POLITYKA OCHRONY DANYCH OSOBOWYCH

w

OKTA sp. z o.o. z siedzibą w Warszawie
KRS 0000631335, NIP: 5252672173
(dalej: „Administrator”)

WSTĘP

1. Niniejszy dokument zatytułowany "Polityka ochrony danych osobowych" ma za zadanie stanowić mapę wymogów, zasad i regulacji ochrony danych osobowych w spółce OKTA sp. z o.o. z siedzibą w Warszawie.
2. Polityka ochrony danych osobowych powstała w oparciu o wyniki przeprowadzonej szczegółowo przez Administratora analizy ryzyka.
3. Niniejszy dokument został sporządzony nadto w celu wykazania, że dane osobowe są przetwarzane i zabezpieczone przez Administratora zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczenia danych, w tym z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (dalej: RODO).
4. Niniejsza Polityka ochrony danych osobowych jest polityką ochrony danych osobowych w rozumieniu RODO i stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z ww. rozporządzeniem, a także usprawnienie i usystematyzowanie organizacji pracy Administratora.
5. Polityka zawiera:
   a) opis zasad ochrony danych obowiązujących u Administratora
   b) odwołania do załączników uszczegóławiających (takich jak procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach).
6. Za wdrożenie, nadzór i monitorowanie przestrzegania Polityki ochrony danych osobowych odpowiada zarząd Administratora, który w wypełnianiu swoich obowiązków może korzystać ze wsparcia audytorów zewnętrznych.

I. DEFINICJE

Niniejszym ustala się następujące definicje użyte w Polityce:

1) Administrator - OKTA sp. z o. o. z siedzibą w Warszawie ul. Grażyny 15 lok 232, 02-548 Warszawa wpisanej do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m.st. Warszawy, XII Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS: 0000631335, NIP: 5252672173, która decyduje o celach i sposobach Przetwarzania Danych osobowych,
2) Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną przez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznego, fizjologicznego, genetycznego, umysłowego, ekonomicznego, kulturowego lub społecznego (tożsamość tej osoby fizycznej),
3) Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie Osobie upoważnionej uprawnionej do wykonywania czynności w systemie informatycznym, w przypadku Przetwarzania Danych osobowych w takim systemie, definicja ta obejmuje również wszelkiego rodzaju hasła dostępów do innych systemów,
4) Osoba upoważniona – osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, której ustawa nadaje osobowość prawną, upoważniona przez Administratora h do Przetwarzania Danych osobowych,

5) **Podmiot przetwarzający** – organizacja lub osoba, której Administrator powierzył przetwarzanie Danych osobowych (np. dostawcy systemów IT, księgowość zewnętrzna),
6) **Polityka** – niniejsza „Polityka ochrony danych osobowych”,
7) **Profilowanie** – dowolna forma zautomatyzowanego przetwarzania Danych osobowych, które polega na wykorzystaniu Danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się,
8) **Przetwarzanie** – dowolna zautomatyzowana (np. poprzez profilowanie) lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na Danych osobowych lub w zbiorach Danych osobowych, które realizowane są poprzez zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych,
9) **Rejestr Czynności** – Rejestr Czynności Przetwarzania Danych Osobowych,
10) **Rejestr Kategorii** – Rejestr Kategorii Czynności Przetwarzania Danych Osobowych,
11) **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.

II ANALIZA RYZYKA

1. Podstawą do stworzenia niniejszej Polityki w jej obecnym kształcie była przeprowadzona przez Administratora analiza ryzyka. Raport z przeprowadzonej analizy ryzyka pozwolił Administratorowi dobrać odpowiednie środki techniczne i organizacyjne dla zabezpieczenia bezpieczeństwa odpowiadającego ryzyku, przy uwzględnieniu stanu wiedzy technicznej, kosztów wdrażania, charakteru, zakresu, kontekstów, celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych.
2. Administrator nie podejmuje czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób. W przypadku planowania takiego działania Administrator wykona czynności określone w art. 35 i nast. RODO.

III. POSTANOWIENIA OGÓLNE

1. Celem niniejszej Polityki jest określenie kierunków działań, jakie należy wykonać, wykonywać i podejmować w związku z odpowiednim zabezpieczeniem Danych osobowych oraz ustanowienie zasad, reguł postępowania i wsparcia dla zapewnienia bezpieczeństwa Danych osobowych administrowanych przez Administratora, w szczególności:
   a) określenie zasad zarządzania, ochrony i dystrybucji Danych osobowych Przetwarzanych w formie papierowej i/lub w formie elektronicznej, w tym w systemach informatycznych,
   b) określenie standardów zapewniających bezpieczeństwo Przetwarzania Danych osobowych w formie papierowej i/lub w formie elektronicznej, w tym w systemach informatycznych,
   c) określenie procedury postępowania podczas incydentu, który będzie związany z Danymi osobowymi.
2. Polityka dotyczy wszystkich Danych osobowych administrowanych przez Administratora, niezależnie od formy ich Przetwarzania (przetwarzane tradycyjne, zbiory ewidencyjne, systemy informatyczne) oraz niezależnie od

tego, czy Dane osobowe są lub mogą być Przetwarzane w zbiorach danych.

3. Zawarte w Polityce postanowienia, w tym obowiązek ochrony informacji stanowiących Dane osobowe obejmuje wszystkich pracowników oraz inne osoby wykonujące usługi, na podstawie innego stosunku prawnego, przy pomocy których Administrator wykonuje swoje czynności, mające dostęp do Danych osobowych, bez względu na sposób pozyskania informacji stanowiących Dane osobowe.
4. Polityka jest przechowywana w wersji elektronicznej w pamięci komputera będącego do wyłącznej dyspozycji Administratora lub osoby wskazanej przez Administratora oraz w wersji papierowej w siedzibie Administratora i jest dostępna do wglądu dla Osoby upoważnionej w sposób nieograniczony, w każdym czasie.
5. Polityka jest udostępniana do wglądu Osobie upoważnionej na jej wniosek, a także osobie, której ma zostać nadane upoważnienie do Przetwarzania Danych osobowych, przed nadaniem jej upoważnienia przez Administratora, celem zapoznania się z jej treścią. Wgląd do Polityki może nastąpić poprzez okazanie wersji papierowej Polityki lub poprzez przesłanie przez Administratora Polityki w postaci pliku w formacie .pdf na adres poczty e – mail osoby wnioskującej o zapoznanie się z Polityką.
6. Osoba upoważniona lub osoba, której ma zostać nadane upoważnienie do Przetwarzania Danych osobowych może skierować do Administratora zapytanie w przypadku, gdyby treść Polityki była niezrozumiała lub, gdyby pojawiły się wątpliwości co do interpretacji zapisów Polityki.
7. Osoba upoważniona może w każdym czasie zgłosić swój wniosek do Administratora, zawierający propozycję zmian w treści Polityki.
8. Kontakt z Administratorem, o którym mowa w ust. 6 i 7 powyżej może nastąpić osobiście lub za pomocą kanałów kontaktu wskazanych w pkt. I ust. 1 powyżej, to jest w formie pisemnej przesłanej listem zwykłym lub poleconym, wiadomości e – mail lub przy pomocy kontaktu telefonicznego.
9. Dla skutecznej realizacji Polityki Administrator zapewnia:
   a) odpowiednie do zagrożeń i kategorii Danych osobowych objętych ochroną, środki techniczne i rozwiązania organizacyjne,
   b) kontrolę i nadzór nad Przetwarzaniem Danych osobowych,
   c) monitorowanie zastosowanych środków ochrony Danych osobowych.
10. Monitorowanie zastosowanych środków ochrony przez Administratora Danych obejmuje m.in. badanie działania Osoby upoważnionej, badanie naruszania zasad dostępu do Danych osobowych, zapewnienie integralności plików, ochrona przed atakami zewnętrznymi oraz wewnętrznymi.
11. Administrator na bieżąco będzie analizował ryzyko związane z naruszeniem ochrony Danych osobowych, w szczególności będzie badał potencjalne elementy mogące stworzyć zagrożenie naruszenia ochrony Danych osobowych, a w przypadku wykrycia takiego zagrożenia, będzie je odpowiednio dokumentował.
12. Administrator zapewnia, że czynności wykonywane w związku z Przetwarzaniem i zabezpieczeniem Danych osobowych są zgodne z Polityką oraz odpowiednimi przepisami prawa.

