

Polityka bezpieczeństwa danych osobowych

Wersja	
Właściciel	
Data zatwierdzenia	
Data wejścia w życie	
Zatwierdzający	

SPIS TREŚCI

§ 1. DEFINICJE	3
§ 3. OBOWIĄZEK ZAPOZNANIA SIĘ Z PROCEDURĄ.....	4
§ 4. OBOWIĄZKI ADMINISTRATORA DANYCH OSOBOWYCH	4
§ 5. ZBIERANIE DANYCH OSOBOWYCH ORAZ PRAWA PODMIOTÓW DANYCH OSOBOWYCH.....	5
§ 6. REJESTR (KATEGORII) CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH	6
§ 7. ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH	6
§ 8. NARUSZENIE BEZPIECZEŃSTWA DANYCH OSOBOWYCH.....	6
§ 9. POWIERZENIE PRZETWARZANIA DANYCH PODMIOTOM ZEWNĘTRZNYM	6
§ 10. WSPÓŁPRACA Z ORGANEM NADZORCZYM	7

§ 1. DEFINICJE

1. **Administrator (ADO)** – spółka z siedzibą
2. **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;
3. **Koordynator ds. RODO** – osoba, wyznaczona przez Administratora do pełnienia funkcji koordynatora ochrony danych;
4. **Naruszenie ochrony danych osobowych** – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
5. **Pracownik** – osoba świadcząca pracę u Administratora - bez względu na formę zatrudnienia;
6. **Polityka** – niniejszy dokument;
7. **Przetwarzanie danych osobowych** – oznacza jakąkolwiek operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
8. **Podmiot przetwarzający (PP)** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza lub będzie przetwarzał dane osobowe w imieniu Administratora;
9. **RODO** – 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 osobowych).

§ 2. CEL

1. Celem Polityki jest określenie zasad przetwarzania danych osobowych, które pozwolą zapewnić ich bezpieczeństwo zgodnie z wymogami stawianymi przez przepisy dot. ochrony danych osobowych, w tym zwłaszcza z przepisami RODO.
2. Polityka Bezpieczeństwa stanowi wykaz dokumentów, które stosowane są przez w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych.
3. Polityka obowiązuje od dnia zatwierdzenia jej przez Administratora. Zmiany i przegląd Polityki dokonywane są przez Koordynatora ds. RODO.
4. Koordynator ds. RODO wspiera Administratora w realizacji jego obowiązków wynikających z Polityki oraz właściwych przepisów o ochronie danych osobowych.

§ 3. OBOWIĄZEK ZAPOZNANIA SIĘ Z PROCEDURĄ

Każdy Pracownik ma obowiązek zapoznania się z niniejszą Polityką oraz stosowania się do jej postanowień.

§ 4. OBOWIĄZKI ADMINISTRATORA DANYCH OSOBOWYCH

1. W celu zapewnienia bezpieczeństwa danych osobowych Administrator jest zobowiązany w szczególności do:
 - a) stałego nadzoru nad treścią Polityki;
 - b) wydawania, modyfikowania, odbierania upoważnienia do przetwarzania danych osobowych osobom, które mają te dane przetwarzać.
 - c) prowadzenia rejestru osób upoważnionych do przetwarzania danych osobowych.
 - d) prowadzenia rejestru (kategorii) czynności przetwarzania danych osobowych.
 - e) zawierania umów powierzenia przetwarzania danych osobowych zgodnie z art. 28 RODO, w sytuacji, gdy dochodzi do powierzenia przetwarzania danych osobowych.
2. Przetwarzając dane osobowe Administrator kieruje się w szczególności następującymi zasadami:
 - a) **zasadą przetwarzania danych osobowych zgodnie z prawem** – przetwarzanie danych osobowych powinno następować w oparciu o jedną z podstaw prawnych wskazanych w art. 6 ust. 1 oraz art. 9 ust. 2 RODO;
 - b) **zasadą minimalizacji danych osobowych** – przetwarzane mogą być tylko dane osobowe adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
 - c) **zasadą prawidłowości** – przetwarzane mogą być tylko dane osobowe, które są prawidłowe i w razie potrzeby uaktualniane (Administrator powinien podejmować wszelkie działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane);
 - d) **zasadą integralności i poufności danych osobowych** – dane osobowe powinny być przetwarzane w sposób zapewniający odpowiednie ich bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz

- przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych;
- e) **zasadą privacy by design** - uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, Administrator – zarówno przy określeniu sposobów przetwarzania, jak i w czasie samego przetwarzania, wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą;
 - f) **zasadą privacy by default** - Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślne dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

