POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH W EVEREST CONSULTING & SZKOLENIA MARCIN KOTTAS

REJESTR ZMIAN W DOKUMENCIE

Data [RRRR-MM-DD]	Autor	Wersja	Opis zmian
2024-09-30	Przemysław Paliwoda KANCELARIA KPRIU PALIWODA	2.0	Całościowa aktualizacja dotychczasowej wersji obowiązującej Polityki 1.0

AKCEPTACJA DOKUMENTU

Data [RRRR-MM-DD]	Osoba akceptująca	Zaakceptowana wersja
2024-09-30		2.0

- DOKUMENT WEWNĘTRZNY -

Spis treści

1. Wprowadzenie

Niniejszy dokument omawia sposób przygotowania i zakres dokumentacji opisującej politykę bezpieczeństwa danych osobowych w firmie Everest Consulting & Szkolenia Marcin Kottas (dalej jako „Administrator", „ADO", „Przedsiębiorstwo", „Firma") w zakresie odnoszącym się do sposobu przetwarzania Danych Osobowych oraz środków ich ochrony spełniających wymogi Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

2. Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1).

2. Cel i zakres dokumentu

1. Celem Polityki Bezpieczeństwa Danych Osobowych jest zapewnienie bezpieczeństwa danych osobowych przetwarzanych w firmie Everest Consulting & Szkolenia Marcin Kottas poprzez wskazanie odpowiednich rozwiązań technicznych i organizacyjnych oraz określenie obowiązków i odpowiedzialności osób zobowiązanych do realizacji procedur wewnętrznych, w tym Instrukcji Zarządzania Systemami Informatycznymi, służącym do przetwarzania Danych Osobowych, przy jednoczesnym spełnieniu wszelkich wymogów obowiązującego prawa.
2. W dokumencie tym zawarto najważniejsze zasady zgodnie z którymi realizowany jest proces ochrony informacji zawierających Dane osobowe przetwarzane w Przedsiębiorstwie.
3. Zasady określone w niniejszej Polityce mają zastosowanie do wszystkich Danych Osobowych zawartych w zbiorach danych, jak również poza nimi, przetwarzanych w systemach informatycznych oraz w sposób tradycyjny, których Przedsiębiorstwo jest Administratorem lub Podmiotem przetwarzającym w rozumieniu przepisów Rozporządzenia PEiR (UE) 2016/679.
4. Niniejsza Polityka zawiera również odwołania do załączników uszczegóławiających (wzorcowe procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych) stanowiących integralną część Polityki.

3. Powiązane akty prawne i dokumenty wewnętrzne

1. 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) (Dz. Urz. UE L 119 z 04.05.2016).
2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781 ze zm.).

4. Definicje i Skróty

Administrator Danych Osobowych lub **ADO** – Everest Consulting & Szkolenia Marcin Kottas, NIP 6342347106, ul. Górnośląska 15, 43-200 Pszczyna, która samodzielnie lub wspólnie z innymi administratorami ustala cele i sposoby przetwarzania Danych osobowych.

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.

Dostępność informacji – zapewnienie, że osoby mają dostęp do informacji i związanych z nią aktywów wtedy, gdy istnieje taka potrzeba (w odpowiednim zakresie, miejscu i czasie).

Elektroniczny nośnik informacji – materiał lub urządzenie umożliwiające zapisywanie, przechowywanie, przenoszenie i/lub odczytywanie danych w postaci cyfrowej lub analogowej. Przykładami elektronicznych nośników informacji mogą być dyski twarde, pamięci elektroniczne typu flash, dyski CD/DVD/BD, dyski magnetyczne, magnetooptyczne i optyczne, urządzenia przenośne z pamięcią elektroniczną (m.in. telefony komórkowe, urządzenia typu handheld, aparaty cyfrowe, notesy elektroniczne, odtwarzacze multimedialne), itp.

Informacje chronione – informacje sklasyfikowane jako chronione, zgodnie z wymogami obowiązujących aktów prawnych oraz z wewnętrznymi procedurami Przedsiębiorstwa.

Integralność informacji – właściwość zapewniająca dokładność i kompletność informacji oraz metod jej przetwarzania.

Incydent bezpieczeństwa – zdarzenie lub seria zdarzeń, które bezpośrednio zagraża bezpieczeństwu informacji ze względu na poufność, dostępność i integralność informacji.

Naruszenie ochrony Danych osobowych – incydent bezpieczeństwa prowadzący do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do Danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

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 powszechnie obowiązującym prawem, nie są uznawane za odbiorców.

Ograniczenie przetwarzania – oznaczenie przechowywanych Danych osobowych w celu ograniczenia ich przyszłego przetwarzania.

Osoba upoważniona – osoba upoważniona przez Przedsiębiorcę do przetwarzania Danych osobowych, za pomocą pisemnego upoważnienia.

Podmiot przetwarzający lub **Procesor** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza Dane osobowe w imieniu Administratora Danych Osobowych.

Poufność – zapewnienie o nieudostępnianiu i nieujawnianiu danych nieautoryzowanym osobom, podmiotom lub procesom.

Polityka – niniejsza Polityka Bezpieczeństwa Danych Osobowych Przedsiębiorstwa.

Prezes UODO – Prezes Urzędu Ochrony Danych Osobowych.

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.

Przetwarzanie – operacja lub zestaw operacji wykonywanych na Danych osobowych lub zestawach Danych osobowych, w sposób zautomatyzowany lub niezautomatyzowany, takie jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie, udostępnianie, dopasowywanie, łączenie, ograniczanie, usuwanie lub niszczenie.

Pseudonimizacja – przetworzenie Danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

Rozliczalność – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

Rozporządzenie lub **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).

Ryzyko – prawdopodobieństwo wykorzystania przez określone zagrożenie podatności aktywów, czego skutkiem mogą być określone straty. Ryzyko można opisać jako prawdopodobieństwo wystąpienia niepożądanego incydentu oraz związanych z nim następstw.

Strona trzecia – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które mogą przetwarzać dane osobowe z upoważnienia administratora lub podmiotu przetwarzającego.

System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych, systemy e-mail, gdzie dochodzi do przetwarzania Danych osobowych.

Tradycyjny nośnik informacji – przedmiot fizyczny niezwiązany z informatyką i komputerami, na którym możliwe jest zapisanie informacji oraz z którego możliwe jest późniejsze odczytanie tej informacji. Przykładami tradycyjnych nośników mogą być wydruki papierowe, folia, taśmy itp.

u.o.d.o. – Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.

Usuwanie danych – nieodwracalne zniszczenie Danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.

