

Polityka Ochrony Danych Osobowych

PRZEDSIĘBIORSTWO HANDLOWO USŁUGOWE „KYUBI” Paweł Kubiak

Gorczyn 77, 98-100 Łask

1	Wstęp.....	2
1.1	Definicje.....	2
1.2	Zasady ogólne przetwarzania danych osobowych.....	4
2	Ocena skutków (analiza ryzyka)	6
2.1	Opis operacji przetwarzania (inwentaryzacja aktywów)	6
2.2	Ocena niezbędności oraz proporcjonalności (zgodność z przepisami RODO)	6
2.3	Analiza ryzyka	7
2.4	Plan postępowania z ryzykiem	9
3	Upoważnienia	9
4	Instrukcja postępowania z incydentami.....	10
5	Regulamin Ochrony Danych Osobowych	11
6	Szkolenia	11
7	Rejestr czynności przetwarzania	11
8	Audyty	12
9	Procedura przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego (BCP)	12
10	Wykaz zabezpieczeń.....	12

1 WSTĘP

Polityka Ochrony Danych Osobowych 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).

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

1.1 DEFINICJE

Administrator (danych) - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

RODO – rozporządzenie parlamentu europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016)

Dane osobowe - to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną poprzez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden lub więcej czynników specyficznych dla fizycznego, fizjologicznego, genetycznego, umysłowego, ekonomicznego, kulturowego lub społecznego. tożsamość tej osoby fizycznej.

Przetwarzanie danych osobowych to dowolna zautomatyzowana lub niezautomatyzowana operacja lub zestaw operacji wykonywanych na danych osobowych lub w zestawach danych osobowych i obejmuje zbieranie, rejestrowanie, organizowanie, strukturyzowanie, przechowywanie, adaptację lub zmianę, wyszukiwanie, konsultacje, wykorzystanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, wyrównanie lub połączenie, ograniczenie, usunięcie lub zniszczenie danych osobowych.

Ograniczenie przetwarzania - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania

Anonimizacja- zmiana danych osobowych w wyniku której dane te tracą charakter danych osobowych

Zgoda osoby, której dane dotyczą - oznacza dowolne, dowolnie określone, konkretne, świadome i jednoznaczne wskazanie osoby, której dane dotyczą, za pomocą oświadczenia lub wyraźnego działania potwierdzającego, wyrażającego zgodę na przetwarzanie danych osobowych z nim związanych. Zgoda musi być udokumentowana we właściwy sposób, aby ją udowodnić.

Ocena skutków w ochronie danych - to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo i, jeśli to konieczne, z uczestnictwem inspektora ochrony 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.

Podmiotem danych jest każda osoba fizyczna, która jest przedmiotem przetwarzanych danych.

Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

Podmiot przetwarzający (Processor) to osoba fizyczna lub prawna, organ publiczny, agencja lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu administratora.

Inspektor Ochrony Danych (IOD) - to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi/Podmiotowi przetwarzającemu/pracownikom w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego.

Pseudonimizacja - oznacza 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.

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 naturalnego życia seksualnego osoby lub orientację seksualną. W zależności od obowiązującego prawa, specjalne kategorie danych osobowych mogą również zawierać informacje o środkach zabezpieczenia społecznego lub postępowaniach administracyjnych i karnych oraz o sankcjach.

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.

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.

1.2 ZASADY OGÓLNE PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator przetwarza dane osobowe w oparciu o:
 - 1) Legalność- Administrator dba o ochronę prywatności i przetwarza dane zgodnie z prawem;
 - 2) Bezpieczeństwo- Administrator zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stałe działania w tym zakresie;
 - 3) Prawa jednostki- Administrator umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje;
 - 4) Rozliczalność- Administrator dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność przetwarzania z RODO.

2. Administrator przetwarza dane w osobowe z poszanowaniem następujących zasad:
 - 1) W oparciu o podstawę prawną i zgodnie z prawem (legalizm);
 - 2) Rzetelnie i uczciwie (rzetelność);
 - 3) W sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
 - 4) W konkretnych celach i nie „na zapas” (minimalizacja);
 - 5) Nie więcej niż potrzeba (adekwatność);
 - 6) Z dbałością o prawidłowość danych (prawdziwość);
 - 7) Nie dłużej niż potrzeba (czasowość);

8) Zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo);

3. System ochrony danych osobowych Administratora składa się z następujących elementów:

- 1) **Inwentaryzacja danych**- proces polegający na zidentyfikowaniu zbiorów danych osobowych, zawierający w szczególności:
 - 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
- 2) **Rejestr czynności przetwarzania**- Administrator prowadzi rejestr czynności przetwarzania jeśli przepisy RODO nakładają na niego taki obowiązek. W celu ustalenia konieczności prowadzenia rejestru czynności przetwarzania, Administrator posiłkowo przeprowadza analizę ryzyka naruszenia praw lub wolności osób, których dane dotyczą. Szczegółowe zasady analizy ryzyka określa pkt 2.3 niniejszej Polityki.
- 3) **Obsługa praw jednostki**- Administrator spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
 - a. Obowiązki informacyjne- Administrator przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków;
 - b. Możliwość wykonania żądań- Administrator weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających;
 - c. Obsługa żądań- Administrator zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO i dokumentowane;
 - d. Zawiadomienie o naruszeniach- Administrator stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

- 4) Ocena skutków- szczegółowy zasady przeprowadzenia oceny skutków opisana została w procedurze określonej w Rozdziale 2 niniejszej Polityki.

