

POLITYKA OCHRONY DANYCH OSOBOWYCH
w TPSI Sp. z o.o.

ROZDZIAŁ I
Informacje wstępne

§ 1

1. Postanowienia ogólne
2. Niniejszy dokument zatytułowany Polityka ochrony danych osobowych ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w TPSI Sp. z o.o.
3. Niniejsza polityka jest polityką ochrony danych osobowych w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz.Urz. UE L 119, s. 1).

§ 2

Glosariusz i wykaz skrótów

Określenia i skróty użyte w Polityce oznaczają:

- 1) administrator – osoba fizyczna lub prawna, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych;
- 2) ADO – administrator, podmiot, o którym mowa w pkt 9 poniżej;
- 3) dane – dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu;
- 4) dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, przetwarzane przez ADO zarówno w systemach informatycznych lub w wersji papierowej;
- 5) dane wrażliwe – dane specjalne i dane karne;
- 6) dane specjalne – dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej;
- 7) dane karne – dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa;
- 8) osoba – osoba, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu;
- 9) Spółka – TPSI Sp. z o.o. z siedzibą w Warszawie, ul. Czterech Wiatrów 51, wpisana do Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla m.st. Warszawy pod numerem KRS 0000674199, numer identyfikacji podatkowej (NIP): 9512435846, REGON 36709488000000. Wysokość kapitału zakładowego: 5000,00 zł.
- 10) przetwarzający lub podmiot przetwarzający – osoba fizyczna lub prawna, organ publiczny, jednostka, lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

- 11) 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;
- 12) IOD – Inspektor Ochrony Danych – osoba powołana przez ADO, odpowiedzialna m.in. za monitorowanie przestrzegania RODO;
- 13) osoba zatrudniona – każda osoba zatrudniona w Spółce posiadających dostęp do danych osobowych, będąca pracownikiem Spółki lub niebędąca pracownikiem Spółki ale świadcząca usługi na rzecz Spółki, z wyłączeniem osób prowadzących działalność gospodarczą świadczących usługi na rzecz Spółki na podstawie art. 28 RODO;
- 14) Polityka – niniejsza Polityka ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu;
- 15) przetwarzanie danych osobowych – wykonywanie jakichkolwiek operacji na danych osobowych, takich jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie, niezależnie od formy, w jakiej wykonywane są te czynności;
- 16) RCPD lub Rejestr – Rejestr Czynności Przetwarzania Danych Osobowych;
- 17) RODO – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz.Urz. UE L 119, s. 1);
- 18) nośnik danych – dyskiety, płyty CD/DVD, pamięć flash, dyski twarde, taśmy magnetyczne lub inne urządzenia służące do przechowywania plików z danymi stanowiące samodzielne urządzenie lub część urządzenia, np. w stacjach roboczych, komputerach przenośnych, drukarkach, skanerach;
- 19) osoba upoważniona – osoba zatrudniona, posiadająca upoważnienie do przetwarzania danych osobowych wydane przez ADO.

§ 3

Deklaracja kierownictwa

Kierownictwo Spółki, świadome wagi problemów związanych z ochroną prawa do prywatności, w tym w szczególności prawa osób fizycznych powierzających swoje dane osobowe do właściwej i skutecznej ochrony tych danych, deklaruje:

- 1) zamiar podejmowania wszystkich działań niezbędnych dla ochrony praw i usprawiedliwionych interesów Spółki związanych z bezpieczeństwem danych osobowych;
- 2) zamiar upowszechnienia zasad bezpieczeństwa przetwarzania danych osobowych określonych niniejszą Polityką oraz dokumentami powiązanymi;
- 3) zamiar stałego podnoszenia świadomości oraz kwalifikacji osób przetwarzających dane osobowe w Spółce w zakresie problematyki bezpieczeństwa danych;
- 4) zamiar traktowania obowiązków osób zatrudnionych jako należących do kategorii

- podstawowych obowiązków oraz stanowczego egzekwowania ich wykonania;
- 5) zamiar zapewnienia bieżącego nadzoru nad przestrzeganiem obowiązujących zasad bezpieczeństwa przetwarzania danych;
 - 6) zamiar podejmowania w niezbędnym zakresie współpracy z instytucjami powołanymi do ochrony danych osobowych.