Użytkownik Systemu Informatycznego lub **USI** – osoba upoważniona do dostępu do zasobów Systemu informatycznego posiadająca upoważnienie do przetwarzania Danych osobowych w tym systemie. Użytkownikami są zarówno współpracownicy cywilnoprawni oraz pracownicy firmy.

Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

Zagrożenie – potencjalna przyczyna niepożądanego incydentu/naruszenia, którego skutkiem może być szkoda dla systemu bądź aplikacji przetwarzającej Dane osobowe. Każda sytuacja, która powoduje niedostępność danych (czasowa lub trwała), uniemożliwienie przetwarzania danych, niekontrolowany wypływ, ujawnienie, utratę lub przekłamanie – jest zagrożeniem dla przetwarzanych danych, niezależnie od tego czy stanowiła celowy sabotaż, czy przypadkowe działanie.

Zbiór Danych osobowych – uporządkowany zestaw Danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

Zgoda (osoby, której dane dotyczą) – 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.

5. Postanowienia ogólne

1. Za opracowanie i zatwierdzenie niniejszego dokumentu odpowiedzialny jest właściciel firmy – Kottas Marcin (dalej również jako „Przedsiębiorca", „Właściciel").

2. Za stosowanie zasad i procedur wynikających z niniejszego dokumentu odpowiedzialni są wszyscy Pracownicy i Współpracownicy Firmy mający dostęp do Danych osobowych.

6. Zasady przetwarzania Danych osobowych

Filary ochrony danych w Firmie EVEREST CONSULTING & SZKOLENIA MARCIN KOTTAS

(1)**Legalność** – Firma dba o ochronę prywatności i przetwarza dane zgodnie z prawem.

(2) **Bezpieczeństwo** – Firma zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.

(3) **Prawa Jednostki** – Firma umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.

(4) **Rozliczalność** – Firma dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

1. Przedsiębiorstwo przechowuje i przetwarza Dane osobowe zgodnie z obowiązującymi przepisami prawa, z poszanowaniem następujących zasad:
    a. w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
    b. rzetelnie i uczciwie (rzetelność);
    c. w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
    d. w konkretnych celach i nie „na zapas" (minimalizacja);
    e. nie więcej niż potrzeba (adekwatność);
    f. z dbałością o prawidłowość danych (prawidłowość);
    g. nie dłużej niż potrzeba (czasowość);
    h. zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).
2. Przetwarzanie odbywa się na podstawie art. 6 ust. 1 Rozporządzenia oraz w przypadku szczególnych kategorii danych na podstawie art. 9 ust. 2 Rozporządzenia.
3. W stosunku do osób, których Dane osobowe są zbierane przez Firmę realizowany jest obowiązek informacyjny wynikający z przepisów Rozporządzenia, z wyjątkiem sytuacji określonych w art. 13 ust. 4 Rozporządzenia oraz art. 14 ust. 5 Rozporządzenia.
4. Firma umożliwia i ułatwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te terminowo realizuje.
5. Przetwarzanie Danych osobowych realizowane jest wyłącznie w ramach oznaczonych, adekwatnych i zgodnych z prawem celów i Dane osobowe nie są poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami.

6.1. Upoważnienia do przetwarzania Danych osobowych, Oświadczenia o zachowaniu poufności

1. Do przetwarzania Danych osobowych zgromadzonych w zbiorach i ewidencjach Przedsiębiorstwa mogą być dopuszczone wyłącznie **osoby posiadające pisemne upoważnienie.**

2. Upoważnienia nadawane są wszystkim pracownikom oraz współpracownikom realizującym zadania na podstawie umów cywilnoprawnych (B2B, umowa zlecenie, umowa o dzieło), którzy w ramach realizacji swoich zadań będą przetwarzać Dane osobowe.
3. Przedsiębiorca może odmówić nadania upoważnienia do przetwarzania danych osobowych w przypadku, gdy osoba, w stosunku do której złożono wniosek o nadanie upoważnienia, nie gwarantuje ochrony danych osobowych, w szczególności w zakresie nieuprawnionego ich udostępnienia osobom nieupoważnionym, przetwarzania z naruszeniem przepisów prawa oraz utratą, uszkodzeniem lub nieuprawnionym zniszczeniem tych danych.
4. Wzór upoważnienia do przetwarzania danych osobowych stanowi **Załącznik nr 4 do Polityki.**
5. Zmiana zajmowanego stanowiska służbowego lub komórki organizacyjnej wymaga zmiany upoważnienia, jeżeli wpływa na zakres przetwarzanych przez współpracownika lub pracownika Danych osobowych.
6. Upoważnienie obowiązuje od daty wystawienia do dnia nadania nowego upoważnienia, cofnięcia upoważnienia lub wygaśnięcia.
7. Upoważnienie wygasa automatycznie z chwilą rozwiązania umowy o pracę lub rozwiązania stosunku cywilnoprawnego, łączącego upoważnionego z Przedsiębiorstwem.
8. Cofnięcie upoważnienia następuje:
   a. w przypadku stwierdzenia nieuprawnionego udostępnienia Danych osobowych osobom nieupoważnionym, dopuszczenia do ich zabrania przez osobę nieuprawnioną, przetwarzania z naruszeniem obowiązujących przepisów prawa oraz w przypadku zmiany, utraty, uszkodzeniu lub zniszczeniu Danych osobowych z winy osoby posiadającej upoważnienie;
   b. po zakończeniu pracy lub zakończenia stosunku cywilnoprawnego (ustaniu czynności) na stanowisku związanym z przetwarzaniem i dostępem do Danych osobowych (osoba dalej jest pracownikiem lub współpracownikiem ADO, ale nie przetwarza już Danych osobowych).
9. Cofnięcie upoważnienia może nastąpić na wniosek bezpośredniego przełożonego Osoby upoważnionej lub z inicjatywy Przedsiębiorcy.
10. Przedsiębiorstwo prowadzi Ewidencję Osób upoważnionych do przetwarzania Danych osobowych, której wzór stanowi **Załącznik nr 5 do Polityki**.
11. **Przed przystąpieniem do przetwarzania Danych osobowych, Osoba upoważniona przechodzi szkolenie** z zakresu przepisów prawa związanych z ochroną Danych osobowych (Rozporządzenie i u.o.d.o.) oraz zasad przetwarzania obowiązujących w Przedsiębiorstwie.
12. **Po odbyciu szkolenia, Osoba upoważniona podpisuje Oświadczenie o zapoznaniu się z obowiązującymi przepisami prawa oraz aktami wewnętrznymi Przedsiębiorstwa w zakresie ochrony Danych osobowych oraz zachowaniu Danych osobowych i sposobu ich zabezpieczenia w tajemnicy.**
13. Obowiązek zachowania tajemnicy jest nieograniczony czasowo, nie podlega wypowiedzeniu, obowiązuje także po ustaniu zatrudnienia lub innego stosunku łączącego daną osobę z Firmą.
14. Każda osoba przetwarzająca Dane osobowe ma obowiązek przetwarzania ich w granicach udzielonego jej upoważnienia.
15. Każda osoba przetwarzająca Dane osobowe jest zobowiązana do zachowania ich w tajemnicy oraz zapewnienia ich Poufności, Integralności i Rozliczalności.
16. Zakres upoważnienia może również być określony w umowie o pracę lub współpracę.
17. Osoba upoważniona zobowiązana jest podpisać oświadczenie lub umowę, która określa odpowiedzialność w zakresie ochrony danych osobowych.

