenia upoważnienia do przetwarzania danych osobowych.

2.1. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

Przetwarzanie danych osobowych w strukturze Administratora Danych odbywa się zgodnie z ogólnymi zasadami przetwarzania danych osobowych określonymi w art. 5 RODO.

Oznacza to, że dane osobowe przetwarza się:

• zgodnie z prawem, w oparciu o co najmniej jedną przesłankę legalności przetwarzania danych osobowych wskazaną w art. 6 lub 9 RODO (zasada legalności);

• w sposób rzetelny przy uwzględnieniu interesów i rozsądnych oczekiwań osób, których dane dotyczą (zasada rzetelności);

• w sposób przejrzysty dla osób, których dane dotyczą (zasada przejrzystości);

• w konkretnych, wyraźnych i prawnie uzasadnionych celach (zasada ograniczenia celu);

• w zakresie adekwatnym, stosownym oraz niezbędnym dla celów, w których są przetwarzane (zasada minimalizacji danych);

• przy uwzględnieniu ich prawidłowości i ewentualnego uaktualniania (zasada prawidłowości);

• przez okres nie dłuższy, niż jest to niezbędne dla celów, w których są przetwarzane (zasada ograniczenia przechowywania);

• w sposób zapewniający odpowiednie bezpieczeństwo (integralność i poufność).

Administrator Danych wraz z Inspektorem Ochrony Danych Osobowych gwarantują, że określone decyzje odnoszące się do procesów przetwarzania danych osobowych zostały przeanalizowane z punktu widzenia zgodności z ogólnymi zasadami przetwarzania danych, a przede wszystkim, że są z nimi zgodne.

2.2. ZAKRES PRZETWARZANIA DANYCH OSOBOWYCH

Polityka ma zastosowanie w stosunku do wszystkich danych osobowych przetwarzanych przez Administratora Danych, niezależnie od formy ich przetwarzania tj. elektroniczna lub papierowa oraz tego, czy są to dane przetwarzane w zbiorach danych, w zestawach czy stanowią one pojedyncze informacje osobowe. Administrator Danych prowadzi Rejestr Czynności Przetwarzania, który stanowi element polityki bezpieczeństwa ochrony danych w przedsiębiorstwie. W odniesieniu do sensytywnych danych osobowych zasadą jest ich nieprzetwarzanie.

2.3. ZAKRES DOPUSZCZENIA OSÓB DO PRZETWARZANIA DANYCH OSOBOWYCH

Administrator Danych realizując Politykę, w zakresie udostępniania danych osobowych w ramach wewnętrznej struktury, zezwala na ich przetwarzanie w systemie informatycznym lub w wersji papierowej wyłącznie osobom, które uzyskały uprzednie, stosowne upoważnienie do przetwarzania danych osobowych. Upoważnienie do przetwarzania danych osobowych, nadawane jest indywidualnie, z wyraźnym wskazaniem, jakie zbiory danych obejmuje swoim zakresem.

3. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

Administrator Danych realizując Politykę dopuszcza, by dane osobowe, których jest administratorem były przetwarzane poza własnymi strukturami organizacyjnymi. Może się to odbywać wyłącznie na drodze powierzenia danych, w określonym celu i zakresie, podmiotowi przetwarzającemu na mocy umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego. Podstawowym warunkiem dopuszczalności powierzenia przetwarzania danych w imieniu administratora jest poddanie planowanego outsourcingu analizie, która powinna zapewnić, że wybór podmiotu przetwarzającego został uzależniony od zapewnienia wystarczających gwarancji ochrony danych.

3.1. ZASADY POWIERZANIA

Zawierana przez Administratora Danych umowa powierzenia przetwarzania danych osobowych musi być zgodna z postanowieniami art. 28 RODO, tj. w szczególności określać:

• przedmiot powierzenia;

• czas trwania powierzenia;

• charakter i cel przetwarzania;

• rodzaj powierzanych danych osobowych;

• kategorie osób, których dane dotyczą;

• warunki podpowierzenia przetwarzania danych;

• obowiązki i prawa Administratora Danych;

• obowiązki podmiotu przetwarzającego.

