1 WSTĘP

Polityka Bezpieczeństwa Informacji (PBI) jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

PBI stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

2 OCENA SKUTKÓW (ANALIZA RYZYKA)

Ocena skutków jest formalną, określoną w art. 37 RODO procedurą przeprowadzenia analizy ryzyka. Jeżeli Administrator nie jest zobowiązany do przeprowadzenia oceny skutków, może mimo to stosować poniższą procedurę do przeprowadzenia analizy ryzyka na potrzeby wykazania rozliczalności spełnienia wymagań RODO.

W przypadku powołania Inspektora Ochrony Danych – ocena skutków musi być wykonana z jego współudziałem.

Inspektor Ochrony Danych (IOD) odpowiedzialny jest za:

1. Informowanie ADO o obowiązkach spoczywających na nim na podstawie Rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie w tej sprawie.
2. Monitorowanie przestrzegania Rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk ADO w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty.
3. Udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 Rozporządzenia.
4. Współpracę z Urzędem Ochrony Danych Osobowych.
5. Pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 Rozporządzenia, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

6. Pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia.
7. Doradzanie ADO w zakresie wdrożenia stosownych środków fizycznych, organizacyjnych i technicznych w celu zapewnienia bezpieczeństwa danych osobowych.
8. Sporządzanie na żądanie opinii w zakresie zabezpieczenia danych osobowych.
9. Sporządzanie wzorów dokumentów oraz zapisów umownych dotyczących ochrony danych osobowych.
10. Sporządzanie na żądanie opinii na temat sposobu wykonania obowiązku informacyjnego oraz opracowywanie wzorów stosownych zapisów dotyczących zgody na przetwarzanie danych osobowych.
11. Udział w przeglądach i aktualizacji wewnętrznych aktów normatywnych w zakresie ochrony danych osobowych.
12. Opiniowanie umów w zakresie ochrony danych osobowych.
13. Przygotowywanie propozycji odpowiedzi na skargi osób trzecich w zakresie ochrony danych osobowych.
14. Współpraca z organami ścigania, wymiaru sprawiedliwości oraz egzekucyjnymi w zakresie udzielania informacji (na podstawie osobnego pełnomocnictwa, udzielonego przez ADO).
15. Prowadzenie rejestru zbiorów/czynności przetwarzania danych osobowych przetwarzanych przez ADO.
16. Współpraca z ADO oraz kierownikami poszczególnych komórek organizacyjnych
    w zakresie analizy ryzyka dotyczącej ochrony danych osobowych.
17. Organizowanie szkoleń dla pracowników ADO w zakresie ochrony danych osobowych:
    a) minimum raz w roku dla wszystkich pracowników,
    b) za każdym razem dla nowego przyjętego pracownika.

Inspektora Ochrony Danych wspiera zgodnie ze swoimi kompetencjami **Administrator Systemów Informatycznych** oraz odpowiada za zapewnianie przestrzegania przepisów o ochronie danych osobowych, a w szczególności za:

1. Nadzorowanie opracowania i aktualizowania dokumentacji, opisującej sposób przetwarzania danych w systemach informatycznych, oraz przestrzegania zasad w niej określonych.

Upoważnienia dla **Inspektora Ochrony Danych i Administratora Systemów Informatycznych** stanowią **Załącznik nr 1 do PBI.**

2.1 CZYNNOŚCI PRZETWARZANIA (INWENTARYZACJA AKTYWÓW)

1. W celu dokonania analizy ryzyka wymagane jest zidentyfikowanie danych osobowych, które należy zabezpieczyć. Dane te w postaci zbiorów (kategorii osób) zostały wykazane w **Rejestrze Czynności Przetwarzania Danych Osobowych** stanowiącym **Załącznik nr 2 do PBI.**
2. Rejestr Czynności Przetwarzania Danych Osobowych powinien obejmować takie informacje, jak:
   a) opis kategorii osób, których dane dotyczą (nazwę zbioru),
   b) opis kategorii danych osobowych,
   c) cele przetwarzania,
   d) kategorie odbiorców,
   e) jeśli jest to możliwe planowane terminy usunięcia poszczególnych kategorii danych,
   f) jeśli jest to możliwe ogólny opis technicznych i organizacyjnych środków bezpieczeństwa,

   oraz dodatkowe informacje:
   g) funkcjonalny opis czynności przetwarzania (proces przetwarzania),
   h) aktywa służące do przetwarzania danych osobowych (Informacje, Programy i Systemy operacyjne, Infrastruktura IT, Infrastruktura, Pracownicy i współpracownicy, Outsourcing).

