POLITYKA OCHRONY DANYCH OSOBOWYCH

Innova-Med sp. z o.o.

Data wprowadzenia:	19-02-2020 r.
Wersja:	1.0
Daty aktualizacji:	-
Opracował:	
Zatwierdził:	Michał Brancewicz Prezes zarządu Paulina Maria Pająk Wiceprezes zarządu

SPIS TREŚCI

INFORMACJE OGÓLNE

1. CEL POLITYKI OCHRONY DANYCH OSOBOWYCH

Polityka ochrony danych osobowych została opracowana i wdrożona w strukturze Administratora Danych w celu zapewnienia zgodności przetwarzania danych osobowych z wymogami obowiązujących w tym zakresie polskich i europejskich 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 roku o ochronie danych osobowych (tekst jedn. Dz. U. z 2018, poz. 1000).

Polityka ochrony danych osobowych ma zastosowanie do wszystkich pracowników Administratora Danych, którzy w zakresie swoich obowiązków służbowych przetwarzają dane osobowe, jak również innych osób, które z upoważnienia Administratora Danych uzyskały dostęp do danych osobowych. Każda z tych osób została zapoznana z najważniejszymi procedurami bezpieczeństwa danych opisanymi w Polityce ochrony danych osobowych i zobowiązana do ich przestrzegania w zakresie wynikającym z przydzielonych zadań. Osoby, o których mowa złożyły oświadczenie o zapoznaniu się z postanowieniami niniejszej Polityki oraz zobowiązały się do ich stosowania.

Wszelkie wątpliwości dotyczące sposobu interpretacji zapisów Polityki ochrony danych osobowych, powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą.

2. DEFINICJE

1. **Administrator Danych (ADO)** – Innova-Med sp. z o.o. z siedzibą w Łodzi 90-365, ul. ks. bpa Wincentego Tymienieckiego 16 G/ 66, wpisana do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla Łodzi- Śródmieścia w Łodzi, XX Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000802853 posiadająca NIP 7252292477, REGON 384336870, kapitał zakładowy w wysokości 100 000, 00 zł
2. **dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"), 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,
3. **Inspektor Ochrony Danych (IOD) –** 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,
4. **Polityka** – niniejsza Polityka ochrony danych osobowych,
5. **pracownik** – osoba współpracująca z Administratorem Danych na podstawie umowy o pracę lub umowy cywilnoprawnej,
6. **przetwarzanie** – operacja 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,
7. **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),
8. **Ustawa** – Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2018, poz. 1000),
9. **państwo trzecie** – państwo nienależące do Europejskiego Obszaru Gospodarczego.

3. ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ OCHRONY DANYCH OSOBOWYCH ORAZ ZAKRES ZASTOSOWANIA

Polityka 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 Administratora Danych. Polityka odnosi się całościowo do problemu zabezpieczenia danych osobowych, tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych.

Politykę ochrony danych osobowych stosuje się do wszelkich czynności, stanowiących w myśl RODO, przetwarzanie danych osobowych. Bez względu na źródło pochodzenia danych osobowych, ich zakres, cel zebrania, sposób przetwarzania lub czas przetwarzania, stosowane są zasady ujęte w 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.

OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

1. STRUKTURA ORGANIZACJI OCHRONY DANYCH OSOBOWYCH

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

1. Administrator Danych,
2. Administrator Systemów Informatycznych (o ile występuje),
3. Osoby upoważnione do przetwarzania danych osobowych.

1.1. ADMINISTRATOR DANYCH

1. Administrator Danych wyznacza:
   - 1.1. IOD,
   - 1.2. Administratora Systemów Informatycznych (o ile uzna to za niezbędne i konieczne)
2. Administrator Danych jest odpowiedzialny za:
   - 2.1. zapewnienie odpowiednich środków organizacyjnych i technicznych w celu zapewnienia i wykazania przetwarzania danych osobowych zgodnie z określonymi w RODO zasadami przetwarzania danych osobowych,
   - 2.2. jeśli uzna to za konieczne, wdrożenie odpowiednich procedur ochrony danych osobowych,
   - 2.3. 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,
   - 2.4. zapewnienie środków umożliwiających prawidłowa realizację praw osób, których dane dotyczą,
   - 2.5. prowadzenie rejestru czynności przetwarzania danych osobowych,
   - 2.6. prowadzenie rejestru kategorii przetwarzania dokonywanych w imieniu innego administratora,
   - 2.7. współpracę z organem nadzorczym w ramach wykonywania przez niego swoich zadań,
   - 2.8. wdrożenie odpowiednich środków organizacyjnych i technicznych, aby zapewnić stopień bezpieczeństwa odpowiadający istniejącemu ryzyku naruszenia praw lub wolności osób, których dane dotyczą,

