

POLITYKA OCHRONY DANYCH OSOBOWYCH

WORKERSOLUTION SP. Z O.O.

UL. JOSEPHA CONRADA 51 , 31-357 KRAKÓW

NIP: 6511738046

Spis treści

Rozdział 1. Cel regulacji.....	3
Rozdział 2. Przedmiot polityki i obszar stosowania	4
Rozdział 3. Skróty i definicje	4
Rozdział 4. Role i odpowiedzialności w procesie	8
przetwarzania danych osobowych	8
Rozdział 5. Ogólne zasady przetwarzania danych osobowych.....	9
Rozdział 6. Obowiązek informacyjny	12
Rozdział 7. Transfer danych i mapowanie procesów	13
Rozdział 8. Reagowanie na przypadki naruszenia ochrony danych osobowych	18
Rozdział 9. Retencja danych.....	18
Rozdział 10. Środki organizacyjne dotyczące ochrony danych osobowych.....	18
Rozdział 11. Zasady funkcjonowania Polityki	22
Rozdział 12. Załączniki.....	22

Rozdział 1. Cel regulacji

1. Wdrożona przez **WORKERSOLUTION SP. Z O.O. UL. JOSEPHA CONRADA 51 , 31-357 KRAKÓW, NIP: 6511738046** (zwaną dalej „Spółką” lub „Administratorem”) „Polityka Ochrony Danych Osobowych”, zwana dalej „Polityką”, określa role, odpowiedzialności oraz zasady przetwarzania danych osobowych w imieniu administratora oraz w ramach jego aktywności. Celem Polityki jest zdefiniowanie i zapewnienie:
 - 1) Zgodności przetwarzania danych osobowych z wymaganiami RODO i przepisami prawa, łącznie z zagwarantowaniem praw osób, których dane są przetwarzane,
 - 2) Zabezpieczenia danych osobowych przed utratą, zniszczeniem lub ujawnieniem, w tym przetwarzanych w systemach informatycznych i za pomocą nowoczesnych technik przetwarzania,
 - 3) Realizacji praw osób fizycznych w zakresie dysponowania danymi osobowymi (których osoby te są podmiotem), tj. prawa do: informacji o zakresie przetwarzania (co obejmuje prawo do uzyskania kopii przetwarzanych danych osobowych), sprostowania danych, usunięcia danych (inaczej „prawo do bycia zapomnianym”), ograniczenia przetwarzania danych, przenoszenia, sprzeciwu oraz sprzeciwu wobec automatyzowanego podejmowania decyzji, w tym profilowania, cofnięcia zgody na przetwarzanie danych osobowych,
 - 4) Skutecznego zarządzania incydentami bezpieczeństwa, w tym incydentami naruszenia ochrony danych,
 - 5) Zgodnego z prawem zarządzania transferem danych osobowych pomiędzy administratorem a podmiotem trzecim.
2. Dokument został opracowany zgodnie z wymogami określonymi w Rozporządzeniu 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), dalej zwanym „RODO”.
3. Użytkownikami niniejszego dokumentu są wszyscy pracownicy zatrudnieni na stałe lub tymczasowo przez administratora oraz wszystkie osoby świadczące na jego rzecz usługi na podstawie umowy cywilnoprawnej, o charakterze zbliżonym do umów o pracę.

Rozdział 2. Przedmiot polityki i obszar stosowania

1. Polityka obejmuje swoim zakresem wszystkie procesy, w ramach których Spółka przetwarza dane osobowe. Polityka stanowi jednocześnie zbiór zasad określających:
 - 1) Podstawy prawne przetwarzania danych osobowych (przesłanki przetwarzania) poprzez odniesienie do wymagań RODO,
 - 2) Powołanie stosownych ról i określenie ich odpowiedzialności w procesie przetwarzania danych osobowych z odniesieniem do struktur organizacyjnych ADO oraz Organu Nadzorczego,
 - 3) Zasady definiujące sposób przetwarzania danych przez administratora.
2. Polityka znajduje zastosowanie do wszystkich rodzajów danych osobowych przetwarzanych przez administratora, niezależnie od miejsca i sposobu ich przetwarzania, a w szczególności do następujących podmiotów danych:
 - 1) Klientów lub/oraz osób działających w imieniu Klienta,
 - 2) Pracowników (w tym pracowników tymczasowych), osób ubiegających się o zatrudnienie, osób współpracujących z administratorem,
 - 3) Kontrahentów lub/oraz osób działających w imieniu Kontrahenta,
 - 4) Zarządu Spółki,
 - 5) Innych podmiotów, których dane są przetwarzane w ramach prowadzonej działalności.
3. Polityka ma zastosowanie również do przypadków przetwarzania transgranicznego.
4. Polityka ma zastosowanie we wszystkich procesach, w ramach których Spółka występuje jako administrator, współadministrator lub procesor (podmiot przetwarzający).