6.2. Powierzenie przetwarzania Danych osobowych

1. Rozporządzenie (art. 28) oraz niniejsza Polityka przewidują możliwość powierzenia przetwarzania Danych osobowych zewnętrznym podmiotom (Podmiotom przetwarzającym).
2. **Powierzenie przetwarzania Danych osobowych Podmiotowi przetwarzającemu następuje w formie pisemnej umowy powierzenia lub innego instrumentu prawnego, które podlega prawu Unii lub prawu polskiemu (dalej jako „Umowa powierzenia").**
3. Przed podpisaniem umowy powierzenia Podmiot przetwarzający musi zagwarantować, że wdrożył odpowiednie środki techniczne i organizacyjne celem spełnienia wymogów Rozporządzenia i innych obowiązujących przepisów prawa dotyczących ochrony Danych osobowych.
4. Umowa powierzenia Danych osobowych musi określać:
   a. przedmiot i czas trwania przetwarzania,
   b. charakter i cel przetwarzania,
   c. rodzaj Danych osobowych oraz kategorie osób, których dane dotyczą,
   d. obowiązki i prawa ADO,
   e. obowiązki Podmiotu przetwarzającego.
5. Pracownik lub współpracownik informuje o potrzebach realizacji procesu na zewnątrz organizacji.
6. Przedsiębiorca na podstawie zebranych informacji, czy podmiot zewnętrzny do realizacji zleconego procesu musi przetwarzać dane osobowe, określa maksymalny zakres danych osobowych podlegających powierzeniu.
7. Przedsiębiorca przygotowuje Umowę powierzenia przetwarzania Danych osobowych zgodną ze wzorem stanowiącym **Załącznik nr 3 do Polityki**. Dopuszcza się stosowanie innego wzoru umowy powierzenia przetwarzania Danych osobowych z zastrzeżeniem, iż będzie ona zawierała wszystkie elementy wskazane w przedstawionym w załączniku wzorze. **Przy weryfikacji podmiotu oraz wzoru umowy Przedsiębiorca kieruje się wymogami wynikającymi z przepisów RODO.**
8. Podmiot, któremu powierzono przetwarzanie Danych osobowych, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie powierzenia.
9. **Przedsiębiorstwo prowadzi Ewidencję zawartych umów powierzenia przetwarzania** Danych osobowych zgodnie ze wzorem stanowiącym **Załącznik nr 3a do Polityki.**
10. Zawarcie umowy powierzenia przetwarzania Danych osobowych konieczne jest również w sytuacji, gdy to Przedsiębiorstwu zostają powierzone do przetwarzania Dane osobowe przez podmiot trzeci – Przedsiębiorstwo występuje w roli Podmiotu przetwarzającego.
11. Działając jako podmiot przetwarzający Przedsiębiorstwo prowadzi rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu innego administratora, zawierający następujące informacje: a) nazwę i dane kontaktowe administratora, w imieniu którego działa podmiot przetwarzający; b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów; c) inny podmiot przetwarzający (podwykonawca, jeżeli dotyczy).

6.3. Obowiązek informacyjny

1. Przedsiębiorstwo może pozyskać dane osobowe bezpośrednio od osoby, której dane dotyczą jak i z innych źródeł w tym źródeł publicznie dostępnych.

2. **Przedsiębiorstwo realizuje obowiązek informacyjny względem osób, których dane dotyczą, a które ma zamiar przetwarzać, zamieszczając klauzule informacyjne (spełniające wymagania art. 13 ust. 1 i ust. 2 Rozporządzenia) w miejscach, w których zbierane są Dane osobowe.**
3. W przypadku pozyskania danych osobowych nie bezpośrednio od osoby, której dane dotyczą Przedsiębiorstwo informuje osobę, której dane pozyskała przedstawiając jej odpowiednią klauzulę informacyjną (spełniającą wymagania art. 14 ust. 1 i 2 Rozporządzenia) w rozsądnym terminie po pozyskaniu Danych osobowych – **najpóźniej w ciągu miesiąca**.
4. Jeżeli Dane osobowe pozyskane niebezpośrednio od osoby, której dotyczą mają być przetwarzane w celu komunikacji z tą osobą, odpowiednia klauzula informacyjna powinna być przedstawiona tej osobie najpóźniej **przy pierwszej komunikacji** z tą osobą.

6.4. Żądania osób

1. Przedsiębiorstwo realizuje prawa osób fizycznych, których dane dotyczą zgodnie z wymaganiami art. 15-22 Rozporządzenia.
2. Przed przystąpieniem do realizacji żądania Przedsiębiorstwo weryfikuje tożsamość osoby składającej żądanie. W tym celu Przedsiębiorstwo może zażądać od tej osoby dodatkowych informacji niezbędnych do potwierdzenia jej tożsamości.
3. Przedsiębiorstwo bez zbędnej zwłoki – najpóźniej w terminie miesiąca od otrzymania żądania – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem na podstawie art. 15–22 Rozporządzenia.
4. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania Przedsiębiorstwo informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia.
5. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.
6. **Przedsiębiorstwo prowadzi Rejestr wszystkich żądań i realizacji uprawnień osób, których dane dotyczą.**

6.4.1. Prawa osób trzecich

Realizując prawa osób, których dane dotyczą, Przedsiębiorstwo wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby, której dane dotyczą, 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), Przedsiębiorstwo może się zwrócić do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową realizacji żądania.

6.4.2. Nieprzetwarzanie

Przedsiębiorstwo informuje osobę, której dane dotyczą, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw a Przedsiębiorstwo nie przetwarza żadnych danych osobowych żądającego.

6.4.3. Odmowa

Przedsiębiorstwo w uzasadnionych przypadkach w ciągu miesiąca od otrzymania żądania, informuje osobę, której dane dotyczą, o odmowie jego rozpatrzenia i o prawach z tym związanych.

