ZARZĄDZENIE nr 31/2025

Wójta Gminy Czernikowo

z dnia 24 marca 2025 r.

w sprawie ustalenia metodyki analizy ryzyka naruszenia praw i wolności osób fizycznych oraz oceny skutków dla ochrony danych w Urzędzie Gminy Czernikowo

Na podstawie art. 24 pkt 1 i 35 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) (Dz. Urz. UE L Nr 119 s. 1) zarządza się, co następuje:

§ 1. W celu zapewnienia skutecznej realizacji procesu zarządzania ryzykiem bezpieczeństwa danych osobowych w Urzędzie Gminy Czernikowo ustala się metodykę analizy ryzyka naruszenia praw i wolności osób fizycznych oraz oceny skutków dla ochrony danych w Urzędzie Gminy Czernikowo, stanowiące załącznik do niniejszego Zarządzenia.

§ 2. Wykonanie Zarządzenia powierza się kierownikom komórek organizacyjnych oraz pozostałym pracownikom Urzędu Gminy Czernikowo.

§ 3. Zarządzenie wchodzi w życie z dniem 24 marca 2025 r.

Wójt
Gminy Czernikowo
Tomasz Krasicki

Załącznik do Zarządzenia Nr 31/2025
z dnia 24 marca 2025 r.

Metodyka analizy ryzyka naruszenia praw i wolności osób fizycznych oraz oceny skutków dla ochrony danych w Urzędzie Gminy Czernikowo

Załącznik do Zarządzenia Nr 31/2025
z dnia 24 marca 2025 r.

§ 1 WSTĘP

Mając na względzie obowiązek określenia w procesie przetwarzania danych osobowych prawdopodobieństwa i skutków ryzyka naruszenia praw lub wolności osób, których przetwarzanie dotyczy, Administrator wprowadza do stosowania metodykę szacowania ryzyka oraz oceny skutków dla ochrony danych (DPIA) w stosunku do aktualnie prowadzonych, jak i planowanych operacji przetwarzania danych osobowych.

Administrator ma świadomość odpowiedzialności prawnej w kontekście przetwarzanych danych osobowych, dlatego wdraża takie środki techniczne, organizacyjne i informatyczne, które zapewnią bezpieczeństwo przetwarzanych danych osobowych. Zastosowane środki techniczne, organizacyjne i informatyczne podlegają doskonaleniu.

Administrator w procesie przetwarzania danych uwzględnia ochronę danych osobowych w fazie projektowania z uwzględnieniem zasady domyślnej ochrony danych.

Administrator ma świadomość, iż prowadzenie Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA) jest procesem ciągłym, a nie jednorazowym.

§ 2 ANALIZA RYZYKA NARUSZENIA PRAW I WOLNOŚCI OSÓB FIZYCZNYCH I OCENA SKUTKÓW DLA OCHRONY DANYCH

1. Ilekroć jest mowa o:

1) **Administratorze Danych Osobowych (ADO)** – należy przez to rozumieć Wójta Gminy Czernikowo, nazywany również Podmiotem;
2) **RODO** – należy przez to rozumieć 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 Nr 119 s. 1);
3) **Inspektorze Ochrony Danych (IOD)** – osoba wyznaczona na podstawie art. 37 ust. 1 lit. a) RODO;
4) **Informatyku** - osoba wyznaczona przez administratora odpowiedzialna za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych do przetwarzania danych osobowych, zwany dalej informatykiem. W przypadku niewyznaczenia informatyka, jego obowiązki wykonuje administrator lub wykonywanie zadań w zakresie obsługi informatycznej może także zostać powierzone zewnętrznej firmie specjalizującej się w obsłudze TI;
5) **aktywach** – należy przez to rozumieć wszystko to, co ma wartość administratora danych osobowych przetwarzanych; do aktywów (podstawowych i wspierających) zaliczyć można procesy przetwarzania danych osobowych, wszelkie informacje dotyczące funkcjonowania podmiotu, w tym przetwarzane dane osobowe, pracowników, siedzibę, organizację, sprzęt, oprogramowanie informatyczne, czy sieć komputerową;
6) **naczelniku/kierowniku** – należy przez to rozumieć osoby kierujące komórkami, działającymi na prawach wydziału/referatu, komórkami organizacyjnymi w Urzędzie Gminy Czernikowo;
7) **istotności ryzyka** – należy przez to rozumieć iloczyn prawdopodobieństwa wystąpienia ryzyka oraz potencjalnego wpływu jego wystąpienia;
8) **kontekście** – należy przez to rozumieć wszystkie informacje wiążące się z działaniem podmiotu, w tym informacje dotyczące środowiska prawnego, społecznego, finansowego czy też technologicznego, np. przepisy prawne, obowiązujące procedury wewnętrzne;