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

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

2.11. zapewnienie odpowiednich środków w celu dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych w sytuacji, jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w tym, jeżeli zajdą ku temu odpowiednie przesłanki, konsultację z organem nadzorczym,

2.12. nadawanie upoważnień do przetwarzania danych osobowych oraz prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,

2.13. zapewnienie legalności przekazywania danych osobowych do podmiotów trzecich,

2.14. w przypadku powołania IOD:

2.14.1. zapewnienie, że jest on właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych,

2.14.2. wspieranie IOD 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,

2.14.3. zagwarantowanie by IOD nie działał pod wpływem presji i nie otrzymywał instrukcji dotyczących wykonywania swoich zadań,

2.14.4. publikację danych kontaktowych IOD oraz zawiadomienie o nich organu nadzorczego.

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

12. INSPEKTOR OCHRONY DANYCH

1. W chwili obecnej ADO nie powołał Inspektora Ochrony Danych Osobowych z uwagi na niespełnienie przesłanek prawnych warunkujących konieczność jego powołania. Jednak w przypadku rozpoczęcia przetwarzania szczególnych kategorii danych osobowych na dużą skalę ADO powoła Inspektora ochrony danych. Do tego momentu zadania określone w niniejszym rozdziale wypełniać będzie Administrator danych.
2. Funkcję IOD pełni osoba wyznaczona przez Administratora Danych.
3. Wzory dokumentów wyznaczenia oraz odwołania IOD znajdują się w załączniku do Polityki.
4. IOD 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.
5. Do zadań powołanego IOD będzie należeć:
    - 5.1. informowanie o obowiązkach wynikających z RODO oraz innych właściwych przepisów Unii lub państw członkowskich o ochronie danych osobowych oraz doradzanie w tym zakresie,
    - 5.2. monitorowanie przestrzegania RODO oraz innych właściwych przepisów Unii lub państw członkowskich o ochronie danych osobowych,
    - 5.3. monitorowanie przestrzegania wdrożonych procedur ochrony danych osobowych,
    - 5.4. doradztwo w zakresie podziału obowiązków (np. między współadministratorami, Administratorem Danych a podmiotem przetwarzającym lub pomiędzy pracownikami Administratora Danych),
    - 5.5. działania zwiększające świadomość pracowników Administratora Danych w zakresie obowiązków wynikających z RODO lub przyjętych procedur,
    - 5.6. szkolenia dla pracowników Administratora Danych uczestniczących w operacjach przetwarzania danych,
    - 5.7. przeprowadzanie audytów w zakresie przestrzegania RODO i wdrożonych procedur ochrony danych osobowych,
    - 5.8. udzielanie na żądanie zaleceń, co do oceny skutków dla ochrony danych osobowych oraz monitorowanie jej wykonania,
    - 5.9. współpraca z organem nadzorczym oraz pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych,
    - 5.10. pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

1.3. ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

1. Funkcję ASI pełni osoba wyznaczona przez Administratora Danych.
2. Wzory dokumentów wyznaczenia oraz odwołania ASI znajdują się w załączniku do Polityki.
3. Do zadań ASI należy:
   - 3.1. prowadzenie rejestru nadanych uprawnień do systemów informatycznych,
   - 3.2. opracowywanie oraz aktualizacja Załącznika nr 7 do Polityki, który stanowi ogólny opis technicznych środków bezpieczeństwa wdrożonych w strukturze Administratora Danych,
   - 3.3. nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,
   - 3.4. podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,
   - 3.5. identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych,
   - 3.6. sprawowanie nadzoru nad kopiami zapasowymi;
   - 3.7. inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych,
   - 3.8. podejmowanie innych czynności w zakresie zabezpieczenia przetwarzania danych w systemach informatycznych,
   - 3.9. dokonywanie cyklicznych przeglądów aktualności i stosowania procedur z zakresu przetwarzania danych w systemach informatycznych, na podstawie opracowanego planu przeglądów.
   - 3.10. ścisła współpraca z IOD w zakresie bezpieczeństwa i zasad przetwarzania danych osobowych w systemach informatycznych.