6.4.4. Dostęp do danych i wydanie kopii danych

1. Na żądanie osoby, której dane dotyczą, związane z dostępem do jej danych, Przedsiębiorstwo informuje daną osobę czy przetwarza jej dane oraz przekazuje szczegóły przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela dostępu do danych.
2. Dostęp do danych może być zrealizowany przez wydanie kopii danych.
3. Przedsiębiorstwo może odmówić udzielenia informacji wymienionych w pkt 1 osobie, której dane dotyczą, gdy udostępnienie informacji spowodowałoby:
   a. ujawnienie wiadomości zawierających informacje niejawne;
   b. zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego;
   c. zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa;
   d. istotne naruszenie dóbr osobistych osób, których dane dotyczą lub innych osób.
4. Przedsiębiorstwo może również odmówić podjęcia działań, jeżeli wniosek o udzielenie informacji jest nieuzasadniony lub nadmierny (zbyt częsty).
5. O decyzji dotyczącej niepodjęcia działań Przedsiębiorstwo musi poinformować wnioskodawcę niezwłocznie, nie później niż w terminie miesiąca od otrzymania żądania. Przedsiębiorstwo podaje w decyzji przyczyny niepodjęcia działań oraz informuje o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

6.4.5. Sprostowanie danych

1. Przedsiębiorstwo dokonuje sprostowania nieprawidłowych danych na żądanie osoby, której dane dotyczą.
2. Przedsiębiorstwo ma prawo odmówić sprostowania danych, chyba że osoba, której dane dotyczą, w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga.
3. W przypadku sprostowania danych, Przedsiębiorstwo informuje osobę, której dane dotyczą, o odbiorcach danych, na żądanie tej osoby.

6.4.6. Uzupełnienie danych

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

6.4.7. Usunięcie danych

1. Na żądanie osoby, której dane dotyczą, Przedsiębiorstwo usuwa dane, gdy:

a. dane nie są niezbędne do celów, w których zostały zebrane, ani przetwarzane w innych zgodnych z prawem celach,
b. zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,
c. osoba ta wniosła skuteczny sprzeciw względem przetwarzania tych danych,
d. dane były przetwarzane niezgodnie z prawem,
e. konieczność usunięcia wynika z obowiązku prawnego,
f. żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. profil dziecka na portalu społecznościowym, udział w konkursie na stronie internetowej).

2. Przedsiębiorstwo określa sposób obsługi prawa do usunięcia danych, 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.
3. Jeżeli dane podlegające usunięciu zostały upublicznione Przedsiębiorstwo podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe o potrzebie usunięcia danych i dostępu do nich.
4. W przypadku usunięcia danych, Przedsiębiorstwo informuje osobę, której dane dotyczą, o odbiorcach danych, na żądanie tej osoby.

6.4.8. Ograniczenie przetwarzania

1. Przedsiębiorstwo dokonuje ograniczenia przetwarzania danych na żądanie osoby, której dane dotyczą, gdy:
   a. osoba ta kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,
   b. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
   c. nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
   d. osoba ta wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.
2. W trakcie ograniczenia przetwarzania Przedsiębiorstwo 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.
3. Przedsiębiorstwo informuje osobę, której dane dotyczą, przed uchyleniem ograniczenia przetwarzania.
4. W przypadku ograniczenia przetwarzania danych Przedsiębiorstwo informuje osobę, której dane dotyczą, o odbiorcach danych, na żądanie tej osoby.

6.4.9. Przenoszenie danych

Na żądanie osoby, której dane dotyczą, Przedsiębiorstwo 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

Przedsiębiorstwu, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej w ramach systemów informatycznych.

6.4.10. Sprzeciw w szczególnej sytuacji

Jeżeli osoba, której dane dotyczą, zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są w oparciu o uzasadniony interes lub o powierzone w ramach zadania realizowanego w interesie publicznym, Przedsiębiorstwo uwzględni sprzeciw, o ile nie zachodzą ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

6.4.11. Sprzeciw względem marketingu bezpośredniego

Jeżeli osoba, której dane dotyczą, zgłosi sprzeciw względem przetwarzania jej danych na potrzeby marketingu bezpośredniego (w tym ewentualnie profilowania), Przedsiębiorstwo uwzględnia sprzeciw i zaprzestaje takiego przetwarzania.

6.4.12. Prawo do ludzkiej interwencji przy zautomatyzowanym podejmowaniu decyzji

W sytuacjach gdy Przedsiębiorstwo przetwarza dane w sposób automatyczny, w tym w oparciu o profilowanie i w konsekwencji podejmuje względem osób, których dane dotyczą, decyzje wywołujące skutki prawne lub inaczej istotnie wpływające na osobę, Przedsiębiorstwo zapewnia możliwość odwołania się do interwencji i decyzji człowieka, chyba że taka automatyczna decyzja:

a. jest niezbędna do zawarcia lub wykonania umowy z odwołującą się osobą,
b. jest wprost dozwolona przepisami prawa,
c. opiera się na wyraźnej zgodzie odwołującej osoby.

6.5. Uwzględnienie ochrony Danych osobowych w fazie projektowania oraz domyślna ochrona Danych osobowych

1. Przedsiębiorstwo zobowiązuje się do ochrony Danych osobowych na każdym etapie ich przetwarzania począwszy od etapu tworzenia nowych projektów związanych z przetwarzaniem Danych osobowych.
2. Każdy nowy projekt, którego częścią jest przetwarzanie Danych osobowych (np. zakup i stosowanie nowego systemu informatycznego, serwera, aplikacji; powierzenie administrowanych Danych osobowych nowemu Podmiotowi przetwarzającemu) musi gwarantować zastosowanie odpowiednich środków technicznych i organizacyjnych ochrony tych danych przed rozpoczęciem wejścia w życie projektu tzn. przed rozpoczęciem przetwarzania Danych osobowych.
3. Każdy nowy projekt, którego częścią jest przetwarzanie Danych osobowych w oparciu o prawnie uzasadniony interes (art. 6 ust. 1 lit. f Rozporządzenia) wymaga przeprowadzenia testu równowagi.
4. Podczas projektowania odpowiednich środków technicznych i organizacyjnych ochrony Danych osobowych Przedsiębiorstwo bierze pod uwagę:
   a. stan wiedzy technicznej,
   b. koszt wdrożenia określonych zabezpieczeń,
   c. charakter, zakres, kontekst i cele przetwarzania,

d. ryzyko naruszenia praw lub wolności osób fizycznych wynikające z przetwarzania ich danych osobowych.

