Polityka Bezpieczeństwa Danych Osobowych

Pełny zakres dostępu do dokumentu – odczyt, modyfikacja, usuwanie, dodawanie:

1. Administrator,
2. Inspektor Ochrony Danych.

Zakres dostępu do dokumentu – odczyt:

1. Pracownicy, stażyści, wolontariusze, praktykanci,
2. Podmioty trzeci, które mają dostęp do danych osobowych na mocy zawartych umów.

Spis treści

1 Wstęp

1. Zarządzanie bezpieczeństwem informacji jest pojęciem obejmującym zasady zarządzania systemem chroniącym istotne aktywa oraz sposoby reagowania na zagrożenia dla tych aktywów. Zapewnienie odpowiedniej wiedzy zarządzających Spółką oraz siecią informatyczną w zakresie pojawiających się nowych zagrożeń oraz metod ochrony danych osobowych jest kolejnym elementem zapewnienia bezpieczeństwa. Pracownicy, wykonawcy, stażyści, praktykanci obsługujący systemy przetwarzające informacje są ogniwem zabezpieczeń, na którego skuteczność wpływa również zapewnienie rzetelnej informacji w zakresie sposobu bezpiecznego użytkowania aktywów instytucji.
2. Zastosowanie niniejszej Polityki ma zapewnić zabezpieczenia adekwatne i proporcjonalne do kategorii danych, jednocześnie dopasowane do poziomu zagrożeń występujących dla przetwarzanych i przechowywanych informacji objętych ochroną w tym danych osobowych. W szczególności ochrona powinna być adekwatna do oszacowanych ryzyk.
3. W celu zapewnienia bezpieczeństwa danych osobowych wprowadza się spójny system Ochrony Danych Osobowych.
5. Polityka ta opisuje ogólne zasady ochrony danych osobowych obowiązujące w Arrant, zasady zarządzania ryzykiem, role i zadania osób uczestniczących w procesie przetwarzania informacji oraz Ochrony Danych Osobowych.

2 Cel

1. Celem Polityki, w zakresie ochrony danych osobowych, jest zapewnienie adekwatnej do ryzyka ochrony, w tym poufności, integralności, dostępności oraz rozliczalności przetwarzanych danych osobowych, w tym między innymi danych osobowych zbieranych z wykorzystaniem monitoringu wizyjnego. Polityka jest jednocześnie dokumentem określającym zadania osób funkcyjnych, pracowników i osób trzecich świadczących usługi lub realizujących dostawy, usługi sprzątania lub roboty budowlane.
2. Dla skutecznej realizacji niniejszej Polityki, Administrator zapewnia:
    1) szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony,
    2) okresowe szacowanie ryzyka zagrożeń dla zbiorów danych,
    3) okresową ocenę skutków dla ochrony danych osobowych,
    4) kontrolę, monitoring i nadzór nad przetwarzaniem danych osobowych,
    5) monitorowanie zastosowanych środków ochrony,
    6) możliwość realizacji wytycznych zawartych w Kodeksach, o których mowa w art. 40 RODO,
    7) wdrożenie odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku, w tym między innymi w stosownym przypadku:
        a) pseudonimizację i szyfrowanie danych osobowych,
        b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,

c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,

8) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

3. Zasady i regulacje niniejszej Polityki nie mogą zmieniać ani zastępować obowiązujących przepisów prawnych.

4. Ponadto, celem Polityki, w zakresie bezpieczeństwa danych osobowych, jest:

1) zagwarantowanie właściwej ochrony informacji, w tym odpowiedniego poziomu bezpieczeństwa danych osobowych bez względu na jakim nośnik u jest zapisana,

2) zapewnienie ciągłości procesów przetwarzania danych osobowych,

3) ograniczenie występowania zagrożeń dla bezpieczeństwa danych osobowych,

4) właściwe reagowanie na incydenty i naruszenia ochrony danych osobowych.

5. Realizacja przyjętych celów będzie zrealizowana poprzez:

1) wskazanie sposobu organizacji systemu ochrony danych osobowych,

2) wyznaczenie zadań i odpowiedzialności związanych z zapewnieniem ochrony danych osobowych,

3) wyznaczenie właścicieli procesów przetwarzania, którzy odpowiadają za zapewnienia adekwatnego poziomu bezpieczeństwa przetwarzanych danych,

4) wdrożenie i utrzymanie niezbędnych zabezpieczeń organizacyjnych i technicznych,

5) zapoznanie się przez wszystkich pracowników, stażystów, wolontariuszy, praktykantów, wykonawców i osoby realizujące zadania na zlecenie Spółki z właściwymi politykami i procedurami bezpieczeństwa informacji i ochrony danych osobowych, obowiązującymi w związku z wykonywanymi obowiązkami,

6) reakcja na zagrożenia, incydenty i naruszenia dla bezpieczeństwa danych osobowych w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących,

7) ciągłe podnoszenie świadomości pracowników w obszarze bezpieczeństwa informacji, a szczególnie ochrony danych osobowych.

3 Zakres stosowania

1. Polityka Ochrony Danych Osobowych, w tym danych osobowych stosowana jest przez:

1) Administratora,

2) Inspektora Ochrony Danych,

3) pracowników, stażystów, wolontariuszy i praktykantów,

4) podmioty trzecie (w tym ich pracowników i współpracowników), które mogą mieć dostęp do danych osobowych.

2. Niniejszy dokument dotyczy wszystkich komórek organizacyjnych oraz wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, a także innych osób uzyskujących dostęp do informacji przetwarzanych w Spółce (np. pracowników firm zewnętrznych realizujących prace na rzecz Spółki oraz organizacji związanych, stażystów, praktykantów, wolontariuszy).

3. Dokument ma zastosowanie do wszystkich informacji chronionych, w tym danych osobowych, niezależnie od formy, w jakiej są przechowywane (papierowej, elektronicznej i innej).

4. Z dokumentem polityki muszą zapoznać się : Zarząd, IOD, administratorzy systemów, właściciele procesów.

5. Zasady zawarte w niniejszym dokumencie muszą być przestrzegane przez wszystkie osoby mające dostęp do danych osobowych.

6. Każde naruszenie bezpieczeństwa danych osobowych powinno być zgłaszane IDO lub w przypadku naruszeń bezpieczeństwa dotyczących systemów informatycznych do IT Menadżera. W przypadku naruszenia zasad związanych z danymi osobowymi należy zgłaszać do Inspektora Ochrony Danych.

7. Pracownicy/użytkownicy przetwarzający dane osobowe obowiązani są dołożyć należytej staranności w celu ochrony interesu osób, których dane są gromadzone i przetwarzane, a w szczególności należy przestrzegać, aby dane te były:

   1) przetwarzane zgodnie z aktami prawa powszechnie obowiązującego i aktami wewnętrznymi,

   2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,

   3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,

   4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania

   oraz by wypełniany był obowiązek informacyjny, w przypadkach wskazanych w przepisach prawa powszechnie obowiązującego.

8. Naruszenie postanowień Polityki Bezpieczeństwa Ochrony Danych Osobowych może skutkować zablokowaniem dostępu pracownika/użytkownika do informacji chronionych i Systemów. W przypadku ciężkich naruszeń, takie działanie może prowadzić do wszczęcia postępowania dyscyplinarnego oraz do rozwiązania bądź wypowiedzenia umowy. W przypadku poniesienia strat w wyniku naruszenia, Spółka Arrant może dochodzić roszczeń odszkodowawczych na drodze sądowej.

4 Terminologia

1. Określenia używane w dalszej treści Polityki oznaczają:

   1) **IOD** – Inspektor Ochrony Danych;

2) **ADO/Administrator** – Prezes Zarządu Arrant lub osoba, która została wyznaczona przez Prezesa Zarządu do wypełniania w jego imieniu obowiązków związanych z przetwarzaniem danych osobowych;

3) **Dane osobowe** – 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) **Dostępność danych** - rozumie się przez to właściwość zapewniającą, że dane są udostępniane dla upoważnionego podmiotu wtedy, gdy ich potrzebuje do przetwarzania;

5) **Integralność danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

6) **Naruszenie ochrony danych osobowych** - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

7) **Odbiorca danych** – osoba fizyczna lub prawna, organ publiczny, jednostka 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 powszechnie obowiązującym, nie są jednak uznawane za odbiorców - przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania; przy czym przez sformułowanie „strona trzecia", rozumie się 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;

8) **Osoba upoważniona do przetwarzania danych osobowych** – osoba, która złożyła ADO oświadczenie o zachowaniu w tajemnicy przetwarzanych danych i stosowanych sposobach zabezpieczenia tych danych, posiadająca imienne upoważnienie wydane przez ADO, określające imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych oraz identyfikator, jeżeli dane są przetwarzane w systemie informatycznym;

9) **Podmiot przetwarzający** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora,

10) **Przetwarzanie** - operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

11) **Poufność danych** - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;

12) **Rozliczalność danych** - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

13) **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);

14) **Spółka** - Arrant Sp. z o.o.;

15) **Usuwanie danych** – trwałe zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

16) **Ustawa** - ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych;

17) **Uwierzytelnianie** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

18) **Użytkownik/pracownik (w tym podmiotu trzeciego)** - osoba przetwarzająca dane w systemie informatycznym oraz poza nim (np. dokumentacji w formie tradycyjnej), niezależnie od formy zatrudnienia lub formy prawnej wiążącej Spółkę z tą osobą; w szczególności mogą być to osoby zatrudnione na umowę o pracę, stażyści, praktykanci, osoby realizujące zadania na podstawie podpisanej umowy cywilnoprawnej;

19) **Zbiór danych** – to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

20) **Zgoda osoby, której dane dotyczą** – oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

2. Organizacja systemu ochrony danych osobowych odbywa się w odniesieniu do zmieniającego się otoczenia prawnego i technologicznego. Uwzględniane są również wyniki analizy ryzyka i wyniki oceny skutków. W procesy decyzyjne zaangażowane jest Kierownictwo Spółki.