9) **podatności** – należy przez to rozumieć słabość, która może być wykorzystana przez zagrożenie, powodując niekorzystne skutki dla danego podmiotu, jak np. luka w systemie informatycznym;
10) **ryzyku** – należy przez to rozumieć możliwość zaistnienia zdarzenia, które będzie miało wpływ na realizację założonych celów; ryzyko jest mierzone wpływem (skutkami) oraz prawdopodobieństwem wystąpienia;
11) **Zasadach** – należy przez to rozumieć Zasady i tryb zarządzania ryzykiem bezpieczeństwa danych osobowych;
12) **Zespole** – należy przez to rozumieć wyznaczonych pracowników do przeprowadzenia procedury szacowania ryzyka.

2. Celem opracowanej metodyki jest ustalenie sposobu zarządzania ryzykiem bezpieczeństwa danych osobowych przetwarzanych w podmiocie z uwzględnieniem ryzyka naruszenia praw lub wolności osób fizycznych, których dane dotyczą.
Metodyka określa:
1) Analizę Ryzyka Ogólnego,
2) Ocenę Skutków Dla Przetwarzania Danych (DPIA).

3. Wynikiem przeprowadzonego procesu szacowania ryzyka jest określenie adekwatnych, do zagrożeń i prawdopodobieństwa ich wystąpienia, środków technicznych, organizacyjnych i informatycznych niezbędnych do osiągnięcia akceptowalnego poziomu ryzyka.
1) Zarządzanie ryzykiem ma na celu podejmowanie działań zmierzających do podnoszenia poziomu bezpieczeństwa ochrony danych osobowych przetwarzanych w podmiocie uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych. Oznacza to między innymi, że dane osobowe przetwarzane przez administratora powinny być zabezpieczone przed nieuprawnionymi zmianami, ujawnieniem nieupoważnionym osobom, zniszczeniem, utratą lub uszkodzeniem. Czynności podejmowane w ramach tych działań oraz zastosowane środki techniczne, organizacyjne i informatyczne będą zależne od środowiska, w jakim dane są przetwarzane;
2) Pojęcie ochrony danych należy utożsamiać z pojęciem bezpieczeństwa informacji, stosowanym w literaturze z zakresu bezpieczeństwa teleinformatycznego. Wg normy PN-ISO/IEC-17799:2005[2] przez bezpieczeństwo informacji należy rozumieć zachowanie poufności, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności i niezawodności. Wymienione właściwości, wg definicji zawartych w PN-I13335-1[3], polegają odpowiednio na:
   a) **Poufność danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
   b) **Integralność danych** – rozumie się przez to właściwość zapewniającą, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
   c) **Dostępność** - zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne,
   d) **Rozliczalność** – zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
   e) **Autentyczność** – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji),

f) **Niezaprzeczalność** – brak możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie,

g) **Niezawodność** – zapewnieniu spójności oraz zamierzonych zachowań i skutków.

3) Poprzez zarządzanie ryzykiem bezpieczeństwa ochrony danych osobowych należy rozumieć działania polegające na:

a) identyfikacji czynności,
b) określeniu zagrożeń,
c) szacowaniu ryzyka,
d) postępowaniu z ryzykiem,
e) akceptowaniu ryzyka,
f) monitorowaniu ryzyka,
g) informowaniu o ryzyku w odniesieniu do zidentyfikowanego procesu przetwarzania danych osobowych.

4. Monitorowanie procesu zarządzania ryzykiem bezpieczeństwa danych osobowych w podmiocie i dokumentowanie tych czynności jest elementem wywiązania się z obowiązku ciążącego na ADO – zapewnienia przetwarzania zgodnego z ogólnym rozporządzeniem o ochronie danych.