6.6. Rejestr Czynności Przetwarzania Danych, Rejestr Kategorii Czynności Przetwarzania Danych

1. Przedsiębiorstwo prowadzi **Rejestr Czynności Przetwarzania Danych**, w ramach którego inwentaryzuje oraz monitoruje sposoby, w jakie wykorzystuje Dane osobowe, których jest Administratorem. Rejestr stanowi formę dokumentowania czynności przetwarzania danych, pełni 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. W Rejestrze, dla każdej czynności przetwarzania danych, którą Administrator uznała za odrębną dla potrzeb Rejestru, Administrator odnotowuje co najmniej: (i) nazwę czynności, (ii) cel przetwarzania, (iii) opis kategorii osób, (iv) opis kategorii danych, (v) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu, jeśli podstawą jest uzasadniony interes, (vi) sposób zbierania danych, (vii) opis kategorii odbiorców danych (w tym przetwarzających), (viii) informację o przekazaniu poza EU/EOG; (ix) ogólny opis technicznych i organizacyjnych środków ochrony danych.
2. Rejestr Czynności Przetwarzania Danych prowadzony jest w wersji elektronicznej przy wykorzystaniu wzoru stanowiącego **Załącznik nr 1 do Polityki.**
3. Przedsiębiorstwo prowadzi Rejestr Kategorii Czynności Przetwarzania Danych, których jest Podmiotem przetwarzającym.
4. Rejestr Kategorii Czynności Przetwarzania Danych prowadzony jest w wersji elektronicznej zgodnie ze wzorem stanowiącym **Załącznika nr 1a do Polityki.**

6.7. Retencja danych osobowych

1. Okres przetwarzania Danych osobowych zależy od celu i podstawy prawnej przetwarzania.
2. Okres przetwarzania danych może także wynikać z przepisów, gdy stanowią one podstawę przetwarzania.
3. W przypadku przetwarzania danych na podstawie prawnie uzasadnionego interesu ADO – np. ze względów bezpieczeństwa lub w celu marketingu bezpośredniego – dane przetwarzane są przez okres umożliwiający realizację tego interesu lub do momentu zgłoszenia skutecznego sprzeciwu względem przetwarzania danych.
4. Jeśli przetwarzanie Danych osobowych odbywa się na podstawie zgody, dane przetwarzane są do czasu jej wycofania.
5. Gdy podstawę przetwarzania stanowi niezbędność przetwarzania do zawarcia i wykonania umowy, dane są przetwarzane do momentu jej rozwiązania.
6. Okres przetwarzania danych może być przedłużony w przypadku, gdy przetwarzanie jest niezbędne do ustalenia lub dochodzenia roszczeń lub obrony przed roszczeniami, a po tym okresie – jedynie w przypadku i w zakresie, w jakim będą wymagać tego przepisy prawa.
7. Po upływie okresu przetwarzania dane są nieodwracalnie usuwane lub anonimizowane.
8. Okresy przechowywania danych osobowych zostały zawarte w Rejestrze Czynności Przetwarzania Danych.

6.8. Przekazywanie Danych osobowych do Państwa Trzeciego

Przedsiębiorstwo przy przekazywaniu Danych osobowych do Państw trzecich oraz organizacji międzynarodowych w rozumieniu Rozporządzenia kieruje się ściśle wytycznymi zawartymi w Rozdziale V Rozporządzenia.

7. Zarządzanie przetwarzaniem Danych Osobowych, odpowiedzialność

7.1. Administrator Danych Osobowych (ADO)

W rozumieniu przepisów Rozporządzenia, Przedsiębiorstwo jako ADO jest podmiotem ustalającym cele i sposoby przetwarzania danych osobowych. Przedsiębiorstwo przeprowadziła Analizę Ryzyka, mającą na celu weryfikację potencjalnych zagrożeń dla ochrony Danych osobowych oraz konieczność zastosowania odpowiednich środków zabezpieczeń Danych osobowych. Przeprowadzona Analiza ryzyka zawiera informacje o:

a. czynnościach przetwarzania,
b. charakterze przetwarzania danych osobowych,
c. zakresie przetwarzania danych osobowych,
d. kontekście przetwarzania danych osobowych,
e. celu przetwarzania danych osobowych,
f. podatnościach, zagrażających bezpieczeństwu danych osobowych,
g. prawdopodobieństwie wystąpienia podatności,
h. skutkach wystąpienia danej podatności dla integralności danych,
i. skutkach wystąpienia danej podatności dla dostępności danych,
j. skutkach wystąpienia danej podatności dla poufności danych,
k. poziomie ryzyka,
l. zastosowanych zabezpieczeniach,
m. skutkach wystąpienia danej podatności dla integralności, dostępności i poufności danych po uwzględnieniu zabezpieczeń,
n. końcowej ocenie ryzyka, uwzględniającej wdrożone zabezpieczenia.

Przedsiębiorstwo na bieżąco uaktualnia analizę ryzyka, biorąc pod uwagę w szczególności zmieniające się uwarunkowania techniczne w zakresie potencjalnych zagrożeń systemów informatycznych oraz istniejących zabezpieczeń, zwiększających poziom ochrony Danych osobowych.

Przedsiębiorstwo jako ADO przetwarzając Dane osobowe zobowiązana jest do podejmowania stosownych działań w celu ochrony przetwarzanych danych osobowych, a w szczególności:

a. wprowadza dokumentację opisującą sposób przetwarzania danych tj. m.in.: Politykę Bezpieczeństwa Danych Osobowych wraz z załącznikami;

b. zapewnia niezbędne środki potrzebne do zagwarantowania bezpieczeństwa przetwarzania Danych osobowych;

c. zapewnia przetwarzanie Danych osobowych zgodnie z powszechnie obowiązującymi przepisami prawa oraz wewnętrznymi regulacjami i zawartymi umowami;

d. zapewnia poprawność merytoryczną Danych osobowych i adekwatność w stosunku do celów, w jakich są przetwarzane;

e. zapewnia przechowywanie Danych osobowych w sposób umożliwiający identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania;

f. dopuszcza Osoby upoważnione do przetwarzania Danych osobowych nadając im upoważnienia pisemne;

g. może powierzyć innemu podmiotowi przetwarzanie danych zawierając umowę powierzenia przetwarzania Danych osobowych

h. podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania Danych osobowych.

i. prowadzi Rejestr Czynności Przetwarzania Danych i Rejestr Kategorii Czynności Przetwarzania Danych.

j. informuje Podmiot przetwarzający oraz pracowników, którzy przetwarzają Dane osobowe, o obowiązkach na nich spoczywających w zakresie powszechnie obowiązujących przepisów dot. ochrony Danych osobowych i doradza im w tej sprawie.

k. monitoruje przestrzeganie wewnętrzne powszechnie obowiązujących przepisów prawa o ochronie danych, niniejszej Polityki i innych wewnętrznych regulacji.

l. prowadzi działania zwiększające świadomość personelu przetwarzającego Dane osobowe.

m. współpracuje z organem nadzorczym (Prezesem Urzędu Ochrony Danych Osobowych).