5 Organizacja ochrony danych osobowych

Rola i zadania Administratora

1. Administratorem w rozumieniu RODO oraz Ustawy jest Zarząd Spółki Arrant. Reprezentuje go Prezes Zarządu lub osoba przez niego wskazana, która w jego imieniu wykonuje zadania związane z ochroną danych zbieranych i przetwarzanych w Spółce (ilekroć w Polityce mowa jest o Administratorze należy przez niego rozumieć Prezesa Zarządu lub osobę, która w jego imieniu wykonuje zadania związane z ochroną danych – w przypadku wskazania przez Prezesa Zarządu takiej osoby). Administrator stosownie do obowiązków i uprawnień określonych w przepisach prawa powszechnie obowiązującego i aktów prawa wewnętrznego jest odpowiedzialny za dane osobowe gromadzone i przetwarzane w Spółce Arrant oraz za ich bezpieczeństwo, w szczególności:

   a) samodzielnie lub wspólnie z innymi wskazanymi osobami ustala cele i sposoby przetwarzania danych osobowych;

b) nadzoruje stworzenie warunków odpowiednich do gromadzenia, przetwarzania, ochrony, modyfikacji i usuwania w Spółce Arrant danych osobowych zgodnie z obowiązującymi przepisami prawa powszechnie obowiązującego i aktami prawa wewnętrznego oraz zapewnia w tym celu niezbędne środki;

c) udziela pisemnych upoważnień dla osób przetwarzających dane osobowe;

d) zapewnia realizację praw osób, których dane osobowe są przetwarzane (m.in. prawo wglądu, poprawiania danych i wniesienia sprzeciwu wobec przetwarzanych danych);

e) reprezentuje Spółkę Arrant w postępowaniach przed organami publicznymi oraz w kontaktach z podmiotami trzecimi w sprawach związanych z pozyskiwaniem, przetwarzaniem, ochroną i powierzeniem danych osobowych;

f) analizuje sprawozdania Inspektora Ochrony Danych, weryfikuje ocenę ryzyka i ocenę skutków związane z przetwarzaniem danych osobowych, a także decyduje o formach przeciwdziałania ewentualnym zagrożeniom;

g) zapewnia udział osób o odpowiednich kompetencjach i wiedzy (pracowników Administratora i podmiotów zewnętrznych) przy realizacji audytów i weryfikacji systemu ochrony danych osobowych prowadzonego przez Inspektora Ochrony Danych, o której mowa w pkt 4.2.7 niniejszej Polityki;

h) zapewnia Inspektorowi Ochrony Danych zasoby niezbędne do należytego wykonania obowiązków.

2. Informacja o ewentualnym wyznaczeniu osoby, która w imieniu Prezesa Zarządu wykonuje zadania związane z ochroną danych zawarta jest w załączniku nr 7.

3. Administrator jest odpowiedzialny za przestrzeganie przepisów RODO i musi być w stanie wykazać ich przestrzeganie (tzw. zasada rozliczalności RODO). Administrator zapewnia:

1) przetwarzanie danych osobowych zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość").

2) zbieranie danych osobowych w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami („ograniczenie celu").

3) adekwatność danych osobowych; dane osobowe powinny być stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych").

4) prawidłowość danych osobowych i w razie potrzeby ich uaktualnianie; podejmuje wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość").

5) przechowywanie danych osobowych w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania").

6) przetwarzanie w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub

uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

4. Ewentualne przekazanie innemu Administratorowi danych osobowych pozyskanych od osoby trzeciej (tj. od osoby, której te dane nie dotyczą) w celach marketingowych należy zawsze poprzedzić poinformowaniem wszystkich osób, których dane mają być przetwarzane o niniejszym (w tym o zmianie celu przetwarzania) i o przysługującym im prawie wniesienia sprzeciwu.

5. Oświadczenie osób, których dane Spółka Arrant ma przetwarzać (o wypełnieniu obowiązków informacyjnych) może zostać potwierdzone złożeniem podpisu pod odpowiednią klauzulą lub przez zaznaczenie odpowiedniego pola (np. na stronie internetowej w odpowiednim systemie) lub w inny sposób, o ile jednoznacznie wskazuje to na wywiązanie się z obowiązków informacyjnych i zapewnia utrwalenie informacji o wypełnieniu obowiązku informacyjnego.

Obowiązki i uprawnienia Inspektora Ochrony Danych

1. Inspektor Ochrony Danych realizuje obowiązki zgodnie z wymaganiami obowiązującego prawa, aktów prawa wewnętrznego przy uwzględnieniu ryzyka i oceny skutków związanych z czynnościami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

2. Osoby, których dane są gromadzone i przetwarzane mogą kontaktować się z Inspektorem Ochrony Danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy przepisów prawa powszechnie obowiązującego i aktów prawa wewnętrznego Spółki Arrant.

3. Inspektor Ochrony Danych jest zobowiązany do zachowania w tajemnicy lub poufności informacji pozyskanych w trakcie wykonywania swoich zadań, zgodnie z przepisami prawa powszechnie obowiązującego i regulacjami wewnętrznymi.

4. Inspektor Ochrony Danych zobowiązany jest w szczególności do:

   1) informowania Administratora oraz pracowników, wolontariuszy, stażystów, praktykantów, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy powszechnie obowiązujących przepisów prawa oraz aktów prawa wewnętrznego w zakresie ochrony danych osobowych i doradzanie im w tej sprawie,

   2) nadzorowania i monitorowania przestrzegania powszechnie obowiązujących przepisów prawa oraz aktów prawa wewnętrznego w zakresie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu Administratora i podmiotów trzecich uczestniczącego w operacjach przetwarzania oraz wykonywanie powiązanych z tym audytów,

   3) udziału w ocenie skutków dla ochrony danych zgodnie z art. 35 RODO oraz monitorowanie wykonania zaleceń opracowanych w wyniku wykonania oceny,

   4) współpracy z organem nadzorczym,

   5) pełnienia funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach,

6) weryfikacji zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych w Spółce Arrant oraz weryfikacji zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych przez podmioty trzecie, które na mocy zawartej umowy mają dostęp do danych osobowych gromadzonych w Spółce Arrant (w tym w miejscu przetwarzania danych przez podmioty trzecie) oraz opracowanie w tym zakresie, co najmniej raz na kwartał, sprawozdania dla Administratora na formularzu, którego wzór stanowi załącznik nr 2 do niniejszej Polityki,

7) przygotowywania do 15 grudnia każdego roku Planu sprawdzeń na następny rok i przedstawienie go do akceptacji Administratorowi, a po jego zatwierdzeniu realizuje go; Plan sprawdzeń jest określeniem harmonogramu weryfikacji systemu ochrony danych osobowych i w okresie pięciu lat sprawdzenia powinny łącznie objąć:

    a) zabezpieczenia: organizacyjne i techniczne zbiorów danych osobowych (w tym w szczególności w zakresie monitoringu wizyjnego),

    b) system informatyczny służący do przetwarzania danych osobowych,

    c) kompletność zidentyfikowanych procesów przetwarzania,

    d) przesłanki legalności przetwarzania danych osobowych,

    e) przesłanki legalności przetwarzania danych szczególnie chronionych,

    f) zakres i cel przetwarzania danych,

    g) merytoryczna poprawność danych i ich adekwatność do celu przetwarzania,

    h) obowiązek informacyjny,

    i) profilowanie,

    j) przekazywanie danych do państwa trzeciego, w tym do krajów spoza Unii Europejskiej,

    k) powierzenie przetwarzania danych osobowych (w tym zakres i poprawność skonstruowania umów powierzenia przetwarzania danych zawartych przed dniem 25 maja 2018 r. w celu dostosowania postanowień do postanowień RODO) oraz weryfikacji miejsc przetwarzania danych przez podmioty trzecie (w tym w siedzibach, czy też w miejscu, w którym przetwarza się dane w podmiocie trzecim),

    l) zabezpieczenia danych: organizacyjne i techniczne,

    m) zgodność dokumentacji przetwarzania danych osobowych z obowiązującymi przepisami prawa powszechnie obowiązującego i stosowanymi w Spółce Arrant zabezpieczeniami, technologiami, systemami i itp.,

    n) opracowania i aktualizowania niniejszej Polityki,

8) wspieranie Administratora w realizacji przygotowywania odpowiedzi na żądania osób, których dane dotyczą, uzyskania od Właściciela procesu przetwarzania, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, uzyskanie dostępu do nich wraz z zakresem właściwych informacji o danych osobowych,

9) informowania o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania osób, które wystąpiły z takim żądaniem,

10) prowadzenia i aktualizacji rejestru czynności przetwarzania,

11) prowadzenia i aktualizacji rejestru naruszeń bezpieczeństwa,

12) przygotowania i przekazywania do podpisu do Administratora zgłaszania o naruszeniu ochrony danych osobowych do organu nadzorczemu oraz zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych – zgodnie z postanowieniami art. 33 i 34 RODO,

13) prowadzenia i aktualizacji rejestru umów powierzenia przetwarzania danych,

14) nadzorowania i monitorowania procesu profilowania,

15) nadzorowanie procesu zbierania danych za pomocą monitoringu wizyjnego i wykorzystania danych w ten sposób uzyskanych,

16) opiniowania umów zawieranych z podmiotami trzecimi w zakresie ich zgodności z przepisami prawa powszechnie obowiązującego i wewnętrznego w zakresie ochrony danych osobowych i w porozumieniu z Właścicielem Zbioru zakresu dostępu podmiotu trzeciego do danych osobowych udzielanego na mocy zawieranej umowy (w tym umów powierzenia przetwarzania),

17) organizowania spotkań z personelem i współpracownikami podmiotów trzecich przed zawarciem umowy lub niezwłocznie po jej zawarciu celem omówienia zasad dostępu do danych osobowych gromadzonych przez Spółkę Arrant oraz zasad ich przetwarzania, modyfikowania, ochrony i usuwania,

18) nadzorowania i monitorowania realizacji obowiązku informacyjnego, zgodnie z wymogami RODO,

19) prowadzenia rejestru zgłoszonych sprzeciwów dotyczących przetwarzania danych osobowych i wniosków o zaprzestanie lub ograniczenie przetwarzania danych,

20) informowanie Administratora o wystąpieniu naruszenia bezpieczeństwa danych osobowych,

21) w porozumieniu z podmiotem odpowiedzialnym za obsługę prawną przygotowania wzorów klauzul informacyjnych i umów powierzenia przetwarzania danych oraz dystrybucja ich do komórek organizacyjnych,

22) gromadzenia potwierdzenia (dotyczy formy papierowej) wywiązania się z obowiązku informacyjnego oraz weryfikacji prawidłowości gromadzenia potwierdzeń w systemach informatycznych,

23) prowadzenia ewidencji upoważnień do przetwarzania danych osobowych oraz dokumentacji związanej z udzielaniem upoważnień,

24) wspierania Administratora w wykazaniu jednej z przesłanek przetwarzania danych osobowych, o których mowa w art. 6–11 RODO,

25) w porozumieniu z IT Managerem wykonania szacowania ryzyka i oceny skutków przed wprowadzeniem nowej technologii (np. nowego systemu informatycznego, w którym przetwarzane będą dane osobowe) wraz z administratorem systemu i właścicielem zasobu oraz w zakresie wykorzystania monitoringu wizyjnego,

26) prowadzenie rejestru kategorii czynności przetwarzania.

5. Szczegółowy zakres zadań Inspektora Ochrony Danych określony jest w zakresie obowiązków lub w umowie na świadczenie usług, o której mowa w pkt 5.3.2 niniejszej Polityki.

6. W przypadku nieokreślenia w Dokumentacji wzorów rejestrów, ewidencji czy też innych wymaganych dokumentów, Inspektor Ochrony Danych opracowuje stosowne wzory i prowadzi dokumentację, zgodnie z tymi wzorami.