5. Osoby wyznaczone przez ADO biorą udział i monitorują prawidłowe funkcjonowanie procesu zarządzania ryzykiem bezpieczeństwa danych osobowych w podmiocie. Zapewniają i odpowiadają za systematyczną identyfikację zagrożeń i zabezpieczeń, ocenę ich wpływu na ryzyko oraz postępowanie z ryzykiem bezpieczeństwa danych osobowych w podmiocie, w celu zapewnienia zgodnego z RODO przetwarzania oraz dokumentowania całego procesu zarządzania ryzykiem, spełniając tym samym wymóg rozliczalności podejmowanych działań.

6. Na analizę ryzyka składa się: szacowanie ryzyka, postępowanie z ryzykiem oraz akceptowanie ryzyka.

1) Szacowanie ryzyka ma na celu określenie co może się zdarzyć (kiedy, gdzie, jak i dlaczego) oraz jak dotkliwe straty mogą powstać i polega na:

a) identyfikowaniu zagrożeń,
b) analizie ryzyka,
c) ocenie ryzyka;

2) W ramach identyfikacji zagrożeń określany jest:

a) Kontekst,
b) identyfikacja aktywów,
c) identyfikacja zagrożeń,
d) identyfikacja istniejących zabezpieczeń,
e) identyfikacja podatności,
f) identyfikacja następstw – skutków;

3) Posiadając zidentyfikowane aktywa, zagrożenia oraz zastosowane zabezpieczenia można przeprowadzić identyfikację podatności na urzeczywistnienie się określonych zagrożeń. Istotne jest, że samo istnienie podatności nie powoduje jeszcze szkody. Jej powstanie jest możliwe dopiero po zmaterializowaniu się zagrożenia, które wykorzysta daną podatność. Analiza podatności dotyczy aktywów podstawowych: przetwarzanych danych i zastosowanych do przetwarzania urządzeń, jak i aktywów wspierających: sprzęt, oprogramowanie, sieć komputerowa, pracownicy, siedziba, organizacja;

4) W przypadku aktywów, jakimi są dane osobowe, podatnością może być sam fakt wykorzystania danych w innym celu niż zamierzony;
5) Podczas identyfikacji następstw wyznaczone osoby przez ADO określają rodzaj incydentów – niepożądanych lub niespodziewanych zdarzeń, sposób, w jaki dane zagrożenie może wykorzystać określoną podatność oraz przedstawiają jego skutki;
6) Dokonanie analizy ryzyka polega na:
   a) oszacowaniu następstw ze szczególnym uwzględnieniem możliwości naruszenia praw lub wolności osób fizycznych,
   b) oszacowaniu prawdopodobieństwa incydentu,
   c) określeniu poziomu ryzyka;
7) Oceniając następstwa urzeczywistnienia się zagrożeń, w przypadku danych osobowych, należy uwzględnić, poza innymi czynnikami, także dotkliwe, przewidziane w RODO kary finansowe, które mogą być nakładane przez organ nadzorczy na administratora i podmioty przetwarzające w przypadku niewywiązywania się przez nie z nałożonych obowiązków właściwej ochrony danych. Szacowanie następstw dla określonych zagrożeń powinno uwzględniać zarówno materialny, jak i niematerialny charakter;
8) Przyjmuje się, że zasadniczym rodzajem reakcji na ryzyko jest działanie lub przeniesienie ryzyka. Przeniesienie oznacza przekazanie ryzyka podmiotowi zewnętrznemu, np. ubezpieczenie budynku będącego siedzibą podmiotu, powierzenie przetwarzania danych osobowych w drodze umowy przy zastosowaniu zasad zgodnych z RODO, ze wskazanymi obowiązującymi normami, dobrymi praktykami. Działanie może obejmować w szczególności ustanowienie nowych lub zintensyfikowanie istniejących mechanizmów kontroli, a także działania o innym charakterze (np. przeszkolenie pracowników, wprowadzenie zmian organizacyjnych, wystąpienie o dodatkowe środki finansowe, wprowadzenie dodatkowych wymogów informacyjnych, podjęcie lub nasilenie działań kontrolnych itp.).