7.2. Użytkownik Systemu Informatycznego (USI)

USI jako Osoba upoważniona do przetwarzania Danych osobowych w systemach informatycznych Przedsiębiorstwa, w których przetwarzane są dane osobowe jest zobowiązany do:

a. znajomości oraz bezwzględnego przestrzegania zasad bezpieczeństwa przetwarzania informacji określonych w Polityce oraz innych dokumentach wewnętrznych oraz powszechnie obowiązujących przepisach prawa, mających w tym zakresie zastosowanie,

b. przetwarzania Danych osobowych tylko w wyznaczonych do tego celu pomieszczeniach służbowych (lub wyznaczonych ich częściach),

c. zabezpieczania Danych osobowych oraz dokumentów zawierających Dane osobowe przed dostępem osób nieupoważnionych za pomocą środków określonych w Polityce, Instrukcjach, jak też wytycznych przełożonych,

d. zgłaszania potrzeby zniszczenia wszystkich zbędnych nośników elektronicznych (np. dyski zewnętrzne, pendrive) zawierających Dane osobowe w sposób uniemożliwiający ich odzyskanie,

e. nieudzielania informacji o Danych osobowych innym podmiotom, chyba, że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy przesłanki określone w tych przepisach zostały spełnione,

f. stosowania się do zaleceń Przedsiębiorcy w zakresie przetwarzania danych osobowych,

g. niezwłocznego informowania Przedsiębiorcy o wszelkich nieprawidłowościach dotyczących bezpieczeństwa przetwarzanych Danych osobowych, a w szczególności zawiadamiania o wszelkich przypadkach utraty lub kradzieży dokumentów lub innych nośników zawierających dane osobowe.

8. Obszar przetwarzania Danych osobowych

1. Obszar przetwarzania danych osobowych stanowią miejsca, w których Przedsiębiorstwo przetwarza Dane osobowe zarówno w formie papierowej, jak i w systemie informatycznym.
2. Miejsca, w których przetwarzane są dane osobowe, są zabezpieczone w sposób zapewniający rozliczalność i poufność przetwarzanych danych.

9. Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

9.1. Organizacyjne środki ochrony danych osobowych

1. Dopuszczanie do przetwarzania Danych osobowych wyłącznie osób posiadających upoważnienie w przedmiotowym zakresie.
2. Prowadzenie Ewidencji osób upoważnionych do przetwarzania Danych osobowych.
3. Opracowanie i wdrożenie dokumentacji w zakresie ochrony Danych osobowych.
4. Szkolenia upoważnionych osób w zakresie obowiązujących przepisów ochrony Danych osobowych oraz wewnętrznych regulacji stosowanych w celu zabezpieczenia danych.
5. Zobowiązanie osób upoważnionych do przetwarzania Danych osobowych do zachowania ich w tajemnicy.
6. Osoby upoważnione do przetwarzania Danych osobowych nie mogą ich ujawniać w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych lub wynikających z umowy o współpracy, w ramach udzielonego upoważnienia do przetwarzania danych.
7. Niedopuszczalne jest wynoszenie materiałów zawierających Dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych lub wynikających z umowy o współpracy bez zgody Przedsiębiorcy. Za bezpieczeństwo i zwrot materiałów zawierających Dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.

9.1.1. Organizacyjne zasady bezpiecznego przetwarzania Danych osobowych w wersji papierowej

1. Decydując się na korzystanie podczas pracy zdalnej z dokumentacji papierowej, należy podjąć działania mające na celu ograniczenie ryzyka związanego z utratą Dostępności, Integralności i Poufności Danych osobowych.
2. Należy ocenić niezbędność wykorzystywania dokumentacji papierowej podczas pracy zdalnej, biorąc pod uwagę charakter danych, cele, dla których są przetwarzane oraz dostępne środki. Konieczna jest także ocena czy do wykonywania pracy niezbędny jest dostęp do Danych Osobowych, czy też jest możliwe skorzystanie z dokumentów zanonimizowanych.
3. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających Dane osobowe musi odbywać się z wykorzystaniem niszczarek, w sposób uniemożliwiający odczytanie zawartej w nich treści.
4. Wydruki zawierające Dane osobowe należy niezwłocznie odbierać z drukarek.
5. Udostępnione dokumenty są przechowywane przez pracowników przez okres niezbędny do wykonania określonego zadania.
6. Liczba dokumentów udostępnianych pracownikowi jest ograniczona w stosunku do celu przetwarzania Danych osobowych.
7. Pracownicy zobowiązani są do odpowiedniego zabezpieczenia Danych osobowych w miejscu wykonywania pracy zdalnej (przechowywanie dokumentów w zamykanych na klucz szufladach lub szafach, przestrzeganie zasady czystego biurka, zabezpieczenie dokumentów przed wglądem nieuprawnionych osób trzecich, m. in. członków rodziny).