Rozdział 3. Skróty i definicje

Definicje używane w niniejszej Instrukcji mają następujące znaczenie:

1. **Administrator; Administrator Danych Osobowych (ADO)** – (ang. Data Controller) oznacza podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
2. **Anonimizacja** – nieodwracalne pozbawianie danych osobowych elementów pozwalających na identyfikację, przez co osoba nie może zostać zidentyfikowana przy rozsądnym nakładzie czasu, środków i za pomocą technologii przez administratora lub inną osobę. Zasady przetwarzania danych osobowych nie mają zastosowania do danych zanonimizowanych, ponieważ nie są to w dalszym ciągu dane osobowe;

3. **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;
4. **Dane szczególnej kategorii** - dane osobowe, które z racji swego charakteru są szczególnie wrażliwe w świetle podstawowych praw i wolności, wymagają szczególnej ochrony, gdyż kontekst ich przetwarzania może powodować poważne ryzyko dla podstawowych praw i wolności. Do takich danych osobowych zaliczają się dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby;
5. **DPIA** – (ang. *Data Protection Impact Assessment*), to obowiązkowa dla ADO ocena skutków operacji przetwarzania dla ochrony danych osobowych, wynikająca wprost z przepisów RODO;
6. **IT** (ang. *information technology*) – całokształt zagadnień, metod, środków i działań związanych z przetwarzaniem informacji. Stanowi połączenie zastosowań informatyki i telekomunikacji, obejmuje również sprzęt komputerowy oraz oprogramowanie, a także narzędzia i inne technologie związane z przetwarzaniem, przesyłaniem, przechowywaniem, zabezpieczaniem i prezentowaniem informacji;
7. **Odbiorca danych** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem, **nie są jednak uznawane za „odbiorców danych”**;
8. **Ograniczenie przetwarzania** - oznacza oznakowanie (ang. *Labelling*) przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
9. **Prezes UODO; Organ Nadzorczy** – Prezes Urzędu Ochrony Danych Osobowych, tj. organ właściwy powołany przepisami lokalnymi do nadzoru w zakresie wypełnienia obowiązków RODO.
10. **Podprocesor** – oznacza podmiot przetwarzający, któremu Procesor (a więc podmiot przetwarzający, któremu ADO powierzył przetwarzanie), powierza dane do dalszego przetwarzania. Na podmiot taki nałożone zostają te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między ADO a podmiotem przetwarzającym (procesorem);

11. **Privacy by Default** – angielska nazwa, która ilekroć pojawia się w tekście niniejszego dokumentu, oznacza podejście wdrażania odpowiednich środków technicznych i organizacyjnych, 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;
12. **Privacy by Design** – angielska nazwa, która ilekroć pojawia się w tekście niniejszego dokumentu, oznacza podejście wdrażania odpowiednich środków technicznych i organizacyjnych, takich jak pseudonimizacja czy anonimizacja, zaprojektowanych w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą;
13. **Procesor (podmiot przetwarzający)** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora (na zlecenie, w ramach umowy, realizacji usługi, itd.);
14. **Profilowanie** - oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, polegającego na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
15. **Przetwarzanie informacji** – 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;
16. **Przetwarzanie transgraniczne** – przetwarzanie danych osobowych, które odbywa się w ramach działalności jednostek organizacyjnych w więcej niż jednym państwie członkowskim administratora lub podmiotu przetwarzającego w Unii posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim; albo przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego w Unii, ale które znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim;

- 17. Pseudonimizacja** – przetworzenie danych osobowych w taki sposób, by nie można ich było przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Ze względu na to, że spseudonimizowane dane są w dalszym ciągu danymi osobowymi, przetwarzanie spseudonimizowanych danych musi odbywać się zgodnie z zasadami Polityki;
- 18. Rejestr Czynności Przetwarzania** – oznacza rejestr prowadzony elektronicznie lub papierowo przez ADO, który zawiera co najmniej informacje dotyczące przetwarzania danych osobowych, określone w art. 30 ust. 1 RODO;
- 19. Rejestr Kategorii Czynności Przetwarzania**- rejestr prowadzony elektronicznie lub papierowo, przez procesora, który określa zlecone mu przez administratora danych osobowych procesy przetwarzania danych osobowych;
- 20. Retencja (Okres Retencji)** – oznacza okres przetwarzania danych, który nie może być dłuższy, niż to wynika z celu takiego działania. Parametrem retencji jest (wyrażony w miesiącach lub latach) termin zakończenia przetwarzania danych.
- 21. RODO, Rozporządzenie** - 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;
- 22. Strona trzecia** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;
- 23. Właściciel Biznesowy (WB)** – osoba kierującą jednostką organizacyjną lub osoba na jednoosobowym samodzielnym stanowisku, która jest odpowiedzialna za kształtowanie przepływu danych osobowych w danym obszarze oraz dokonywanie wybranych czynności z zakresu ochrony danych osobowych. Właściciel może, ale nie musi być głównym użytkownikiem przetwarzającym dane osobowe. Właściciel zobowiązany jest stosować zapisy procedur dotyczących przetwarzania danych osobowych, a w szczególności rekomendować ADO cele przetwarzania, przygotowywać – po konsultacji z IOD - klauzule informacyjne i zgody, przy każdorazowym zapewnieniu zgodności tych działań z przepisami prawa;

- 24. Współadministrator** – Administrator danych osobowych, który działa wspólnie z innym Administratorem danych osobowych w zakresie wspólnego ustalania celów i sposobów przetwarzania danych osobowych, a także określenia odpowiednich zakresów swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO. Obowiązki te w szczególności obejmują kwestie takie jak wykonywanie przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, chyba że przypadające im obowiązki i ich zakres określa prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu administratorzy ci podlegają;
- 25. Zapis danych osobowych** – pojedynczy rekord danych osobowych zarejestrowany na nośniku elektronicznym lub zapisany w dokumentach papierowych.