7. Proces szacowania ryzyka w sposób określony powyżej, kończy jego ocena i ustalenie planu postępowania z ryzykiem.
   1) Identyfikacja zagrożeń jest dokonywana w odniesieniu do czynności określanych dla przetwarzanych danych osobowych w Rejestrze Czynności Przetwarzania;
   2) Identyfikowanie zagrożeń można również przeprowadzać w działaniach doraźnych – każdorazowo, przy zmianie aktywa, jego zabezpieczeń lub otrzymania informacji, mającej wpływ na szacowanie ryzyka;
   3) Identyfikację zagrożeń w działaniach doraźnych – przeprowadza się, w przypadku:
      a) zaobserwowania zagrożenia dla systemu, którego zmaterializowanie się nastąpiło, w okresie krótszym, niż w czasie zaplanowanej okresowej identyfikacji ryzyk, a zwłoka w identyfikacji zagrożenia ma istotne znaczenie dla systemu,
      b) wystąpienia incydentu teleinformatycznego, którego skutkiem była utrata bezpieczeństwa informacji mająca charakter katastrofalny,
      c) przed oddaniem systemu do eksploatacji;

   4) Szacowanie ryzyka przeprowadza się nie rzadziej niż raz na trzy lata, a także w przypadku wystąpienia w podmiocie naruszenia ochrony danych osobowych o wadze krytycznej oraz ujawnienia nowej czynności w Rejestrze Czynności Przetwarzania.
8. Administrator przetwarza dane osobowe opisane w Rejestrze Czynności Przetwarzania, a także w Rejestrze Wszystkich Kategorii Przetwarzania. Dane są przetwarzane zarówno w formie dokumentacji tradycyjnej, jak i elektronicznej. Zgromadzone w ten sposób informacje stanowią

aktywa podmiotu, przez które należy rozumieć nie tylko dane osobowe będące w posiadaniu administratora, ale także inne zasoby tj. posiadana wiedza pracowników, sprzęt, oprogramowanie, środki techniczne i organizacyjne związane z przetwarzaniem danych osobowych. W politykach ochrony danych, politykach zarządzania systemem informatycznym oraz w Rejestrze Czynności Przetwarzania zawarto opis wprowadzonych zabezpieczeń organizacyjnych, technicznych i informatycznych zapewniających ochronę przetwarzanych danych osobowych. Z przetwarzanymi danymi osobowymi związane są aktywa główne i wspomagające
Określenie ich wartości, a także sklasyfikowanie czynności przetwarzania pod kątem konieczności przeprowadzania oceny skutków dla ochrony danych (DPIA) przeprowadzają osoby wyznaczone przez ADO.

Przyjęto skalę jakościową wartości danych osobowych przedstawioną w poniższej tabeli.

Wartość danych osobowych	Opis
Bardzo wysoka 4	Utrata bezpieczeństwa w zakresie poufności, integralności lub dostępności całkowicie uniemożliwia realizację danego procesu lub procesów. Utrata bezpieczeństwa w zakresie poufności, integralności lub dostępności może powodować bardzo poważne reperkusje prawne. Przetwarzana jest duża ilość danych wrażliwych lub danych o charakterze osobistym. Utrata bezpieczeństwa może prowadzić do poważnego naruszenia prywatności osoby fizycznej. Utrata bezpieczeństwa w zakresie poufności, integralności lub dostępności może powodować rozgłos medialny na skalę krajową
Wysoka 3	Utrata bezpieczeństwa w zakresie poufności, integralności lub dostępności może znacząco zakłócić realizację danego procesu lub procesów. Utrata bezpieczeństwa w zakresie poufności, integralności lub dostępności może powodować reperkusje prawne. Przetwarzana jest duża ilość danych zwykłych. Przetwarzana jest niewielka ilość danych wrażliwych lub danych o charakterze osobistym. Utrata bezpieczeństwa może prowadzić do ograniczonej utraty prywatności osoby fizycznej. Utrata bezpieczeństwa w zakresie poufności, integralności lub dostępności może powodować rozgłos medialny na skalę regionalną.
Średnia 2	Utrata bezpieczeństwa w zakresie poufności, integralności lub dostępności może utrudnić realizację danego procesu, jednak można przywrócić pracę łatwo dostępnymi środkami. Utrata bezpieczeństwa w zakresie poufności, integralności lub dostępności może powodować problemy natury prawnej. Utrata bezpieczeństwa w zakresie poufności, integralności lub dostępności może powodować umiarkowane zainteresowanie mediów lokalnych. Przetwarzane są dane zwykłe w dużych ilościach i regularnie.