2 OCENA SKUTKÓW (ANALIZA RYZYKA)

Ocena skutków jest formalną, określoną w art. 35 RODO procedurą przeprowadzenia analizy ryzyka za wykonanie której odpowiada Administrator. 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.

2.1 OPIS OPERACJI 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 [załączniku nr 1- 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

2.2 OCENA NIEZBĘDNOŚCI ORAZ PROPORCJONALNOŚCI (ZGODNOŚĆ Z PRZEPISAMI RODO)

W ramach przeprowadzenia oceny skutków (analizy ryzyka) Administrator 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 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)
5. opracowano klauzule informacyjne dla powyższych osób,
6. istnieją umowy powierzenia z podmiotami przetwarzającymi (art. 28), wykaz podmiotów przetwarzających prowadzony jest w [załączniku nr 3 Rejestr umów powierzenia](#)
7. potwierdzenie spełnienia powyższych wymagań prawnych RODO znajduje się w [załączniku nr 1 Wykaz zbiorów danych osobowych](#) oraz/lub w [załączniku nr 2 Rejestr czynności prowadzony przez Administratora](#).

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, zbioru klientów, dla procesu wysyłania informacji handlowej z bazy marketingowej banku)

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

Wyznaczenie zagrożeń

1. Administrator jest odpowiedzialny za określenie listy zagrożeń, które mogą wystąpić w przetwarzaniu danych w zbiorze, dla kategorii osób lub w procesie przetwarzania

- Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zidentyfikowanych aktywów

Wyliczenie ryzyka dla zagrożeń

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

Tabela A PRAWDOPODOBIENSTWO WYSTĄPIENIA ZAGROŻENIA	SKALA (WAGA)
zagrożenie niskie	1
zagrożenie średnie	2
zagrożenie wysokie	3

Tabela B SKUTKI WYSTĄPIENIA ZAGROŻENIA	SKALA (WAGA)
małe (do 5000 PLN, rozmiar naruszeń- nieprzekraczający 10 osób)	1
średnie (<5000-10000 PLN, rozmiar naruszeń <10- 50 osób)	2
duże (<10000 PLN, rozmiar naruszeń <50 osób)	3

Porównanie wyliczonych ryzyk ze skalą i określenie dalszego postępowania z ryzykiem

- Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem
- 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)	3-6

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 (np. zakaz wnoszenia komputerów przenośnych poza obszar organizacji)
 - c. Redukcja – zastosowanie zabezpieczeń w celu obniżenia ryzyka (np. zaszyfrowanie pendrivów z danymi wnoszonych poza firmę)
3. Analizę ryzyka przeprowadza się w specjalnym szablonie (programie) [Załączniku nr 4- Arkusz analizy ryzyka RODO](#)

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
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.
2. Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa.
3. Upoważnienia nadawane są do zbiorów przez Administratora. Upoważnienia określają zakres operacji na danych zgodnie z [załącznikiem nr 5 Upoważnienie do przetwarzania danych osobowych](#).
4. Upoważnienia mogą być nadawane w formie poleceń, np. upoważnienia do przeprowadzenia kontroli, audytów, wykonania czynności służbowych, udokumentowanego polecenia administratora w postaci umowy powierzenia.

4 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 upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu bezpośredniego przełożonego
2. Do typowych podatności bezpieczeństwa danych osobowych należą w szczególności:
 - 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 / ekranu, ochrony hasel, niezamykanie pomieszczeń, szaf, biurek);
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
 - a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
 - b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardej dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych);
 - c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania)
4. W przypadku stwierdzenia wystąpienia incydentu, Administrator (lub w przypadku powołania – IOD) 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.

5. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze w [załączniku nr 6- Formularz Rejestracji Incydentu](#).
6. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych.
7. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorcemu.

5 REGULAMIN OCHRONY DANYCH OSOBOWYCH

Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania.

Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania.

6 SZKOLENIA

1. Każda osoba przed dopuszczeniem do pracy z danymi osobowymi winna być poddana przeszkoleniu i zapoznana z przepisami RODO.
2. Za przeprowadzenie szkolenia odpowiada Administrator.
3. Po przeszkoleniu z zasad ochrony danych osobowych, uczestnicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania.

7 REJESTR CZYNNOŚCI PRZETWARZANIA

Administrator prowadzi rejestr czynności przetwarzania jeśli przepisy RODO nakładają na niego taki obowiązek. W rejestrze tym zamieszcza się wszystkie następujące informacje:

- a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów,
a także gdy ma to zastosowanie - przedstawiciela administratora oraz inspektora ochrony danych;
- b) cele przetwarzania;
- c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;

- d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
- e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;
- f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
- g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.

8 AUDYTY

Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

W tym celu Administrator stosuje procedurę audytów – [załącznik nr 7](#)

9 PROCEDURA PRZYWRÓCENIA DOSTĘPNOŚCI DANYCH OSOBOWYCH I DOSTĘPU DO NICH W RAZIE INCYDENTU FIZYCZNEGO LUB TECHNICZNEGO (BCP)

Zgodnie z art. 32 RODO, Administrator powinien zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego. Administrator opracował procedury przywracania, opisane w [załączniku nr 8](#).

10 WYKAZ ZABEZPIECZEŃ

1. Administrator prowadzi szczegółowe procedury które stosuje w celu ochrony danych osobowych wraz z wykazem zabezpieczeń, zgodnie z [Instrukcją zarządzania RODO](#).
2. W Instrukcji wskazano stosowane zabezpieczenia proceduralne oraz zabezpieczenia jako środki techniczne i organizacyjne.
3. Instrukcja jest aktualizowana po każdej analizie ryzyka / ocenie skutków.