9.1.2. Organizacyjne zasady bezpiecznego przetwarzania Danych osobowych w wersji elektronicznej

1. Osoby przetwarzające dane osobowe w systemach informatycznych posiadają indywidualne i niepowtarzalne identyfikatory (loginy) oraz hasła dostępu.
2. Przydzielony raz identyfikator danemu użytkownikowi nie może być przydzielony innej osobie, chyba że zachodzą szczególne ku temu przesłanki, a ponowne przydzielenie tego samego identyfikatora nie będzie prowadziło do możliwości korzystania z tegoż identyfikatora przez więcej niż jedną osobę oraz nie wykluczy możliwości bezpośredniej i nie budzącej wątpliwości identyfikacji osoby korzystającej z tego identyfikatora.
3. Wszyscy USI, korzystający z systemów informatycznych, w których przetwarzane są dane osobowe, mają obowiązek stosowania haseł spełniających wymogi bezpieczeństwa na poziomie wysokim oraz dokonywania zmian haseł **nie rzadziej niż co 90 dni.**
4. Zabronione jest ujawnianie haseł jak również korzystanie z identyfikatorów innych użytkowników.
5. Haseł dostępu do komputera oraz baz danych zawierających Dane osobowe nie wolno umieszczać przy komputerze oraz w niezamykanych szafkach/szufladach (karteczki, notesy, kalendarze itp.), ani zapisywać w pamięci przeglądarek internetowych.
6. Przyznanie, zmiana lub usunięcie uprawnień użytkownika do przetwarzania Danych osobowych w poszczególnych aplikacjach realizowane jest na wniosek pisemny bądź ustny przełożonego.
7. Monitory ekranowe powinny być ustawione w taki sposób, aby uniemożliwić osobom nieuprawnionym podgląd wyświetlanych Danych osobowych.
8. Udając się na przerwę w pracy, należy zastosować blokadę monitora lub wylogować się z systemu. Zaleca się ustawienie automatycznej blokady ekranu po kilku minutach bezczynności Użytkownika.
9. Wysyłając Dane osobowe mailem należy upewnić się czy prawidłowo został wpisany e-mail adresata wiadomości.
10. Przed wysłaniem plików zawierających szczególne kategorie Danych osobowych, należy te pliki zaszyfrować stosując programy szyfrujące (np. Zip, 7Z, wbudowany mechanizm haseł w plikach pakietu Microsoft Office). Hasło wysyłamy zawsze inną drogą komunikacyjną (telefon, sms).
11. Wysyłając wiadomości do wielu adresatów będących osobami fizycznymi, adresy mailowe należy dodawać do kopii ukrytej tzw. UDW lub BCC (nie dotyczy wysyłania wiadomości do współpracowników).
12. Zabronione jest używanie służbowego adresu mailowego do celów prywatnych.
13. Zabronione jest klikanie w linki i otwieranie załączników z nieznanych źródeł.
14. W przypadku przetwarzania Danych osobowych na komputerach przenośnych należy zachować szczególną ostrożność przy ich transporcie, a Użytkownicy powinni stosować zasady bezpieczeństwa co najmniej takie jak w obszarze przetwarzania.
15. Zaleca się łączenie z Internetem i firmową siecią za pośrednictwem bezpiecznego łącza VPN.
16. Komputery wykorzystywane do pracy powinny posiadać zainstalowany aktualny program antywirusowy oraz firewall.
17. Komputery przenośne muszą mieć zaszyfrowany dysk twardy.
18. Pracownik stosuje się do przyjętej procedury uwierzytelnianie użytkownika, w tym wieloetapowego, podczas logowania do systemów, w których przetwarzane są Dane osobowe.
19. Komputery wykorzystywane do pracy powinny posiadać możliwość automatycznego backupu danych. Jeżeli nie jest to możliwe, Użytkownicy powinni przeprowadzać procedurę backupową ręcznie.

20. Pracownicy zobowiązani są do odpowiedniego zabezpieczenia stosowanych w pracy smartfonów (blokada ekranu, PIN, szyfrowanie danych, możliwość łączenia z Internetem i firmową siecią za pośrednictwem bezpiecznego łącza VPN, możliwość automatycznego backupu danych).
21. W przypadku konieczności zgrywania Danych osobowych na nośniki zewnętrzne, dopuszcza się korzystanie wyłącznie z szyfrowanych urządzeń.

9.2. Techniczne środki ochrony Danych osobowych

1. Systemy informatyczne służące do przetwarzania Danych osobowych są wyposażone w mechanizmy uwierzytelnienia użytkownika oraz kontroli dostępu do danych (na poziomie logowania do systemu).
2. Tam gdzie zachodzi taka potrzeba Przedsiębiorstwo stosuje - wymusza uwierzytelnianie wieloetapowe.
3. Zastosowano środki kryptograficznej ochrony danych dla Danych osobowych przekazywanych drogą teletransmisji.
4. Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.
5. Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
6. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przed utratą poprzez wykonywanie kopii zapasowych.
7. Szyfrowanie dysków komputerów przenośnych.

10. Kluczowe zasady składające się na system ochrony danych Przedsiębiorstwa gdzie indziej nie sklasyfikowane

1. Inwentaryzacja danych. Administrator dokonuje identyfikacji zasobów danych osobowych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja), w tym:

a) przypadków przetwarzania danych specjalnych i danych „kryminalnych" (**dane wrażliwe**);

b) przypadków przetwarzania danych osób, których administratora nie identyfikuje (**dane niezidentyfikowane** np. osób objętych monitoringiem wizyjnym);

c) współadministrowania danymi.

2. Rejestry. Administrator opracowuje, prowadzi i utrzymuje Rejestry wymagane przepisami prawa. Rejestry są narzędziem rozliczania zgodności z ochroną danych.

3. Podstawy prawne. Administrator zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:

a) utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość,

b) inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy przetwarza dane na podstawie prawnie uzasadnionego interesu.

4. Eksport danych. Administrator weryfikuje czy nie przekazuje danych do państw trzecich (czyli poza UE, Norwegię, Lichtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce.

5. Dla zapewnienia bezpieczeństwa danych i informacji stosuje się następujące środki organizacyjne:

a. Pomieszczenia w których są przetwarzane dane osobowe powinny być zamykane na klucz.

b. Dostęp do kluczy posiadają tylko upoważnieni pracownicy i współpracownicy.

c. Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy. W przypadku pomieszczeń, do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności.

d. Dane w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych, a następnie muszą być chowane do szaf.

e. Dostęp do komputerów, na których są przetwarzane dane - mają tylko upoważnieni pracownicy i współpracownicy. Nie należy udostępniać osobom nieupoważnionym tych komputerów.

f. W przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami - należy dokonać tego z zachowaniem szczególnej ostrożności.

g. Nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie), aby nie zostały na nich dane osobowe.

h. W wypadku niemożliwości skasowania danych z nośnika (płyta CD-ROM) - należy taką płytę zniszczyć fizycznie.

i. Niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną.

j. Sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz,

k. Błędne lub nieaktualne wydruki i wersje papierowe zawierające dane osobowe lub inne informacje chronione - niszczone są za pomocą niszczarki lub w inny mechaniczny sposób uniemożliwiający powtórne ich odtworzenie.

11. Postępowanie w sytuacji Naruszenia ochrony Danych osobowych

1. Naruszenie ochrony Danych osobowych stanowi incydent bezpieczeństwa prowadzący do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do Danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
2. Do incydentów bezpieczeństwa mogących prowadzić do naruszenia ochrony Danych osobowych należą:
   a. zdarzenia losowe zewnętrzne – pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności;
   b. zdarzenia losowe wewnętrzne – awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków i Użytkowników, utrata/zagubienie dokumentów, utrata/zagubienie przenośnych komputerów, pendrive'ów, dysków zewnętrznych;
   c. umyślne incydenty zewnętrzne – włamanie do systemu informatycznego lub pomieszczeń; kradzież danych/sprzętu przez osobą z zewnątrz firmy; atak hackerski, którego skutkiem może być wyciek informacji; atak phishingowy; działanie wirusów i innego szkodliwego oprogramowania;

d. umyślne incydenty wewnętrzne – ujawnienie Danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych; kradzież dokumentacji z danymi przez pracownika.