7. Inspektor Ochrony Danych jest uprawniony w szczególności do:

   a) wstępu do pomieszczeń, w których przetwarzane są dane osobowe,

   b) wstępu do pomieszczeń, w których gromadzone są informacji o przetwarzaniu danych osobowych,

   c) odbierania wyjaśnień od osób przetwarzających dane osobowe,

   d) dokumentowania ustaleń i dokonywania innych czynności niezbędnych do wykonania jego zadań wynikających z RODO, Ustawy, aktów prawa wewnętrznego i zakresu jego obowiązków/zakresu umowy o świadczenie usług.

   Szczegółowy zakres uprawnień Inspektora Ochrony Danych określa RODO i Ustawa.

Powołanie i odwołanie Inspektora Ochrony Danych oraz jego podległość służbowa

1. Administrator powołuje Inspektora Ochrony Danych.
2. Inspektor Ochrony Danych może być członkiem personelu Administratora lub wykonywać zadania na podstawie umowy o świadczenie usług. Inspektor Ochrony Danych podlega bezpośrednio Administratorowi. Administrator zapewnia Inspektorowi Ochrony Danych zasoby niezbędne do wykonania zadań określonych w przepisach prawa powszechnie obowiązującego oraz dostęp do danych osobowych i czynności przetwarzania, a także zasoby niezbędne do utrzymania jego fachowej wiedzy.
3. Inspektor Ochrony Danych powinien:

   1) posiadać pełną zdolność do czynności prawnych oraz korzystać z pełni praw publicznych,

   2) posiadać fachową wiedzę na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO, ustawie i aktach prawa wewnętrznego Spółki Arrant,

   3) wykonywać zadania niezależnie i bez konfliktu interesów,

   4) mieć wiedzę w zakresie europejskiego i krajowego prawa ochrony danych oraz praktyk ochrony danych, a także szczegółową wiedzę na temat RODO,

   5) posiadać wiedzę na temat systemów informatycznych służących do przetwarzania, a także potrzeb i sposobów zabezpieczania przetwarzanych danych osobowych

   i nie może być karany za przestępstwo popełnione z winy umyślnej.

4. Administrator może powierzyć Inspektorowi Ochrony Danych wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania zadań, o których mowa w niniejszej Polityce.
5. W przypadku powołania Inspektora Ochrony Danych Administrator jest zobowiązany dokonać stosownego zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych zgodnie z wymogami prawa powszechnie obowiązującego. Administrator zawiadamia Prezesa Urzędu Ochrony Danych Osobowych o każdej zmianie danych Inspektora oraz jego odwołaniu przez Administratora lub w przypadku jego śmierci.

6. W przypadku powierzenia przez Prezesa Zarządu wykonywania zadań związanych z ochroną danych innej osobie, Inspektor Ochrony Danych w zakresie wykonywania zadań merytorycznych oraz organizacyjnie podlega tej osobie. Kwestie sporne w zakresie organizacji i wykonywania zadań związanych z gromadzeniem, przetwarzaniem, ochroną i usuwaniem danych między osobami pełniącymi ww. funkcje rozstrzygane są przez Prezesa Zarządu.

Obowiązki pracowników i innych osób zaangażowanych w przetwarzanie danych osobowych

1. W realizacji obowiązków w zakresie przetwarzania danych osobowych osoba wykonująca zadania Administratora jest wspierana przez:
   1) Prezesa Zarządu, jeżeli powierzył wykonywanie zadań Administratora innej osobie,
   2) Inspektora Ochrony Danych,
   3) Właścicieli procesów,
   4) podmioty trzecie świadczące usługi na rzecz Spółki Arrant w zakresie gromadzenia, przetwarzania, ochrony i usuwania danych osobowych,
   5) Kierowników komórek organizacyjnych.
2. Do zadań szczegółowych osób wskazanych powyżej należą:

2.1. W odniesieniu do wszystkich kierowników komórek organizacyjnych:
   1) zapewnienie, aby przetwarzanie danych osobowych w podlegających im komórkach organizacyjnych (niezależnie od formy tych danych - papierowej lub elektronicznej) odbywało się w zgodzie z obowiązującymi przepisami,
   2) zapewnienie przestrzegania postanowień właściwych Kodeksów, o których mowa w art. 40 RODO, a dodatkowo w odniesieniu do wskazanych poniżej osób, określonych szczególnych zadań,
   3) przeciwdziałanie zagrożeniom dla bezpiecznego przetwarzania danych osobowych oraz tworzenie technicznych i organizacyjnych warunków dla bezpiecznego przetwarzania, np. poprzez zapewnienie miejscom związanym z przetwarzaniem zabezpieczeń (fizycznych, antywłamaniowych i przeciwpożarowych), dozoru (pracowników ochrony), ograniczenie dostępu do nich osób nieuprawnionych.

2.2. W odniesieniu do Właścicieli procesów:
   1) identyfikowanie oraz zgłaszanie systemów i procesów przetwarzania danych osobowych do Inspektora Ochrony Danych celem wpisania ich do odpowiednich rejestrów i ewidencji – (w Dokumentacji prowadzonej w Spółce Arrant),
   2) zapewnienie archiwizacji, likwidacji lub anonimizacji danych osobowych niezwłocznie po ustaniu podstawy do ich przetwarzania, w przypadku stwierdzenia, że nie jest możliwe bezpieczne ich przetwarzanie zgodne z przepisami lub Dokumentacją oraz w przypadku wniesienia zasadnego sprzeciwu do przetwarzania danych osobowych lub wniosku o zaprzestanie przetwarzania danych osobowych,

3) zapewnienie bezpiecznego usunięcia danych osobowych w przypadku uzasadnionego żądania niezwłocznego usunięcia danych osobowych, bez zbędnej zwłoki,

4) powiadamianie o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania.

3. Osoby przetwarzające dane osobowe w imieniu Spółki Arrant (szczególnie jej pracownicy, stażyści, wolontariusze oraz pracownicy/współpracownicy podmiotów, z którymi zostały zawarte umowy powierzenia przetwarzania oraz pracownicy/współpracownicy podmiotów trzecich, którzy mają dostęp do danych na mocy zawartej umowy) powinny we wszystkich działaniach związanych z przetwarzaniem danych osobowych, dochowywać należytej staranności i przestrzegać obowiązujących zasad ochrony danych osobowych określonych w przepisach prawa powszechnie obowiązującego i aktów prawa wewnętrznego.

4. Wszystkie osoby przetwarzające dane osobowe z użyciem systemów i podsystemów informatycznych muszą zostać poinformowane o osobach i ich danych kontaktowych pełniących funkcje: Inspektora Ochrony Danych i Administratora Systemu Informatycznego (co najmniej w odniesieni do danych i systemu, którego używają). Wiedza ta jest niezbędna szczególnie w przypadkach, gdy bezpieczeństwo systemu lub integralność zbioru danych jest zagrożona.

6 Zgody na przetwarzanie danych osobowych

Zgoda osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

1. Zgoda powinna być dobrowolna.

2. Zgoda nie jest uważana za dobrowolną, gdy:

   1) istnieje wyraźny brak równowagi między osobą, której dane dotyczą, a administratorem, w szczególności, gdy administrator jest organem publicznym i dlatego jest mało prawdopodobne, by w tej konkretnej sytuacji zgodę wyrażono dobrowolnie we wszystkich przypadkach.

   2) nie można jej wyrazić z osobna na różne operacje przetwarzania danych osobowych, mimo że w danym przypadku byłoby to stosowne,

   3) od zgody uzależnione jest wykonanie umowy – w tym świadczenie usługi – mimo że do jej wykonania zgoda nie jest niezbędna.

3. Odwołanie zgody na przetwarzanie danych osobowych powinno być tak samo łatwe, jak jej udzielenie.

7 Obowiązek informacyjny

1. Administrator zobowiązany jest na etapie gromadzenia danych (niezależnie od tego, czy zbiera je bezpośredniego od osób, których one dotyczą, czy też pozyskania ich od podmiotu trzeciego) powiadomić osoby, których dane gromadzi o przysługujących im prawach oraz przekazać informacje o zasadach i celu przetwarzania danych osobowych (wypełnienie „obowiązków informacyjnych" wskazanych w art. 12, 13, 14, 22 i 25 RODO).

2. Zgodnie z art. 13 ust. 1 i 2 RODO, do niezbędnych elementów obowiązku informacyjnego, zaliczyć należy podanie:

   1) nazwy i adresu Administratora oraz adresu poczty elektronicznej i numeru faksu i telefonu oraz gdy ma to zastosowanie, tożsamości i danych kontaktowych przedstawiciela Administratora,
   2) danych kontaktowych Inspektora Ochrony Danych,
   3) celu przetwarzania danych osobowych oraz podstawy prawnej przetwarzania,
   4) informacji o odbiorcach danych osobowych lub o kategoriach odbiorców,
   5) informacji o zamiarze transferu danych osobowych do państwa trzeciego, ze szczególnym uwzględnieniem:

      a) przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej,
      b) stwierdzenia lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony lub - w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO - wzmianki o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych,

   6) okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteriach ustalania tego okresu,
   7) informacji 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 lub art. 9 ust. 2 lit. a RODO – informacji o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
   9) informacji o prawie wniesienia skargi do organu nadzorczego,
   10) informacji 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) informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

3. W przypadku zbierania danych osobowych z innego źródła niż od osoby, której dane dotyczą, zgodnie z art. 14 ust. 1 i 2 RODO, informacja powinna być poszerzona o:

   1) kategorie odnośnych danych osobowych;
   2) źródle pochodzenia danych osobowych, a jeżeli ma to zastosowanie, o pochodzeniu ich ze źródeł powszechnie dostępnych.

4. Informacje, o której mowa w pkt 7.2 niniejszej Polityki każdorazowo należy przekazać indywidualnie osobie, której dane dotyczą przed podjęciem działań z jej danymi, a także dokumentować (najlepiej na piśmie podpisanym przez osobę, której dane dotyczą), że obowiązek informacyjny przez Spółkę Arrant został wypełniony. Jeśli zamiast formy papierowej do gromadzenia danych wykorzystuje się systemem informatyczny to musi on zapewniać zapisanie w trwałej i wiarygodnej formie, że osoba podająca swoje dane za jego pomocą uzyskała informacje w zakresie określonym w przepisach prawa

powszechnie obowiązującego. Klauzula powinna być zrozumiała dla osób, których dane mają być gromadzone i przetwarzane. Poświadczenie wykonania obowiązku informacyjnego może polegać na wypełnieniu odpowiednich formularzy (w tym w formie elektronicznej). Istotne jest, aby pola potwierdzające wyrażenie zgody na zbieranie i przetwarzanie danych w formularzu nie były domyślnie zaznaczane.

5. Treść klauzuli należy skonsultować każdorazowo z Inspektorem Ochrony Danych w celu potwierdzenia zgodności z obowiązującymi przepisami prawa powszechnie obowiązującego.

6. Informowanie, o którym mowa w pkt 7.2 i 7.3 niniejszej Polityki powinno się dokonać bez prośby zainteresowanego. Powinno być ono wykonane w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Należy uwzględniać także to, że informowana osoba musi mieć możliwość wniesienia sprzeciwu wobec przetwarzania jej danych i należy stworzyć jej warunki do wyrażenia tego sprzeciwu.