IV. FILARY OCHRONY DANYCH OSOBOWYCH U ADMINISTRATORA

W przedsiębiorstwie Administratora przyjęto następujące zasady nadrzędne stanowiące filary ochrony danych osobowych:

a) Legalność – Administrator dba o ochronę prywatności i przetwarza dane osobowe zgodnie z prawem i wyłącznie w oparciu o jedną z podstaw prawnych przetwarzania Danych wymienionych w art. 6 i 9 RODO,
b) Bezpieczeństwo – Administrator zapewnia odpowiedni poziom bezpieczeństwa Danych, podejmując stale działania w tym zakresie,
c) Prawa jednostki – Administrator umożliwia osobom, których dane przetwarza, wykonywanie swoich praw

i prawa te realizuje,

d) **Rozliczalność** – Administrator dokumentuje to, w jaki sposób spełnia obowiązki w zakresie ochrony danych osobowych, aby w każdej chwili móc wykazać zgodność Przetwarzania z powszechnie obowiązującym prawem.

V. SYSTEM OCHRONY DANYCH

System ochrony danych u Administratora składa się z następujących elementów:

a) **Inwentaryzacja danych** – Dane osobowe przetwarzane przez Administratora Danych gromadzone są w zbiorach danych. Administrator dokonuje identyfikacji zasobów danych osobowych, które przetwarza, kategorii danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych;

b) **Rejestry** – Administrator opracowuje, prowadzi i utrzymuje Rejestr Czynności przetwarzania Danych Osobowych, a także szereg innych rejestrów mających za zadanie wsparcie zarządzania przetwarzaniem Danymi, nadzoru i monitoringu przetwarzania. Nadto rejestry są narzędziem rozliczania zgodności przetwarzania danych z ochroną danych u Administratora. Wzór Rejestru Czynności, oraz Wzór Rejestru Kategorii stanowią załączniki do niniejszej Polityki;

c) **Podstawy prawne** – Administrator zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze Czynności i Rejestrze Kategorii, w tym:
   - utrzymuje rejestr zarządzania zgodami na przetwarzanie danych,
   - inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy Administrator przetwarza dane na podstawie prawnie uzasadnionego interesu Administratora;

d) **Obsługa praw jednostki** – Administrator spełnia obowiązki informacyjne względem osób, których dane przetwarza oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
   - **obowiązki informacyjne** – Administrator przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków,
   - **możliwość wykonana żądań** – Administrator weryfikuje i – w zgodnym z prawem zakresie - zapewnia możliwość efektywnego wykonania zgłoszonego żądania,
   - **obsługa żądań** – Administrator zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany przez RODO a także, aby były one udokumentowane,
   - **zawiadamianie o naruszeniach** – Administrator stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych;

e) **Minimalizacja** – Administrator posiada zasady zarządzania minimalizacją, a w tym:
   - zasady zarządzania adekwatnością danych,
   - zasady reglamentacji i zarządzania dostępem do danych,
   - zasady zarządzania okresem przechowywania danych i weryfikacji dalszej przydatności;

f) **Przetwarzający** - Administrator powierza przetwarzanie danych jedynie podmiotom, które gwarantują spełnienie wymogów Administratora, co do warunków i weryfikacji przetwarzania danych, zawartych kompleksowo w umowie powierzenia przetwarzania danych. Wzór umowy powierzenia danych osobowych stanowi załącznik do niniejszej Polityki (możliwe jest stosowanie przez Administratora równoważnych lub zbliżonych treściowo wzorców umowy powierzenia przetwarzania danych);

g) **Eksport danych** - Administrator weryfikuje, czy dane nie są przekazywane do państw trzecich lub do organizacji międzynarodowych oraz zapewnia zgodne z prawem warunki takiego przekazywania, jeśli ma

ono miejsce;

h) Privacy by design - Administrator zarządza zmianami wpływającymi na prywatność. W tym celu procesy uruchamiania nowych projektów i inwestycji przez Administratora uwzględniają konieczność oceny wpływu zmiany na ochronę danych, analizę ryzyka, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu;

i) Privacy by default - Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania;

j) Bezpieczeństwo – Administrator zapewnia odpowiedni poziom bezpieczeństwa danych w tym:
   - przeprowadza analizy ryzyka dla czynności przetwarzania danych,
   - przeprowadza ocenę skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie,
   - dostosowuje środki ochrony danych do ustalonego ryzyka, w tym zabezpiecza obszar przetwarzania Danych osobowych,
   - stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych - zarządza incydentami.

VI. INWENTARYZACJA DANYCH OSOBOWYCH I REJESTRY

1. Administrator co do zasady Przetwarza Dane osobowe zwykłe.
2. Administrator identyfikuje przypadki, w których przetwarza lub może przetwarzać dane szczególnych kategorii oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania takich danych. Na chwilę sporządzenia niniejszej Polityki, Administrator nie przetwarza danych szczególnych kategorii, poza danymi dotyczącymi zdrowia pracowników Administratora, koniecznymi w kontekście medycyny pracy.
3. Administrator prowadzi Rejestr Czynności Przetwarzania Danych Osobowych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe. Rejestr pełni również rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.
4. W Rejestrze dla każdej czynności przetwarzania danych, którą Administrator uznał za odrębną dla potrzeb Rejestru, Administrator odnotowuje co najmniej:
   - nazwę czynności,
   - cel przetwarzania,
   - opis kategorii osób,
   - opis kategorii danych,
   - opis szczególnych kategorii danych,
   - opis kategorii odbiorców danych (w tym przetwarzających), w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,
   - kategorie odbiorców danych,
   - sposób przetwarzania danych,
   - sposób zbierania danych,

- podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu Administratora, jeśli podstawą jest uzasadniony interes,
- okres przechowywania danych/planowany termin usunięcia poszczególnych kategorii danych
- ogólny opis technicznych i organizacyjnych środków ochrony danych
- informację o przekazaniu poza EU/EOG (w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń).

5. Rejestr zawiera także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych Administrator rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść Rejestru ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej.
6. Rejestr prowadzony jest w formie elektronicznej.
7. Administrator nie przetwarza danych osób, których nie identyfikuje.
8. Administrator nie przetwarza danych dzieci.
9. Administrator nie dokonuje i nie planuje profilowania przetwarzanych danych ani nie podejmuje decyzji w sposób zautomatyzowany. Jednakowoż, w przypadku zmian w podnoszonej kwestii, Administrator zobowiązuje się identyfikować przypadki, w których będzie dokonywał profilowania przetwarzanych danych, jak również zobowiązuje się zastosować mechanizmy zapewniające zgodność tego procesu z prawem.
10. Administrator nie przetwarza danych osobowych na zasadach współadministrowania.
11. Administrator prowadzi również Rejestru Kategorii, w którym uwzględnił odnotowywanie co najmniej:
    - kategorii przetwarzania,
    - ogólnego opisu technicznych i organizacyjnych środków bezpieczeństwa,
    - nazwy i danych kontaktowych administratora,
    - nazwy i danych kontaktowych współadministratora,
    - nazwy i danych kontaktowych przedstawiciela administratora,
    - Inspektora ochrony Danych administratora,
    - czasu trwania przetwarzania,
    - informacji o przekazaniu poza EU/EOG i związanych z tym działaniem środkami bezpieczeństwa,
    - informacji o podpowierzaniu przetwarzania danych.
12. Rejestr Kategorii– w kontekście wymogów zawartych w RODO - zawiera kolumny nieobowiązkowe. W kolumnach nieobowiązkowych Administrator może rejestrować informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść Rejestru Kategorii ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej.
13. Rejestr Kategorii prowadzony jest w formie elektronicznej.

