POLITYKA BEZPIECZEŃSTWA

Administrator danych:

EKOBAK Marcin Grochla ul. Dworcowa 26B, 44-180 Toszek

Spis treści

Wprowadzenie

Instrukcja stanowi wykaz procedur oraz stosowanych środków technicznych i organizacyjnych mających na celu, zgodnie z art. 32 RODO, zabezpieczyć przetwarzane dane osobowe. Administrator danych jest zobowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Administrator danych zobowiązany jest zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane. W tym celu prowadzona jest dokumentacja opisująca sposób przetwarzania danych oraz środki zapewniające należytą ochronę.

Administrator danych – EKOBAK Marcin Grochla ul. Dworcowa 26B, 44-180 Toszek.
Administrator systemów informatycznych – EKOBAK Marcin Grochla ul. Dworcowa 26B, 44-180 Toszek
Inspektor ochrony danych (IOD) – administrator danych sam wykonuje czynności inspektora ochrony danych.

Rozdział I – Definicje

1. **Analiza ryzyka** – proces mający na celu oszacowanie wagi ryzyka rozumianej jako funkcja prawdopodobieństwa wystąpienia skutku i krytyczności jego następstw dla przedsiębiorstwa.
2. **Dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. 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 PESEL, wizerunek, adres email, numer telefonu, numer rachunku bankowego, numer rejestracyjny pojazdu, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
3. **Elektroniczny nośnik** – urządzenie elektroniczne, na którym przechowuje się dane osobowe w celu jego ponownego odtworzenia w systemie informatycznym.
4. **Odbiorca danych** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.
5. **Obszar przetwarzania danych** – lokalizacje, budynki, pomieszczenia lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.
6. **Organ nadzorczy** – Urząd Ochrony danych osobowych.

7. **Opis przepływu danych** – sposób przepływu danych pomiędzy poszczególnymi systemami informatycznymi i obszarami przetwarzania danych.
8. **Opis struktury zbiorów** – opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi.
9. **Państwo trzecie** – to państwo nienależące do Europejskiego Obszaru Gospodarczego.
10. **Przetwarzane danych** – to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
11. **Anonimizacja** – zmiana danych osobowych w wyniku której dane te tracą charakter danych osobowych.
12. **Pseudonimizacja** – przetwarzanie danych osobowych w taki sposób (np. poprzez zastępowanie nazw liczbami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym w celu zapewnienia, że dane osobowe nie są przypisane do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
13. **RODO** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) z dnia 27 kwietnia 2016 r. (Dz. Urz. UE. L Nr 119, str. 1).
14. **Inspektor Ochrony Danych (IOD)** – to osoba lub podmiot formalnie wyznaczony przez administratora danych w celu informowania i doradzania administratorowi danych, administratorowi systemu informatycznego, podmiotowi przetwarzającemu (procesorowi), pracownikom w zakresie niniejszej polityki bezpieczeństwa i obowiązującego prawa o ochronie danych osobowych, monitorowania i przestrzegania ochrony danych osobowych oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.
15. **Szczególne kategorie danych osobowych** – ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące życia seksualnego osoby lub orientację seksualną. W zależności od obowiązującego prawa, szczególne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych, karnych oraz o sankcjach.
16. **Profilowanie** – jest dowolną formą zautomatyzowanego przetwarzania danych osobowych, która 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.

17. **Naruszenie ochrony danych osobowych** – jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.
18. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
19. **Środki techniczne i organizacyjne** – to środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.
20. **Ustawa** – rozumie się przez to ustawę z 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018, poz.1000).
21. **Usuwanie danych** – to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
22. **Użytkownik systemu** – osoba, której został przydzielony przez administratora systemu indywidualny identyfikator w systemie informatycznym w powiązaniu z niezbędnymi uprawnieniami dostępowymi w tym systemie.
23. **Wykaz zbiorów** – to wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.
24. **Zabezpieczenie danych w systemie informatycznym** – to wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
25. **Zbiór danych** – każdy uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
26. **Zgoda osoby, której dane dotyczą** – to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści, zgoda może być odwołana w każdym czasie.
27. **Aktywa** – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych.
28. **Naruszenie ochrony danych osobowych** (incydent) - to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
29. **Zagrożenie** - potencjalne naruszenie (potencjalny incydent).
30. **Skutki** - rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia).
31. **Ryzyko** - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów.