1.4. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Każda osoba, która uzyskała upoważnienie do przetwarzania danych, zobowiązana jest do ich ochrony w sposób zgodny z przepisami RODO, Ustawy oraz postanowieniami Polityki.
2. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu upoważnienia.
3. Naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy skutkuje poniesieniem odpowiedzialności na podstawie przepisów Ustawy oraz stanowi ciężkie naruszenie obowiązków pracowniczych i 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. 917 ze zm.) bądź rozwiązania stosunku cywilnoprawnego.

C. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. OGÓLNE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. 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:

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

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

   1.3 w sposób przejrzysty dla osób, których dane dotyczą (*zasada przejrzystości*),

   1.4 w konkretnych, wyraźnych i prawnie uzasadnionych celach (*zasada ograniczenia celu*),

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

   1.6 przy uwzględnieniu ich prawidłowości i ewentualnego uaktualniania (*zasada prawidłowości*),

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

   1.8 w sposób zapewniający odpowiednie bezpieczeństwo (*integralność i poufność*).

2. Administrator Danych gwarantuje, 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. ZAKRES PRZETWARZANYCH DANYCH OSOBOWYCH

1. Polityka ma zastosowanie w stosunku do wszystkich danych osobowych przetwarzanych przez Administratora Danych, niezależnie od formy ich przetwarzania (elektroniczna lub papierowa) oraz tego, czy są to dane przetwarzane w zbiorach danych, w zestawach czy stanowią one pojedyncze informacje osobowe.
2. Wykaz zbiorów danych osobowych, których administratorem jest Administrator Danych oraz procesów przetwarzania zachodzących w tych zbiorach stanowi załącznik do Polityki.
3. Administrator Danych prowadzi:
   - 3.1. rejestr czynności przetwarzania danych osobowych, których jest administratorem,
   - 3.2. rejestr kategorii czynności przetwarzania dokonywanych w imieniu administratorów, którzy powierzyli mu przetwarzanie danych.
4. Rejestr, o którym mowa w pkt 3.1. może zawierać co najmniej następujące informacje:
   - 4.1. nazwę oraz dane kontaktowe Administratora Danych oraz wszelkich współadministratorów,
   - 4.2. gdy ma to zastosowanie imię, nazwisko lub nazwę oraz dane kontaktowe swojego przedstawiciela,
   - 4.3. imię i nazwisko oraz dane kontaktowe IOD,
   - 4.4. cele przetwarzania,
   - 4.5. opis kategorii osób, których dane dotyczą,
   - 4.6. opis kategorii danych osobowych,
   - 4.7. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,
   - 4.8. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,
   - 4.9. jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
   - 4.10. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.
5. Rejestr, o którym mowa w pkt 3.2. może zawierać co najmniej następujące informacje:
   - 5.1. nazwę oraz dane kontaktowe Administratora Danych,
   - 5.2. imię i nazwisko lub nazwę oraz dane kontaktowe każdego administratora, w imieniu którego działa Administrator Danych,
   - 5.3. gdy ma to zastosowanie, imię, nazwisko lub nazwę oraz dane kontaktowe przedstawiciela każdego administratora, w imieniu którego działa Administrator Danych,

5.4. gdy ma to zastosowanie, imię i nazwisko oraz dane kontaktowe IOD każdego administratora, w imieniu którego działa Administrator Danych,

5.5. kategorie przetwarzań dokonywanych w imieniu każdego z administratorów,

5.6. gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,

5.7. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

6. Administrator Danych prowadzi rejestry, o których mowa w pkt 3 w formie elektronicznej oraz papierowej.

7. W przypadku zgłoszenia przez organ nadzoru żądania w tym zakresie, Administrator Danych udostępnia mu prowadzone przez siebie rejestry.

3. DOPUSZCZENIE OSÓB DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator Danych realizując Politykę, w zakresie udostępniania danych osobowych w ramach własnej (wewnętrznej) struktury, zezwala na ich przetwarzanie w systemie informatycznym lub w wersji papierowej wyłącznie osobom, które uzyskały uprzednie, stosowne upoważnienie do przetwarzania danych osobowych.
2. Upoważnienie do przetwarzania danych osobowych nadawane jest po przeprowadzeniu szkolenia lub zaznajomieniu w innej formie, osoby upoważnianej z zasadami ochrony danych osobowych obowiązującymi w strukturze Administratora Danych.
3. Upoważnienie do przetwarzania danych osobowych, nadawane jest zgodnie z opracowaną i wdrożoną na tą okoliczność procedurą.
4. Administrator Danych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, której wzór stanowi załącznik do Polityki.

4. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. 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.
2. 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. Zawierana przez Administratora Danych umowa powierzenia przetwarzania danych osobowych musi być zgodna z postanowieniami art. 28 RODO, tj. w szczególności określać:
   - 3.1. przedmiot powierzenia,
   - 3.2. czas trwania powierzenia,
   - 3.3. charakter i cel przetwarzania,
   - 3.4. rodzaj powierzanych danych osobowych,
   - 3.5. kategorie osób, których dane dotyczą,
   - 3.6. warunki podpowierzenia przetwarzania danych,
   - 3.7. obowiązki i prawa Administratora Danych,
   - 3.8. obowiązki podmiotu przetwarzającego.
4. Umowa powierzenia może zostać zawarta w formie pisemnej, w tym elektronicznej.
5. Za zawieranie umów powierzenia przetwarzania danych osobowych odpowiadają osoby składające oświadczenie woli w imieniu administratora danych zgodnie z dokumentami rejestrowymi Administratora Danych.
6. Administrator Danych przed planowanym rozpoczęciem współpracy z podmiotem przetwarzającym, jest zobowiązany poinformować o tym IOD (o ile został powołany) oraz skonsultować z nim postanowienia zawieranej umowy w zakresie powierzenia przetwarzania danych osobowych.
7. Umowa powierzenia przetwarzania danych osobowych podpisywana jest zgodnie z zasadami reprezentacji Administratora Danych lub udzielonymi pełnomocnictwami.
8. Każdorazowe dokonanie powierzenia danych osobowych musi zostać obligatoryjnie odnotowane w rejestrze czynności przetwarzania danych osobowych.
9. Administrator Danych ma prawo kontroli podmiotów przetwarzających, którym powierzył przetwarzanie danych osobowych.

10. Administrator Danych w zakresie prowadzonej przez siebie działalności może przetwarzać również dane osobowe powierzone przez podmioty, na rzecz których świadczy usługi. Przyjęcie danych w powierzenie przez Administratora Danych musi zostać obligatoryjnie odnotowane w rejestrze kategorii czynności przetwarzania danych osobowych.

5. UDOSTĘPNIENIE DANYCH OSOBOWYCH

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

6. PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH

1. Przekazywanie danych, których administratorem jest Administrator Danych do państw trzecich i organizacji międzynarodowych, może się odbywać wyłącznie po spełnieniu warunków przewidzianych w Rozdziale V RODO.

2. Przekazywanie danych do państw trzecich może mieć formę zarówno powierzenia przetwarzania danych osobowych oraz udostępnienia danych osobowych, co oznacza, że w zależności od rodzaju przekazania, należy wziąć również pod uwagę postanowienia podrozdziałów 4 i 5 Polityki.

3. Przekazanie danych osobowych, których administratorem jest Administrator Danych do państwa trzeciego może nastąpić w sytuacji, jeżeli Komisja Europejska wydała decyzję, że dane państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Takie przekazanie nie wymaga specjalnego zezwolenia.

4. W przypadkach braku decyzji Komisji Europejskiej, o której mowa w pkt 3, dokonanie transferu danych do państwa trzeciego jest możliwe, gdy Administrator Danych samodzielnie zapewni odpowiednie zabezpieczenia i pod warunkiem, że będą obowiązywały egzekwowalne prawa osób, których dane dotyczą i skuteczne środki ochrony prawnej za pomocą:

4.1. wiążących reguł korporacyjnych (*Binding Corporate Rules*) zatwierdzonych przez organ nadzorczy, mających zastosowanie do każdego z członków grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą,

4.2. standardowych klauzul ochrony danych (*Standard Contracual Clauses*) przyjętych lub zatwierdzonych przez Komisję Europejską,

4.3. zatwierdzonego kodeksu postępowania, lub

4.4. zatwierdzonego mechanizmu certyfikacji.

5. W szczególnych przypadkach, dopuszcza się przekazanie danych osobowych przez Administratora Danych do państwa trzeciego pomimo braku decyzji Komisji Europejskiej, o której mowa w pkt 3 oraz zapewnienia odpowiednich zabezpieczeń, o których mowa w pkt 4. Do tych szczególnych przypadków zalicza się przekazanie danych pod warunkiem, że:

5.1. osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którymi może się dla niej wiązać proponowane przekazanie, wyrazi na nie wyraźną zgodę,

5.2. przekazanie jest niezbędne do wykonania umowy zawartej z osobą, której dane dotyczą,

5.3. przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, której dane dotyczą,

5.4. przekazanie jest niezbędne ze względu na ważne względy interesu publicznego,

5.5. przekazanie jest niezbędne ze względu na posiadane roszczenia,

5.6. przekazanie jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą lub

5.7. przekazanie nastąpi z publicznego rejestru.