Rozdział 4. Role i odpowiedzialności w procesie przetwarzania danych osobowych

1. Administrator **nie wyznaczył Inspektora Ochrony Danych Osobowych, choć zakłada współpracę z osobą odpowiedzialną za obszar ochrony danych osobowych** w ramach działalności administratora, odpowiadającą w szczególności za:
- 1) Informowanie ADO, podmiotów i osób przetwarzających dane osobowe w imieniu ADO o ich obowiązkach wynikających z RODO,
 - 2) Monitorowanie przestrzegania Rozporządzenia, przepisów prawa oraz polityk wewnętrznych w dziedzinie ochrony danych osobowych,
 - 3) Przygotowanie oraz aktualizację wewnętrznej dokumentacji z zakresu ochrony danych osobowych obowiązujących w Spółce, w tym niniejszą Politykę wraz z załącznikami oraz projektami umów powierzenia, rejestrów wymaganych przez RODO;
 - 4) Udzielanie na żądanie administratora zaleceń, wskazań i opinii w zakresie ochrony danych osobowych;
 - 5) Koordynowanie współpracy z Organem Nadzorczym i pełnienie – w razie potrzeby – w stosunku do niego funkcji punktu kontaktowego,
 - 6) Informowanie administratora o zaistniałych incydentach naruszenia ochrony danych osobowych lub przedkładanie na żądanie administratora wskazań i opinii w tym zakresie,
 - 7) Udzielanie rekomendacji dotyczących udostępniania danych osobowych odbiorcom danych”.

2. Pracownicy administratora, w tym Właściciele Biznesowi (WB), odpowiadają za:

- 1) Współpracę z osobą wskazaną przez administratora za ochronę danych osobowych, w szczególności w zakresie zapewnienia praw osób, których dane są przetwarzane, w zakresie informowania o przetwarzaniu ich danych, odpowiadania na zapytania oraz wykonywanie wskazanych operacji na danych,
- 2) Wnioskowanie o udzielenie użytkownikom upoważnienia do przetwarzania danych osobowych,
- 3) Nadzór nad Procesorami w obszarze zgodnym z umową przetwarzania danych co do celów, zakresu i czasu przetwarzania,
- 4) Przestrzeganie przyjętych przez administratora zasad przetwarzania danych osobowych, określonych w **Rozdziale nr 5**, w tym zasady minimalizacji danych oraz zasady ograniczenia przechowania danych osobowych,
- 5) Wykonywanie operacji na danych osobowych zgodnie z nadanymi uprawnieniami i zakresem upoważnienia do przetwarzania danych osobowych,
- 6) Stosowanie mechanizmów zabezpieczających,
- 7) Uczestnictwo w szkoleniach celem porządkowania i doskonalenia wiedzy z zakresu przetwarzania danych osobowych,
- 8) Zgłaszanie incydentów naruszenia bezpieczeństwa danych osobowych,
- 9) Przetwarzanie danych osobowych na podstawie i w zakresie udzielonego przez Spółkę upoważnienia do przetwarzania danych osobowych.

Rozdział 5. Ogólne zasady przetwarzania danych osobowych

1. Zasady ochrony danych osobowych określają podstawowe obowiązki organizacji zajmujących się przetwarzaniem danych osobowych. Zgodnie z art. 5 ust. 2 RODO „administrator jest odpowiedzialny za przestrzeganie przepisów i musi być w stanie wykazać ich przestrzeganie”. Zasady ochrony danych osobowych to następujące zasady:
 - 1) **Zgodności z prawem, rzetelności i przejrzystości** - dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
 - 2) **Ograniczenia celu** - dane osobowe muszą być zbierane w konkretnych, wyraźnych oraz prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
 - 3) **Minimalizacji danych** - dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane; o ile to możliwe, Spółka stosuje podczas przetwarzania danych osobowych anonimizację lub pseudonimizację w celu zmniejszenia ryzyka naruszenia praw osób, których dane dotyczą;

- 4) **Prawidłowości** - dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;
 - 5) **Ograniczenia przechowywania** - dane osobowe muszą być przechowywane przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;
 - 6) **Integralności i poufności** - uwzględniając stan wiedzy technicznej i inne dostępne środki bezpieczeństwa, koszty wdrożenia, prawdopodobieństwo i wagę zagrożenia dla prywatności, należy zastosować odpowiednie środki techniczne i organizacyjne w celu zapewnienia właściwej ochrony danych osobowych, w tym ochrony przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieupoważnionym dostępem lub ujawnieniem;
 - 7) **Rozliczalności** – Spółka, działając w charakterze administratora danych osobowych, jest odpowiedzialny za przestrzeganie powyższych zasad i musi być w stanie wykazać ich przestrzeganie;
2. Przyjmuje się, iż przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:
- 1) Osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
 - 2) Przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
 - 3) Przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
 - 4) Przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
 - 5) Przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
 - 6) Przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem. Przesłanka nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