7. Wykonanie obowiązku informacyjnego jest zadaniem osoby przyjmującej dane osobowe, która po otrzymaniu potwierdzenia jego wykonania (w przypadku, gdy realizowany jest on w formie papierowej) przekazuje dowód wykonania obowiązku informacyjnego do Inspektora Ochrony Danych.

8. Inspektor Ochrony Danych zobowiązany jest do dokonywania przeglądu danych zgromadzonych i przetwarzanych przez Spółkę Arrant oraz stosowanych klauzul informacyjnych i informować o wynikach przeglądu Administratora. W przypadku stwierdzenia, że stosowane dotychczas klauzule informacyjne nie spełniają wymogów określonych w art. 12, 13, 14, 22 i 25 RODO, osoby, których dane są zgromadzone i przetwarzane przez Spółkę Arrant zostaną poinformowane o przysługujących im prawach stosownie do wymogów RODO. Nadzór nad prawidłowością wykonania tego zadania powierza się Inspektorowi Ochrony Danych, który ustali zakres i sposób realizacji tego obowiązku z Administratorem.

8 Informowanie o przetwarzanych danych osobowych

1. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych osobowych przetwarzanych i przechowywanych w Spółce Arrant, a zwłaszcza prawo do uzyskania wyczerpującej informacji o przetwarzanych danych osobowych, które jej dotyczą.

2. Na wniosek osoby, której dane dotyczą, Inspektor Ochrony Danych w porozumieniu z kierownikami komórek organizacyjnych i Właścicielami procesów jest zobowiązany do udzielania informacji zgodnie z pkt 7 niniejszej Polityki. Informacja powinna być udzielona formie pisemnej, a jej treść musi być powszechnie zrozumiała.

3. W razie wniesienia żądania oraz wykazania przez osobę, której dane osobowe dotyczą, że jej dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem przepisów prawa powszechnie obowiązującego albo są zbędne do realizacji celu, dla którego zostały zebrane, Właściciel procesu w porozumieniu z Inspektorem Ochrony Danych i jeśli dotyczy Administratorem Systemu jest obowiązany, bez zbędnej zwłoki, dokonać uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, chyba że dotyczy to danych osobowych, w odniesieniu do których tryb ich uzupełnienia, uaktualnienia lub sprostowania określają odrębne przepisy.

4. Osoba, której dane dotyczą, ma prawo wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach przetwarzania niezbędnego do wykonania określonych prawem zadań realizowanych dla dobra publicznego lub niezbędnego dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo

odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą, gdy Administrator zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu Administratorowi danych.

5. W przypadku opisanym w pkt 8.3 niniejszej Polityki dalsze przetwarzanie kwestionowanych danych jest niedopuszczalne. Administrator może jednak pozostawić w zbiorze imię lub imiona i nazwisko osoby oraz numer PESEL lub adres wyłącznie w celu uniknięcia ponownego wykorzystania danych tej osoby w celach objętych sprzeciwem.

9 Szczególne kategorie danych osobowych

1. Szczególne kategorie danych osobowych, zwane również danymi wrażliwymi, to pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.
2. Przesłanką legalności przetwarzania szczególnych kategorii danych osobowych mogą być tylko warunki, o których mowa w art. 9 RODO.
3. W przypadku przetwarzania danych, o których mowa w pkt 9.1, przeprowadzane jest obligatoryjnie szacowanie ryzyka i ocena skutków.
4. Postanowienia ust. 3 stosuje się odpowiednio w przypadku użytkowania monitoringu wizyjnego.

10 Współadministrowanie danymi

1. W przypadku wspólnego przetwarzanie danych w zbiorach przez Spółkę Arrant z innym podmiotem, na mocy zawartej umowy lub porozumienia, ustalają one wspólnie cele i sposoby przetwarzania danych (są współadministratorami danych). W drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z przepisów prawa powszechnie obowiązującego oraz aktów prawa wewnętrznego obowiązujących w obu podmiotach, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14 RODO, chyba że przypadające im obowiązki i ich zakres określa prawo powszechnie obowiązujące. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą.
2. Uzgodnienia, o których mowa w pkt 10.1 niniejszej Polityki, należycie odzwierciedlają odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a osobami, których dane dotyczą. Zasadnicza treść uzgodnień jest udostępniana osobom, których dane dotyczą.
3. Niezależnie od uzgodnień, o których mowa w pkt 10.1 niniejszej Polityki, osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wynikające z przepisów prawa powszechnego wobec każdego z Administratorów.
4. Informacja o współadministrowaniu zbiorem danych (wskazanie współadministratorów) odnotowywane jest w rejestrze czynności przetwarzania.

11 Umowy powierzenia i przetwarzanie danych na mocy przepisów prawa powszechnie obowiązującego

1. Administrator:

   1) przekazuje dane do podmiotów trzecich zgodnie z przepisami prawa powszechnie obowiązującego, w szczególności do: Zakładu Ubezpieczeń Społecznych, Urzędu Skarbowego, Państwowej Inspekcji Pracy, sądów powszechnych, Policji, Agencji Bezpieczeństwa Wewnętrznego, Centralnego Biura Antykorupcyjnego, Straży Granicznej,

   2) powierza przetwarzanie danych osobowych innemu podmiotowi w drodze umowy zawartej w na piśmie, która określa zasady przetwarzania i zabezpieczenia danych osobowych.

4. W przypadku zawarcia umowy powierzenia przetwarzania danych osobowych z podmiotem trzecim, jednocześnie zobowiązuje się ten podmiot w formie pisemnej do zachowania poufności powierzanych do przetwarzania danych osobowych oraz sposobów ich zabezpieczeń. Zobowiązanie powinno pozostać w mocy również po zakończeniu przetwarzania.

5. Podmiot, któremu powierzono przetwarzanie danych osobowych, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

6. Podmiot, któremu powierzono przetwarzanie danych osobowych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

7. Rejestr umów powierzenia Inspektor Ochrony Danych prowadzi zgodnie ze wzorem zawartym w załączniku nr 6.

8. Rejestr kategorii czynności przetwarzania prowadzi Inspektor Ochrony Danych zgodnie ze wzorem zawartym w załączniku nr 3.

9. Przykładowy wzór umowy powierzenia przetwarzania zawarty jest w załączniku nr 9.

12 Przekazanie danych do państwa trzeciego lub organizacji międzynarodowej

1. Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, gdy Komisja Europejska stwierdzi, że to 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.

2. W razie braku decyzji, o której mowa w pkt 12.1 niniejszej Polityki Administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej wyłącznie, gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą i skuteczne środki ochrony prawnej.

3. W razie braku decyzji stwierdzającej odpowiedni stopień ochrony określonej w pkt 12.1 niniejszej Polityki oraz braku odpowiednich zabezpieczeń, o których mowa w pkt 12.2 niniejszej Polityki, w tym wiążących reguł korporacyjnych, jednorazowe lub wielokrotne przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej mogą nastąpić wyłącznie pod warunkiem, że:

   a) osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którymi – ze względu na brak decyzji stwierdzającej odpowiedni stopień ochrony oraz na brak odpowiednich zabezpieczeń – może się dla niej wiązać proponowane przekazanie, wyraźnie wyraziła na nie zgodę,

   b) przekazanie jest niezbędne do wykonania umowy między osobą, której dane dotyczą, a administratorem lub do wprowadzenia w życie środków przedumownych podejmowanych na żądanie osoby, której dane dotyczą,

   c) przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, których dane dotyczą, między administratorem a inną osobą fizyczną lub prawną,

   d) przekazanie jest niezbędne ze względu na ważne względy interesu publicznego,

   e) przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń,

   f) przekazanie jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą, lub innych osób, jeżeli osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody lub przekazanie następuje z rejestru, który zgodnie z prawem Unii lub prawem państwa członkowskiego ma służyć za źródło informacji dla ogółu obywateli i który jest dostępny dla ogółu obywateli lub dla każdej osoby mogącej wykazać prawnie uzasadniony interes – ale wyłącznie w zakresie, w jakim w danym przypadku spełnione zostały warunki takiego dostępu określone w prawie Unii lub w prawie państwa członkowskiego.

4. Szczegółowe zasady przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej określone zostały określone w RODO. O wyrażenie zgody na przekazanie danych występuje Właściciel procesu, wskazując cel i zakres przekazywanych danych. Zgodę na ich przekazanie do państwa trzeciego lub organizacji międzynarodowej może wydać Administrator po zasięgnięciu opinii Inspektora Ochrony Danych. Właściciel procesu zobowiązany jest bezwzględnie przestrzegać postanowień RODO przy przekazywaniu danych do państwa trzeciego lub organizacji międzynarodowej.

13 Procedura nadawania i odbierania upoważnień do przetwarzania oraz nadawania i odbierania uprawnień dostępu do danych osobowych

1. W celu zapewnienia kontroli nad przetwarzaniem danych osobowych dopuszczonymi do ich przetwarzania są wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych nadawane przez Administratora.

2. Upoważnienia nie są wydawane członkom Zarządu, którzy uprawnieni są do dostępu do gromadzonych danych osobowych od momentu powołania ich na członka Zarządu Spółki.

3. Udzielone upoważnienia są ewidencjonowane przez Inspektora Ochrony Danych. Dopuszczalne jest ewidencjonowanie upoważnień zarówno w formie papierowej, jak i w formie elektronicznej (centralne repozytorium). W ewidencji prowadzonej w wersji elektronicznej dopuszcza się zapisywanie uprawnień do danego systemu odrębnie dla poszczególnych modułów.

a) Upoważnień do przetwarzania danych osobowych udziela się pracownikom indywidualnie, na piśmie, co najmniej w jednym egzemplarzu (z przeznaczeniem do akt osobowych). Osobie upoważnionej należy umożliwić otrzymanie drugiego egzemplarza, lub potwierdzonej „za zgodność z oryginałem" kopii upoważnienia.

b) Uzyskanie upoważnienia do przetwarzania danych osobowych jest podstawowym warunkiem uzyskania uprawnień do przetwarzania danych osobowych z wykorzystaniem systemu informatycznego. Uprawnienia przyznawane użytkownikowi w danym systemie informatycznym powinny odpowiadać zakresowi uprawnień przyznanemu mu w treści pisemnego upoważnienia. Jeżeli pracownik powinien uzyskać upoważnienie uprawniające go do przetwarzania danych w różnych systemach informatycznych wówczas co do zasady informację do jakich systemów (modułów) powinien on otrzymać, należy wskazać w treści wniosku o wydanie upoważnienia (powinno być wydane jedno upoważnienie).

4. Rozszerzenie lub zmiana upoważnienia powinna prowadzić do zastąpienia poprzedniego upoważnienia nowym, ale dopuszcza się wydanie nowego upoważnienia w zakresie zwiększonych uprawnień. Ustanie, zmiana i wygaśnięcie upoważnień zostaje odnotowane w ewidencji upoważnień, ale wpisy dotyczące takich upoważnień nie są z niej usuwane.