ROZDZIAŁ II

Stosowanie zasad ochrony danych

§ 4

Zasady ochrony danych

1. Polityka ma zastosowanie do ochrony danych przetwarzanych w Spółce w formie tradycyjnej jak i elektronicznej na nośnikach danych oraz w systemach informatycznych, w których przetwarzane są dane.
2. Polityka ma zastosowanie do ochrony danych przetwarzanych w Spółce występującej jako administrator danych jak również występującej jako podmiot przetwarzający.
3. Spółka przetwarza dane osobowe z poszanowaniem następujących zasad:
 - 1) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
 - 2) rzetelnie i uczciwie (rzetelność);
 - 3) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
 - 4) w konkretnych celach i nie „na zapas” (minimalizacja);
 - 5) w zakresie nie większym niż jest to konieczne (adekwatność);
 - 6) z dbałością o prawidłowość danych (prawidłowość);
 - 7) nie dłużej niż jest to niezbędne (czasowość);
 - 8) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

§ 5

System ochrony danych

System ochrony danych osobowych w Spółce składa się z następujących elementów:

- 1) inwentaryzacja danych – Spółka dokonuje identyfikacji zasobów danych, kategorii danych, zależności pomiędzy zasobami danych, zrozumienia cyklu życia danych od momentu ich zebrania do momentu ich usunięcia;
- 2) Rejestr – Spółka opracowuje, prowadzi i utrzymuje RCPD;
- 3) podstawy prawne – Spółka zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze;
- 4) prawa osób – Spółka spełnia obowiązki informacyjne względem osób, których dane przetwarza oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania;
- 5) przetwarzający – Spółka posiada zasady doboru przetwarzających dane na rzecz Spółki, wymogów co do warunków przetwarzania (umowy powierzenia);
- 6) export danych – Spółka posiada zasady weryfikacji i identyfikacji przekazywania danych

do państw trzecich lub organizacji międzynarodowych oraz zapewnia zgodnie z prawem warunki takiego przekazywania;

- 7) minimalizacja – Spółka posiada zasady i metody zmierzające do spełnienia zasady minimalizacji w tym w szczególności zasady zarządzania adekwatnością, dostępnością oraz czasowością przetwarzania danych;
- 8) bezpieczeństwo – Spółka zapewnia odpowiedni do ryzyka poziom bezpieczeństwa, w tym:
 - a. przeprowadza analizę ryzyka dla czynności przetwarzania danych lub ich kategorii,
 - b. przeprowadza ocenę skutków dla ochrony danych w przypadku gdy ryzyko naruszenia praw i wolności osób jest wysokie,
 - c. dostosowuje środki ochrony danych do ustalonego ryzyka,
 - d. stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenia zidentyfikowanego naruszenia ochrony danych.

§ 6

Rejestr Czynności Przetwarzania Danych

1. RCPD stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację zasady rozliczalności – rozliczenie obowiązków ochrony danych określonych w RODO.
2. Spółka prowadzi RCPD, w którym inwentaryzuje, dokumentuje i monitoruje sposób w jaki wykorzystuje dane osobowe.
3. RCDP może zwierać także pola nieobowiązkowe, nieokreślone w art. 30 RODO. W polach nieobowiązkowych Spółka rejestruje informacje w miarę potrzeb i możliwości.
4. Za prowadzeni Rejestru odpowiedzialny jest ADO lub osoba przez niego wyznaczona.

ROZDZIAŁ III

Prawa i żądania osób

§ 7

Ogólne zasady realizacji praw i żądań osób

1. Spółka dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza jako administrator.
2. Spółka dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.
3. Spółka zapewnia adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostek i obowiązków informacyjnych.
4. Spółka poprzez wdrożenie odpowiednich środków technicznych i organizacyjnych zapewnia, że wszelkie żądania osób, których dane Spółka przetwarza jako podmiot przetwarzający, zostaną przekazane do właściwego administratora w przeciągu 24 godzin od dnia otrzymania żądania.
5. Realizując prawa i żądania osób, których dane dotyczą, Spółka wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. Realizacja praw i żądań osób, nie może

niekorzystnie wpłynąć na prawa i wolności innych osób.