Rozdział II – Administrator danych

1. Administrator danych jest zobowiązany w szczególności do:

a) opracowania i wdrożenia polityki bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym przetwarzającym dane osobowe,
b) stałego nadzoru nad treścią polityki bezpieczeństwa oraz instrukcją zarządzania systemem informatycznym,
c) wydawania i anulowania upoważnienia do przetwarzania danych osobowych osobom, które mają te dane przetwarzać, jeśli zatrudnia pracowników,
d) prowadzenia wykazu osób upoważnionych do przetwarzania danych osobowych,
e) prowadzenia wykazu obszarów przetwarzania,
f) prowadzenia wykazu zbiorów danych osobowych,
g) prowadzenia opisu sposobu przepływu danych,
h) dokonywania aktualizacji dokumentów wymienionych powyżej,
i) wykazania przestrzegania zasad przetwarzania danych opisanych w RODO.

2. Administrator danych jest zobowiązany do przetwarzania następujących zasad przetwarzania danych osobowych:
a) zgodności z prawem – przetwarzanie danych powinno następować zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą,
b) ograniczenia celu – zbieranie danych powinno się odbywać w konkretnych, wyraźnych i prawnie uzasadnionych celach, dane nie powinny być przetwarzane dalej w sposób niezgodny z tymi celami (dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami),
c) minimalizacji danych – przetwarzane mogą być tylko dane adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane,
d) prawidłowości – przetwarzane mogą być tylko dane prawidłowe i w razie potrzeby uaktualniane (administrator jest zobowiązany do podjęcia wszelkich działań, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane),
e) ograniczenia przechowywania – dane powinny być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne realizacji celów, dla których dane te są przetwarzane, dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych, historycznych lub do celów statystycznych, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy RODO w celu ochrony praw i wolności osób, których dane dotyczą,
f) integralności i poufności – dane powinny być przetwarzane w sposób zapewniający odpowiednie ich bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

Rozdział III – Rejestr czynności przetwarzania

1. W celu dokonania analizy ryzyka wymagane jest zidentyfikowanie danych osobowych, które należy zabezpieczyć. Dane te w postaci zbiorów (kategorii osób) zostały wykazane w załączniku – wykaz zbiorów danych osobowych.
2. Opis zbiorów (kategorii osób) powinien obejmować takie informacje, jak:
   a) nazwę zbioru (opis kategorii osób),
   b) opis celów przetwarzania,
   c) charakter, zakres, kontekst danych osobowych,
   d) odbiorcy danych,
   e) funkcjonalny opis operacji przetwarzania,
   f) aktywa służące do przetwarzania danych osobowych (informacje, programy, systemy operacyjne, infrastruktura IT, infrastruktura, pracownicy i współpracownicy, outsourcing),
   g) informacja o konieczności wpisu do rejestru czynności przetwarzania,
   h) informacja o konieczności przeprowadzenia oceny skutków dla zbioru.
3. Rejestr czynności przetwarzania przez administratora danych (lub jeśli jest powołany – inspektora ochrony danych) zamieszczony jest w załączniku rejestr czynności z charakterystyką zbiorów danych osobowych.

Rozdział IV – Zbieranie danych osobowych

1. W przypadku zbierania danych od osób, których dane dotyczą dokonujący tej czynności zobowiązany jest do poinformowania osoby, której dane dotyczą o:
   a) swojej tożsamości i danych kontaktowych oraz, gdy ma to zastosowanie, tożsamości i danych kontaktowych swojego przedstawiciela,
   b) gdy ma to zastosowanie – danych kontaktowych inspektora ochrony danych,
   c) celach przetwarzania danych osobowych, oraz podstawie prawnej przetwarzania,
   d) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f RODO – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią,
   e) odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,
   f) gdy ma to zastosowanie – o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych,
   g) okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, o kryteriach ustalania tego okresu,
   h) prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,

i) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO – o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,

j) prawie wniesienia skargi do organu nadzorczego,

k) tym, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,

l) zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

2. Jeżeli administrator danych będzie planował dalsze przetwarzanie danych osobowych w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem zobowiązuje się do poinformowania osoby, której dane dotyczą, o tym innym celu oraz do udzielenia jej wszelkich innych stosownych informacji, zgodnych z RODO.

3. Jeżeli danych osobowych administrator danych nie pozyskał od osoby, której dane dotyczą, administrator podaje osobie, której dane dotyczą, informacje wymienione w ust. 1 powyżej, jak również informuje o źródle pochodzenia danych osobowych, a gdy ma to zastosowanie czy pochodzą one ze źródeł publicznie dostępnych. Informacje te należy podać:

a) w rozsądnym terminie po pozyskaniu danych osobowych, najpóźniej w ciągu miesiąca, mając na uwadze konkretne okoliczności przetwarzania danych osobowych,

b) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą, najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą,

c) jeżeli administrator danych planuje ujawnić dane osobowe innemu odbiorcy, najpóźniej przy ich pierwszym ujawnieniu.

4. Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora danych potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:

a) celach przetwarzania,

b) kategoriach odnośnych danych osobowych,

c) o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych,

d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu,

e) o prawie do żądania od administratora danych sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania,

f) o prawie wniesienia skargi do organu nadzorczego,

g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą, wszelkie dostępne informacje o ich źródle,

h) o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz o istotnych informacjach dotyczących zasad ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

5. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przekazaniem.
6. Administrator danych dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator danych może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.
7. Prawo do uzyskania kopii, o której mowa w ust. 6 powyżej, nie może niekorzystnie wpływać na prawa i wolności innych osób.

Rozdział V – Ocena niezbędności oraz proporcjonalności

1. W ramach przeprowadzenia oceny skutków (analizy ryzyka) administrator danych lub podmiot przetwarzający (procesor) zobowiązany jest do spełnienia wobec nich obowiązków prawnych. W szczególności należy zapewnić, że:
   a) dane te są legalnie przetwarzane (na podstawie art. 6, 9),
   b) dane te są adekwatne w stosunku do celów przetwarzania,
   c) dane te są przetwarzane przez określony czas,
   d) wobec tych osób wykonano tzw. obowiązek informacyjny (art. 12, 13 i 14) wraz ze wskazaniem ich praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, odwołania zgody),
   e) opracowano klauzule informacyjne dla powyższych osób – załącznik klauzul informacyjnych,
   f) istnieją umowy powierzenia z podmiotami przetwarzającymi (art. 28) zgodnie z załącznikiem - umowa powierzenia danych osobowych (wykaz podmiotów przetwarzających prowadzony jest w załączniku – rejestr umów powierzenia),
   g) potwierdzenie spełnienia powyższych wymagań prawnych RODO znajduje się w załączniku – wykaz zbiorów danych osobowych.

Rozdział VI – Analiza ryzyka

1. Ocena skutków jest formalną, określoną w art. 37 RODO procedurą przeprowadzenia analizy ryzyka za wykonanie której odpowiada administrator danych, przed przetwarzaniem, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka dla praw i wolności osób fizycznych jako rodzaju przetwarzania danych osobowych i zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych.
2. W przypadku powołania inspektora ochrony danych (IOD) – ocena skutków musi być wykonana z jego współudziałem.

3. Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.
4. Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru lub grupy zbiorów (kategorii osób) lub dla procesów przetwarzania (np. dla zbioru pracowników, zbioru klientów, dla procesu wysyłania informacji handlowej z bazy marketingowej).
5. Wyznaczenie zagrożeń:
   a) administrator danych jest odpowiedzialny za określenie listy zagrożeń, które mogą wystąpić w przetwarzaniu danych w zbiorze, dla kategorii osób lub w procesie przetwarzania,
   b) zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zidentyfikowanych aktywów,
   c) wykaz zagrożeń znajduje się w załączniku – lista potencjalnych zagrożeń,
6. Wyliczenie ryzyka dla zagrożeń:
   a) administrator danych określa prawdopodobieństwo (P) wystąpienia poszczególnych zagrożeń w zbiorze lub w procesie przetwarzania,
   b) proponowaną skalę prawdopodobieństwa prezentuje tabela nr. 1,
   c) administrator danych określa skutki (S) wystąpienia incydentów, uwzględniając straty finansowe, utratę reputacji, sankcje lub skutki karne,
   d) proponowaną skalę skutków prezentuje tabela nr. 2,
   e) administrator danych wylicza ryzyka (R) dla wszystkich zagrożeń i ich skutków w/g formuły: R = P * S.

Tabela nr. 1.

Prawdopodobieństwo wystąpienia naruszenia)	Skala (waga)
zagrożenie niskie	1
zagrożenie średnie	2
zagrożenie wysokie	3

Tabela nr. 2.

Skutki wystąpienia zagrożenia	Skala (waga)
małe (do 10000 PLN, incydent prasowy lokalny)	1
średnie (10000 – 100000 PLN, incydent prasowy ogólnopolski)	2
duże (od 100000 PLN, naruszenie prawa)	3

7. Porównanie wyliczonych ryzyk ze skalą i określenie dalszego postępowania z ryzykiem:

a) administrator danych porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem,
b) proponowaną skalę ryzyka prezentuje tabela nr. 3.

Tabela nr. 3.