5. W aktach osobowych pracownika przechowuje się egzemplarz oryginalny upoważnienia do przetwarzania danych osobowych podpisany własnoręcznie przez pracownika, co jednocześnie jest potwierdzeniem, że pracownik:

a) przyjął treść upoważnienia do wiadomości,

b) zapoznał się z regulaminem danych osobowych,

c) znane mu są zasady przetwarzania danych osobowych, a ponadto zasady te akceptuje i zobowiązuje się ich przestrzegać.

6. Upoważnienia do przetwarzania danych osobowych udzielane są również pracownikom i współpracownikom podmiotów trzecich, które na mocy zawartych umów otrzymują dostęp do danych zgromadzonych przez Spółkę Arrant lub którym powierzono przetwarzanie danych osobowych. Postanowienia pkt. 1-5 stosuje się odpowiednio, z zastrzeżeniem, że upoważnienia te przechowywane są przez kierownika jednostki organizacyjnej odpowiedzialnej za merytoryczne wykonanie umowy.

7. Upoważnienia do przetwarzania danych osobowych udzielane są również stażystom, praktykantom i wolontariuszom. Postanowienia pkt. 1-5 stosuje się odpowiednio. Upoważnienia przekazywane są do podmiotu odpowiedzialnego za obsługę kadrową Spółki.

8. Rozwiązanie stosunku pracy lub odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych. Zakończenie współpracy z podmiotem trzecim powoduje wygaśnięcie upoważnienia do przetwarzania danych udzielonych pracownikom i współpracownikom tego podmiotu. Zakończenie stażu, praktyki, wolontariatu powoduje wygaśniecie upoważnienia.

14 Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

1. Wykaz budynków, pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe obejmuje miejsca, w których wykonuje się operacje na danych osobowych, w szczególności:

   a) zbieranie,

   b) utrwalanie,

   c) przechowywanie,

   d) opracowywanie,

   e) zmienianie,

   f) rozpowszechnianie lub innego rodzaju udostępnianie,

   g) usuwanie lub niszczenie,

   h) organizowanie,

   i) porządkowanie,

   j) adaptowanie lub modyfikowanie,

   k) pobieranie,

   l) przeglądanie,

   m) wykorzystywanie,

   n) ujawnianie poprzez przesłanie,

   o) dopasowywanie lub łączenie,

   p) ograniczanie.

   Należą do nich również miejsca, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe (pomieszczenia, w których znajdują się: szafy z dokumentacją pisemną, szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe, serwery i inne urządzenia komputerowe, jak np. macierze dyskowe, na których dane osobowe są przetwarzane na bieżąco, skrytki bankowe, archiwum). Do obszaru chronionego zalicza się również pomieszczenia, gdzie składowane są uszkodzone komputerowe nośniki danych (taśmy, dyski, płyty CD, uszkodzone komputery i inne Urządzenia z nośnikami) zawierające dane osobowe.

2. Wzór wykazu budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego jest prowadzony zgodnie ze wzorem opracowanym przez Inspektora Ochrony Danych w formie elektronicznej, na podstawie przekazanych mu informacji przez kierowników poszczególnych komórek organizacyjnych. Wchodzi on w skład Polityki i ją uzupełnia. Nie stanowi on informacji jawnej (pozostaje wyłącznie do użytku wewnętrznego dla celów Administratora).

3. Szczególny nacisk położony jest na bezpieczeństwo strefy przetwarzania danych. Związane jest to z koniecznością zapewnienia optymalnych warunków ochrony dla przetwarzanych informacji. W związku z powyższym przebywanie wewnątrz obszaru określonego, jako obszar przetwarzania danych, osób nieuprawnionych do dostępu do danych

osobowych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych lub za zgodą Administratora.

15 Rejestr czynności przetwarzania

1. Rejestr czynności przetwarzania prowadzony jest zgodnie z wymogami określonymi w art. 30 RODO. Prowadzony jest on w formie elektronicznej lub pisemnej przez Inspektora Ochrony Danych.
2. Rejestr czynności przetwarzanie zawiera co najmniej następujące informacje:
   a) imię i nazwisko lub nazwę oraz dane kontaktowe Administratora oraz Inspektora Ochrony Danych;
   b) cele przetwarzania;
   c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
   d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
   e) 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;
   f) planowane terminy usunięcia poszczególnych kategorii danych;
   g) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.
3. Załącznik nr 4 do niniejszej Polityki zawiera wzór rejestru czynności przetwarzania jest prowadzony zgodnie z tym wzorem przez Inspektora Ochrony Danych.

16 Rejestr kategorii czynności przetwarzania

Inspektor Ochrony Danych zobowiązany jest prowadzić Rejestr kategorii czynności przetwarzania na podstawie informacji przekazanych mu przez kierowników komórek organizacyjnych, dla danych osobowych powierzonych do Arrant. Wzór Rejestru kategorii czynności przetwarzania stanowi załącznik nr 3 do niniejszej Polityki.

17 Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

1. Administrator zobowiązany jest do zastosowania, adekwatnych do stwierdzonego poziomu ryzyka i oceny skutków dla poszczególnych systemów środków technicznych i organizacyjnych dla zapewnienia poufności, integralności, dostępności i rozliczalności przetwarzanych danych.
2. Przestrzeganie przepisów o ochronie danych osobowych zapewnia się w szczególności przez:

a) zapewnianie osobom przetwarzającym możliwości zapoznania się osób przetwarzających dane osobowe z przepisami i zasadami ochrony danych osobowych,

b) zobowiązanie do uzyskania upoważnień do przetwarzania przed rozpoczęciem realizacji zadań związanych z dostępem do danych osobowych,

c) obowiązek zgłoszenia zbioru danych do rejestru zbiorów danych osobowych prowadzonego przez Inspektora Ochrony Danych,

d) ewidencjonowanie informacji o uprawnieniach osób przetwarzających dane,

e) organizowanie szkoleń z zakresu ochrony i bezpieczeństwa przetwarzania danych osobowych,

f) aktualizowanie Dokumentacji i weryfikację się przestrzeganie zasad w niej określonych poprzez prowadzenie cyklicznych sprawdzeń oraz sporządzanie ze sprawdzeń sprawozdań dla Administratora,

g) przyznawanie uprawnień w systemach odpowiednio do zakresu określonego w upoważnieniu,

h) prowadzane na bieżąco zmiany w metodach przetwarzania danych osobowych dla dostosowania przetwarzania do obowiązujących przepisów,

i) szacowanie ryzyka i dokonywanie oceny skutków przetwarzania.

3. W zakresie środków organizacyjnych Administrator wdraża System Ochrony Danych Osobowych zapewniający adekwatny do ryzyka poziom poufności, integralności i dostępności danych, a w szczególności:

1) Regulamin Ochrony Informacji Arrant,

2) Ewidencje osób upoważnionych do przetwarzania danych osobowych,

3) Rejestr umów powierzenia przetwarzania danych osobowych,

4) Rejestr czynności przetwarzania,

5) Rejestr kategorii czynności przetwarzania,

6) Rejestr naruszeń bezpieczeństwa danych osobowych,

4. W zakresie środków technicznych Administrator wdraża:

1) kontrolę dostępu do obszarów fizycznych przetwarzania danych osobowych,

2) kontrolę dostępu do systemów informatycznych,

3) kryptografię w systemach informatycznych,

4) zasady regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania,

5) kontrolę dostępu do danych gromadzonych w związku ze stosowaniem monitoringu wizyjnego,

6) zabezpieczenia przed utratą danych, w tym zapasowe zasilanie, wykonywanie kopii zapasowych:

a) urządzenia, dyski lub inne elektroniczne nośniki informacji zawierające dane osobowe, przeznaczone do: likwidacji, przekazania podmiotowi nieuprawnionemu do przetwarzania danych osobowych, naprawy –

pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,

b) systemy chroniące dostęp z sieci publicznej do systemów przetwarzających dane osobowe zapewniają:

- kontrolę przepływu informacji pomiędzy systemem teleinformatycznym, a siecią publiczną,
- kontrolę działań inicjowanych z sieci publicznej i systemu teleinformatycznego.

18 Reagowanie na naruszenia bezpieczeństwa danych osobowych zgodnie z RODO

1. Każde naruszenie bezpieczeństwa danych osobowych wymaga odpowiedniej reakcji, w tym w szczególności poinformowania o wystąpieniu naruszenia Inspektora Ochrony Danych, który ma obowiązek poinformowania o niniejszym niezwłocznie Administratora. Obowiązek w tym zakresie spoczywa na wszystkich pracownikach i osobach trzecich, które uzyskały dostęp na mocy zawartej umowy do danych gromadzonych w Spółce Arrant.
2. Obowiązek poinformowania o wystąpieniu naruszenia Inspektora Ochrony Danych spoczywa również na podmiotach przetwarzających. Każda osoba odpowiedzialna za umowę zawieraną pomiędzy Administratorem a podmiotem przetwarzającym jest zobowiązana do zamieszczenia w tej umowie stosownego zobowiązania do informowania Inspektora Ochrony Danych o wystąpieniu naruszenia bezpieczeństwa danych osobowych.
3. Podstawą do podjęcia decyzji o sposobie reagowania na incydent jest ocena skutków incydentu, której dokonuje Inspektor Ochrony Danych wraz z właścicielem zasobu/procesu, którego incydent dotyczy oraz Administratorem Systemu, jeżeli dotyczy.
4. W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki – nie później niż w terminie 72 godzin od stwierdzeniu naruszenia – zgłasza je, stosownie do postanowień art. 55 RODO, organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
5. W przypadku zgłoszenia wystąpienia naruszenia po upływie 72 godzin do zgłoszenia dołącza się wyjaśnienie przyczyn opóźnienia.
6. W przypadku, gdy naruszenie może powodować wysokie ryzyko naruszeni praw i wolności osób fizycznych, Administrator informuje osoby, których dane dotyczą.
7. Rejestr naruszeń bezpieczeństwa danych osobowych prowadzony jest przez Inspektora Ochrony Danych w formie elektronicznej lub papierowej, zgodnie ze wzorem zawartym w załączniku nr 5 do niniejszej Polityki.

19 Ocena skutków

1. Jeżeli operacje przetwarzania mogą wiązać się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, przeprowadza się ocenę skutków dla ochrony danych w celu oszacowania w szczególności źródła, charakteru, specyfiki i powagi tego ryzyka. Wyniki oceny uwzględniane są przy określaniu odpowiednich środków, które należy zastosować, by

wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z wymogami prawa powszechnie obowiązującego. Jeżeli ocena skutków dla ochrony danych wykaże, że operacje przetwarzania powodują wysokie ryzyko, którego nie może zminimalizować odpowiednimi środkami z punktu widzenia dostępnej technologii i kosztów wdrożenia, przed rozpoczęciem przetwarzania należy skonsultować się z Prezesem Urzędu Ochrony Danych.