6. Spółka informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.
7. Spółka informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.
8. Spółka dokumentuje obsługę spełnienia obowiązków informacyjnych, zawiadomień i żądań osób, w tym odnotowuje fakt wydania pierwszej kopii danych.
9. Spółka może wprowadzić cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie.

§ 8

Realizacja praw i żądań osób

1. **Dostęp do danych [art. 15 RODO]** – na żądanie osoby dotyczące dostępu do jej danych, Spółka informuje osobę o szczegółach przetwarzania, a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany poprzez wydanie kopii danych.
2. **Sprostowanie danych [art. 16 RODO]** – Spółka dokonuje niezwłocznego sprostowania danych na żądanie osoby, której dane dotyczą. Spółka ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Spółka informuje osobę o odbiorcach danych, na żądanie tej osoby.
3. **Usunięcie danych [art. 17 RODO]** – na żądanie osoby, Spółka usuwa dane, gdy:
 - 1) dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach;
 - 2) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania;
 - 3) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych;
 - 4) dane były przetwarzane niezgodnie z prawem;
 - 5) konieczność usunięcia wynika z obowiązku prawnego.

Spółka określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17 ust. 3 RODO.

Jeżeli dane podlegające usunięciu zostały upublicznione przez Spółkę, Spółka podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, o potrzebie usunięcia danych i dostępu do nich.

W przypadku usunięcia danych Spółka informuje osobę o odbiorcach danych, na żądanie tej osoby.

4. **Ograniczenie przetwarzania [art. 18 RODO]** – Spółka dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

- 1) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość;
- 2) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
- 3) Spółka nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
- 4) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Spółki zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

W trakcie ograniczenia przetwarzania Spółka przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.

Spółka informuje osobę przed uchyleniem ograniczenia przetwarzania.

W przypadku ograniczenia przetwarzania danych Spółka informuje osobę o odbiorcach danych, na żądanie tej osoby.

5. **Przenoszenie danych [art. 20 RODO]** – na żądanie osoby Spółka wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła Spółce, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Spółki.
6. **Sprzeciw w szczególnej sytuacji [art. 21 ust. 1 RODO]** – jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Spółkę w oparciu o uzasadniony interes Spółki lub o powierzone Spółce zadanie w interesie publicznym, Spółka uwzględni sprzeciw, o ile nie zachodzą po stronie Spółki ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.
7. **Sprzeciw względem marketingu bezpośredniego [art. 21 ust. 3 RODO]** – jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Spółkę na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), Spółka uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

ROZDZIAŁ IV

Adekwatne środki bezpieczeństwa

§ 9

Bezpieczeństwo

1. Spółka zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych.
2. Spółka przeprowadza i dokumentuje szacowanie ryzyka dla czynności przetwarzania danych osobowych występujących w Spółce. Spółka stosuje metodykę szacowania ryzyka przyjętą w Spółce.
3. Spółka analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.
4. Spółka ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym Spółka ustala przydatność i stosuje takie środki i podejście jak:
 - 1) pseudonimizacja danych;
 - 2) szyfrowanie danych;
 - 3) tworzenie kopii zapasowych;
 - 4) cykliczne szkolenia z zakresu ochrony danych dla osób zatrudnionych;
 - 5) inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
 - 6) środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

§ 10

Ocena skutków dla ochrony danych

1. Spółka dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z szacowaniem ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.
2. Spółka stosuje metodykę oceny skutków przyjętą w Spółce.