Niska 1	Utrata bezpieczeństwa w zakresie poufności, integralności lub dostępności może w niewielkim stopniu utrudnić realizację danego procesu, jednak główne zadania w zakresie danego procesu mogą być nadal realizowane. Przetwarzane są dane zwykłe w niewielkich ilościach i sporadycznie

Sklasyfikowanie czynności przetwarzania pod kątem konieczności przeprowadzenia Oceny skutków dla ochrony danych (DPIA) następuje w oparciu o art. 35 RODO, w przypadku:

1) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
2) przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10;
3) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie,

oraz Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony oraz wytycznych Grupy Roboczej art. 29 WP 248 rew. 01 17/PL, zgodnie z którymi w sytuacji wystąpienia co najmniej dwóch z poniższych kryteriów należy przeprowadzić ocenę skutków dla ochrony danych:

1) Ewaluacja lub ocena, w tym profilowanie i przewidywanie (analiza behawioralna) w celach wywołujących negatywne skutki prawne, fizyczne, finansowe lub inne niedogodności dla osób fizycznych;
2) Zautomatyzowane podejmowanie decyzji wywołujących skutki prawne, finansowe lub podobne istotne skutki;
3) Systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie wykorzystujące elementy rozpoznawania cech lub właściwości obiektów, które znajdą się w monitorowanej przestrzeni. Do tej grupy systemów nie są zaliczane systemy monitoringu wizyjnego, w których obraz jest nagrywany i wykorzystywany tylko w przypadku potrzeby analizy incydentów naruszenia prawa;
4) Przetwarzanie szczególnych kategorii danych osobowych i dotyczących wyroków skazujących i czynów zabronionych (danych wrażliwych wg opinii WP 29);
5) Przetwarzanie danych biometrycznych wyłącznie w celu identyfikacji osoby fizycznej bądź w celu kontroli dostępu;
6) Przetwarzanie danych genetycznych;
7) Dane przetwarzane na dużą skalę, gdzie pojęcie dużej skali dotyczy: liczby osób, których dane są przetwarzane, zakresu przetwarzania, okresu przechowywania danych oraz geograficznego zakresu przetwarzania;
8) Przeprowadzanie porównań, ocena lub wnioskowanie na podstawie analizy danych pozyskanych z różnych źródeł;
9) Przetwarzanie danych dotyczących osób, których ocena i świadczone im usługi są uzależnione od podmiotów lub osób, które dysponują uprawnieniami nadzorczymi i/lub ocennymi;
10) Innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych;
11) Gdy przetwarzanie samo w sobie uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy;

12) Przetwarzanie danych lokalizacyjnych.

Wyniki identyfikacji czynności wraz z przypisanymi im wartościami oraz informacją dot. konieczności przeprowadzenia oceny skutków dla ochrony danych określa się wg wzoru stanowiącego załącznik nr 1.

9. Wyznaczone osoby przez ADO uczestniczą w analizie ryzyka, na którą składa się: szacowanie ryzyka, postępowanie z ryzykiem, akceptowanie ryzyka.
We wstępnej fazie analizy ryzyka określić należy rodzaje zagrożeń, ich źródła oraz kontekst przetwarzania danych, a także aktywa wspomagające.

Podczas identyfikacji ryzyka, należy przeanalizować źródła zagrożeń wraz z ich wewnętrznymi i zewnętrznymi uwarunkowaniami oraz możliwymi scenariuszami rozwoju wydarzeń.

Przykłady zagrożeń w obszarze przetwarzania i ochrony danych osobowych
(listę należy sukcesywnie uaktualniać poprzez analizowanie zagrożeń i ich modyfikację)
Zagrożenia dla bezpieczeństwa teleinformatycznego:

1) Utrata danych;
2) Wyciek danych;
3) Awaria sprzętu lub oprogramowania;
4) Brak lub nieaktualne oprogramowanie antywirusowe, dedykowane i operacyjne;
5) Przyznawanie użytkownikom uprawnień administratora;
6) Przechwycenie danych podczas teletransmisji;
7) Szkodliwe oprogramowanie;
8) Włamanie do sieci.

Zagrożenia dla bezpieczeństwa fizycznego:

1) Niewłaściwe zabezpieczenie przechowywanych dokumentów;
2) Zbyt długie przechowywanie danych papierowych lub danych w wersji elektronicznej;
3) Niewłaściwe niszczenie elektronicznych nośników informacji;
4) Brak niszczarek dokumentów tradycyjnych;
5) Brak podtrzymywania energii urządzeń informatycznych;
6) Brak lub nieodpowiednie zabezpieczenie strefy przetwarzania danych;
7) Dostęp do pomieszczeń dla osób nieuprawnionych;
8) Nieskuteczne zabezpieczenie przeciwpożarowe;
9) Zalanie pomieszczeń.