Via. INNE REJESTRY

1. Poza Rejestrem, opisanymi powyżej, w celu zapewnienia odpowiedniego standardu ochrony danych osobowych i w celu sprawniejszego zarządzania danymi, jak i uprawnieniami osób przetwarzających dane osobowe, Administrator utworzył następujące rejestry:
    - REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH,
    - REJESTR ŻĄDAŃ I REALIZACJI PRAW OSÓB, KTÓRYCH DOTYCZĄ DANE OSOBOWE,
    - REJESTR UPOWAŻNIEŃ,
    - REJESTR UMÓW POWIERZENIA DANYCH OSOBOWYCH,

- REJESTR ZGÓD NA PRZETWARZANIE DANYCH OSOBOWYCH,
- REJESTR KLAUZUL INFORMACYJNYCH I ICH ZMIAN.

2. Rejestry powyższe mają także służyć realizacji wymogu rozliczalności w zakresie zarządzania danymi, monitorowania ich przepływami oraz ich ewidencjonowania - wynikającymi z RODO lub standardów przepływu danych u Administratora.

VII. PODSTAWY PRAWNE PRZETWARZANIA

1. Administrator dokumentuje w Rejestrze Czynności podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.
2. Wskazując w dokumentach ogólną podstawę prawną (np. zgoda, umowa, obowiązek prawny, uzasadniony interes Administratora), Administrator dookreśla podstawę w precyzyjny i czytelny sposób, gdy jest to potrzebne. Np. dla zgody - wskazując jej zakres, gdy podstawą jest prawo - wskazując konkretny przepis i inne dokumenty, np. umowę, porozumienie administracyjne, żywotne interesy - wskazując kategorie zdarzeń, w których się zmaterializują, uzasadniony interes - wskazując konkretny cel, np. marketing własny, dochodzenie roszczeń.
3. Administrator wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (e-mail, telefon, SMS itp.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).
4. Pracownicy/współpracownicy/zleceniobiorcy Administratora mają obowiązek znać podstawy prawne, na jakich dokonują konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes Administratora, pracownik ma obowiązek znać konkretny realizowany przetwarzaniem interes Administratora.

VIII. OBSŁUGA PRAW JEDNOSTKI

1. Administrator dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.
2. Administrator ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie informacji na temat przetwarzania danych w łatwej do zauważenia, ogólnodostępnej przestrzeni, zamieszczenie wyraźnej, czytelnej i prostej w odbiorze informacji o metodach zapoznania się z informacjami o przetwarzaniu danych przy drzwiach wejściowych do lokalu przedsiębiorstwa, a także poprzez zamieszczenie na stronie internetowej Administratora stosownej klauzuli informacyjnej, informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich, w tym wymaganiach dotyczących identyfikacji i metodach kontaktu z Administratorem.
3. Administrator nie pobiera opłat za realizację praw jednostki w zakresie żądań dotyczących przetwarzania danych osób, za wyjątkiem sytuacji opisanych szczegółowo w *„Polityce realizacji praw osób, których dane dotyczą”*.
4. Administrator dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.
5. Administrator wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.
6. W celu realizacji praw jednostki Administrator zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Administratora, zintegrować te dane,

wprowadzać do nich zmiany i usuwać w sposób zintegrowany (załącznik do Polityki - *„Polityka realizacji praw osób, których dane dotyczą”).*

7. Administrator dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób zgodnie z załącznikiem do Polityki – wzorem Rejestru żądań i realizacji praw osób, których dotyczą dane osobowe.

VIIIa. OBOWIĄZKI INFORMACYJNE

1. Administrator określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.
2. Administrator informuje osobę o:
   a) przetwarzaniu jej danych przy pozyskiwaniu danych od tej osoby,
   b) przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej,
   c) planowanej zmianie celu przetwarzania danych.
3. W zależności od kanału pozyskania danych osobowych, obowiązek informacyjny realizowany jest wg następujących procedur:
   - w przypadku pozyskiwana danych podczas pierwszego kontaktu w trakcie bezpośredniego kontaktu w lokalu Administratora, informacja o przetwarzaniu danych przesyłana jest niezwłocznie (tuż po uzyskaniu adresu poczty elektronicznej) na wskazany przez osobę adres poczty elektronicznej, a dodatkowo, osoba, której dane dotyczą informowana jest o możliwości zapoznania się z informacją o przetwarzaniu danych w lokalu Administratora przy drzwiach wejściowych do lokalu lub na tablicy ogłoszeń w miejscu ogólnodostępnym dla osób przybyłych do lokalu Administratora;

   - w przypadku pozyskiwana danych podczas pierwszego kontaktu drogą poczty elektronicznej, informacja o przetwarzaniu danych przesyłana jest niezwłocznie w wiadomości zwrotnej na wskazany przez osobę adres poczty elektronicznej;

   - w przypadku pozyskiwana danych podczas pierwszego kontaktu telefonicznego, informacja (warstwowa) o przetwarzaniu danych podawana jest w zakresie podstawowych danych dotyczących Administratora danych osobowych, z odesłaniem do szczegółowej informacji o przetwarzaniu danych:
     - na stronie internetowej Administratora: www.okta.com.pl oraz
     - udostępnionej w lokalu Administratora

Wzór powyższej informacji(dopuszczalne są również komunikaty zbliżone treściowo do poniższego z uwzględnieniem aktualizacji danych teleadresowych):

„W związku z nawiązanym przez Panią/Pana kontaktem, informuję, iż Administratorem Pani/Pana danych osobowych jest Okta sp. z o.o. z siedzibą w Warszawie, przy ul. Grażyny 15 lok 232, 02-548 Warszawa NIP: 5252672173. Z Administratorem można skontaktować się pod adresem siedziby, dzwoniąc pod numer: +48 790 30 30 78 lub wysyłając wiadomość pod adres e-mail: rodo@okta.com.pl.

Szczegółowa informacja dotycząca przetwarzania Pani/Pana danych osobowych przez Administratora, zamieszczona jest na stronie internetowej Administratora pod adresem: www.okta.com.pl oraz w lokalu Administratora

Prosimy o zapoznanie się z ich treścią, a w razie pytań służymy dodatkowymi wyjaśnieniami.”

4. Administrator stworzył zindywidualizowane informacje o przetwarzaniu danych osobowych dedykowane i dopasowane do różnych kategorii osób, w tym dla:
    - pracowników
    - kandydatów do pracy
    - współpracowników
    - zleceniobiorców
    - kontrahentów
    - uczestników szkoleń i warsztatów
    - osób korzystających z formularza kontaktowego udostępnionego na stronie internetowej Administratora
    - użytkowników fanpage'a Administratora w ramach portalu społecznościowego Facebook

(Załączniki do Polityki - wzory informacji o przetwarzaniu danych osobowych dla różnych kategorii osób).

5. Administrator prowadzi i aktualizuje Rejestr zmian w klauzulach informacyjnych stosowanych w ramach jego przedsiębiorstwa (wzór Rejestru zmian w klauzulach informacyjnych stanowi załącznik do Polityki).
6. Informacje o przetwarzaniu danych zawierają informację o wersji informacji i dacie ostatniej aktualizacji.
7. Administrator informuje Osobę o planowanej zmianie celu przetwarzania danych.
8. Administrator informuje osobę przed uchyleniem ograniczenia przetwarzania.
9. Administrator informuje odbiorców danych o prostowaniu, usunięciu lub ograniczeniu Przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).
10. Administrator informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.
11. Administrator bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby zgodnie ze Wzorem Powiadomienia o naruszeniu ochrony danych osobowych – zawiadomienie osoby, której dane dotyczą" – stanowiącym załącznik do niniejszej Polityki.