2. Przy ocenie skutków należy uwzględnić charakter, zakres, kontekst i cele przetwarzania oraz źródła ryzyka. Ocena skutków powinna w szczególności obejmować planowane środki, zabezpieczenia i mechanizmy mające minimalizować to ryzyko, zapewniać ochronę danych osobowych oraz wykazać przestrzeganie przepisów prawa powszechnie obowiązującego i aktów prawa wewnętrznego. Jeżeli operacje na danych będą się wiązały z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych oraz jeżeli zostaną spełnione kryteria wskazane w pkt 21.3 i 21.4 niniejszej polityki obowiązkowe będzie przeprowadzenie oceny skutków przetwarzania dla ochrony danych osobowych. Należy zaznaczyć, iż pojęcie „praw i wolności osób fizycznych" odnosi się w szczególności do prawa do prywatności, ale także do prawa do wolności wypowiedzi, swobody poruszania się, zakazu dyskryminacji, swobody myśli, prawa do wolności i swobody przekonań oraz poglądów religijnych.

3. Ocena skutków przeprowadzana jest w szczególności dla operacji przetwarzania:

   1) które ze względu na swój charakter, zakres, kontekst i cele mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych; takie rodzaje operacji przetwarzania obejmują w szczególności operacje, które wiążą się w szczególności z użyciem nowych technologii,

   2) o dużej skali – które służą przetwarzaniu znacznej ilości danych osobowych i które mogą wpłynąć na dużą liczbę osób, których dane dotyczą, oraz które mogą powodować wysokie ryzyko, na przykład (ze względu na swój szczególny charakter) gdy zgodnie ze stanem wiedzy technicznej stosowana jest na dużą skalę nowa technologia – oraz do innych operacji przetwarzania powodujących wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, w szczególności gdy operacje te utrudniają osobom, których dane dotyczą, wykonywanie przysługujących im praw,

   3) w których dane osobowe przetwarza się w celu podjęcia decyzji wobec konkretnej osoby fizycznej po dokonaniu systematycznej, kompleksowej oceny czynników osobowych osób fizycznych na podstawie profilowania tych danych lub po przetworzeniu szczególnych kategorii danych osobowych, danych biometrycznych lub danych osobowych dotyczących wyroków skazujących, naruszeń prawa lub odnośnych,

   4) w przypadku monitorowania na dużą skalę miejsc publicznie dostępnych – w szczególności za pomocą urządzeń optyczno-elektronicznych – lub wszelkich innych operacji, względem których Prezes Urzędu Ochrony Danych uznaje, że przetwarzanie może powodować wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, w szczególności dlatego, że operacje te uniemożliwiają osobom, których dane dotyczą, wykonywanie prawa lub korzystania z usługi lub umowy lub mają systematyczny charakter i dużą skalę.

4. Przeprowadzając ocenę skutków odpowiedzieć sobie należy na następujące pytania:

   1) czy przetwarzane dane podlegają profilowaniu (m.in. czy dokonywana jest ocena lub przyznawana jest punktacja na podstawie przewidywań Administratora w związku z profilowaniem danych, szczególnie jeżeli prognozowanie dotyczy efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą),

   2) czy przetwarzanie danych obejmuje automatyczne podejmowanie decyzji, które wywierają znaczący wpływ na prawa osoby, której dotyczą,

3) czy wykonywany jest systematyczny monitoring na dużą skalę miejsc dostępnych publicznie,

4) czy przetwarzane są dane szczególnych kategorii, o których mowa w art. 9 RODO lub dane dotyczące wyroków skazujących, naruszeń prawa lub związanych z tym środków bezpieczeństwa,

5) czy zbiory danych podlegają łączeniu,

6) czy dane osobowe są przetwarzane z wykorzystaniem innowacyjnych technologii lub z wykorzystaniem innowacyjnych środków organizacyjnych, w szczególności dotyczących identyfikacji osób fizycznych z zastosowaniem linii papilarnych lub z wykorzystaniem biometrii,

7) czy dane są przekazywane poza Unię Europejską,

8) czy dane są przetwarzane na dużą skalę,

9) czy operacje przetwarzania utrudniają osobom, których dane dotyczą, wykonywanie przysługującym ich praw.

W przypadku pozytywnej odpowiedzi na co najmniej dwa z ww. pytań przeprowadzenie oceny skutków jest obowiązkowe.

5. Przez sformułowanie „przetwarzaniem na dużą skalę" rozumie się przetwarzanie spełniające łącznie następujące przesłanki:

1) liczba podmiotów danych jest znaczna „liczbowo" lub jako proporcja pewnej populacji,

2) ilość danych lub zakres różnych danych jest znaczący,

3) czas przetwarzania jest znaczący,

4) geograficzny zakres przetwarzanych danych jest szeroki.

6. Ocena skutków nie jest wymagana w przypadku, gdy przetwarzanie nie prowadzi do wysokiego ryzyka naruszenia praw i wolności osób, a zostało już dopuszczone w bardzo podobnym procesie przetwarzania, ma podstawę prawną w prawie Unii Europejskiej lub w państwie członkowskim lub gdy przetwarzanie znajduje się na liście operacji zwolnionych z oceny skutków przez organ nadzorczy, który ustala i podaje do publicznej wiadomości wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych.

7. Jeżeli rodzaj przetwarzania danych osobowych znajduje się na wykazie rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych prowadzonym przez UODO, należy przeprowadzić taką ocenę wraz z szacowaniem ryzyka.

20 Organizacja ochrony danych osobowych

Zarządzanie ochroną danych osobowych w Spółce odbywa się:

1) na poziomie strategicznym – prowadzone jest zarządzanie strategią rozwoju i doskonalenia Polityki w odniesieniu do zmieniającego się otoczenia prawnego i technologicznego, jak również w oparciu o wyniki analizy ryzyka; w procesy decyzyjne tego poziomu zaangażowany jest Zarząd Spółki

2) na poziomie taktycznym – tworzone są standardy bezpieczeństwa informacji w tym danych osobowych oraz zasady kontroli ich wypełniania w stosowanych rozwiązaniach i systemach informatycznych oraz przestrzegania w praktyce używania tych rozwiązań i systemów; w te procesy decyzyjne zaangażowane jest kierownictwo poszczególnych komórek organizacyjnych związanych z zarządzaniem bezpieczeństwem informacji;

3) na poziomie operacyjnym – prowadzona jest administracja bezpieczeństwem danych osobowych pod kątem pełnego stosowania standardów bezpieczeństwa oraz rozwiązywania sytuacji zakłóceń wynikających z naruszenia tych standardów.

Procesy zarządzania ochroną danych osobowych

Zarządzanie ryzykiem

Strategicznym elementem zarządzania aktywami i bezpieczeństwem danych osobowych w Spółce jest przeprowadzanie okresowego szacowania ryzyka i opracowania planów postępowania z ryzykiem. Wyniki szacowania ryzyka stanowią podstawę podejmowania wszelkich działań w zakresie utrzymania i doskonalenia zabezpieczeń danych osobowych Spółki. Proces zarządzania ryzykiem inicjuje Prezes Zarządu Arrant.

Szacowanie ryzyka

1. Podstawowym kryterium oceny ryzyk jest ich poziom. Postepowanie z ryzykiem zakłada modyfikację ryzyka za pomocą odpowiednio skutecznych zabezpieczeń w obszarach prawnym, organizacyjnym, fizycznym oraz informatycznym.
2. Na podstawie wyników analizy ryzyka opracowywane są plany postępowania dla ryzyka większego niż ustalony poziom ryzyka akceptowalnego oraz dla ryzyka związanego z niezgodnością z przepisami prawa.
3. Szacowanie ryzyka jest przeprowadzana regularnie, nie rzadziej niż raz do roku, ryzyka są regularnie raportowane do Zarządu oraz do zainteresowanych stron. Szacowanie ryzyka przeprowadzana jest również po wprowadzeniu zmian mających wpływ na system bezpieczeństwa danych osobowych.

Dobieranie i stosowanie zabezpieczeń

1. Cele stosowania zabezpieczeń i zabezpieczenia są dobierane na podstawie:
   1) zapisów obowiązujących aktów prawnych,
   2) wyników przeprowadzonej analizy ryzyka w bezpieczeństwie danych osobowych,
   3) wyników oceny skutków w zakresie ochrony danych osobowych,
   4) dobrych praktyk uznanych w obrocie profesjonalnym.
2. Zabezpieczenia wybierane są w obszarach:
   1) fizycznym,

2) organizacyjnym,

3) technicznym.

Utrzymanie i doskonalenie systemu ochrony danych osobowych

System ochrony danych osobowych jest udoskonalany poprzez podjęcie następujących działań:

1) przeprowadzanie działań korygujących oraz ocena ich skuteczności,

2) przeprowadzanie działań zapobiegawczych oraz ocena ich skuteczności,

3) informowanie zainteresowanych stron o działaniach i udoskonaleniach.

Zarządzanie dostępem

Dostęp do aktywów oraz zasobów informacyjnych Spółki jest realizowany za pomocą zatwierdzonych sposobów postępowania oraz mechanizmów kontrolnych w obszarach fizycznego dostępu do informacji oraz zatwierdzonych przez Arrant polityk/reguł zabezpieczania danych w systemach informatycznych.

Identyfikacja procesów przetwarzania danych osobowych

1. Inspektor Ochrony Danych prowadzi ***Rejestr czynności przetwarzania*** - na podstawie informacji przekazanych mu przez Właściciela Procesu. Rejestr prowadzony jest w formie elektronicznej.
2. Właściciel Procesu zobowiązany jest do niezwłocznego (nie później niż w terminie 5 dni roboczych od dnia zaistnienia zmiany) przekazywania do Inspektora Ochrony Danych informacji o wprowadzonych zmian w procesie, w tym w szczególności w zakresie zmiany zakresu przetwarzanych danych, zmianie celu przetwarzania, zmianie zabezpieczeń procesu przetwarzania i aktywów wspomagających.
3. Wdrożenie i nadzór nad zabezpieczeniem przetwarzania danych, w tym:
   1) przystosowanie warunków przetwarzania danych w procesie do warunków zgodnych z obowiązującymi przepisami,
   2) wnioskowanie o wydanie upoważnień do przetwarzania danych osobowych i nadzór nad aktualnością upoważnień w zakresie podległych im pracowników.
4. Na wniosek kierownika komórki organizacyjnej, skierowany do Inspektora Ochrony Danych, wydawane są upoważnienia/zmieniane są upoważnienia do przetwarzania danych. Wzór upoważnienia stanowi załącznik nr 10 do niniejszej Polityki.

Zarządzanie incydentami i naruszeniami ochrony danych osobowych

Zarządzanie incydentami związanymi z bezpieczeństwem informacji jest realizowane za pomocą następujących działań:

1) monitorowania i wykrywania naruszeń bezpieczeństwa danych osobowych w obszarach fizycznego dostępu,

2) monitorowania i wykrywania naruszeń bezpieczeństwa danych osobowych w systemach teleinformatycznych.

Zasady zarządzania naruszeniami zostały określone w dokumencie ***Procedura zarządzania naruszeniami ochrony danych osobowych***.