2.2 OCENA NIEZBĘDNOŚCI ORAZ PROPORCJONALNOŚCI (ZGODNOŚĆ Z PRZEPISAMI RODO)

W ramach przeprowadzenia oceny skutków (analizy ryzyka) Administrator/ Podmiot przetwarzający dane osobowe zobowiązany jest do spełnienia wobec nich obowiązków prawnych. W szczególności należy zapewnić, że:

1. Dane te są legalnie przetwarzane (na podstawie art. 6, 9).
2. Dane te są adekwatne w stosunku do celów przetwarzania.
3. Dane te są przetwarzane przez określony czas (retencja danych).
4. Wobec osób, których dane są przetwarzane 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).
5. Opracowano **Klauzule Informacyjne** dla powyższych osób oraz podmiotów zgodnie z **Załącznikiem nr 3a i 3b do PBI.**
6. Opracowano **Umowy Powierzenia** z podmiotami przetwarzającymi (art. 28) zgodnie z **Załącznikiem nr 4 do PBI.**

2.3 ANALIZA RYZYKA

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.

Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru lub grupy zbiorów (kategorii osób) lub dla procesów przetwarzania (np. dla zbioru pracowników).

2.3.1 Definicje

1. Aktywa – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych.
2. Naruszenie (Incydent) ochrony danych osobowych - 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.
3. Zagrożenie - potencjalne naruszenie (potencjalny incydent).
4. Skutki - rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia).
5. Ryzyko - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów.

2.3.2 Wyznaczenie zagrożeń

1. Administrator jest odpowiedzialny za określenie listy zagrożeń naruszenia poufności, dostępności i integralności, które mogą wystąpić w przetwarzaniu danych w zbiorze, lub w procesie przetwarzania.
2. Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zidentyfikowanych aktywów.

2.3.3 Wyliczenie ryzyka dla zagrożeń

1. Administrator określa Prawdopodobieństwo (**P**) wystąpienia poszczególnych zagrożeń w zbiorze lub w procesie przetwarzania.
2. Proponowaną skalę prawdopodobieństwa prezentuje Tabela A.
3. Administrator określa Skutki (**S**) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne.
4. Proponowaną Skalę skutków prezentuje Tabela B.
5. Administrator wylicza Ryzyka (R) dla wszystkich zagrożeń i ich skutków w/g formuły: **R = P * S**

Tabela A PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	**SKALA (WAGA)**
zagrożenie bardzo niskie	0,1-0,2
zagrożenie niskie	0,3-0,4
zagrożenie średnie	0,5-0,6
zagrożenie wysokie	0,7-0,8
zagrożenie bardzo wysokie	0,9-1

Tabela B SKUTKI WYSTĄPIENIA ZAGROŻENIA	**SKALA (WAGA)**
małe (do 10000 PLN, incydent prasowy lokalny)	1-2
średnie (10000-100000 PLN, incydent prasowy ogólnopolski)	3-8
duże (od 100000 PLN, naruszenie prawa)	9-10

2.3.4 Porównanie wyliczonych ryzyk ze skalą i określenie dalszego postępowania z ryzykiem

1. Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem.
2. Proponowaną skalę Ryzyka prezentuje Tabela C.

Tabela C POZIOM RYZYKA	**WARTOŚĆ [R = P*S]**
ryzyko pomijalne i akceptowalne (akceptujemy)	1-2
ryzyko jest opcjonalne (akceptujemy albo obniżamy)	3-8
ryzyko jest nieakceptowalne (musimy obniżyć)	9-10

2.3.5 Reakcja na wartość ryzyka

1. Akceptacja ryzyka – zabezpieczenia są właściwe – brak potrzeby stosowania dodatkowych zabezpieczeń
2. Działania obniżające ryzyko, które może zastosować Administrator:
    a. Przeniesienie –przerzucenie ryzyka (outsourcing, ubezpieczenie)
    b. Unikanie – eliminacja działań powodujących ryzyko
3. Redukcja – zastosowanie zabezpieczeń w celu obniżenia ryzyka.
4. Analizę ryzyka przeprowadza się zgodnie z wzorem **Arkusza Analizy Ryzyka i Mapowania Procesów w Zakresie Ochrony Danych Osobowych** stanowiącym **Załącznik nr 5 PBI.**

2.3.6 Ponowna analiza ryzyka

Ponowna analiza ryzyka przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów, nowych procesów przetwarzania, zmiany prawne).

2.4 PLAN POSTĘPOWANIA Z RYZYKIEM

1. Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne zgodnie z **Planem Postępowania z Ryzykiem**, którego wzór stanowi **Załącznik nr 6 do PBI**.
2. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń.