3. Jeżeli przetwarzanie w celu innym niż cel, w którym dane osobowe zostały zebrane, nie odbywa się na podstawie zgody osoby, której dane dotyczą, ani prawa Unii lub prawa państwa członkowskiego, administrator – aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane – bierze pod uwagę między innymi:
 - 1) Wszelkie związki między celami, w których zebrano dane osobowe, a celami zamierzonego dalszego przetwarzania;
 - 2) Kontekst, w którym zebrano dane osobowe, w szczególności relację między osobami, których dane dotyczą, a administratorem;
 - 3) Charakter danych osobowych, w szczególności czy przetwarzane są szczególne kategorie danych osobowych lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa;
 - 4) Ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą;
 - 5) Istnienie odpowiednich zabezpieczeń, w tym ewentualnie szyfrowania lub pseudonimizacji.
4. Zgoda na przetwarzanie danych osobowych powinna być pozyskana od każdego podmiotu danych, ale tylko wtedy, gdy nie istnieje inna uzasadniona podstawa przetwarzania danych osobowych.
5. Należy uzyskać osobną zgodę na każdy cel przetwarzania danych osobowych. Osoba, której dane dotyczą (podmiot danych) ma prawo odmówić zgody na przetwarzanie danych w niektórych celach, a wyrazić zgodę na inne. Zgodę osoby, której dane dotyczą można uzyskać w następujący sposób:
 - 1) Osoba, której dane dotyczą podpisuje się pod każdym celem przetwarzania z osobną, jeśli wyraża na niego zgodę;
 - 2) Osoba, której dane dotyczą przekreśla te cele przetwarzania, na które nie wyraża zgody, a pod spodem składa podpis potwierdzający wyrażenie zgody na te cele, które nie zostały przekreślone;
 - 3) W przypadku wyrażania przez osobę, której dane dotyczą zgody na przetwarzanie przez stronę internetową lub stosowną aplikację, poprzez zaznaczenie kwadracika, który znajdować będzie się przy każdym celu.
6. Nie jest dopuszczalne uzależnianie zawarcia umowy od wyrażenia zgody na przetwarzanie w celach innych niż wykonanie niniejszej umowy.
7. Każda osoba, której dane dotyczą może złożyć wniosek dotyczący realizacji swoich praw wynikających z RODO. Szczegółowe zasady opisujące organizację przyjmowania oraz tryb postępowania przy obsłudze wniosków w zakresie realizacji praw osób, których dane dotyczą na podstawie RODO określa „Procedura obsługi praw osoby, której dane dotyczą w zakresie ochrony danych”, stanowiąca **Załącznik nr 1 do Polityki**.

Rozdział 6. Obowiązek informacyjny

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator podaje zainteresowanej osobie następujące informacje:
 - 1) Swoją tożsamość i dane kontaktowe oraz dane kontaktowe inspektora ochrony danych;
 - 2) Cele przetwarzania danych osobowych oraz podstawę prawną ich przetwarzania;
 - 3) Jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;
 - 4) Informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją, przy czym jako „odbiorcy danych” nie traktuje się organów publicznych, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem;
 - 5) Gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez organ nadzorczy odpowiedniego stopnia ochrony;
 - 6) Okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
 - 7) Informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
 - 8) Jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) RODO lub art. 9 ust. 2 lit. a) RODO – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
 - 9) Informacje o prawie wniesienia skargi do organu nadzorczego;
 - 10) Informację czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
 - 11) Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz najbardziej istotnych informacji o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
2. Obowiązku informacyjnego, określonego w ust. 1, nie dopełnia się, gdy – i w zakresie, w jakim – osoba, której dane dotyczą, dysponuje już tymi informacjami.
3. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą (Wtórny Obowiązek Informacyjny), administrator zobowiązany jest **dodatkowo wskazać osobie, której dane dotyczą źródło pozyskania jego danych osobowych.**

4. Obowiązku informacyjnego, określonego w ust. 3, nie dopełnia się, gdy – i w zakresie, w jakim :
 - 1) Dane są przetwarzane przez administratora na podstawie przepisów prawa,
 - 2) Osoba, której dane dotyczą dysponuje już tymi informacjami;
 - 3) Dane przewidziane do zbierania są ogólnie dostępne;
 - 4) Udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku;
 - 5) Dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w ramach powszechnie obowiązujących przepisów prawa, w tym ustawowym obowiązkiem zachowania tajemnicy.
5. Spółka realizuje obowiązek informacyjny, o którym mowa w ust. 1 powyżej, za pośrednictwem Klauzul Informacyjnych, których wzór określa **Załącznik nr 2** do Polityki. Wzory stosowanych klauzul administrator udostępnia na stronie internetowej w zakładce „RODO”.

Rozdział 7. Transfer danych i mapowanie procesów

1. Administrator zakłada, iż dla właściwego określenia funkcji i ról dwóch lub większej ilości podmiotów prawnych, pomiędzy którymi dochodzi do transferu danych osobowych, konieczna jest dokładna analiza treści umowy (relacji prawnej) łączącej oba podmioty na tle powszechnie obowiązujących przepisów prawa. Właściwe określenie formy przekazania danych osobowych pomiędzy kilkoma podmiotami jest kluczowe dla zapewnienia zgodności z przepisami RODO późniejszego przetwarzania takich danych osobowych.
2. Podmioty, pomiędzy którymi następuje transfer danych osobowych, mogą występować w różnych rolach prawnych, w zależności od tego, czy będziemy mieć do czynienia z powierzeniem czy udostępnieniem danych osobowych, tj. w roli **administratora danych lub podmiotu przetwarzającego** (tzw. procesora).
3. Administrator to podmiot, który **samodzielnie ustala cele i sposoby przetwarzania danych osobowych, ma rzeczywisty wpływ na to, co dzieje się z danymi osobowymi i który określa w jakim celu są one gromadzone i dalej przetwarzane**, decyduje o tym kiedy i komu przekazać dane, przy czym wykonuje te działania w ramach obowiązujących przepisów prawa. Przetwarzanie przez niego danych osobowych musi odbywać się na podstawie co najmniej jednej z tzw. przesłanek legalizujących. Podmiot przetwarzający (Procesor) jest podmiotem, który przetwarza dane osobowe w imieniu administratora, robi to wyłącznie w zakresie i celu, jakie zostały określone przez administratora danych, a jego prawa i obowiązki w zakresie przetwarzanych danych zasadniczo określa umowa powierzenia przetwarzania danych osobowych.