Zagrożenia dla bezpieczeństwa prawnego:

1) Zbieranie błędnych danych, stosowanie nieaktualnych druków i formularzy;
2) Przetwarzanie zbyt szerokiego zakresu danych;
3) Przetwarzanie niezgodnie z celem określonym w przepisach prawa;
4) Stosowanie nieaktualnych przepisów;
5) Konieczność dostosowania się do zmian w przepisach;
6) Problemy ze zgłaszaniem incydentów do organu nadzorującego;
7) Niewyznaczenie Inspektora Ochrony Danych;
8) Brak skutecznej kontroli zapisów umownych;
9) Nieskuteczna lub brak kontroli legalności przetwarzania danych;

10) Niewłaściwe realizowanie obowiązków informacyjnych;
11) Brak procedur realizowania praw osób, których dane dotyczą.

Zagrożenia dla bezpieczeństwa organizacyjno-osobowego:

1) Wykorzystanie prywatnego sprzętu informatycznego;
2) Nieumiejętne posługiwanie się oprogramowaniem i sprzętem IT;
3) Brak szkolenia personelu;
4) Niewystarczająca wiedza osób zaangażowanych w proces przetwarzania;
5) Brak skutecznego nadzoru nad bezpieczeństwem informacji;
6) Niefrasobliwe rozmowy;
7) Zbyt małe zaangażowanie w proces zabezpieczania danych;
8) Otwieranie korespondencji mailowej od niezaufanych nadawców;
9) Udostępnianie danych osobom nieupoważnionym;
10) Dopuszczanie do przetwarzania osób nieupoważnionych.

Zagrożenie wewnętrzne umyślne i nieumyślne:

1) Korzystanie w celach służbowych z prywatnej poczty elektronicznej;
2) Brak stosowania opcji „kopia ukryta" w korespondencji elektronicznej skutkującej; ujawnieniem adresów e-mail wszystkich odbiorców;
3) Wyrzucenie dokumentów do śmieci bez zniszczenia;
4) Udostępnianie haseł innym osobom;
5) Wynoszenie służbowych danych (bez zgody ADO);
6) Dopuszczanie do przetwarzania osób nieupoważnionych;
7) Otwieranie korespondencji mailowej od niezaufanych nadawców;
8) Przebywanie w pomieszczeniach osób nieupoważnionych bez nadzoru;
9) Upublicznienie nagrania z monitoringu wizyjnego w Internecie.

Zagrożenie zewnętrzne umyślne i nieumyślne:

1) Włamanie do biura;
2) Włamanie do systemu informatycznego;
3) Uruchomienie znalezionego laptopa;
4) Przeczytanie błędnie przesłanej korespondencji;
5) Niewłaściwe wykonanie umowy powierzenia danych;
6) Zastosowanie socjotechnik wobec użytkowników;
7) Udostępnienie WiFi w celu zapoznania się z zawartością urządzeń;
8) Przesłanie wiadomości e-mail ze złośliwym oprogramowaniem.

Identyfikację zagrożeń zgodnie z załącznikiem nr 2 przeprowadza zespół dokonujący szacowania oraz inne osoby wskazane przez administratora

Źródła ryzyka

Źródła ryzyka	Opis
Wewnętrzne źródło ludzkie działające przypadkowo	Pracownicy, praktykanci, stażyści, interesanci
Wewnętrzne źródło ludzkie działające celowo	Pracownicy, praktykanci, stażyści, interesanci
Zewnętrzne źródło ludzkie działające przypadkowo	Dostawcy usług, klienci, serwisanci, osoby sprzątające, interesanci

Zewnętrzne źródło ludzkie działające celowo	Hakerzy, goście, dawni pracownicy, konkurenci, organizacje przestępcze, interesanci
Wewnętrzne źródło inne niż ludzkie	Rury wodociągowe, materiały łatwopalne, technologia
Zewnętrzne źródło inne niż ludzkie	Malware, trojan, ransomware, wirus, katastrofy naturalne

Kontekstu przetwarzania

Na ryzyko w zakresie ochrony danych wpływają czynniki zarówno zewnętrzne, jak i wewnętrzne. Działalność podmiotu wiąże się ze spełnianiem oczekiwań wielu stron. Strony i ich oczekiwania stanowią kontekst działalności podmiotu, a oczekiwania względem przepływu i bezpieczeństwa informacji są kryteriami ryzyka, które powinno podlegać bieżącej analizie i ocenie. Elementy stanowiące zewnętrzny i wewnętrzny kontekst organizacyjny zostały zidentyfikowane i opisane w tabeli poniżej.