VIIIb. ŻĄDANIA OSÓB

1. Administrator realizuje prawa żądań osób, których dane są przetwarzane w następującym zakresie:
    a) Prawa osób trzecich - realizując prawa osób, których dane dotyczą, Administrator wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste), Administrator może się zwrócić do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu do czasu zapewnienia gwarancji ochrony praw i wolności osób trzecich,
    b) Nieprzetwarzanie - Administrator informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw,
    c) Odmowa - Administrator informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych,
    d) Dostęp do danych - na żądanie osoby dotyczące dostępu do jej danych Administrator informuje osobę, czy przetwarza jej dane, oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela osobie dostępu

do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie nieodpłatnych kopii danych (przy pierwszym egzemplarzu kopii).

e) Kopie danych - na żądanie Administrator wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Administrator może wprowadzić cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie danych. Cena kopii danych skalkulowana zostanie na podstawie oszacowanego jednostkowego kosztu obsługi żądania wydania kopii danych,

f) Sprostowanie danych - Administrator dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Administrator ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby,

g) Uzupełnienie danych - Administrator uzupełnia i aktualizuje dane na żądanie osoby. Administrator ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Administrator nie musi przetwarzać danych, które są Administratorowi zbędne). Administrator może polegać na oświadczeniu osoby co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Administrator procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne,

h) Usunięcie danych - Na żądanie osoby Administrator usuwa dane, gdy:
   - dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane,
   - osoba, której dane dotyczą, cofnęła zgodę będąca podstawą do przetwarzania danych zgodnie z art. 6 ust. 1 lit. a) RODO, a brak jest innej podstawy przetwarzania,
   - osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania danych, o którym mowa w lit. k) poniżej i nie występują okoliczności, o których mowa w lit. k) poniżej,
   - dane osobowe są przetwarzane niezgodnie z prawem,
   - dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii Europejskiej lub prawie polskim,
   - dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. profil dziecka na portalu społecznościowym, udział w konkursie na stronie internetowej),
   - Administrator określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO,
   - jeżeli dane podlegające usunięciu zostały upublicznione przez Administratora, Administrator podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe o potrzebie usunięcia danych i dostępu do nich,
   - w przypadku usunięcia danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby,

i) Ograniczenie przetwarzania - Administrator dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:
   - osoba kwestionuje prawidłowość danych - na okres pozwalający sprawdzić ich prawidłowość,

- przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
- Administrator nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
- osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją — do czasu stwierdzenia, czy po stronie Administratora zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

W trakcie ograniczenia przetwarzania Administrator przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego. Administrator informuje osobę przed uchyleniem ograniczenia przetwarzania. W przypadku ograniczenia przetwarzania danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby,

j) Przenoszenie danych - na żądanie osoby Administrator wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Administratorowi, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej w systemach informatycznych Administratora,

k) Sprzeciw w szczególnej sytuacji - jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Administratora w oparciu o uzasadniony interes Administratora lub o powierzone Administratorowi zadanie w interesie publicznym, Administrator uwzględni sprzeciw, o ile nie zachodzą po stronie Administratora ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

l) Sprzeciw względem marketingu bezpośredniego - jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Administratora na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), Administrator uwzględni sprzeciw i zaprzestanie takiego przetwarzania,

m) Prawo do ludzkiej interwencji przy automatycznym przetwarzaniu – Administrator nie przetwarza danych w sposób automatyczny. Jeżeli jednak Administrator zdecydowałby się przetwarzać dane w sposób automatyczny, w tym w szczególności profilować osoby, i w konsekwencji podejmować względem osoby decyzje wywołujące skutki prawne lub inaczej istotnie wpływające na tę osobę, Administrator zapewni możliwość odwołania się do interwencji i decyzji człowieka po stronie Administrator, chyba że taka automatyczna decyzja:
    - jest niezbędna do zawarcia lub wykonania umowy między odwołującą się osobą a Administratorem, lub
    - jest wprost dozwolona przepisami prawa, lub
    - opiera się na wyraźnej zgodzie odwołującej osoby.

Szczegółowy opis realizacji praw osób, których dane dotyczą, ze wskazaniem odpowiednich terminów, procedur szczegółowych czy odstępstw od pełnienia żądań osoby, zawarty jest w Polityce realizacji praw osób, których dane dotyczą, stanowiącej załącznik do niniejszej Polityki.

IX. PODMIOTY PRZETWARZAJĄCE

1. Administrator może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej lub elektronicznej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO i tylko jeżeli są to dane, które może ujawnić bez naruszenia tajemnicy zawodowej.
2. Przed powierzeniem przetwarzania danych osobowych Administrator w miarę możliwości uzyskuje informacje o dotychczasowych praktykach procesora dotyczących zabezpieczenia danych osobowych.
3. Administrator posiada narzędzia doboru podmiotów przetwarzających dane na rzecz Administrator opracowane w celu zapewnienia, aby przetwarzający dawali wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na Administratorze.
4. Głównym narzędziem realizującym gwarancje wskazane powyżej, jest posługiwanie się opracowanym na potrzeby Administratora wzorcem *„Umowy powierzenia przetwarzania danych”*, stanowiącym załącznik do Polityki (lub w wyjątkowych sytuacjach korzystanie z innych wzorców, zawierających minimalne wymagania co do umowy powierzenia przetwarzania danych określone w art. 28 RODO), a także zestaw pytań audytowych, służących weryfikacji potencjalnego procesora pod względem jego standardów ochrony danych osobowych.

X. EKSPORT DANYCH

1. Administrator nie będzie przekazywał Danych osobowych do państwa trzeciego (poza Europejski Obszar Gospodarczy – EOG) poza sytuacjami, w których:
    a) następuje to na wniosek i za wyraźną zgodą osoby, której Dane osobowe dotyczą,
    b) Dane osobowe mogą być przekazywane za pośrednictwem poczty elektronicznej w sytuacji, gdyby serwer poczty znajdował się poza terytorium Unii Europejskiej,
    c) Dane osobowe mogą być przekazywane za pośrednictwem portali społecznościowych.
2. W przypadku przekazywania danych poza EOG Administrator Danych Osobowych zapewnia ochronę transgranicznego przetwarzania danych przy zastosowaniu właściwych środków bezpieczeństwa.
3. Administrator zapewnia, że żaden podmiot – poza podmiotami świadczącymi niezbędne usługi na rzecz Administratora - nie uzyskuje dostępu do jakichkolwiek danych, które pozwalałyby mu na ustalenie tożsamości klientów Administratora.
4. W przypadku wyjątków, o których mowa w niniejszym paragrafie, opisane przekazywanie danych odbywa się w oparciu o jedną z poniższych zasad:
    a) stosowną umowę zawartą pomiędzy Administratorem a danym podmiotem, zawierającą standardowe klauzule ochrony danych,
    b) współpracę z podmiotami przetwarzającymi dane osobowe w państwach, w odniesieniu do których została wydana stosowna decyzja Komisji Europejskiej,
    c) stosowanie wiążących reguł korporacyjnych zatwierdzonych przez właściwy organ nadzorczy,
    d) wyrażoną zgodę.
5. Osoby, których dane są Przetwarzane są informowane o przekazywaniu danych osób poza EOG.
6. Administrator rejestruje w Rejestrze przypadki eksportu danych, czyli przekazywania danych poza EOG.

XI. PRIVACY BY DESIGN

1. Administrator zarządza wszelkimi zmianami mającymi wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania.

2. W tym celu zasady prowadzenia nowych projektów i inwestycji rozwojowych Administratora będą odwoływać się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność, ochronę danych, uwzględnienia i zaprojektowania bezpieczeństwa oraz minimalizacji przetwarzania danych już na etapie planowania projektu czy inwestycji.
3. Zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania, Administrator wdraża odpowiednie środki techniczne i organizacyjne, zaprojektowane w celu skutecznej realizacji zasad ochrony danych oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą.
4. Wdrażając odpowiednie środki techniczne i organizacyjne, Administrator uwzględnia stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania.