4. Administrator zakłada, iż transfer danych osobowych realizowany na rzecz innego podmiotu jest możliwy w oparciu o **powierzenie danych osobowych** lub **udostępnienie danych osobowych**.
5. Jeżeli administrator w celu wykonania zawartej z innym podmiotem umowy głównej **powierza** takiemu podmiotowi zewnętrznemu do przetwarzania dane osobowe, każdorazowo podpisuje z podmiotem trzecim jako Procesorem (Podmiotem przetwarzającym) **dodatkowo „Umowę powierzenia”**, **której wzór określa Załącznik nr 4 do Polityki**, tj. „Wzory dokumentów stosowanych przez Spółkę w zakresie ochrony danych osobowych”.
6. Przykładem transferu danych, o którym mowa w **ust. 5 powyżej**, jest powierzenie przez Spółkę do przetwarzania danych osobowych podmiotowi trzeciemu wykonującemu na rzecz Spółki usługi w obszarze IT lub w zakresie kadrowo płacowym (rachunkowym), a także w ramach wykonywania na rzecz Spółki przez podmiot trzeci usług w obszarze BHP, w tym szkolenia BHP.
7. W sytuacji, w której **podmiot trzeci w celu wykonania umowy głównej powierza Spółce dane osobowe do przetworzenia**, podmiot ten powinien zawrzeć ze Spółką „Umowę powierzenia”, co stanowi wypełnienia obowiązku określonego w art. 28 RODO. Umowa określa obowiązki Spółki jako Podmiotu Przetwarzającego w zakresie ochrony danych osobowych.
8. Ponieważ **udostępnienie danych osobowych** stanowi przekazanie danych do podmiotu, który samodzielnie będzie decydował o celach i sposobach przetwarzania tych danych, udostępniając dane osobowe administrator przekazuje je innemu administratorowi **bez zlecenia mu konkretnej czynności**, w trakcie której dochodzi do przetwarzania danych osobowych przez podmiot trzeci.
9. **Udostępnienie stanowi formę przetwarzania** danych osobowych, co oznacza, że aby udostępnić dane osobowe, administrator musi dysponować ku temu odpowiednią przesłanką legalizującą. Skutkiem udostępnienia danych osobowych, jest utrata kontroli nad przetwarzaniem przekazanych danych. W momencie udostępnienia, administrator przestaje już decydować o celach i sposobach przetwarzania danych. Będzie już do tego uprawniony podmiot, który te dane odebrał. Oznacza to, że odpowiedzialność za przetwarzanie danych osobowych, dla jednego podmiotu kończy się, a dla drugiego zaczyna, w momencie przekazania tych danych.
10. Przykładem transferu danych, o którym mowa w **ust. 8 oraz 9 powyżej**, jest transfer danych realizowanych przez Spółkę na rzecz podmiotów uprawnionych na podstawie powszechnie obowiązujących przepisów prawa (Policja, Sąd, Prokuratura, ZUS, US itp.). W takim przypadku podstawą prawną udostępnienia danych jest **art. 6 ust. 1 lit. c) RODO**, tj. obowiązek prawny ciążyący na Spółce.

11. Formą udostępnienia danych przez Spółkę innemu podmiotowi jest także **przekazanie przez Spółkę danych osobowych swoich pracowników podmiotowi trzeciemu korzystającemu z usługi „outsourcingu pracowników”**, rozumianej tutaj jako metoda organizacji i zarządzania, polegająca na względnie trwałym, długoterminowym, opartym na kontrakcie, przeniesieniu przez podmiot korzystający z outsourcingu odpowiedzialności za realizację określonych obszarów działalności gospodarczej (zadań, funkcji lub procesów) na stronę wyspecjalizowanego partnera zewnętrznego (tutaj: Spółka).
12. Przy takim założeniu „odbiorca usługi outsourcingowej” kwalifikowany jest tutaj jako niezależny administrator danych osobowych. Wynika to z faktu, że po jego stronie występują **własne środki przetwarzania i własne cele**, które mogą obejmować m. in.: czynności związane z udostępnieniem lokalu i pomieszczeń, w których są wykonywane usługi, weryfikację jakości, wydajności, czasu trwania usługi, zaopatrzenie w środki ochrony indywidualnej outsourcingowanych pracowników, ewentualne przekazania narzędzi niezbędnych do realizacji usługi, w tym przetwarzanie danych w ramach innych form monitoringu, o których mowa w art. 22³ Kodeksu Pracy, oraz inne uzasadnione czynności.
13. Spółka jako Pracodawca, będąca administratorem danych osobowych pracowników outsourcingowanych innemu podmiotowi, udostępnia dane osobowe swoich pracowników w ramach w/w usługi na podstawie **art. 6 ust. 1 lit. f) RODO**, tj. prawnie uzasadniony interes administratora, a w przypadku danych osobowych szczególnej kategorii (dane dotyczące zdrowia) na podstawie **art. 9 ust. 2 lit. b) RODO** lub **art. 9 ust. 2 lit. h) RODO**.
14. Na „odbiorcy usługi outsourcingowej”, jako niezależnemu administratorowi, ciąży obowiązek wynikający z art. 13 lub/oraz 14 RODO, tj. „obowiązek informacyjny”, dotyczący procesów, w ramach których przetwarza on dane osobowe pracowników outsourcingowanych.
15. Polityka uwzględnia w całokształcie procesów przetwarzania danych osobowych dwa istotne podejścia realizacji zasad przetwarzania danych osobowych:
- 1) Privacy by Design,
 - 2) Privacy by Default.
16. Ilekroć Spółka występuje w roli administratora, podejmuje następujące działania w celu zgodnego z prawem przetwarzania danych osobowych:
- 1) Ustala cel i zakres (tj. sposoby) przetwarzania, identyfikuje przepływ danych osobowych adekwatnie do celu przetwarzania;
 - 2) Wykonuje w określonych sytuacjach analizę DPIA w oparciu o „*Procedurę Oceny Skutków dla Ochrony Danych, Ogólnej Analizy Ryzyka oraz Testu Równowagi*”, stanowiącą **Załącznik nr 3** do Polityki;
 - 3) Dokonuje pomiaru ryzyka dla przetwarzanych przez siebie danych w oparciu o „*Procedurę Oceny Skutków dla Ochrony Danych, Ogólnej Analizy Ryzyka oraz Testu Równowagi*”, stanowiącą **Załącznik nr 3** do Polityki;