Kontekst zewnętrzny

Lp.	Podmioty	Wpływ podmiotu na aspekt (TAK/NIE)	Cel / wymagania / oczekiwania
1	Mieszkańcy	TAK	Oczekiwanie sprawnego działania, racjonalne kosztowo realizowanie zadań podmiotu publicznego.
2	Urząd Gminy	TAK	Sprawna realizacja zadań administracyjnych powierzonych podmiotowi publicznemu w tym zadania zlecone, podejmowanie działań w ramach ustalonego prawa, przestrzeganie przepisów
3	Instytucje publiczne regulujące pracę podmiotu	TAK	Sprawna realizacja zadań powierzonych
4	Jednostki organizacyjne innych podmiotów (szkoły, przedszkola, dom kultury, muzeum, GOPS, świetlica środowiskowa, OS i R, biblioteka, spółki gminne)	NIE	Utrzymanie wsparcia dla własnych jednostek organizacyjnych, w tym w zakresie dostarczania usług elektronicznych (łącze internetowe, hosting usług serwerowych, sprawna komunikacja z urzędem).
5	Organizacje pozarządowe na terenie gminy (kluby sportowe, organizacje pożytku publicznego)	TAK częściowo	Wsparcie dla działalności klubów, patronat nad wydarzeniami sportowymi.

6.	Podmioty przetwarzające administratora (umowy powierzenia)	TAK	Realizacja usług dla administratora powierzonych podmiotom zewnętrznym

Kontekst wewnętrzny

Lp.	Opis	Wpływ podmiotu na aspekt	Cele / wymagania / oczekiwania
1	Kadra kierownicza	TAK	Bezpieczeństwo zasobów informacyjnych, dostęp do bieżącej informacji zarządczej, unikanie i zapobieganie incydentom związanym z utratą bądź zniszczeniem danych.
2	Pracownicy	TAK	Bezpieczeństwo pracy użytkowników, dostępność środków wymiany informacji, uzyskiwanie informacji na poziomie umożliwiającym sprawne realizowanie powierzonych zadań, zabezpieczanie danych osobowych na stanowisku pracy
3	Systemy wsparcia informacji	TAK	Systemy wymiany informacji działają w oparciu o sprawną infrastrukturę sieciowo serwerową. Wymagają utrzymania jej na poziomie pozwalającym na sprawne przekazywanie danych między aplikacjami i bazami danych a terminalami. Utrzymanie sprawności funkcjonowania wymaga adekwatnych nakładów finansowych
4	Infrastruktura Informatyczna (sieci, węzły komunikacyjne, serwery)	TAK	Infrastruktura informatyczna pozwala na sprawne przekazywanie danych pomiędzy aplikacjami, bazami danych. Utrzymanie sprawności funkcjonowania wymaga adekwatnych nakładów finansowych
5	Obsługa informatyczna	TAK	Zatrudnia informatyka
6	Otoczenie prawne przepisy prawa	TAK	Wymaga ciągłej analizy i aktualizacji stosowanych przepisów
7	Administrator jako podmiot przetwarzający (umowy powierzenia)	TAK	Realizacja usług, zadań, celów w imieniu i na polecenia zewnętrznego podmiotu

Aktywa Wspomagające

Kategoria aktywów wspomagających	Rodzaje aktywów wspomagających	Opis aktywów wspomagających
Informatyczne	Sprzęt	Komputery, serwery, laptopy. Urządzenia peryferyjne – drukarki, skanery
	Nośniki danych	Używane są dyski twarde w komputerach stacjonarnych i laptopach, Pendrive, płyty CD/DVD. Do użytkowania dostępne są tylko Pendrive zarejestrowane, podlegają kontroli.
	Komunikacja elektroniczna	Sieć LAN
	Oprogramowanie	Systemy operacyjne, aplikacje, poczta elektroniczna, bazy danych. Systemem operacyjnym Windows 10, Microsoft Oprogramowanie licencjonowane, program antywirusowy.
Fizyczne	Lokalizacja	Pomieszczenia domowe, korzystanie z sieci internetowej domowej lub szkolnej
	Infrastruktura	Szafa zamykana na klucz zamykane drzwi.
Organizacyjne	Ludzie	Pracownicy podmiotów przetwarzających administratorzy IT.
	Dokumenty papierowe	Notatki
	Komunikacja tradycyjna	Poczta elektroniczna