Umowa powierzenia może zostać zawarta w formie pisemnej, w tym elektronicznej. Umowa powierzenia przetwarzania danych osobowych podpisywana jest zgodnie z zasadami reprezentacji Administratora Danych lub udzielonymi pełnomocnictwami. Każdorazowe dokonanie powierzenia danych osobowych musi zostać obligatoryjnie odnotowane w rejestrze czynności przetwarzania danych osobowych.

4. UDOSTĘPNIANIE DANYCH OSOBOWYCH

Administrator Danych realizując Politykę dopuszcza, by dane osobowe, których jest administratorem były przekazywane innym administratorom w formie udostępnienia danych. Udostępnienie danych osobowych może nastąpić tylko w oparciu o co najmniej jedną przesłankę spośród wskazanych w art. 6 RODO i art. 9 RODO. Podmioty lub kategorie podmiotów, którym udostępnia się dane osobowe muszą zostać obligatoryjnie wskazane w rejestrze czynności przetwarzania danych osobowych.

5. PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH

Przekazywanie danych, których administratorem jest Administrator Danych do państw trzecich może się odbywać wyłącznie po spełnieniu warunków przewidzianych w Rozdziale V RODO. Przekazywanie danych do państw trzecich może mieć formę zarówno powierzenia przetwarzania danych osobowych oraz udostępnienia danych osobowych.

6. WSPÓŁADMINISTROWANIE DANYMI OSOBOWYMI

Administrator Danych w zakresie przetwarzanych przez siebie danych osobowych dopuszcza możliwość przyjęcia modelu współadministrowania danymi osobowymi zgodnie z art. 26 RODO.

6.1. ZASADY WSPÓŁADMINISTROWANIA

Współadministrowanie danymi może zachodzić wówczas, jeżeli Administrator Danych oraz co najmniej jeden inny podmiot, wspólnie ustalają cele i sposoby przetwarzania danych osobowych. Oznacza to, że w danym procesie przetwarzania danych osobowych muszą zostać spełnione równocześnie trzy warunki, tj. Administrator Danych oraz co najmniej jeden inny podmiot muszą:

• być administratorami w rozumieniu art. 4 pkt 7 RODO;

• wspólnie ustalić cele przetwarzania danych;

• wspólnie ustalić sposoby techniczne i organizacyjne przetwarzania danych osobowych.

7. AUDYTY ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Audyty zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz procedurami wdrożonymi w strukturze Administratora Danych przeprowadzane są przez IODO.

8. REALIZACJA PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ

Administrator Danych uwzględnia w zachodzących w jego strukturze procesach przetwarzania danych osobowych, procedury i zasady ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy przepisów RODO, w tym, w szczególności:

• prawo do wycofania wyrażonej zgody (art. 7 ust. 3 RODO);

• prawo dostępu przysługujące osobie, której dane dotyczą (art. 15 RODO);

• prawo do sprostowania danych (art. 16 RODO);

• prawo do usunięcia danych (prawo do bycia zapomnianym) (art. 17 RODO);

• prawo do ograniczenia przetwarzania (art. 18 RODO);

• prawo do przenoszenia danych (art. 20 RODO);

• prawo sprzeciwu (art. 21 RODO);

• prawo do niepodlegania decyzjom opartym na zautomatyzowanym przetwarzaniu (art. 22 RODO).

9. OCENA SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH – DATA PROTECTION IMPACT ASSESSTMENT

Administrator Danych dokonuje oceny skutków dla ochrony danych w celu opisania przetwarzania danych osobowych oraz oceny jego konieczności i proporcjonalności, a także w celu wspomagania zarządzania ryzykiem naruszenia praw i wolności osób fizycznych wynikającym z przetwarzania ich danych osobowych. W strukturze Administratora Danych ocena skutków dla ochrony danych osobowych stanowi narzędzie ułatwiające przestrzeganie wymogów określonych w RODO, a także wykazanie, że podjęto odpowiednie środki w celu zapewnienia przestrzegania przepisów RODO.