3 UPOWAŻNIENIA

1. Administrator odpowiada za nadawanie/anulowanie upoważnień do przetwarzania danych w zbiorach papierowych, systemach informatycznych zgodnie z procedurą określoną w **Regulaminie Ochrony Danych Osobowych** stanowiącym **Załącznik nr 7 do PBI.**
2. Wzór **Upoważnienia** stanowi **Załącznik nr 8 do PBI**.
3. Wzór **Rejestru Osób Przetwarzających Dane Osobowe w Podmiocie Posiadających Upoważnienie** stanowi **Załącznik nr 9 do PBI**. Administrator (Inspektor Ochrony Danych) prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych. Ewidencja ma charakter pomocniczy i nie jest wymagana przepisami RODO. Ewidencja prowadzona jest w oprogramowaniu.

4 POSTĘPOWANIE Z NARUSZENIAMI OCHRONY DANYCH OSOBOWYCH I INCYDENTAMI ZAGRAŻAJĄCYMI BEZPIECZEŃSTWU DANYCH OSOBOWYCH

1. Postępowanie z naruszeniami ochrony danych osobowych określa niniejsze PBI, w tym procedura opisana w **Regulaminie Ochrony Danych Osobowych** stanowiącym **Załącznik nr 7 do PBI, która** 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.
2. W przypadku stwierdzenia wystąpienia incydentu, Administrator prowadzi postępowanie wyjaśniające w toku, którego:
   a) ustala zakres i przyczyny incydentu oraz jego ewentualne skutki,
   b) inicjuje ewentualne działania dyscyplinarne,
   c) działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu,
   d) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.
3. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, Administrator zgodnie z art. 33 RODO 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.
4. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze zgodnie z **Rejestrem Naruszeń Danych Osobowych i Incydentów Zagrażających Bezpieczeństwu Danych Osobowych**, którego wzór **Załącznik nr 10 do PBI.**

5 AUDYTY

1. Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.
2. Celem audytów wewnętrznych jest ocena czy system ochrony danych osobowych jest skutecznie wdrożony i funkcjonuje zgodnie z wymaganiami RODO. Audyty prowadzone są w sposób obiektywny i bezstronny. Przestrzegana jest zasada, że audytorzy nie audytują własnej pracy.
3. Administrator (ewentualnie IOD):

   a) jest odpowiedzialny za przeprowadzanie audytów wewnętrznych:

      a. zgodnie z **Planem Audytów w Zakresie Ochrony Danych Osobowych,** którego wzór stanowi **Załącznik nr 11 do PBI** tzw. **audyty planowe,**
      b. **nieplanowych tzw. wyrywkowych,**
      c. doraźnie **w przypadku incydentu,**

   b) opracowuje programy audytów biorąc pod uwagę ważność procesów przetwarzania oraz audytowanych obszarów, jak też wyniki wcześniejszych audytów.
   c) ew. wyznacza audytora do przeprowadzenia audytu,

4. Audytor jest zobowiązany do:

   a) przygotowania się do przeprowadzenia audytu, zapoznając się z opisem audytowanego obszaru, stosowanych procedur i wyników poprzednich audytów,
   b) realizacji działań audytowych mających na celu uzyskanie obiektywnych dowodów potwierdzających poprawność realizowanych zadań, procedur, polityk, zabezpieczeń, celów, spełniania wymagań RODO,
   c) z identyfikowania tzw. uchybienia lub spostrzeżenia w przypadku stwierdzenia uchybień mających wpływ na skuteczność działania systemu ochrony danych zgodnego z RODO,
   d) udokumentowania wyniku audytu w postaci sporządzenia **Notatki z Czynności Przeprowadzonych w Toku Audytu w Zakresie Ochrony Danych Osobowych** zgodnie z **Załącznikiem nr 12 do PBI** i przekazania Administratorowi (ewentualnie IOD w przypadku, gdy nie jest audytorem).

5. Administrator (ewentualnie IOD) dokonuje przeglądu i analizy wyniku audytu
   oraz decyduje o inicjowaniu działań korygujących, w przypadku zaistnienia poważnych uchybień.

6 ZABEZPIECZENIA

Administrator stosuje stosowane zabezpieczenia w celu ochrony danych osobowych, w tym m.in.:

1. Opisane w Instrukcji **Zarządzania Systemem Informatycznym,** stanowiącej **Załącznik nr 13 do PBI,** zabezpieczenia proceduralne oraz zabezpieczenia jako środki techniczne i organizacyjne.
2. **Regulamin Ochrony Danych Osobowych** stanowiący **Załącznik nr 7 do PBI,** mający na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania.

7 POSTANOWIENIA KOŃCOWE

1. Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania zgodnie z **Klauzulą Poufności**, której wzór stanowi patrz **Załącznik nr 14 do PBI**.
2. W sprawach nieuregulowanych w niniejszym dokumencie zastosowanie mają odpowiednie przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016) oraz ustawy o ochronie danych osobowych z dnia 10 maja 2018 r.

Administrator

….....
Podpis

Inspektor Ochrony Danych	Administrator Systemów Informatycznych
….....…....	.....
Podpis	Podpis