ROZDZIAŁ V

Naruszenia ochrony danych

§ 11

Identyfikacja i zgłaszanie naruszeń

1. Spółka, występująca jako ADO, stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych w terminie 72 godzin od ustalenia naruszenia.
2. Spółka, występująca jako podmiot przetwarzający, stosuje procedury na identyfikację, ocenę i zgłoszenie incydentów ochrony do właściwego administratora w terminie 24 godzin od momentu jego stwierdzenia.
3. Spółka stosuje procedury dotyczące postępowania z naruszeniami przyjęte w Spółce.

ROZDZIAŁ VI

Powierzenia danych

§ 12

Przetwarzający

1. Spółka posiada zasady doboru i weryfikacji podmiotów przetwarzających opracowane w celu zapewnienia, aby przetwarzający dawali wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na Spółce, np., poprzez stosowanie wzorców umów powierzenia.
2. Spółka przyjmuje minimalne wymagania co do umowy powierzenia przetwarzania danych określone w art. 28 RODO, w przypadku:
 - 1) relacji: Spółka (administrator) – dostawca lub podwykonawca (podmiot przetwarzający);
 - 2) relacji: Spółka (podmiot przetwarzający) – dostawca lub podwykonawca (podmiot podprzetwarzający);
 - 3) relacji: odbiorca (administrator) – Spółka (podmiot przetwarzający).
3. Spółka rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z zasad powierzenia danych osobowych określonych w § 4.

ROZDZIAŁ VII

Obszar przetwarzania danych

§ 13

Obszar przetwarzania danych

1. Obszar przetwarzania danych osobowych w Spółce obejmuje:
 - 1) budynki, lokale i pomieszczenia, w których przetwarzane są dane osobowe (miejsca, w których wykonuje się operacje na danych osobowych, a także informacje o podmiotach, którym Spółka powierzyła przetwarzanie danych osobowych);
 - 2) miejsca, gdzie przechowuje się nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające elektroniczne nośniki informacji);
 - 3) systemy informatyczne służące do przetwarzania danych osobowych.
2. Obszar oraz zasady przetwarzania danych osobowych zostały określone w Wykazie miejsc przetwarzania danych osobowych stanowiącym Załącznik nr 1 (Wykaz miejsc i zasady ochrony pomieszczeń Spółki, w których przetwarza się dane osobowe) do Polityki.
3. Wykaz miejsc przetwarzania danych osobowych prowadzony jest przez ADO lub osobę wyznaczoną przez ADO.
4. ADO może zezwolić na przebywanie w siedzibie Spółki osobom sprzątającym poza godzinami pracy Spółki bez konieczności obecności osoby upoważnionej pod warunkami określonymi w Załączniku nr 1. Osoby sprzątające zobowiązane są do podpisania oświadczenia o zachowaniu poufności.
5. Zezwala się na przetwarzanie danych osobowych na urządzeniach przenośnych lub dokumentach papierowych poza siedzibą Spółki pod warunkiem bezwzględnej ochrony danych przed dostępem do nich osób nieupoważnionych.
6. W Spółce wykorzystuje się następujące główne systemy informatyczne:
 - 1) system operacyjny Windows zainstalowany na stacjach roboczych;
 - 2) program pocztowy Outlook;
 - 3) system CRM Sales Force;
 - 4) system do zarządzania wynikami Spółki i osiągnięciami konsultantów Qlikview;
 - 5) Aplikacje dostępne m.in. w ramach pakietu Office (Word, Excel).

§ 14

Zasoby danych osobowych i systemy ich przetwarzania

1. W Spółce występują zasoby danych osobowych, które zostały określone w Załączniku nr 2 (Wykaz zasobów danych osobowych) do Polityki. Załącznik nr 2 wyszczególnia następujące informacje:
 - 1) nazwa zasobu danych osobowych;
 - 2) oznaczenie statusu Spółki administrator lub podmiot przetwarzający (powierzenie);
 - 3) kategoria osób, których dane dotyczą;
 - 4) nazwy programów komputerowych zastosowanych do przetwarzania danych;

- 5) lokalizacja programów (modułów programowych) używanych do przetwarzania.
2. Załącznik nr 2 prowadzony jest przez ADO lub osobę wyznaczoną przez ADO.