XII. PRIVACY BY DEFAULT

Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

XIII. MINIMALIZACJA

1. Administrator dba o minimalizację przetwarzania danych pod kątem:
   - adekwatności danych do celów (ilości danych i zakresu przetwarzania),
   - dostępu do danych,
   - czasu przechowywania danych.

a) Minimalizacja zakresu - Administrator zweryfikował zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO. Administrator dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok oraz przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach planowanych zmian (privacy by design).

b) Minimalizacja dostępu – Administrator stosuje ograniczenia dostępu do danych osobowych:
   - prawne (zobowiązania do poufności, zakresy upoważnień),
   - fizyczne (zamykanie pomieszczeń, zamykanie szaf z dokumentacją),
   - logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe).
     i. Administrator dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób oraz zmianach podmiotów przetwarzających.
     ii. Administrator dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.

iii. Szczegółowe zasady bezpieczeństwa przetwarzania danych w systemie informatycznym oraz kontroli dostępu logicznego zawarte są w *Polityce Zarządzania Systemem Informatycznym* (załącznik do Polityki).

c) Minimalizacja czasu - Administrator wdraża mechanizmy kontroli cyklu życia danych osobowych u Administratora, w tym weryfikacji dalszej przydatności danych względem wskazanych w Rejestrze.

- Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu, są usuwane z systemów informatycznych Administratora, jak też z kartotek papierowych, jednakże dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów informatycznych przetwarzanych przez Administratora, do czasu wygaśnięcia okresów przedawnienia roszczeń mogących wymagać dostępu do danych archiwizowanych. Procedury archiwizacji i tworzenia kopii zapasowych, uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych. Procedury archiwizacji i tworzenia kopii zapasowych zawarte są w *Polityce Zarządzania Systemem Informatycznym* (załącznik do Polityki).
- Dane przetwarzane w formie kartotek papierowych z upływem okresów wskazanych w Rejestrze mogą być usunięte poprzez:
  - zniszczenie mechaniczne – za pomocą niszczarki, w obecności komisji rewizyjnej w składzie Administrator + 2 świadków niszczenia;
  - anonimizację – nieodwracalny proces polegający na takim odebraniu atrybutów identyfikacyjnych danych, iż na podstawie przekształconych informacji nie sposób jest kiedykolwiek ponownie zidentyfikować osobę, której dane uległy anonimizacji.

XIV. ZARZĄDZANIE BEZPIECZEŃSTWEM

I. Zasady ochrony danych u Administratora

1. Administrator przetwarza Dane z poszanowaniem następujących zasad:
   b) w oparciu o podstawę prawną zgodnie z prawem (legalizm) - w każdym wypadku występuje chociaż jedna z przewidzianych przepisami prawa podstaw dla Przetwarzania Danych osobowych,
   c) rzetelnie i uczciwie (rzetelność) - wobec osoby, której dane dotyczą, wykonywany jest obowiązek informacyjny zgodnie z treścią art. 13 i 14 RODO,
   d) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność),
   e) w konkretnych celach i nie „na zapas" (minimalizacja) - Dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami,
   f) nie więcej niż potrzeba (adekwatność) - Dane osobowe są Przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu Przetwarzania Danych osobowych,
   g) z dbałością o prawidłowość danych (prawidłowość) - Dane osobowe są w razie potrzeby uaktualniane,
   h) nie dłużej niż potrzeba (czasowość) - czas przechowywania Danych osobowych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane, a po tym okresie będą one zanonimizowane bądź usuwane,
   i) zapewniając odpowiednie bezpieczeństwo (bezpieczeństwo) - Dane osobowe są zabezpieczone przed naruszeniami zasad ich ochrony.

II. Analiza ryzyka

1. Administrator przeprowadza i dokumentuje analizy ryzyka oraz adekwatności środków bezpieczeństwa danych osobowych. W tym celu:
   a) Administrator zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania — wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych;
   b) Administrator kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają;
   c) Administrator przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Administrator analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych, uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia;
   d) Administrator ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym Administrator ustala przydatność i stosuje takie środki i podejście, jak:
      I. pseudonimizacja,
      II. szyfrowanie danych osobowych,
      III. inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
      IV. środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
   j) Administrator zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek Przetwarzania Danych osobowych przez Administratora.
   k) Administrator stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i oceny adekwatności, co oznacza, że zastosowane środki ochrony (techniczne i organizacyjne) są adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych.
   l) Administrator dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.
   m) Szczegółowy raport z analizy ryzyka stanowi załącznik do Polityki.

III. Środki techniczne i organizacyjne w tym środki ochrony fizycznej Danych osobowych

1. Administrator Danych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości Przetwarzanych Danych osobowych.
2. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii Danych osobowych.
3. Techniczne i organizacyjne środki ochrony Danych osobowych**,** w tym środki ochrony fizycznej obejmują w szczególności następujące zabezpieczenia:
   a) opracowanie i wdrożenie niniejszej Polityki,
   b) opracowanie i wdrożenie Instrukcji zarządzania systemem informatycznym – (Instrukcja zarządzania systemem informatycznym stanowi załącznik do niniejszej Polityki), regulującej, m.in.:
      - procedury pracy na stanowisku komputerowym,
      - procedury korzystania z poczty elektronicznej i Internetu,

- procedury kasowania danych,
- procedury postepowania z nośnikami danych,

c) przeprowadzanie cyklicznych audytów,
d) dopuszczenie do Przetwarzania Danych wyłącznie Osób upoważnionych, posiadających ważne upoważnienia nadane im przez Administratora – Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik do niniejszej Polityki,
e) prowadzenie przez Administratora rejestru osób upoważnionych do przetwarzania danych,
f) zobowiązane Osób upoważnionych do zapoznania się z przepisami dotyczącymi ochrony Danych osobowych,
g) zobowiązanie Osób upoważnionych do zachowania Danych osobowych oraz sposobu ich zabezpieczania w tajemnicy,
h) stosowanie pisemnych umów powierzenia Przetwarzania Danych osobowych dla współpracy z podwykonawcami Przetwarzającymi Dane osobowe,
i) kontrolę widocznych śladów ingerencji osób trzecich, pożaru, zalania lub innego uszkodzenia przy pierwszym wejściu do obszaru przetwarzania w danym dniu,
j) ustawienie monitorów komputerów, na których Przetwarzane są Dane osobowe w siedzibie Administratora Danych lub w miejscu przez niego wyznaczonym, w sposób uniemożliwiający wgląd osobom nieupoważnionym do Danych osobowych,
k) dokonywanie Przetwarzania Danych osobowych w warunkach zabezpieczających dane przed dostępem do nich osób nieupoważnionych,
l) przestrzeganie zasad przeciwpożarowych w obszarach przetwarzania danych,
m) umieszczanie kluczowych zasobów tak, aby ograniczyć do nich dostęp osób nieupoważnionych (m.in. stosowanie ograniczonej ilości kompletów zasobów kluczowych, dostęp do zasobów kluczowych jedynie wyznaczonych do tego osób),
n) korzystanie ze środków przechowywania i przetwarzania informacji poza siedzibą organizacji wyłącznie za zezwoleniem kierownictwa,
o) zakaz pozostawiania w miejscach publicznych bez nadzoru urządzeń lub nośników wynoszonych poza siedzibę Administratora,
p) stosowanie polityki „czystego biurka”,
q) stosowanie polityki „czystego ekranu”,
r) zakaz korzystania z kopiarek lub innych technik kopiowania (np. skanerów, aparatów cyfrowych) bez autoryzacji kierownictwa,
s) kontrola i nadzór nad Przetwarzaniem danych osobowych,
t) testowanie oprogramowanie przed jego zainstalowaniem,
u) monitorowanie zastosowanych środków ochrony., m.in. poprzez losowe weryfikowanie działań użytkowników,
v) dokonywanie okresowego przeglądu ustanowionych użytkowników systemów i aktualizacja ich nie rzadziej niż raz na rok,
w) przechowywanie kopii zapasowych w formie zaszyfrowanej,
x) usuwane kopii zapasowych niezwłocznie po ustaniu ich użyteczności,
y) nadanie uprawnień pracownikom i dokonywanie aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób oraz zmianach podmiotów przetwarzających,
z) weryfikację i aktualizację dokumentacji z zakresu ochrony danych osobowych oraz weryfikacja przestrzegania zasad i procedur w niej zawartych, polegająca na sprawdzeniu:

- czy dokumentacja zgodna jest z obowiązującymi przepisami prawa,
- czy przewidziane w dokumentacji środki ochrony technicznej i organizacyjnej służące przeciwdziałaniu zagrożeniom są zgodne ze stanem rzeczywistym,
- czy przestrzegane są zasady, procedury i obowiązki wynikające z tej dokumentacji,

aa) przetwarzanie i przechowywanie Danych odbywa się w pomieszczeniu zabezpieczonym drzwiami wyposażonymi w zabezpieczenie w postaci zamka lub kontroli dostępu,

bb) wyposażenie w system alarmowy przeciwwłamaniowy pomieszczeń, w których Przetwarzane są Dane osobowe,

cc) nadzorowanie przez całą dobę przez podmiot zajmujący się profesjonalnie ochroną mienia dostępu do budynku, w którym Przetwarzane są Dane osobowe,

dd) ograniczenie dostępu do pomieszczeń, w których przetwarzane są Dane osobowe jedynie do Osób upoważnionych (inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do przetwarzania Danych osobowych jedynie w towarzystwie Osoby upoważnionej),

ee) zamykanie pomieszczeń tworzących obszar Przetwarzania Danych osobowych na czas nieobecności Osób upoważnionych, w sposób uniemożliwiający dostęp do nich osób nieupoważnionych,

ff) zabezpieczenie pomieszczenia, w którym Przetwarzane są Dane osobowe przed skutkami pożaru za pomocą wolnostojącej gaśnicy,

gg) niszczenie dokumentów zawierających Dane osobowe po ustaniu ich przydatności w sposób mechaniczny, za pomocą niszczarek dokumentów lub podmiotów zajmujących się profesjonalnie niszczeniem dokumentów, posiadających certyfikat bezpieczeństwa, chyba że obowiązujące przepisy prawa wymagają przechowywania dokumentów,

hh) zabezpieczenie dokumentów i innych nośników zawierających Dane osobowe, poprzez wykorzystanie zamykanych szafek,

ii) zapewnienie okresowego wykonywania kopii zapasowych Danych osobowych na przeznaczonych w tym celu przez Administratora nośnikach, takich jak dysk zewnętrzny,

jj) przechowywanie kopii zapasowych zbioru Danych osobowych w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym Dane osobowe Przetwarzane są na bieżąco,

kk) przechowywanie kopii zapasowych/archiwalnych Danych osobowych w zamkniętej, niemetalowej szafie,

ll) stosowanie zakazu spożywania napojów i płynnych posiłków oraz palenia przy urządzeniach i nośnikach Danych.

IV. Środki zabezpieczeń infrastruktury informatycznej i telekomunikacyjnej wykorzystywane przez Administratora Danych w celu zabezpieczenia i zapewnienia ochrony Danych osobowych

1. Dane osobowe Przetwarzane są przy użyciu komputerów przenośnych, zabezpieczonych programem antywirusowym.
2. Dostęp do systemu operacyjnego komputera, w którym Przetwarzane są Dane osobowe, jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem indywidualnego identyfikatora oraz Hasła.
3. Administrator stosuje środki ochrony Danych osobowych przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
4. Administrator stosuje system Firewall do ochrony dostępu do sieci komputerowej.

5. Administrator stosuje mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do Przetwarzania Danych osobowych w przypadku braku aktywności Osoby upoważnionej.
6. Administrator stosuje środki ochrony sieci lokalnej przed działaniami inicjowanymi z zewnątrz przy użyciu sieci firewall,
7. Administrator stosuje wykonywanie kopii zapasowych Danych osobowych na przeznaczonych w tym celu przez Administratora nośnikach, takich jak dysk zewnętrzny,
8. Administrator stosuje wykorzystanie szyfrowania danych przy ich transmisji,
9. Administrator stosuje wygaszacze ekranów,
10. Administartor na bieżąco dokonuje aktualizacji wykorzystywanego oprogramowania,
11. Administartor korzysta z bezpiecznego łącza VPN,
12. zamykanie aktywnych sesji po zakończeniu pracy,
13. wyrejestrowywanie się z aplikacji lub usług sieciowych, kiedy nie są już więcej potrzebne,
14. stosowanie mechanizmów kontroli dostępu do danych przetwarzanych w systemie informatycznym,
15. w przypadku, kiedy dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, zapewnienie, aby:
    -w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator,
    -dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia,
16. zapewnienie, aby identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie mógł być przydzielony innej osobie,
17. system informatyczny służący do przetwarzania danych osobowych zabezpieczony jest, co najmniej przed:
    -działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
    -utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej,
18. urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające Dane osobowe, przeznaczone do:
    - likwidacji — muszą zostać pozbawione wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
    - naprawy — muszą zostać, jeśli jest to możliwe lub zasadne z punktu widzenia naprawy pozbawione wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez Administratora lub Podmiotu przetwarzającego, z którym Administrator zawarł umowę zgodnie z at. 28 RODO,
19. ochrona przed zagrożeniami pochodzącymi z sieci publicznej poprzez co najmniej stosowanie oprogramowania antywirusowego.

Więcej informacji odnośnie środków bezpieczeństwa dla danych osobowych przetwarzanych w Systemie informatycznym Administratora znajduje się w Polityce Zarządzania Systemem Informatycznym, stanowiącej załącznik do niniejszej Polityki.

V. Środki personalne ochrony Danych osobowych

1. Administrator odpowiada za nadawanie/anulowanie upoważnień do Przetwarzania Danych osobowych w zbiorach papierowych czy też w systemach informatycznych.
2. Każda Osoba upoważniona może Przetwarzać Dane osobowe wyłącznie na polecenie Administratora lub na podstawie przepisów obowiązującego prawa.

3. Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli, audytów, wykonania czynności służbowych, udokumentowanego polecenia Administratora w postaci umowy powierzenia.
4. Wszystkie Osoby upoważnione zobowiązane są do Przetwarzania Danych zgodnie z nadanym im upoważnieniem, z obowiązującymi przepisami prawa i zgodnie z ustaloną przez Administratora Polityką, a także innymi dokumentami wewnętrznymi i procedurami związanymi z Przetwarzaniem Danych dostępnych u Administratora.
5. Do obowiązków Administratora Danych w zakresie zatrudniania, zakończenia lub zmiany warunków współpracy pracowników lub współpracowników (osób wykonujących usługi na podstawie innego stosunku prawnego niż umowa o pracę, przy pomocy których Administrator wykonuje swoje czynności) należy dopilnowanie, by osoby te:
    a) były odpowiednio przygotowane do wykonywania swoich obowiązków,
    b) Osoby te były odpowiednio i cyklicznie przeszkolone z zakresu ochrony danych osobowych, w tym wymogów zawartych w RODO, przy czym pierwsze szkolenie powinno odbyć się przed rozpoczęciem przetwarzania danych osobowych u Administratora przez daną osobę,
    c) Osoby te były pisemnie upoważnione do przetwarzania zgodnie ze wzorem upoważnienia stanowiącym załącznik do Polityki (lub równoważnym),
    d) Osoby te zobowiązały się do zachowania Danych osobowych w tajemnicy i do przestrzegania odpowiednich polityk ochrony danych i procedur związanych z przetwarzaniem danych. Wzór odpowiedniego oświadczenia stanowi załącznik do Polityki.
6. Osoby upoważnione zobowiązane są do:
    a) ścisłego przestrzegania zakresu nadanego upoważnienia,
    b) Przetwarzania i ochrony Danych zgodnie z przepisami prawa i regulacjami wewnętrznymi Administratora,
    c) zachowania w tajemnicy Danych oraz sposobów ich zabezpieczenia,
    d) zgłaszania incydentów związanych z naruszeniem bezpieczeństwa Danych oraz niewłaściwym funkcjonowaniem systemów zabezpieczających.
7. Uwzględniając konieczność wykonywania czynności w miejscu, w którym znajdują się nośniki zawierające Dane przez osoby z tzw. „personelu technicznego" (w tym np. osoby z serwisu sprzątającego) niemające upoważnienia do Przetwarzania Danych, Osoby upoważnione obowiązane są w należyty sposób zabezpieczać prowadzoną dokumentację zawierającą Dane, tak w formie papierowej, jak i elektronicznej, aby osoby nieupoważnione nie miały dostępu do treści Danych.
8. Administrator niezwłocznie odwoła udzielone upoważnienie do Przetwarzania Danych, w przypadku zakończenia obowiązywania umowy o pracę lub zakończenia obowiązywania innego stosunku prawnego będącego podstawą do nadania upoważnienia do Przetwarzania Danych, o ile upoważnienie nie zostało udzielone na czas obowiązywania danej umowy.
9. Administrator poza sytuacją wskazaną w ustępie powyżej, w każdym czasie może odwołać udzielone upoważnienie, jeżeli Przetwarzanie Danych przestało być konieczne do realizacji czynności przez Osobę upoważnioną na podstawie zawartych umów z Administratorem lub w przypadku, gdy Osoba upoważniona Przetwarza Dane niezgodnie z nadanym jej upoważnieniem.
10. Administrator będzie prowadził rejestr Osób upoważnionych do Przetwarzania Danych, zawierający m. in. datę nadania i odwołania udzielonego przez Administratora upoważnienia.
11. Administrator powołał Inspektora Ochrony Danych Osobowych
12. Administrator przy nadawaniu upoważnień kieruje się zasadą minimalizmu i adekwatności.

13. W przypadku stwierdzenia okoliczności naruszenia zasad ochrony danych osobowych użytkownik zobowiązany jest do podjęcia wszystkich niezbędnych kroków, mających na celu ograniczenie skutków naruszenia i do niezwłocznego powiadomienia IOD lub Administratora.

XV. OBSZAR PRZETWARZANIA I POLITYKA ZASOBÓW KLUCZOWYCH

1. Obszar, w którym Przetwarzane są Dane stanowi lokal Administratora Danych i obejmuje pomieszczenia biurowe oraz inne pomieszczenia mieszczące się pod adresem wskazanym w rejestrze przedsiębiorców jako adres przedsiębiorstwa Administratora.
2. Dodatkowo obszar, w którym przetwarzane są Dane osobowe, stanowią wszystkie komputery, zarówno stacjonarne, jak i przenośne oraz inne nośniki danych znajdujące w obszarze wskazanym w ust. 1 powyżej.
3. Przebywanie w pomieszczeniach biura spółki Administratora, jest dozwolone w godzinach pracy, przez osoby upoważnione do przetwarzania danych osobowych, przetwarzanych w tych pomieszczeniach.
4. Zabrania się przebywania w pomieszczeniach Administratora poza godzinami pracy, chyba , że Administrator wyrazi na to zgodę.
5. Przebywanie osób nieupoważnionych do przetwarzania danych osobowych, wewnątrz pomieszczeń, jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych lub za zgodą Administratora.
6. Polityka kluczy obejmuje dostępy do budynków i lokali biurowych, w których znajdują się pomieszczenia spółki Administratora.
7. Dostęp do kluczy do budynków i pomieszczeń, w których przetwarzane są dane osobowe, mają wyłącznie osoby upoważnione.
8. Upoważnienia do pobierania kluczy do pomieszczeń mają wyłącznie osoby upoważnione przez zarząd Administratora.
9. Klucze do pomieszczeń pozostają pod osobistym nadzorem osób upoważnionych.
10. Klucze do pomieszczeń wydawane są przez Prezesa Zarządu Administratora i zdawane są na ręce Prezesa Zarządu Administratora równocześnie z odpowiednim wpisem do Ewidencji pobrań kluczy (załącznik do Polityki).
11. Dostęp osób trzecich do lokalów biura Administratora, w których przetwarzane są dane osobowe odbywa się pod ścisłym nadzorem osób upoważnionych.
12. Klucze zapasowe przechowywane są wyłącznie przez Administratora, w innej lokalizacji niż podstawowy zestaw kluczy.
13. Wydawanie kluczy zapasowych upoważnionym pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz przypadkach awaryjnych za zgodą zarządu Administratora. Klucze zapasowe po ich użyciu należy niezwłocznie zwrócić do depozytu kluczy. Każde wydanie kluczy zapasowych odnotowywane jest w Ewidencji pobrań kluczy.
14. Klucze służące do zabezpieczenia biurek i szaf muszą być jednoznacznie opisane.
15. W godzinach pracy klucze do zabezpieczenia biurek i szaf pozostają pod nadzorem pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie przed osobami niepowołanymi.
16. Zabrania się pozostawiania kluczy w biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu oraz po zakończeniu pracy i opuszczeniu lokalu spółki Administratora.
17. Po zakończeniu pracy, klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w zabezpieczonym miejscu.
18. Po zakończeniu pracy, pracownicy są zobowiązani do zabezpieczenia miejsc przechowywania dokumentów z

danymi osobowymi przed dostępem osób trzecich (pomieszczenia, szafy, biurka, szuflady) a także przed zniszczeniem i kradzieżą. W szczególności zobowiązani są do wyłączenia i zabezpieczenia urządzeń elektronicznych oraz elektrycznych, wyłączenia oświetlenia, zabezpieczenia i zamknięcia okien i drzwi.

19. Poza godzinami pracy, klucze do szaf, w których przechowywane są dokumenty zawierające dane osobowe przechowuje się w kasetach lub skrzynkach zamykanych na szyfr.
20. Naruszenie zasad polityki kluczy może spowodować wyciągnięcie konsekwencji wynikających z art. 52 kodeksu pracy oraz z art. 363 § 1. kodeksu cywilnego.

XVI. NARUSZENIA BEZPIECZEŃSTWA

1. W przypadku stwierdzenia naruszenia ochrony Danych Administrator uruchamia procedurę postępowania na wypadek wystąpienia naruszenia ochrony danych, w tym niezwłocznie dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych zgodnie z Procedurą postępowania na wypadek wystąpienia naruszenia ochrony danych – stanowiącą załącznik do niniejszej Polityki.
2. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator zgłasza fakt naruszenia zasad ochrony danych organowi nadzorczemu bez zbędnej zwłoki – jeżeli to wykonalne, nie później niż w terminie 72 godzin od chwili stwierdzenia naruszenia. Wzór formularza Zgłoszenia naruszenia ochrony danych osobowych do UODO określa załącznik do niniejszej Polityki.
3. W przypadku, gdy ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia o incydencie także osobę, której dane dotyczą.
4. Za naruszenie lub próbę naruszenia zasad Przetwarzania i ochrony Danych osobowych uważa się przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych, w szczególności:
    a) naruszenie bezpieczeństwa systemów informatycznych, w których Przetwarzane są Dane osobowe, w razie ich Przetwarzania w takich systemach,
    b) udostępnianie lub umożliwienie udostępniania Danych osobowych osobom lub podmiotom do tego nieupoważnionym,
    c) zaniechaniedopełnienia obowiązku zapewnienia Danym osobowym ochrony,
    d) niedopełnienie obowiązku zachowania w tajemnicy Danych osobowych
    e) przetwarzanie Danych osobowych niezgodnie z założonym zakresem i celem ich zbierania,
    f) spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie Danych osobowych,
    g) naruszenie praw osób, których Dane osobowe są Przetwarzane.
5. Osoba upoważniona zobowiązana jest do podjęcia wszystkich niezbędnych kroków, mających na celu ograniczenie skutków naruszenia ochrony Danych osobowych i do niezwłocznego powiadomienia o tym IOD oraz Administratora.
6. Szczegółowe procedury działania oraz etapy postępowania na wypadek wystąpienia incydentu lub naruszenia bezpieczeństwa danych określa Procedura postępowania na wypadek wystąpienia naruszenia ochrony danych – stanowiącą załącznik do niniejszej Polityki.