3. **W przypadku stwierdzenia lub podejrzenia wystąpienia naruszenia ochrony Danych osobowych, pracownik/współpracownik ma obowiązek:**
   a. **powiadomić Przedsiębiorcę lub bezpośredniego przełożonego o podejrzeniu lub fakcie wystąpienia naruszenia;**
   b. **niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków, a następnie ustalić przyczyny, lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe;**
   c. **zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę;**
   d. **udokumentować wstępnie zaistniałe naruszenie;**
   e. **nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia lub odpowiednio je zabezpieczyć.**
4. Po otrzymaniu zgłoszenia o wystąpieniu lub podejrzeniu wystąpienia naruszenia ochrony Danych osobowych, Przedsiębiorca prowadzi postępowanie wyjaśniające, w toku którego:
   a. wysłuchuje relacji osoby zgłaszającej z zaistniałego naruszenia, jak również relacji każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem;
   b. ustala datę, czas, miejsce wystąpienia naruszenia, jego zakres, przyczyny ujawnienia, skutki oraz wielkość szkód, które zaistniały;
   c. rekomenduje działania naprawcze i prewencyjne.
5. Przedsiębiorca i inni zainteresowani pracownicy/współpracownicy konsultują i oceniają czy powstałe naruszenie może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych, a jeśli tak, to jaka jest waga ryzyka (ryzyko niskie, średnie, wysokie).
6. Ryzyko wystąpienia naruszenia praw i wolności osób fizycznych oceniane jest pod kątem możliwości wystąpienia: uszczerbku fizycznego, szkód majątkowych, szkód niemajątkowych (np. dyskryminacja, kradzież tożsamości lub oszustwa dotyczące tożsamości, strata finansowa, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnione odwrócenie pseudonimizacji lub wszelka inna znaczna szkoda gospodarcza lub społeczna).
7. W przypadku stwierdzenia, że naruszenie może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych, Przedsiębiorca bez zbędnej zwłoki nie później niż w terminie **72 godzin** po stwierdzeniu naruszenia – zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych.
8. Zgłoszenie naruszenia do organu nadzorczego musi co najmniej:
   a. opisywać charakter naruszenia ochrony Danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   b. zawierać imię i nazwisko lub oznaczenie punktu kontaktowego, od którego można uzyskać więcej informacji;
   c. opisywać możliwe konsekwencje naruszenia ochrony Danych osobowych;
   d. opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony Danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
9. W przypadku stwierdzenia, że naruszenie może skutkować WYSOKIM ryzykiem naruszenia praw lub wolności osób fizycznych, Przedsiębiorca bez zbędnej zwłoki zawiadamia osobę,

której dane dotyczą, o takim naruszeniu. Zawiadomienie musi zawierać wszystkie elementy wskazane w pkt 9 powyżej i powinno być sformułowane jasnym i prostym językiem.

10. Zawiadomienie, o którym mowa w pkt 10 powyżej nie jest wymagane, jeżeli spełniono wymagania art. 34 ust. 3 Rozporządzenia.
11. Przedsiębiorca dokumentuje na bieżąco zaistniały przypadek naruszenia.
12. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu, Przedsiębiorca zasięga niezbędnych opinii i proponuje działania naprawcze (w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń) i zarządza termin wznowienia przetwarzania danych.
13. Przedsiębiorca ocenia i dokumentuje skuteczność zakończonych działań naprawczych związanych z naruszeniem.

12. Szkolenia

1. Szkolenia z zakresu bezpieczeństwa informacji Danych osobowych przeprowadzane są dla nowo zatrudnionych pracowników/współpracowników, jak również po wystąpieniu incydentu naruszającego bezpieczeństwo Danych osobowych, w odniesieniu do osoby lub osób, którzy dopuścili się uchybień skutkujących tymże incydentem.
2. Oprócz szkoleń określonych w pkt 1 powyżej, odbywają się również szkolenia okresowe, w tym szkolenia przedstawiające zmiany w przepisach prawa o ochronie Danych osobowych lub zmiany zasad ochrony Danych osobowych.
3. Dopuszcza się przeprowadzanie szkoleń e-learningowych. Celem szkoleń jest podnoszenie świadomości pracowników w zakresie bezpieczeństwa, ochrony oraz przetwarzania Danych osobowych.

13. Postanowienia końcowe

1. Polityka jest wewnętrznym dokumentem firmy objętym obowiązkiem zachowania w poufności przez wszystkie osoby, którym zostanie ujawniona. Do spraw nieuregulowanych w Polityce stosuje się powszechnie obowiązujące przepisy prawa o ochronie Danych osobowych.
2. Polityka podlega stosownym przeglądom i aktualizacjom, w szczególności w sytuacji wprowadzenia zmian w obowiązujących przepisach prawa dotyczących ochrony Danych Osobowych czy też w przypadku wprowadzania znaczących zmian w modelu biznesowym lub działaniach firmy związanych z przetwarzaniem Danych osobowych.
3. Niezależnie od odpowiedzialności określonej w przepisach powszechnie obowiązującego prawa, Pracownicy i Współpracownicy mogą podlegać stosownym konsekwencjom dyscyplinarnym, umownym lub prawnym za nieprzestrzeganie postanowień Polityki.
4. Pracownicy i Współpracownicy zobowiązani są do stosowania przy przetwarzaniu Danych osobowych postanowień zawartych w niniejszej Polityce.
5. Zmiany Polityki wymagają każdorazowo formy pisemnej w postaci aktualizacji Polityki.
6. **Uaktualnienia Załączników nie powodują konieczności wprowadzenia nowej wersji Polityki.**

14. ZAŁĄCZNIKÓW

Wzór upoważnienia do przetwarzania danych osobowych;

Ewidencja osób upoważnionych do przetwarzania danych osobowych;

Wzór oświadczenia o zapoznaniu się z obowiązującymi przepisami prawa w zakresie ochrony danych osobowych oraz zachowaniu danych osobowych i sposobu ich zabezpieczenia;

Wzór umowy powierzenia przetwarzania danych osobowych;

Ewidencja umów powierzenia przetwarzania danych osobowych;

Rejestr Czynności Przetwarzania Danych;

Rejestr Kategorii Czynności Przetwarzania Danych;

Analiza ryzyka wraz z opisem bezpieczeństwa.