Poziom ryzyka	Wartość [R = P*S]
ryzyko pomijalne i akceptowalne (akceptujemy)	1 – 2
ryzyko jest opcjonalne (akceptujemy albo obniżamy)	3 – 6
ryzyko jest nieakceptowalne (musimy obniżyć)	9

8. Reakcja na wartość ryzyka:
   a) akceptacja ryzyka, zabezpieczenia są właściwe (brak potrzeby stosowania dodatkowych zabezpieczeń),
   b) działania obniżające ryzyko, które może zastosować administrator:
      - przeniesienie – przerzucenie ryzyka (outsourcing, ubezpieczenie),
      - unikanie – eliminacja działań powodujących ryzyko (np. zakaz wynoszenia komputerów przenośnych poza firmę),
      - redukcja – zastosowanie zabezpieczeń w celu obniżenia ryzyka (np. zaszyfrowanie pendrive z danymi wynoszonych poza firmę),
   c) wykaz zabezpieczeń znajduje się w załączniku – wykaz zabezpieczeń.
9. Ponowna analiza ryzyka przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów, nowych procesów przetwarzania, zmiany prawne).

Rozdział VII – Zarządzanie ryzykiem

1. W celu skutecznej realizacji zadań związanych z bezpieczeństwem informacji przeprowadzana jest raz w roku oraz przy każdej istotnej zmianie środowiska informatycznego analiza ryzyka.
2. Proces składa się z następujących etapów:
   a) identyfikacji ryzyka,
   b) szacowania ryzyka,
   c) przeciwdziałania ryzyku,
   d) monitorowania i raportowania ryzyka IT.
3. Wyniki analizy ryzyka stanowią podstawę zaprojektowania odpowiednich mechanizmów kontroli dla systemów informatycznych eksploatowanych w organizacji.
4. Wdrażane mechanizmy kontroli powinny być adekwatne do oszacowanego ryzyka, zidentyfikowanych zagrożeń i ich istotności, oraz muszą zapewniać efektywność ekonomiczną.
5. Kontrola adekwatności oraz sposobu funkcjonowania stosowanych mechanizmów kontroli wchodzi w skład zadań administratora systemu i przeprowadzana jest w ramach szacowania ryzyka operacyjnego.

6. Za proces analizy i szacowania ryzyka bezpieczeństwa informacji odpowiedzialny jest administrator danych.
7. W celu zminimalizowania ryzyka związanego z zagrożeniami bezpieczeństwa informacji każdy użytkownik systemu informatycznego powinien być regularnie szkolony z zakresu obsługi systemu i procedur bezpieczeństwa informacji oraz właściwego używania zasobów informatycznych.
8. Wszędzie, gdzie administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne.
9. Administrator danych zobowiązany jest do monitorowania wdrożenia zabezpieczeń.
10. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być poddana przeszkoleniu i zapoznana z przepisami RODO.
11. Za organizowanie szkoleń z zakresu obsługi systemu i procedur bezpieczeństwa informacji oraz właściwego używania zasobów informatycznych odpowiedzialny jest administrator danych (lub jeśli jest powołany – inspektor ochrony danych).
12. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania – załącznik oświadczenie poufności.
13. Regulamin ochrony danych ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania – załącznik regulamin ochrony danych osobowych.
14. Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania – załącznik oświadczenie poufności.
15. Zgodnie z art. 32 RODO, administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
16. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdrożył odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO. Środki te są poddawane przeglądom i na bieżąco uaktualniane – załącznik wykaz zabezpieczeń.
17. W wykazie zabezpieczeń wskazano stosowane zabezpieczenia proceduralne oraz zabezpieczenia jako środki techniczne i organizacyjne.
18. Wykaz zabezpieczeń jest aktualizowany po każdej analizie ryzyka i ocenie skutków.
19. Uwzględniając kategorie przetwarzanych danych oraz potencjalne zagrożenia wprowadza się wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym.
20. W celu ochrony danych osobowych przeprowadzono analizę ryzyka celem zabezpieczenia przed naruszeniami praw lub wolności osób, których dane dotyczą.