6. Administrator Danych przed planowanym przekazaniem danych do państwa trzeciego, jest zobowiązany poinformować o tym IOD (o ile został powołany) oraz skonsultować z nim warunki przekazania tych danych.

7. WSPÓŁADMINISTROWANIE DANYMI OSOBOWYMI

1. Administrator Danych w zakresie przetwarzanych przez siebie danych osobowych dopuszcza możliwość przyjęcia modelu współadministrowania danymi osobowymi zgodnie z art. 26 RODO.
2. 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:
   2.1. być administratorami w rozumieniu art. 4 pkt 7 RODO,
   2.2. muszą wspólnie ustalić cele przetwarzania danych,
   2.3. muszą wspólnie ustalić sposoby (techniczne i organizacyjne) przetwarzania danych osobowych.
3. W przypadku spełnienia warunków, o których mowa w pkt 2 Administrator Danych oraz co najmniej jeden inny podmiot stają się współadministratorami danych w zakresie danego procesu przetwarzania danych osobowych.
4. W przypadku przyjęcia modelu współadministrowania danymi, współadministratorzy danych w drodze wspólnych uzgodnień, w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO.
5. W sytuacji, kiedy w zakresie zachodzących w strukturze Administratora Danych procesów przetwarzania danych osobowych pojawią się procesy, wobec których istnieje prawdopodobieństwo zachodzenia współadministrowania danymi, Administrator Danych informuje o tym fakcie IOD (o ile został powołany).
6. IOD (a jeśli nie został powołany to Administrator danych) dokonuje oceny, czy dany proces przetwarzania spełnia warunki współadministrowania danymi.
7. W przypadku, kiedy wynik oceny, o której mowa w pkt 6 wskazuje na współadministrowanie danymi osobowymi, IOD, przy współudziale pozostałych współadministratorów, opracowuje wspólne uzgodnienia, o których mowa w pkt 4.

Uzgodnienia te powinny znaleźć swoje odzwierciedlanie w umowie zawartej pomiędzy współadminsitratorami.

8. AUDYTY ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

1. Audyty zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz procedurami wdrożonymi w strukturze Administratora Danych przeprowadzane są przez IOD, a jeśli nie został powołany to przez Administratora danych lub inną wskazaną przez niego osobę.
2. Audyt przeprowadza się według opracowanego planu audytów.
2. Plan audytów przygotowuje się na okres nie krótszy niż kwartał i nie dłuższy niż rok z zaznaczeniem, że plan musi obejmować co najmniej jeden audyt.
3. Plan audytów przygotowany w formie elektronicznej lub papierowej jest przedstawiany Administratorowi Danych nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem.
4. W planie audytów zostają uwzględnione następujące kwestie:
    - 4.1. przedmiot, zakres oraz termin przeprowadzenia poszczególnych audytów oraz sposób i zakres ich dokumentowania,
    - 4.2. procesy przetwarzania danych osobowych objęte audytem,
    - 4.3. konieczność weryfikacji zgodności przetwarzania danych osobowych z:
        - 4.3.1. zasadami przetwarzania danych osobowych,
        - 4.3.2. zasadami dotyczącymi zabezpieczenia danych osobowych,
        - 4.3.3. zasadami przekazywania danych osobowych.
5. W toku audytu dokonywane są i dokumentowane czynności, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Opracowuje się również sprawozdanie. Sprawozdanie sporządzane jest w postaci elektronicznej albo w postaci papierowej.
6. IOD lun inna upoważniona osoba przekazuje Administratorowi Danych sprawozdanie nie później niż w terminie 30 dni od zakończenia audytu.
7. Wzór sprawozdania z audytu stanowi załącznik do Polityki.