ROZDZIAŁ VIII

Obowiązki i odpowiedzialność osób uczestniczących w procesie przetwarzania

§ 15

Obowiązki ADO

1. Funkcję ADO pełni Zarząd Spółki.
2. Do najważniejszych obowiązków ADO należy w szczególności:
 - 1) wdrożenie odpowiednich środków technicznych i organizacyjnych w Spółce w celu spełnienia obowiązków spoczywających na Spółce określonych w Polityce i zapewnienia zgodności z RODO;
 - 2) spełnienie obowiązku informacyjnego wobec każdej osoby zatrudnionej w Spółce bez względu na formę zatrudnienia;
 - 3) prowadzenie RCPD. ADO może wyznaczyć jedną z osób upoważnionych do wykonywania tego zadania;
 - 4) zapewnienie wstępnych i okresowych szkoleń z zakresu ochrony danych osobowych dla osób zatrudnionych w Spółce;
 - 5) nadawanie, odbieranie i kontrola upoważnień do przetwarzania danych osobowych osobom zatrudnionym. ADO może wyznaczyć jedną z osób upoważnionych do wykonywania tego zadania;
 - 6) prowadzenie ewidencji osób upoważnionych. ADO może wyznaczyć jedną z osób upoważnionych do wykonywania tego zadania.
3. ADO może powołać IOD.

§ 16

Obowiązki IOD

1. IOD wypełnia swoje obowiązki na podstawie art. 38 i 39 RODO oraz innych przepisów wykonawczych do RODO na poziomie europejskim i krajowym.
2. Do dodatkowych obowiązków IOD poza określonymi w przepisach wskazanych w ust. 1 powyżej należy analiza:
 - 1) umów powierzenia – Rozdział VI;
 - 2) wniosków i żądań osób, których dane dotyczą – Rozdział III;
 - 3) zgodności przekazywania danych osobowych – Rozdział IX.ADO jest zobowiązany uzyskać opinię IOD opracowaną w wyniku przeprowadzania analizy dokumentacji, o której mowa powyżej w niniejszym ustępie.
3. IOD może wyznaczyć swojego zastępcę. Zastępca IOD wykonuje zadania IOD podczas jego nieobecności.
4. W celu realizacji powierzonych obowiązków IOD ma prawo:

- 1) kontrolować osoby zatrudnione w zakresie właściwego zabezpieczenia systemów informatycznych oraz miejsc i pomieszczeń, w których przetwarzane są dane osobowe;
- 2) wydawać osobom zatrudnionym polecenia w zakresie bezpieczeństwa danych osobowych;
- 3) informować ADO o przypadkach naruszenia ochrony danych osobowych;
- 4) żądać od osób zatrudnionych wyjaśnień w sytuacji naruszenia ochrony danych osobowych.

§ 17

Obowiązki osób zatrudnionych

1. Do obowiązków osób zatrudnionych należy w szczególności:
 - 1) przejście szkolenia w zakresie ochrony danych osobowych przed dopuszczeniem do pracy wymagającej przetwarzania danych osobowych w systemach informatycznych lub w wersji papierowej;
 - 2) przestrzeganie Polityki i przepisów określonych w obowiązujących przepisach prawa, w tym w szczególności w RODO;
 - 3) opracowanie, monitorowanie i aktualizowanie dokumentacji dla celów przeprowadzenia szacowania ryzyka dla czynności przetwarzania wykonywanych w ramach zadań realizowanych na rzecz lub zlecenie Spółki;
 - 4) terminowe spełnienie obowiązku informacyjnego w imieniu ADO wobec osób, których dane osobowe są przetwarzane przez Spółkę;
 - 5) występowanie z wnioskiem do ADO o nadanie upoważnienia do przetwarzania danych osobowych lub zmian w tym zakresie;
 - 6) informowanie o zamiarze powierzenia przetwarzania danych do podmiotów przetwarzających – np. nowe umowy z dostawcami lub podwykonawcami Spółki;
 - 7) informowanie o zamiarze otrzymania danych do powierzenia od administratorów danych – np. nowe umowy z klientami Spółki;
 - 8) zgłaszanie do przełożonego incydentów, naruszeń lub podejrzenia wystąpienia naruszeń ochrony danych osobowych bez zbędnej zwłoki;
 - 9) zgłaszanie do przełożonego żądań osób, których dane dotyczą, o czym mowa w Rozdziale III;
 - 10) zgłaszanie do przełożonego zamiaru utworzenia zasobu danych osobowych;
 - 11) zgłaszanie do przełożonego informacji dotyczących zmian w zakresie, celach, okresie, charakterze i sposobach przetwarzania danego zasobu danych osobowych;
 - 12) przestrzeganie obowiązków dotyczących obszaru przetwarzania i zastosowania zabezpieczeń zasobów danych.