Rozdział VIII – Instrukcja postępowania z incydentami

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia

incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba, która poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe bądź posiada informacje mogące mieć wpływ na bezpieczeństwo danych osobowych, jest zobowiązana fakt ten niezwłocznie zgłosić administratorowi danych (lub jeśli jest powołany – inspektorowi ochrony danych), jeśli administrator zatrudnia pracowników.
2. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych administratora danych (lub jeśli jest powołany – inspektora ochrony danych) osoba powiadamiająca powinna:
   a) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków, a następnie ustalić przyczyny, skutki i sprawców zaistniałego zdarzenia, jeżeli jest to możliwe,
   b) zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
   c) udokumentować wstępnie zaistniałe naruszenie,
   d) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia administratora danych lub osoby upoważnionej.
3. Po przybyciu na miejsce naruszenia ochrony danych osobowych administratora danych (lub jeśli jest powołany – inspektor ochrony danych) powinien:
   a) udokumentować wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze – załącznik formularz rejestracji incydentu, nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia administratora danych lub osoby upoważnionej.
   b) podjąć działania na rzecz przywrócenia działań organizacji po wystąpieniu incydentu,
   c) zarekomendować działania zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.
4. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu:
   a) w przypadku naruszenia ochrony danych osobowych, administrator danych (lub jeśli jest powołany – inspektor ochrony danych) bez zbędnej zwłoki, w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia,
   b) zgłoszenie, naruszenia ochrony danych osobowych organowi nadzorczemu, musi co najmniej:
      - 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,
      - zawierać imię i nazwisko oraz dane kontaktowe administratora danych (lub jeśli jest powołany – inspektora ochrony danych) lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
      - opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,

- opisywać środki zastosowane lub proponowane przez administratora danych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

5. Administrator danych (lub jeśli jest powołany – inspektor ochrony danych) dokumentuje zaistniały przypadek naruszenia oraz sporządza sprawozdanie. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania przepisów RODO.
6. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu, administrator danych (lub jeśli jest powołany – inspektor ochrony danych) zasięga niezbędnych opinii i proponuje postępowanie naprawcze (w tym ustosunkowuje się do kwestii odtworzenia danych z zabezpieczeń) oraz zarządza termin wznowienia przetwarzania danych.
7. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator danych (lub jeśli jest powołany – inspektor ochrony danych) bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
8. Zawiadomienie osoby, której dane dotyczą o naruszeniu powinno jasnym i prostym językiem opisywać charakter naruszenia ochrony danych osobowych oraz zawierać przynajmniej następujące informacje: imię i nazwisko oraz dane kontaktowe administratora danych (lub jeśli jest powołany – inspektora ochrony danych) lub oznaczenie innego punktu kontaktowego, możliwe konsekwencje naruszenia ochrony danych osobowych oraz środki zastosowane lub proponowane przez administratora danych (lub jeśli jest powołany – inspektora ochrony danych) w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
9. Zawiadomienie osoby, której dane dotyczą o naruszeniu nie jest wymagane, w następujących przypadkach:
   a) administrator danych wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,
   b) administrator danych zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
   c) wymagałoby ono niewspółmiernie dużego wysiłku, w takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.
10. Do typowych podatności bezpieczeństwa danych osobowych należą:
    a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
    b) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
    c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka lub ekranu monitora, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
11. Do typowych incydentów bezpieczeństwa danych osobowych należą:

a) zdarzenia losowe zewnętrzne (pożar obiektu lub pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata lub zagubienie danych),
c) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych lub sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów lub danych, działanie wirusów i innego szkodliwego oprogramowania).

Rozdział IX – Postanowienia końcowe

1. Wszelkie zasady opisane w polityce bezpieczeństwa są przestrzegane przez osoby upoważnione do przetwarzania danych osobowych ze szczególnym uwzględnieniem dobra osób, których dane te dotyczą.
2. Administrator danych może powierzyć przetwarzanie danych innemu podmiotowi, w drodze umowy zawartej w formie pisemnej. Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, danych zobowiązuje się on korzystać wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Podmiot przetwarzający (procesor) może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie oraz jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36–39 ustawy oraz w RODO oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a ustawy oraz w RODO. W zakresie przestrzegania tych przepisów taki podmiot ponosi odpowiedzialność jak administrator danych. W przypadkach, o których mowa powyżej, odpowiedzialność za przestrzeganie przepisów ustawy i RODO spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową.
3. Polityka bezpieczeństwa obowiązuje od dnia jej zatwierdzenia przez administratora danych.

Wykaz załączników:

1. instrukcja zarządzania systemem informatycznym
2. rejestr obszarów przetwarzania danych osobowych
3. rejestr zbiorów danych osobowych
4. opis przepływu danych
5. rejestr czynności przetwarzania z charakterystyką zbiorów danych osobowych
6. formularz rejestracji incydentu
7. rejestr zabezpieczeń
8. wzór umowy powierzenia danych osobowych
9. rejestr umów powierzenia danych osobowych
10. wzór oświadczenia poufności
11. wzór upoważnienia do przetwarzania danych osobowych
12. rejestr osób upoważnionych do przetwarzania danych osobowych
13. regulamin ochrony danych osobowych

_____	_____	_____
Pieczęć firmowa	Podpis administratora danych	Data