8. REALIZACJA PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ

1. 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:

   1.1. prawo do wycofania wyrażonej zgody (art. 7 ust. 3 RODO),

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

   1.3. prawo do sprostowania danych (art. 16 RODO),

   1.4. prawo do usunięcia danych (*prawo do bycia zapomnianym*) (art. 17 RODO);,

   1.5. prawo do ograniczenia przetwarzania (art. 18 RODO),

   1.6. prawo do przenoszenia danych (art. 20 RODO),

   1.7. prawo sprzeciwu (art. 21 RODO),

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

10. OCHRONA DANYCH OSOBOWYCH W FAZIE PROJEKTOWANIA ORAZ DOMYŚLNA OCHRONA DANYCH OSOBOWYCH

1. Administrator Danych wdraża odpowiednie środki techniczne i organizacyjne, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, nadania przetwarzaniu danych niezbędnych zabezpieczeń oraz zapewnieniu ochrony praw osób, których dane dotyczą.
2. Wdrażając odpowiednie środki techniczne i organizacyjne Administrator Danych uwzględnia:
   2.1. stan wiedzy technicznej,
   2.2. koszt wdrażania,
   2.3. charakter, zakres, kontekst i cele przetwarzania danych,
   2.4. ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania.
3. Administrator Danych wdraża takie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia określonego celu przetwarzania, biorąc pod uwagę: ilość zbieranych danych osobowych, ich zakres, okres ich przechowywania oraz ich dostępność dla innych osób.
4. W szczególności stosowane środki techniczne i organizacje muszą zapewnić, by domyślnie dane osobowe nie były udostępniane nieokreślonej liczbie osób.
5. W pierwszej kolejności, Administrator Danych rozważa, czy cel jakiemu ma służyć projektowane rozwiązane jest możliwy do osiągnięcia bez konieczności przetwarzania danych osobowych. Jeśli tak, należy wybrać takie rozwiązanie.
6. Administrator Danych zapewnia, aby spełnienie warunków wskazanych w pkt 1-5 (tzw. zasady *privacy by design* i *privacy by default*) było odpowiednio udokumentowane np. w formie notatki, maila, raportu z przeprowadzonych testów systemu informatycznego, wydruku z ekranu systemu.

11. ANALIZA RYZYKA I OCENA SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH (PRIVACY IMPACT ASSESSMENT)

1. Analizy ryzyka jest przeprowadzana w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych. Analizę ryzyka przeprowadza się dla wszystkich procesów, w których przetwarzane są dane osobowe.
2. Analizę ryzyka wykonuje Inspektor Ochrony Danych Osobowych, a jeśli nie został powołany to Administrator danych lub osoba przez niego upoważniona. Analiza wykonywana jest cyklicznie, przynajmniej raz w roku w trakcie wykonywanego audytu.
3. Ocenę skutków dla ochrony danych osobowych przeprowadza się tylko wtedy, gdy dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.
4. Ocena skutków jest formalną, określoną w art. 37 RODO, procedurą przeprowadzenia analizy ryzyka za wykonanie której odpowiada Administrator. Jeżeli Administrator nie jest zobowiązany do przeprowadzenia oceny skutków, może mimo to stosować tę procedurę do przeprowadzenia analizy ryzyka na potrzeby wykazania rozliczalności spełnienia wymagań RODO. O konieczności przeprowadzenia oceny skutków dla ochrony danych osobowych decyduje IOD lub ADO.
5. Ocena skutków musi być wykonana ze współudziałem IOD (o ile został powołany) oraz po wyrażeniu przez niego opinii. Administrator Danych może powierzyć Inspektorowi samodzielne wykonanie oceny.
6. Wzór analizy ryzyka stanowi załącznik do Polityki. Inspektor Ochrony Danych działając niezależnie i samodzielnie może wykonywać analizę ryzyka korzystając z innej dokumentacji.

12. INCYDENTY OCHRONY DANYCH OSOBOWYCH

1. Osobami odpowiedzialnymi za bezpieczeństwo danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do pomieszczeń oraz systemów, w których przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia incydentów ochrony danych osobowych, jest: Administrator Danych, IOD oraz ASI (w odniesieniu do danych przetwarzanych w systemach informatycznych.
2. Procedura postępowania z incydentami ochrony danych osobowych stanowi odrębny dokument, z którym Administrator Danych zapoznaje wszystkie osoby, które w jego imieniu przetwarzają dane osobowe na podstawie nadanych przez niego upoważnień.