- 4) Prowadzi i aktualizuje *Rejestr Czynności Przetwarzania* oraz *Rejestr Kategorii Czynności Przetwarzania*, zgodnie z „Wzorami dokumentów stosowanymi przez Spółkę w zakresie ochrony danych osobowych”, stanowiącymi **Załącznik nr 4** do Polityki
- 5) Rozpoczyna przetwarzanie danych osobowych tylko, gdy istnieje zgodna z prawem podstawa przetwarzania tych danych (w tym zbiera zgody na przetwarzanie danych osobowych, gdy to zgoda jest podstawą przetwarzania danych osobowych - i zarazem nie zbiera takich zgód, gdy ADO przetwarza dane osobowe na podstawie innej przesłanki prawnej); zasady wyznaczające sposoby definiowania prawnej przesłanki przetwarzania danych zgodnie z przyjętymi „Wzorami dokumentów stosowanymi przez Spółkę w zakresie ochrony danych osobowych”, stanowiącymi **Załącznik nr 4** do Polityki.
- 6) Realizuje obowiązek informacyjny, zgodnie z przyjętymi „Wzorami dokumentów stosowanymi przez Spółkę w zakresie ochrony danych osobowych”, stanowiącymi **Załącznik nr 4** do Polityki;
- 7) Realizuje prawa podmiotów danych poprzez obsługę dyspozycji, zgodnie z „*Procedurą obsługi praw osoby, której dane dotyczą w zakresie ochrony danych*”, stanowiącą **Załącznik nr 1** do Polityki.
- 8) Wprowadza środki techniczne i organizacyjne związane z bezpieczeństwem danych osobowych zgodnie z odpowiednimi zapisami niniejszej Polityki oraz procedurami powiązanymi;
- 9) Obsługuje incydenty bezpieczeństwa danych osobowych zgodnie z „*Procedurą reagowania na naruszenie ochrony danych osobowych i zawiadomienia o naruszeniu*”, stanowiącą **Załącznik nr 5** do Polityki;
- 10) Jeśli powierza dane „Podmiotowi przetwarzającemu”, sprawuje nad nim kontrolę zgodnie z „*Procedurą obsługi praw osoby, której dane dotyczą oraz przestrzegania przepisów przez stronę trzecią*”, stanowiącą **Załącznik nr 1** do Polityki;
- 11) Przechowuje dane przez zgodnie z zasadami określonymi w niniejszej Polityce;
- 12) Przeprowadza „testy równowagi”, dla wszystkich procesów przetwarzania, dla których podstawą przetwarzania jest prawnie uzasadniony interes administratora zgodnie z „*Procedurą Oceny Skutków dla Ochrony Danych, Ogólnej Analizy Ryzyka oraz Testu Równowagi*”, stanowiącą **Załącznik nr 3** do Polityki;
- 13) Zapewnia, aby osobom przetwarzającym dane osobowe w jego imieniu, zostały wydane upoważnienia do przetwarzania danych osobowych, zgodnie z wzorem określonym we *Wzorach dokumentów stosowanych przez Spółkę w zakresie ochrony danych osobowych*”, stanowiących **Załącznik nr 4** do Polityki