21 Zasady przechowywania dokumentów papierowych i elektronicznych oraz ich archiwizacja

1. Dokumenty papierowe, wydruki komputerowe:

   1) za bezpieczeństwo danych osobowych zapisanych w formie papierowej odpowiedzialni są wszyscy użytkownicy,

   2) wydruki zawierające dane osobowe przechowuje się w pomieszczeniach, stanowiących obszar przetwarzania danych osobowych, zabezpiecza się przed dostępem osób nieupoważnionych,

   3) wszelkie wydruki zawierające inne informacje podlegające ochronie, muszą być przechowywane w miejscu niedostępnym dla osób nieupoważnionych,

   4) w przypadku, gdy do pomieszczeń po godzinach pracy mają dostęp osoby nieupoważnione, dokumenty zawierające dane osobowe zabezpiecza się na ten czas w szafach zamykanych na klucz, dotyczy to również kopii dokumentów,

   5) wydruki zawierające dane osobowe po ich wykorzystaniu lub po upływie czasu ich przydatności, należy niszczyć przy pomocy niszczarki o poziomie skuteczności min. P3 zgodnie z DIN 66399 lub przechowywać w pojemnikach przeznaczonych do bezpiecznego niszczenia dokumentacji,

   6) po zakończeniu każdego dnia pracy obowiązuje zasada „czystego biurka",

   7) archiwizowanie papierowych zbiorów danych osobowych odbywa się w oparciu o obowiązujące w Spółce procedury przechowywania, archiwizacji i niszczenia dokumentów,

   8) klucze do szaf i biurek z dokumentami są zabezpieczane osobiście przez osoby przetwarzające, a w przypadku wdrożenia do eksploatacji depozytora kluczy, w tym depozytorze.

2. Dokumenty elektroniczne - przechowywanie dokumentów:

   1) muszą być tworzone kopie zapasowe dokumentów przetwarzanych w formie elektronicznej,

   2) niestosowanie się do tych zasad (np. przechowywanie dokumentów wyłącznie na dysku lokalnym komputera) może spowodować utratę danych, za którą odpowiada użytkownik.

3. Zasady postępowania w przypadku korzystania z nośników elektronicznych (pendrive'y, zewnętrzne dyski magnetyczne, aparaty fotograficzne, dyktafony, kamery i inne):

   1) za dane przetwarzane i przechowywane na nośnikach elektronicznych odpowiada użytkownik,

2) nośniki elektroniczne zawierające zbiory danych osobowych, przechowuje się w pomieszczeniach stanowiących obszar przetwarzania danych osobowych, w szafach zamykanych na klucz, za przechowywanie tych nośników odpowiedzialni są pracownicy upoważnieni do przetwarzania danych osobowych,

3) wynoszenie na zewnątrz Spółki danych osobowych na nośniku elektronicznym, może odbywać się tylko za zgodą Inspektora Ochrony Danych,

4) informacje chronione znajdujące się na nośnikach przenośnych, wynoszonych poza teren Spółki muszą być szyfrowane,

5) nośniki danych należy przechowywać w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczając je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych),

6) dane osobowe w postaci elektronicznej należy usuwać z nośnika niezwłocznie po ustaniu ich przydatności, w sposób uniemożliwiający ich ponowne odzyskanie,

7) zabrania się wyrzucania do śmieci nośników elektronicznych, w przypadku zużycia, uszkodzenia lub wymiany nośników pamięci należy bezzwłocznie je przekazać do IT Menadżera.

22 Zasady pracy w systemie informatycznym oraz z dokumentacją w formie tradycyjnej

1. Rozpoczynając pracę z systemem należy sprawdzić ogólny stan używanego sprzętu oraz ocenić jakość pracy urządzenia. Należy szczególnie zwrócić uwagę na:
   1) wyświetlane niestandardowe komunikaty,
   2) automatyczne otwieranie się okienek bez związku z czynnościami wykonywanymi na komputerze,
   3) komunikaty od systemu antywirusowego.
2. Uwierzytelnienie użytkownika odbywa się zgodnie z komunikatami uruchamianego systemu. Użytkownik loguje się do systemu używając swojego identyfikatora i hasła.
3. W przypadku blokady konta systemowego, konieczność zmiany hasła lub odblokowania konta musi być zgłaszana do IT Menadżera
4. Podczas pracy z systemie informatycznym użytkownik zobowiązany jest do stosowania podstawowych zasad bezpieczeństwa. Podczas pracy należy pamiętać w szczególności o:
   1) ustawieniu monitorów w sposób uniemożliwiający osobom nieupoważnionym na wgląd i dostęp do wyświetlanych informacji,
   2) blokowaniu dostępu do systemu operacyjnego komputera poprzez naciśnięcie przycisków Logo Windows + L lub Alt+Ctrl+Delete potwierdzając klawiszem ENTER,
   3) blokowaniu dostępu do systemu operacyjnego lub wylogowaniu się z programu przed opuszczeniem stanowiska pracy,
   4) używaniu wygaszacza ekranu chronionego hasłem,

5) nadzorowaniu osób nieupoważnionych przebywających w pomieszczeniach biurowych.

5. Zabrania się w pomieszczeniach pracowniczych:
   1) pozostawiania osoby nieupoważnionej bez nadzoru osoby upoważnionej,
   2) zezwalania na korzystanie przez osobę nieupoważnioną z urządzeń biurowych lub sprzętu komputerowego w systemie.
6. Użytkownik jest zobowiązany do zachowania zasady czystego ekranu, tj.:
   1) wylogowania się z używanego oprogramowania,
   2) zamknięcia otwartych dokumentów i zapisania niezbędnych zmian,
   3) zamknięcie systemu operacyjnego (należy zaczekać na jego całkowite wyłączenie).
7. Po zamknięciu systemu użytkownik sprawdza, czy nie pozostawiono bez nadzoru elektronicznych lub papierowych nośników informacji zawierających dane chronione, w szczególności dane osobowe:
   1) dokumenty i nośniki elektroniczne zabezpiecza w zamykanych szafach i biurkach,
   2) klucze do szaf i biurek zabezpiecza przed dostępem osób nieupoważnionych,
   3) zamyka pomieszczenia biurowe na klucz,
   4) klucze do pomieszczeń zabezpiecza zgodnie z regulacjami wewnętrznymi, np. wynosi poza pomieszczenia komórki organizacyjnej, pozostawia pod nadzorem ochrony budynku, deponuje w depozytorze elektronicznym.

23 Zasady rozpowszechniania

1. Z zapisami Polityki Bezpieczeństwa Danych Osobowych zapoznają się Inspektor Ochrony Danych, Właściciele Procesów, Kierownicy Komórek Organizacyjnych, pracownicy i podmioty trzecie, które mają lub mogą mieć dostęp do danych osobowych gromadzonych w Spółce Arrant.
2. Zmiany w niniejszym dokumencie wprowadzane są zgodnie z Procedurą nadzoru nad dokumentacją i zapisami Systemu Ochrony Danych Osobowych.

24 Odstępstwa od reguł ochrony

Odstąpienie od zasad opisanych w dokumentacji Systemu Ochrony Danych Osobowych jest możliwe wyłącznie po spełnieniu poniższych warunków:

1. zwrócić się z pisemnym wnioskiem do Administratora o odstąpienie od reguł ochrony i uzasadnić we wniosku powód odstąpienia od przyjętych zasad bezpieczeństwa,

2. otrzymanie pisemnej decyzji Administratora Danych Osobowych,
3. postępować zgodnie z wymogami obowiązującego prawa.

25 Lista dokumentów związanych

26 Załączniki

Załącznik nr 1 – Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Lp.	Nazwisko	Imię	Stanowisko	Data udzielenia upoważnienia	Data wstrzymania upoważnienia	Komórka/Jednostka	Zakres upoważnienia	Identyfikator użytkownika w systemie informatycznym	Uwagi
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									
13									
14									
15									
16									
17									
18									
19									
20									
21									
22									
23									
24									
25									
26									
27									
28									
29									
30									
31									
32									
33									
34									
35									
36									
37									
38									
39									
40									
41									
42									
43									
44									

Załącznik nr 2 – Wzór sprawozdania ze sprawdzenia danych osobowych

Sprawozdanie ze sprawdzenia	planowego nr X/20XX pozaplanowego nr ..... (nr kolejny/ rok) * * niepotrzebne skreślić

1. Osoby uczestniczące w sprawdzeniu

2. Opis przeprowadzonych działań

3. Efekty przeprowadzonych działań w po ostatnim sprawdzeniu

4. Zalecenia i wnioski

4.1 Sprawdzenie zabezpieczeń fizycznych i organizacyjnych

4.2 Sprawdzenie zabezpieczeń informatycznych

Dokument sporządził: *(imię, nazwisko, stanowisko, data i podpis)*	Dokument zatwierdził: *(imię, nazwisko, stanowisko, data i podpis)*

5. Wykaz załączników

Podpis:

Załącznik nr 3 – Wzór rejestru czynności przetwarzania

Dane Administratora:

Nazwa i adres: ……

Tel. ……

Fax. …….

e-mail: ……..

Dane Inspektora Ochrony Danych:

……

…….

Dane Przedstawiciela:

……

…….

Lp.	Nazwa procesu przetwarzania	Cel przetwarzania danych	Opis kategorii osób, których dane dotyczą	Rodzaj i zakres danych osobowych	Kategoria odbiorców, którym dane zostały lub będą ujawnione	Informacja o przekazaniu danych do krajów/organizacji UE	Informacja o przekazaniu danych do krajów/organizacji spoza UE	Opis zabezpieczeń danych	Planowany termin usunięcia poszczególnych kategorii danych	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa

Załącznik nr 4 – Wzór rejestru incydentów

Lp.																
Administrator danych lub informacja o współadministratorach danych (nazwa i adres)																
Miejsce																
Forma i nośniki danych																
Właściciele procesów (albo określona osoba gdy wyciek miał miejsce na danych nieprzetwarzanych w zbiorze)																
Charakterystyka naruszenia																
Określenie kogo dotyczą skutki naruszenia																
Kategorie lub rodzaje osób, których dane zostały naruszone																
Rodzaje/kategorie naruszonych danych																
Szacowana liczba osób dotkniętych naruszeniem																
Szacowana liczba rekordów/wpisów w ramach naruszenia																
Skutki naruszenia - dla osób fizycznych (wszystkie możliwe konsekwencje)																
informacja o zgłoszeniu naruszenia do właściwego organu nadzorczego (forma, data i godzina, zgłaszający, link do treści zgłoszenia)																
Ewentualne wyjaśnienie przekroczenia 72h terminu na zgłoszenie																
Ewentualna informacja o zgłoszeniu naruszenia dotkniętym naruszeniem osobom fizycznym (+ link do treści																
Ewentualna informacja o publicznym poinformowaniu o naruszeniu osób fizycznych dotkniętych naruszeniem (+ link do treści zgłoszenia, + powód wybrania tej metody)																
Zastosowane środki w celu minimalizacji skutków naruszenia																
Zastosowane środki w celu wyeliminowania naruszeń tego typu na przyszłość																

Załącznik nr 5 – Wzór rejestru umów powierzenia

Lp.	Data zawarcia umowy	Nazwa i adres podmiotu, któremu dane zostały powierzone	Zakres powierzonych danych	Okres powierzenia	Cel powierzenia

Załącznik nr 6 – Wyznaczenie osoby, pełniącej funkcje Administratora

Prezes Zarządu Spółki Arrant

Warszawa, dnia …….