XVII. PROCEDURA RETENCJI DANYCH

1. Administrator przechowuje dane osobowe w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, dla których dane te pozyskał – zgodnie z art. 5 pkt 1 e RODO – z uwzględnieniem zasady adekwatności, stosowności oraz minimalizmu w kontekście tychże celów.
2. Niszczenie dokumentów zawierających dane osobowe powinno być dokonywane w sposób uniemożliwiający identyfikację osoby, której dane dotyczą.
3. Administrator usuwa dane osobowe, gdy przepisy szczególne regulują obowiązek przetwarzania danych osobowych przez ustalony okres, np. przepisy prawa pracy, prawa podatkowego, ustawa o rachunkowości, kodeks cywilny – po upływie tegoż wskazanego w ustawie okresu.
4. Administrator usuwa dane osobowe, także gdy ustawodawca krajowy lub unijny nie reguluje okresu przechowywania danych osobowych – kierując się zasadą ograniczenia celu, zgodnie z art. 5 pkt 1 b RODO.
5. Administrator ustalając okres przechowywania danych osobowych bierze pod uwagę wartość informacji, koszty związane z zabezpieczeniem danych i ich przetwarzaniem, ryzyko i zobowiązania dotyczące przetwarzania danych osobowych.
6. IODO (lub Administrator w przypadku braku jego wyznaczenia), regularnie sprawdza czy dane są niezbędne do realizacji określonych celów, a jeżeli przestały być niezbędne informuje Administratora o konieczności ich usunięcia (lub usuwa dane w przypadku braku IODO).
7. W celu wsparcia procesu monitoringu okresów retencji u Administratora, może on prowadzić zestawienie okresów retencji.
8. Usuwanie danych osobowych w formie papierowej odbywa się według następujących zasad:
   a) Personel Administratora upoważniony do przetwarzania danych osobowych, zobowiązany jest do niszczenia dokumentów i tymczasowych wydruków w niszczarkach, niezwłocznie po ustaniu celu ich przetwarzania.
   b) Dokumenty powinny być niszczone tak, aby po ich zniszczeniu nie sposób było odczytać zawartych w nich informacji, a w szczególności w sposób uniemożliwiający identyfikację osoby, której dane dotyczą.
   c) Dane osobowe powinny być niszczone przez urządzenia spełniające wymagania co najmniej na poziomie P-3, co oznacza, że fragmenty pozostałe po zniszczeniu nie mogą być większe niż 320 mm2.
9. Usuwanie danych osobowych w formie elektronicznej odbywa się według następujących zasad:
   a) Systemy informatyczne Administratora powinny pozwalać na ustalanie okresów przechowywania danych osobowych.
   b) Systemy informatyczne Administratora powinny umożliwić sprawne usuwanie przez Administratora całości lub części danych.
   c) Systemy informatyczne Administratora powinny uniemożliwiać usuwanie danych przez osoby nieuprawnione do usuwania danych osobowych.
   d) Urządzenia służące do przetwarzania danych osobowych, przed usunięciem danych osobowych pozbawia się nośników informacji.
   e) Nośniki informacji służące do przetwarzania danych osobowych pozbawia się tych danych przed usunięciem, a następnie poddaje się je procedurze przynajmniej trzykrotnego całkowitego nadpisywania.
   f) W przypadku braku możliwości wykonania procedury opisanej w pkt. 5 powyżej (np. w przypadku płyt CD, uszkodzonych dysków) nośniki informacji służące do przetwarzania danych osobowych przed usunięciem poddaje się innym czynnościom skutkującym ich trwałemu fizycznemu uszkodzeniu, uniemożliwiającemu odczytanie danych zgromadzonych na nośniku.

XVIII. POSTANOWIENIA KOŃCOWE

1. Polityka jest wewnętrzną regulacją Administratora i jest objęta tajemnicą przedsiębiorstwa. Każda Osoba upoważniona jest zobowiązana do zachowania treści Polityki w poufności i nieudostępniania jej osobom nieupoważnionym bez wyraźnego polecenia Administratora.
2. Za niedopełnienie obowiązków wynikających z niniejszego dokumentu pracownik ponosi odpowiedzialność na podstawie obowiązujących przepisów prawa, m. in. Kodeksu pracy oraz Kodeksu karnego w odniesieniu do Danych osobowych.
3. Za niedopełnienie obowiązków wynikających z niniejszego dokumentu osoby wykonujące usługi na podstawie innego stosunku prawnego, przy pomocy których Administrator wykonuje swoje czynności, ponoszą odpowiedzialność na podstawie obowiązujących przepisów prawa, m. in. Kodeksu cywilnego oraz Kodeksu karnego w odniesieniu do Danych osobowych.
4. Administrator wskazuje, że w przypadku, gdyby analiza działalności gospodarczej Administratora wymagała zmiany w zakresie bezpieczeństwa Przetwarzanych Danych osobowych lub zmianie uległy okoliczności wpływające na określenie zasad bezpieczeństwa dotyczących Danych osobowych, dokona aktualizacji i dostosowania Polityki, uwzględniając ww. okoliczności. O zmianie Polityki, Administrator powiadomi Osobę upoważnioną na co najmniej 7 dni przed wejściem w życie jej zaktualizowanej treści.
5. Osoba upoważniona zobowiązana jest do zapoznania się z zaktualizowaną treścią Polityki oraz do stosowania się do jej zapisów.
6. Polityka wchodzi w życie z dniem 10.06.2022 r.
7. Data aktualizacji Polityki – 31.01.2026.
8. Integralną część niniejszej Polityki stanowią następujące załączniki:
   a) *Raport z Analizy ryzyka*
   b) *Polityka Zarządzania Systemem Informatycznym*
   c) Wzór *Umowy powierzenia przetwarzania danych osobowych*
   d) Wzór *Rejestru Czynności Przetwarzania Danych*
   e) *Wzór Rejestru Kategorii Czynności Przetwarzania Danych*
   f) Wzór *Rejestru* naruszeń ochrony danych osobowych
   g) Wzór *Rejestru* żądań i realizacji praw osób, których dotyczą dane osobowe
   h) Wzór *Rejestru* upoważnień
   i) Wzór *Rejestru* umów powierzenia danych osobowych
   j) Wzór *Rejestru* zgód na przetwarzanie danych osobowych
   k) Wzór Rejestru klauzul informacyjnych
   l) *Polityka realizacji praw osób, których dane dotyczą*
   m) *Informacje o przetwarzaniu danych osobowych dla poszczególnych kategorii osób*
   n) *Procedura postępowania na wypadek wystąpienia naruszenia ochrony danych*
   o) Wzór formularza *Zgłoszenia naruszenia ochrony danych osobowych* do UODO
   p) Wzór *Powiadomienia o naruszeniu ochrony danych osobowych – zawiadomienie osoby, której dane dotyczą*
   q) Wzór *Upoważnienia do przetwarzania danych osobowych*
   r) Wzór *Oświadczenia* do upoważnienia do przetwarzania danych osobowych
   s) *Wzór Ewidencji pobrań kluczy*