- 14) Zapewnia, aby wydane upoważnienia do przetwarzania danych osobowych zostały wpisane do *Rejestru Upoważnień*, którego wzór określa **Załącznik nr 4** do niniejszej Polityki, tj. *Wzory dokumentów stosowanymi przez Spółkę w zakresie ochrony danych osobowych*”;
- 15) Wydaje upoważnienia do przetwarzania danych osobom przetwarzającym dane osobowe w jego imieniu, których wzory określa **Załącznik nr 4** do Polityki, tj. *Wzory dokumentów stosowanych przez Spółkę w zakresie ochrony danych osobowych*”;
17. Ilekroć Spółka występuje w roli Procesora, wykonuje przy tym następujące działania:
- 1) Ustala zakres przetwarzania danych osobowych w oparciu o umowę powierzenia,
 - 2) Uzupełnia *Rejestr Kategorii Czynności Przetwarzania*,
 - 3) Rozpoczyna przetwarzanie danych osobowych zgodnie z umową powierzenia,
 - 4) Obsługuje dyspozycje podmiotów danych zgodnie z zapisami umowy powierzenia i w ścisłej współpracy z ADO;
 - 5) Wprowadza środki techniczne i organizacyjne związane z bezpieczeństwem danych osobowych, zgodnie z wymaganiami niniejszej Polityki,
 - 6) Obsługuje incydenty bezpieczeństwa danych osobowych, zgodnie z warunkami umowy powierzenia, posilając się w razie potrzeby *”Procedurą reagowania na naruszenie ochrony danych osobowych i zawiadomienia o naruszeniu”*, stanowiącą **Załącznik nr 5** do Polityki.
 - 7) Po zakończeniu świadczenia usług działa zgodnie z postanowieniami umowy powierzenia (np. zwraca wszystkie przetwarzane dane osobowe i usuwa je ze swoich systemów IT).
18. Przetwarzanie danych osobowych przez inny podmiot przetwarzający, nazywany Procesorem, odbywa się wyłącznie na wyraźne zlecenie Administratora na podstawie umowy powierzenia przetwarzania danych osobowych, która podlega prawu Unii Europejskiej lub prawu państwa członkowskiego Unii Europejskiej. Administrator wdrożył standardowy i zunifikowany wzór takiej umowy, określony w **Załączniku nr 4** do Polityki, tj. *Wzorami dokumentów stosowanymi przez Spółkę w zakresie ochrony danych osobowych*”, przy czym administrator może każdorazowo zaakceptować projekt umowy zaproponowany przez stronę trzecią, pod warunkiem pozytywnej akceptacji prawnika lub osoby, o której mowa w **Rozdziale 1**.
19. Zasady dokumentowania i raportowania stanu bezpieczeństwa stosowane przez administratora stanowią podstawowy element wymogów rzetelności i przejrzystości, a zwłaszcza rozliczalności przetwarzania. Dokumentowanie informacji o przetwarzaniu danych jest utrzymywane i aktualizowane w następujących rejestrach:
- 1) *Rejestrze Czynności Przetwarzania* oraz *Rejestrze Kategorii Czynności Przetwarzania*, których wzory określa **Załącznik nr 4** do niniejszej Polityki, tj. *Wzory dokumentów stosowane przez Spółkę w zakresie ochrony danych osobowych*

- 2) *Rejestrze Umów Powierzenia* których wzory określa **Załącznik nr 4** do niniejszej Polityki, tj. *Wzory dokumentów stosowane przez Spółkę w zakresie ochrony danych osobowych*.
20. Zasady dotyczące przetwarzania danych osobowych pracowników Spółki oraz osób ubiegających się o zatrudnienie określa **Załącznik nr 6** do Polityki, tj. *„Zasady dotyczące przetwarzania danych osobowych pracowników Spółki oraz osób ubiegających się o zatrudnienie”*.

Rozdział 8. Reagowanie na przypadki naruszenia ochrony danych osobowych

1. W przypadku gdy administrator stwierdzi naruszenie ochrony danych osobowych lub będzie podejrzewać wystąpienie takiego naruszenia, zobowiązany jest do niezwłocznego przeprowadzenia wewnętrznego dochodzenia i podjęcia właściwych środków naprawczych zgodnie z *„Procedurą reagowania na naruszenie ochrony danych osobowych i zawiadomienia o naruszeniu”*. Jeśli istnieje ryzyko naruszenia praw i wolności osób, których dane dotyczą, niezwłocznie, a jeśli to możliwe, w ciągu 72 godzin od stwierdzenia naruszenia, zawiadamia odpowiednie organy ochrony danych.
2. Administrator wdraża narzędzie, na podstawie którego określa stopień naruszenia praw i wolności osób, których dotyczy naruszenie. **Szczegóły w tym zakresie określa zgodnie z „Procedurą reagowania na naruszenie ochrony danych osobowych i zawiadomienia o naruszeniu”, stanowiącą Załącznik nr 5 do Polityki.**

Rozdział 9. Retencja danych

1. O ile obowiązujące przepisy prawa nie przewidują inaczej lub gdy administrator nie wprowadzi dla danego procesu przetwarzania indywidualnego okresu retencji danych, za wymagany okres retencji uznaje się **5 lat**, licząc od końca roku, w którym sporządzono dany dokument.
2. W ramach wyjątku czas retencji może zostać zmieniony w przypadku:
 - 1) Trwającego dochodzenia prowadzonego przez władze państwa członkowskiego, jeśli istnieje możliwość, że dokumentacja z danymi osobowymi będzie potrzebna, aby administrator mógł wykazać przestrzeganie wszelkich wymogów prawnych;
 - 2) Wykonywania praw ustawowych wynikających z postępowań sądowych uznanych przez lokalne przepisy prawa.
3. Dokumenty, które mogą być rutynowo niszczone, pod warunkiem że nie są wymagane w toczącym się postępowaniu sądowym lub regulacyjnym, to:
 - 1) Ogłoszenia i zawiadomienia na temat codziennych spotkań i innych wydarzeń, w tym zatwierdzenia i przeprosiny;