Zadania Administratora od dnia ……. wypełniać będzie ……

……..
/pieczątka, podpis/

Załącznik nr 7 – Wzór upoważnienia do przetwarzania danych osobowych

(m. p.) Warszawa, dnia ……

UPOWAŻNIENIE

Na podstawie polecenia nr …… z dnia …….. w sprawie wprowadzenia Systemu Ochrony Danych Osobowych w Spółce Arrant w związku z art. 29 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 upoważniam:

Pani/Pana **…….**

(imię, nazwisko)

……..

(stanowisko) (Biuro)

do przetwarzania danych osobowych w zbiorze:

1. **……** w zakresie ……;
2. **……** w zakresie ……;
3. **……** w zakresie ……,

w celu realizacji powierzonych zadań, zlecanych jednorazowo lub na stałe przez przełożonego.

Pani/Pan **……** został przeszkolony w zakresie ochrony danych osobowych i zapoznany z zasadami ochrony danych osobowych i bezpieczeństwa informacji w Arrant Sp. z o.o.

Upoważnienie jest ważne od …….. do …….

Jednocześnie nakładam obowiązek zabezpieczania danych osobowych przed ich udostępnieniem osobom nieuprawnionym, zabraniem, uszkodzeniem lub zniszczeniem, a także, do zachowania ich w tajemnicy. Obowiązek ten istnieje również po zakończeniu ……

(*stażu, praktyki, umowy o pracę, wolontariatu)*

Traci ważność upoważnienie z dnia …….

OŚWIADCZENIE

Oświadczam, że znane są mi przepisy z zakresu ochrony danych osobowych oraz zasady przetwarzanie danych osobowych w Spółce Arrant.

Zobowiązuję się do zachowania danych osobowych przetwarzanych w Arrant Sp. z o.o. oraz sposobu zabezpieczenia w czasie trwania zatrudnienia jak również po ustaniu zatrudnienia, a także do zabezpieczania danych osobowych przed ich udostępnieniem, zabraniem przez osoby nieupoważnione, przetwarzaniem z naruszeniem przepisów prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Oświadczam, że zostałem poinformowany o grożącej, stosownie do przepisów rozdziałów 10 i 12 ustawy o ochronie danych osobowych, odpowiedzialności cywilnej i karnej za niewypełnianie jej wymogów. Niezależnie od odpowiedzialności przewidzianej w w/w przepisach, przyjmuję do wiadomości, że naruszenie zasad ochrony danych osobowych, obowiązujących w Arrant Sp. z o.o., może zostać uznane za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować odpowiedzialnością dyscyplinarną.

Zobowiązuję się przestrzegać regulaminów, instrukcji i procedur obowiązujących w Arrant Sp. z o.o., dotyczących ochrony danych osobowych. Jednocześnie oświadczam, że bez upoważnienia nie będę wykorzystywał(a) danych osobowych ze zbiorów Arrant Sp. z o.o.

Niniejsze zobowiązanie jest bezterminowe i obowiązuje również po zakończeniu współpracy z Arrant Sp. z o.o.

……

(data i podpis osoby upoważnionej)

Załącznik nr 8 – Wzór umowy powierzenia przetwarzania

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Zawarta ……, w dniu …… roku, pomiędzy:

…….. reprezentowanym przez

1.

(zwaną alej **Procesorem**)

a

,

reprezentowaną przez

1.

(zwaną dalej **Administratorem**)

§ 1

Postanowienia ogólne

1. Na mocy niniejszej umowy Administrator danych osobowych zawartych w zbiorze ..... *(nazwa zbioru)* powierza, w zakresie określonym w § 2 niniejszej umowy, przetwarzanie danych osobowych zawartych w tym zbiorze Procesorowi.
2. Zbiór prowadzony jest w formie ……
3. Właścicielem procesu jest osoba pełniąca funkcję ……. *(np. Dyrektora Wsparcia Sprzedaży Arrant).*
4. Administratorem systemu informatycznego, w którym utworzony został zbiór jest …… , tel. …… *(jeżeli dotyczy).*
5. Procesor zapewnia, że:
   a) posiada fachową wiedzę i zasoby koniecznego do należytej realizacji niniejszej umowy, w szczególności wdrożył środki techniczne i organizacyjne, w tym te dotyczące wymogów bezpieczeństwa przetwarzania, odpowiadające wymogom określonym 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 (zwane dalej również ogólnym rozporządzeniem o ochronie danych lub RODO),

b) będzie zabezpieczał interes prawny osób, których dane przetwarza,

c) będzie w pełni przestrzegał wymogów określonych w zatwierdzonym Kodeksie postępowania, o którym mowa w art. 40 RODO lub zatwierdzonych mechanizmach certyfikacji, o których mowa w art. 42 RODO,

d) będzie realizował wytyczne Administratora w zakresie bezpieczeństwa przetwarzanych powierzonych mu danych,

e) dane osobowe będą przetwarzane na terenie Unii Europejskiej i nie będą przekazane do państwa trzeciego lub organizacji międzynarodowej spoza Unii Europejskiej.

6. Procesor nie jest uprawiony do dalszego przekazywania danych osobowych innemu podmiotowi, bez szczegółowej pisemnej zgody Administratora. W zgodzie tej zostaną określone wymogi dotyczące podmiotu, któremu Procesor może powierzyć dane i sposobu postępowania z danymi, w tym ich zabezpieczeń.

§ 2

Określenie zakresu i okresu powierzenia przetwarzania

1. Administrator powierza dane osobowe wchodzące do zbioru wymienionego w § 1 ust. 1 niniejszej umowy. Zakres powierzonych danych obejmuje:
   1) …….
   2) ……

   Administrator oświadcza, że są to dane osobowe ……. *(np. pracowników, klientów).*
2. Procesor uprawiony jest do przetwarzania danych od dnia zawarcia niniejszej umowy do dnia ……. r. / Procesor uprawiony jest do przetwarzania danych przez czas nieokreślony od dnia zawarcia.
3. Procesor zobowiązany jest do natychmiastowego zaprzestania przetwarzania danych w przypadku:
   1) upływu okresu na jaki umowa została zawarta / wypowiedzenia niniejszej umowy;
   2) ustania celu, dla którego niniejsza umowa została zawarta.
4. Po zakończeniu przetwarzania w imieniu Administratora danych, Procesor powinien – zgodnie z decyzją Administratora – zwrócić lub usunąć dane osobowe, chyba że prawo Unii lub prawo państwa członkowskiego, któremu podlega Procesor, nakładają obowiązek przechowywania danych osobowych. Informacja w tym zakresie zostanie przekazywana Procesorowi, w formie pisemnej, przez Administratora, na co najmniej 3 dni robocze przed zakończeniem obowiązywania niniejszej umowy.
5. W przypadku usunięcia danych - Procesor zobowiązany jest poinformować pisemnie Administratora o wykonaniu tej operacji oraz o sposobie jej wykonania - w terminie 3 dni roboczych od dnia wykonania operacji.

§ 3

Określenie celu

Powierzenie przetwarzania danych osobowych następuje w celu

.....

.....

§ 4

Obowiązki Procesora

1. Procesor zobowiązuje się, że:

1) podejmie wszelkie środki wymagane na mocy art. 32 RODO;
2) w miarę możliwości będzie pomagał Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w Rozdziale III RODO;
3) będzie pomagał Administratorowi wywiązać się z obowiązków określonych w art. 32 – 36 RODO;
4) udostępniania Administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w przepisach prawa powszechnie obowiązującego oraz umożliwienia Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji;
5) niezwłocznego informowania Administratora o stwierdzonych Incydentach dotyczących danych zgromadzonych w zbiorze i współpracy z przedstawicielami Administratora przy usuwaniu jego skutków oraz badaniu przyczyn jego wystąpienia.

2. Przetwarzający oświadcza, że jeżeli naruszy przy przetwarzaniu powierzonych mu danych postanowienia RODO, będzie on traktowany jako Administratora w odniesieniu do tego przetwarzania.
3. Procesor oświadcza, że osoby uprawnione do składania oświadczeń woli w jego imieniu oraz jego pracownicy i współpracownicy dopuszczeni do przetwarzania danych złożyli oświadczenia zgodnie ze wzorem zawartym w załączniku nr 1 do umowy. Oświadczenia te zostały przekazane Administratorowi w dniu zawarcia niniejszej umowy. W przypadku konieczności zmiany osób, które będą miały dostęp do przetwarzanych danych, Administrator zostanie poinformowany przez Procesora pisemnie o niniejszym przed dopuszczeniem nowych osób do przetwarzania danych. Wraz z ww. informacją Administratorowi zostanie przekazane oświadczenie wskazane załączniku nr 1.

§ 5

Kary umowne

1. W przypadku nałożenia na Administratora kary administracyjnej za niezgodne z przepisami prawa powszechnie obowiązującego przetwarzanie danych osobowych zgromadzonych w przekazanym zbiorze lub niezgodne z prawem zabezpieczenie tego zbioru, Procesor:
   a) zwróci Administratorowi, w terminie 7 dni od otrzymania informacji w tym zakresie od Administratora, kwotę wynikającą z nałożonej na niego kary,
   b) zapłaci Administratorowi karę umowną w wysokości …….
2. W przypadku ujawnienia danych osobowych przetwarzanych w przekazanym zbiorze - Procesor zapłaci Administratorowi karę umowną w wysokości …….
3. W przypadku naruszenia postanowień niniejszej umowy, w szczególności w zakresie § 1 ust. 5 lit. c, § 1 ust. 6, § 2 ust. 5, § 4 ust. 3 - Procesor zapłaci Administratorowi karę umowną w wysokości ……
4. W przypadku stwierdzenia podczas działań wskazanych w § 4 ust. 1 pkt 4 niniejszej umowy, że Procesor narusza postanowienia RODO wytycznych wskazanych w § 1 ust. 5 lit c - Procesor zapłaci Administratorowi karę umowną w wysokości ……

§ 6

Postanowienia końcowe

1. Strony umowy postanawiają, że będą się kontaktowały za pośrednictwem następujących osób:
   a) ze strony Administratora: ……
   b) ze strony Procesora: ……
2. Zmiana postanowień niniejszej umowy wymaga zachowania formy pisemnej – pod rygorem nieważności, z zastrzeżeniem zmiany postanowień § 1 ust. 1 i § 6 ust. 1. Strony zobowiązują się informować pisemni o zmianie ww. osób – w terminie 3 dni roboczych od wprowadzenia zmian.
3. Umowa została zawarta w czterech egzemplarzach, po dwa dla każdej ze Stron.

…… ……

(data i podpis Administratora) *(data i podpis Procesora)*