§ 5. ZBIERANIE DANYCH OSOBOWYCH ORAZ PRAWA PODMIOTÓW DANYCH OSOBOWYCH

1. W przypadku zbierania danych osobowych od osób, których dane dotyczą, dokonując tej czynności Administrator zobowiązany jest przekazać ww. osobom informacje, o których mowa w art. 13 RODO.
2. Jeżeli danych osobowych Administrator nie pozyskał od osób, których dane dotyczą, Administrator zobowiązany jest przekazać tym osobom, informacje, o których mowa w art. 14 RODO. Informacje te należy podać:
 - a) w rozsądnym terminie po pozyskaniu danych osobowych - najpóźniej w ciągu miesiąca - mając na uwadze konkretne okoliczności przetwarzania danych osobowych;
 - b) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą - najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub
 - c) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy - najpóźniej przy ich pierwszym ujawnieniu.
3. W przypadku, gdy osoba, której dane osobowe są przetwarzane zgłosi żądanie dotyczące dostępu do danych osobowych, ich sprostowania, usunięcia, ograniczenia przetwarzania, przeniesienia danych osobowych, czy też prawa do sprzeciwu przetwarzania danych osobowych, Administrator stosuje procedurę realizacji praw podmiotów danych osobowych.
4. Administrator prowadzi rejestr wniosków o realizację Praw RODO.

§ 6. REJESTR (KATEGORII) CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Prowadzony przez Administratora rejestr czynności przetwarzania danych osobowych oraz rejestr kategorii czynności przetwarzania zawierają informacje, o których mowa w art. 30 RODO.

§ 7. ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator stosuje środki techniczne i organizacje niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych.
2. Administrator przed dopuszczeniem Pracowników, współpracowników Administratora do przetwarzania danych osobowych, zapoznaje ich z Polityką – w zakresie w jakim jest to wymagane na danym stanowisku a następnie nadaje pisemne upoważnienie do przetwarzania danych osobowych. Zapoznanie odbywa się poprzez udostępnienie dokumentu Polityki i przeprowadzenie szkolenia.
3. Administrator stosuje następujące środki ochrony:
 - a)

§ 8. NARUSZENIE BEZPIECZEŃSTWA DANYCH OSOBOWYCH

1. W przypadku zaistnienia okoliczności, które mogą wskazywać na naruszenie ochrony danych osobowych, każdy Pracownik Administratora zobowiązany jest postępować zgodnie z procedurą reagowania na naruszenia ochrony danych osobowych.
2. Administrator przed dopuszczeniem Pracowników do przetwarzania danych osobowych, zapoznaje ich z procedurą reagowania na naruszenia ochrony danych osobowych. Zapoznanie odbywa się poprzez udostępnienie dokumentu Polityki Bezpieczeństwa i przeprowadzenie szkolenia.
3. Administrator prowadzi rejestr wszelkich naruszeń ochrony danych osobowych, a więc również tych które nie podlegają zgłoszeniu organowi nadzorcemu, ani nie wymagają powiadomienia osób, których dane osobowe dotyczą.

§ 9. POWIERZENIE PRZETWARZANIA DANYCH PODMIOTOM ZEWNĘTRZNYM

1. Administrator może powierzyć przetwarzanie danych osobowych innemu podmiotowi, o ile podmiot ten wdrożył odpowiednie środki organizacyjne i techniczne niezbędne dla ochrony praw osób, których te dane dotyczą oraz pod warunkiem zawarcia z nim umowy powierzenia przetwarzania.
2. Przed powierzeniem przetwarzania danych osobowych Administrator, jego Pracownicy zapoznają się z procedurą weryfikacji podmiotu przetwarzającego oraz stosują się do niej.

3. Przed zawarciem umowy powierzenia Administrator wysyła do Podmiotu przetwarzającego arkusz weryfikacyjny. Podmiot przetwarzający zobowiązany jest wypełnić i odesłać Administratorowi rzeczony arkusz.
4. Każdy arkusz weryfikacyjny jest archiwizowany przez Administratora.

§ 10. WSPÓŁPRACA Z ORGANEM NADZORCZYM

1. Każda osoba, w szczególności Pracownik Administratora ma obowiązek przekazać korespondencję od Prezesa Urzędu Ochrony Danych Osobowych lub osoby, której dane dotyczą w zakresie jej praw wynikających z RODO.
2. Administrator współpracuje z Prezesem Urzędu Ochrony Danych Osobowych w przypadku skierowania wystąpienia, kontroli, postępowania wszczętego przez ten organ, zgłoszenia naruszenia ochrony danych osobowych, a także konieczności konsultacji z organem w związku z oceną skutków naruszenia bezpieczeństwa danych osobowych oraz w przypadku jakichkolwiek wątpliwości w zakresie ochrony danych osobowych, które wymagają wyjaśnienia z tym organem.
3. W przypadku wszczęcia kontroli weryfikuje tożsamość i uprawnienie kontrolującego poprzez wyznaczonego przez siebie Koordynatora.