- 2) Prośby o informacje na temat zwykłych kwestii, takich jak na przykład wskazówki dojazdu, rezerwacje na spotkania wewnętrzne bez opłat / kosztów zewnętrznych;
 - 3) Dokumenty przesyłane takie jak listy, strony tytułowe faksów, wiadomości e-mail, bilety określające obieg dokumentów, bilety grzecznościowe i inne elementy dołączone do dokumentów, które jednak niczego do nich nie wnoszą;
 - 4) Informacje o zanotowanych wiadomościach, listy adresowe, dystrybucyjne itp. zastąpione nowymi listami, publikacje administratora, które są nieaktualne lub zostały zastąpione innymi lub magazyny branżowe, katalogi ofertowe, ulotki i biuletyny od dostawców lub innych zewnętrznych organizacji;
 - 5) Kopie dokumentów, na przykład kopie załączone do wiadomości za pomocą opcji CC lub FYI, niezmienione wersje robocze, wydruki obrazu stanu chwilowego lub wyciągi z baz danych i plikiienne.
4. Procedura usuwania musi odbywać się zgodnie ze wszelkimi wymogami ujawnienia informacji, które mogą zostać narzucone w ramach postępowania sądowego, np. jeśli postępowanie sądowe jest w toku, nie należy usuwać powiązanych dokumentów.
 5. Administrator stosuje *Harmonogram Retencji Danych* określający indywidualne okresy retencji danych dla wskazanych tam procesów. *Harmonogram Retencji Danych* znajduje się w **Załączniku nr 4** do Polityki, tj. *Wzory dokumentów stosowane przez Spółkę w zakresie ochrony danych osobowych*.
 6. W **Załączniku nr 7** do Polityki znajduje się wzór oświadczenia, do którego podpisania zobowiązany jest każdy pracownik administratora.

Rozdział 10. Środki organizacyjne dotyczące ochrony danych osobowych

1. Administrator potwierdza wdrożenie następujących środków organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych:
 - 1) Została opracowana i wdrożona polityka ochrony danych osobowych;
 - 2) Została opracowana i wdrożona instrukcja zarządzania systemem informatycznym;
 - 3) Do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające ważne upoważnienia nadane przez Administratora danych;
 - 4) Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych;
 - 5) Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych;
 - 6) Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego;

- 7) Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
 - 8) Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane
 - 9) Kopie zapasowe danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco;
 - 10) Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
 - 11) Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych'
 - 12) Stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe
 - 13) Administrator prowadzi „politykę czystego biurka i ekranu”.
2. Administrator potwierdza wdrożenie następujących środków ochrony fizycznej zapewniające poufność, integralność i rozliczalność przetwarzanych danych osobowych:
- 1) Dane osobowe przetwarzane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmocnionymi, nie przeciwpożarowymi);
 - 2) Budynek, w którym przetwarzane są dane osobowe wyposażone są w system alarmowy przeciwwłamaniowy;
 - 3) Dostęp do pomieszczeń, w których przetwarzane są dane osobowe objęte są systemem kontroli dostępu;
 - 4) Dostęp do budynku, w którym przetwarzane są dane osobowe kontrolowany jest przez system monitoringu z zastosowaniem kamer przemysłowych;
 - 5) Dane osobowe przetwarzane w formie papierowej przechowywane są w zamkniętej niemetalowej szafie;
 - 6) Kopie zapasowe/archiwalne danych osobowych przechowywane są w zamkniętej niemetalowej szafie.
 - 7) Pomieszczenie, w którym przetwarzane są dane osobowe zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy;
 - 8) Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.
3. Administrator potwierdza wdrożenie następujących środków sprzętowych infrastruktury informatycznej i telekomunikacyjnej zapewniających poufność, integralność i rozliczalność przetwarzanych danych osobowych:
- 1) Dane osobowe przetwarzane są przy użyciu komputera przenośnego;

- 2) Komputer służący do przetwarzania danych osobowych nie jest połączony z lokalną siecią komputerową;
 - 3) Zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania;
 - 4) Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
 - 5) Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.
 - 6) Zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł;
 - 7) Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych;
 - 8) Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji;
 - 9) Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia;
 - 10) Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity;
 - 11) Użyto system Firewall do ochrony dostępu do sieci komputerowej.
4. Administrator potwierdza wdrożenie następujących środków ochrony w ramach narzędzi programowych i baz danych zapewniających poufność, integralność i rozliczalność przetwarzanych danych osobowych:
- 1) Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych;
 - 2) Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych;
 - 3) Dostęp do danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;
 - 4) Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym danych osobowych dla poszczególnych użytkowników systemu informatycznego;
 - 5) Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do danych osobowych;
 - 6) Zastosowano kryptograficzne środki ochrony danych osobowych;
 - 7) Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe;

- 8) Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

Rozdział 11. Zasady funkcjonowania Polityki

1. Politykę zatwierdza i wprowadza w życie Prokurent Spółki.
2. Polityka wraz załącznikami podlega co rok cyklicznemu przeglądowi wraz z ewentualną jej aktualizacją.
3. Dokument obowiązuje od dnia podjęcia decyzji przez Prokurenta wprowadzającej niniejszą regulację oraz uchylającej dotychczas obowiązujące dokumenty w tym zakresie.

Rozdział 12. Załączniki

Załącznik nr 1	Procedura obsługi praw osoby, której dane dotyczą oraz przestrzegania przepisów przez stronę trzecią
Załącznik nr 2	Wzory Klauzul Informacyjnych stosowanych przez administratora
Załącznik nr 3	Procedura <i>Oceny Skutków dla Ochrony Danych, Ogólnej Analizy Ryzyka oraz Testu Równowagi</i>
Załącznik nr 4	Wzory dokumentów stosowane przez Spółkę w zakresie ochrony danych osobowych
Załącznik nr 5	Procedura reagowania na naruszenie ochrony danych osobowych i zawiadomienia o naruszeniu
Załącznik nr 6	Zasady dotyczące przetwarzania danych osobowych pracowników Spółki oraz osób ubiegających się o zatrudnienie
Załącznik nr 7	Oświadczenie pracownika o zapoznaniu się z procedurą.

[data i miejsce]

[podpis]