13. OGÓLNE ZASADY BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

1. Dostęp do danych osobowych mogą mieć tylko pracownicy posiadający upoważnienie do ich przetwarzania.
2. Przebywanie osób nieuprawnionych do przetwarzania danych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania, chyba, że dane te są w odpowiedni sposób zabezpieczone przed dostępem.
3. Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem, w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
4. Pracownicy przechowujący dane osobowe zobowiązani są do zabezpieczenia materiałów zawierających dane w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym.
5. Niedopuszczalnym jest wynoszenie materiałów (w tym sprzętu elektronicznego takiego jak komputer, laptop czy telefon) zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.
6. Nikomu nie należy udostępniać indywidualnych haseł i identyfikatorów do systemów informatycznych.
7. Wysyłanie seryjnych wiadomości e-mail wymaga zastosowania opcji *kopia ukryta*.
8. Nie można udzielać informacji dotyczących danych osobowych innym podmiotom na podstawie prośby o takie dane skierowanej w formie zapytania telefonicznego.
9. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. *czystego biurka*, która oznacza nie pozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników. Nie należy pozostawiać danych osobowych w miejscach ogólnodostępnych takich jak np. biurka, blaty, parapety.
10. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe odbywać się musi w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.
11. Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych.
12. W czasie chwilowej nieobecności pracowników w pomieszczeniach, w godzinach pracy jak i po zakończeniu pracy, są oni zobowiązani do zamykania na klucz pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe.

13. Klucze do pomieszczeń, w których przetwarzane są dane osobowe nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia kluczy przed udostępnieniem ich osobom nieupoważnionym.

14. Przed wyjściem z pomieszczenia, w którym przechowywane są dane osobowe należy upewnić się, że zostało ono odpowiednio zabezpieczone (zamknięte okna, drzwi).
15. Po zakończeniu pracy w systemie informatycznym, w którym przechowywane są dane osobowe, należy wylogować się z systemu.
16. Osoba użytkująca komputer przenośny zawierający dane osobowe zobowiązana jest do zachowania szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarzane są dane osobowe. Komputery przenośne i inny sprzęt zawierający dane osobowe może być wynoszony poza obszar przetwarzania danych osobowych tylko na mocy upoważnienia nadanego przez Administratora danych.
17. Na pracowniku pracującym zdalnie spoczywa obowiązek odpowiedniego zabezpieczenia danych tak, aby osoby trzecie nie miały dostępu do danych osobowych.
18. Dane osobowe przesyłane elektronicznie powinny być zabezpieczone hasłem. Hasło to powinno być wysyłane oddzielnym kanałem telekomunikacyjnym.

14. PRZEGLĄDY I AKTUALIZACJA POLITYKI OCHRONY DANYCH OSOBOWYCH

1. Polityka podlega okresowemu przeglądowi pod kątem jej adekwatności, nie rzadziej niż raz do roku.
2. Przeglądu Polityki dokonuje Administrator Danych.
3. Przegląd powinien obejmować, w szczególności ocenę adekwatności Polityki do:
   3.1. procesów funkcjonujących w strukturach Administratora Danych,
   3.2. obowiązujących przepisów prawa odnoszących się do ochrony danych osobowych, którym podlega Administrator Danych.
4. W każdym przypadku, gdy zmianie ulegają przepisy prawa będące źródłem wskazanych w Polityce obowiązków lub zaistnieją istotne zmiany faktyczne w ramach struktury Administratora Danych przegląd Polityki wykonywany jest niezwłocznie.
5. Jeżeli w wyniku przeglądu Polityki stwierdzona zostanie konieczność aktualizacji jej zapisów, Administrator Danych dokonuje aktualizacji Polityki w wymaganym zakresie.

15. ZAŁĄCZNIKI

Załącznik nr 1 Wzór sprawozdania z audytu zgodności przetwarzania danych osobowych

Załącznik nr 2 Wzory wyznaczenia oraz odwołania Inspektora Ochrony Danych

Załącznik nr 3 Wzory wyznaczenia oraz odwołania Administratora Systemów Informatycznych

Załącznik nr 4 Ogólny opis technicznych środków bezpieczeństwa wdrożonych w strukturze Administratora Danych

Dokument sporządzono: Data: 1.03.2020 r. Miejsce: Warszawa	**Pełen podpis Administratora Danych:**	**Pieczęć**

SPRAWOZDANIE Z AUDYTU ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH Z PRZEPISAMI O OCHRONIE DANYCH OSOBOWYCH

……

miejscowość, data

1. Administrator Danych: ……

2. Inspektor Ochrony Danych: ……

3. Data rozpoczęcia audytu: ……

4. Data zakończenia audytu: ……

5. Przedmiot audytu:

……

……

6. Zakres audytu:

……

……

7. Wykaz czynności podjętych w toku audytu:

……

……

8. Opis stanu faktycznego stwierdzonego w toku audytu oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych:

……

……

9. Stwierdzone przypadki naruszenia przepisów o ochronie danych osobowych w zakresie objętym audytem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z prawem:

……..……

……..……

10. Załączniki:

Data i podpis Inspektora Ochrony Danych

Otrzymują:
1 x oryginał Administrator Danych
1 x kopia Inspektor Ochrony Danych

Załącznik nr 2 – Wzory wyznaczenia oraz odwołania Inspektora Ochrony Danych

Wyznaczenie Inspektora Ochrony Danych

Niniejszym, reprezentując Administratora Danych - [NAZWA ADO] z siedzibą w …, ul. …, z dniem …/…/,

wyznaczam

Panią / Pana …….

do pełnienia funkcji **Inspektora Ochrony Danych (IOD)** w [NAZWA ADO].

Upoważniam Panią / Pana …….. do przetwarzania danych osobowych we wszystkich zbiorach Administratora Danych w zakresie niezbędnym dla należytego wykonywania funkcji Inspektora Ochrony Danych.

Data i podpis osoby wyznaczanej do pełnienia funkcji IOD Danych

Data i podpis Administratora

Odwołanie Inspektora Ochrony Danych

Niniejszym, reprezentując Administratora Danych - [NAZWA ADO] z siedzibą w …, ul. …, z dniem …/…/,

odwołuję

Panią / Pana …….

z pełnienia funkcji **Inspektora Ochrony Danych (IOD)** w [NAZWA ADO].

Data i podpis osoby odwoływanej z pełnienia funkcji IOD Danych

Data i podpis Administratora

Wyznaczenie Administratora Systemów Informatycznych

Niniejszym, reprezentując Administratora Danych - [NAZWA ADO] z siedzibą w …, ul. …, z dniem …/…/,

wyznaczam

Panią / Pana ……..

do pełnienia funkcji **Administratora Systemów Informatycznych (ASI)** w [NAZWA ADO].

Zakres obowiązków oraz warunki pełnienia funkcji Administratora Systemów Informatycznych określone zostały w Polityce ochrony danych osobowych wdrożonej w [NAZWA ADO].

Data i podpis osoby wyznaczanej do pełnienia funkcji ASI

Data i podpis Administratora Danych

Odwołanie Administratora Systemów Informatycznych

Niniejszym, reprezentując Administratora Danych - [NAZWA ADO] z siedzibą w …, ul. …, z dniem …/…/ ,

odwołuję

Panią / Pana …….

z pełnienia funkcji **Administratora Systemów Informatycznych (ASI)** w [NAZWA ADO].

Data i podpis osoby odwoływanej z pełnienia funkcji ASI Danych

Data i podpis Administratora

ŚRODKI SPRZĘTOWE INFRANSTRUKTURY INFORMATYCZNEJ I TELEKOMUNIKACYJNEJ

Stosowane środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej	Uwagi
Zbiór danych osobowych przetwarzany jest przy użyciu komputera przenośnego.	
Komputer służący do przetwarzania danych osobowych nie jest połączony z lokalną siecią komputerową.	
Zastosowano urządzenia typu UPS, generator prądu i/lub wydzieloną sieć elektroenergetyczną, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.	
Dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej/ komputerze przenośnym zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła BIOS.	
Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.	
Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem karty procesorowej oraz kodu PIN lub tokena.	
Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem technologii biometrycznej.	
Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.	
Zastosowano systemowe mechanizmy wymuszający okresową zmianę haseł.	
Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.	
Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.	
Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.	
Zastosowano procedurę oddzwonienia (callback) przy transmisji realizowanej za pośrednictwem modemu.	
Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.	
Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.	
Użyto system Firewall do ochrony dostępu do sieci komputerowej.	
Użyto system IDS/IPS do ochrony dostępu do sieci komputerowej.	

ŚRODKI OCHRONY W RAMACH NARZĘDZI PROGRAMOWYCH I BAZ DANYCH

Stosowane środki ochrony w ramach narzędzi programowych i baz danych	Uwagi
Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.	
Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.	
Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.	
Dostęp do zbioru danych osobowych wymaga uwierzytelnienia przy użyciu karty procesorowej oraz kodu PIN lub tokena.	
Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem technologii biometrycznej.	
Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.	
Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.	
Zastosowano kryptograficzne środki ochrony danych osobowych.	
Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.	
Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.	