§ 18

Odpowiedzialność służbowa i karna osób zatrudnionych w Spółce

1. Osoba zatrudniona w Spółce, która nie dopełnia obowiązków określonych w § 17 powyżej,

może podlegać odpowiedzialności karnej oraz, jeśli dotyczy, sankcjom określonym w Kodeksie pracy.

2. Naruszenie zasad ochrony danych osobowych obowiązujących w Spółce może również zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną określoną w przepisach odrębnych.
3. Naruszenie przepisów o ochronie danych osobowych jest zagrożone sankcjami karnymi określonymi w art. 130, 266–269, 287 Kodeksu karnego.

ROZDZIAŁ IX

Przekazywanie danych osobowych

§ 19

Przekazywanie Danych

1. Dane osobowe mogą być przekazywane w następujących przypadkach:
 - 1) osobom zatrudnionym do przetwarzania danych osobowych – na podstawie ważnego upoważnienia i oświadczenia do zachowania tajemnicy;
 - 2) osobom, których dane dotyczą – na podstawie ważnego wniosku osoby, której dane dotyczą;
 - 3) podmiotom przetwarzającym – na podstawie umowy powierzenia lub innego instrumentu prawnego;
 - 4) podmiotom uprawnionym – na podstawie obowiązujących przepisów prawa;
 - 5) innym odbiorcom – jeśli jest to konieczne do prawidłowego wykonania umowy zawartej ze Spółką;
 - 6) stronom trzecim – wyłącznie na podstawie upoważnienia administratora lub podmiotu przetwarzającego.
2. Przekazując dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały przekazane.
3. ADO podejmuje decyzję o przekazaniu danych – na podstawie analizy IDO, o ile IOD został wyznaczony.
4. Odmowa przekazania danych osobowych następuje wówczas, gdy spowodowałoby to istotne naruszenia praw i wolności lub dóbr osobistych osób, których dane dotyczą, lub innych osób oraz jeżeli dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy.

§ 20

Upoważnienia

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez ADO oraz które podpisały oświadczenie o zachowaniu w tajemnicy danych, z którymi mają styczność, oraz środków bezpieczeństwa stosowanych przy przetwarzaniu danych osobowych.

2. Wzór upoważnienia, o którym mowa w ust. 1 powyżej, określa Załącznik nr 3 (Upoważnienie) do Polityki.
3. Wzór oświadczenia, o którym mowa w ust. 1 powyżej, określa Załącznik nr 4 (Oświadczenie) do Polityki.
4. ADO zobowiązany jest do zbierania, ewidencjonowania i przechowywania upoważnień oraz oświadczeń, o których mowa w ust. 1-3 powyżej. Ewidencja upoważnień wyszczególnia co najmniej następujące informacje:
 - 1) imię i nazwisko osoby upoważnionej;
 - 2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych;
 - 3) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.
5. ADO może wyznaczyć osobę odpowiedzialną za prowadzenie ewidencji oraz przechowywanie upoważnień i oświadczeń, o czym mowa w ust. 1-4 powyżej.
6. Każda zmiana w zakresie informacji zawartych w ewidencji, o której mowa w ust. 4 powyżej, podlega niezwłocznemu odnotowaniu przez ADO lub osobę prowadzącą ewidencję.