10. Określenie prawdopodobieństwa wystąpienia ryzyka polega na ocenie możliwości wystąpienia danego zdarzenia. Do określenia prawdopodobieństwa stosowana jest następująca skala określona w poniższej tabeli:

Ocena	Poziom	Prawdopodobieństwo wystąpienia zdarzenia
1	**Bardzo niski**	Ryzyko praktycznie nie występuje
2	**Niskie (mało prawdopodobne)**	Ryzyko wystąpi z niskim prawdopodobieństwem
3	**Średni (umiarkowanie możliwy)**	Ryzyko wystąpi prawdopodobnie w niektórych okolicznościach
4	**Wysoki (prawdopodobny)**	Ryzyko wystąpi prawdopodobnie w większości okoliczności
5	**Bardzo wysokie (prawie pewny)**	Ryzyko wystąpi prawdopodobnie w większości okoliczności – prawie pewne zdarzenie

11. Określenie następstwa (skutku) ryzyka polega na ocenie przewidywanego stopnia konsekwencji zagrożeń dla bezpieczeństwa danych osobowych, w tym skutków dla osób fizycznych i podjęcia działań w celu ich zminimalizowania. Do określenia wpływu następstwa - skutku używana jest następująca skala, określona w poniższej tabeli:

Ocena	Skutek	Istotność ryzyka naruszenia praw i wolności osoby, której dane dotyczą
1	**Nieznaczny (pomijalny)**	Żaden lub bardzo niski wpływ na podmiot danych
2	**Niski (mało znaczący)**	U osoby dotkniętej naruszeniem wywoła ono drobne niedogodności. Niski wpływ na podmiot danych
3	**Średni**	Osoby mogą napotkać niedogodności. Średni negatywny wpływ na podmiot danych, który może doznać nieznacznej utraty prywatności lub którego prawa zostaną w nieznaczny sposób ograniczone
4	**Wysoki (poważny)**	Mogą wystąpić konsekwencje możliwe do pokonania, ale z poważnymi skutkami. Znaczący negatywny wpływ na podmiot danych, w tym częściowa utrata prywatności, zdrowia, środków, reputacji lub ograniczenie w sposób znaczący jego praw
5	**Krytyczny (Katastrofalny)**	Mogą wystąpić znaczące, nawet nieodwracalne konsekwencje. Krytyczny negatywny wpływ na podmiot danych, w tym częściowa utrata prywatności, zdrowia, środków, reputacji lub ograniczenie w sposób znaczący jego praw

12. Skutki dla osób fizycznych, których prawa lub wolności zostały naruszone określa m.in. motyw 85 RODO.

Ryzyko naruszenia praw lub wolności osób fizycznych powstaje, kiedy naruszenie może skutkować fizyczną, materialną lub niematerialną szkodą dla osób fizycznych, których dane naruszono.

Szkodami takimi są w szczególności.:

1) utrata kontroli nad danymi przez podmiot danych;
2) dyskryminacja;
3) naruszenie dóbr osobistych;
4) brak możliwości lub ograniczona możliwość zidentyfikowania osoby;
5) brak możliwości lub ograniczona możliwość skorzystania z uprawnień przez podmiot danych;
6) kradzież tożsamości lub oszustwo dotyczące tożsamości;
7) nadużycia finansowe;
8) straty finansowe;
9) nieuprawnione cofnięcie pseudonimizacji;
10) utrata poufności danych osobowych chronionych tajemnicą zawodową;
11) naruszenie dobrego imienia;
12) lub inne znaczące skutki gospodarcze lub społeczne dla danej osoby fizycznej;

13. Poziom ryzyka uzyskuje się w wyniku iloczynu zdiagnozowanego poziomu prawdopodobieństwa i zdiagnozowanego poziomu skutku.

R (ryzyko) = P (prawdopodobieństwo) * S (skutek)

Ustala się następujące możliwe poziomy istotności ryzyka:

ryzyko niskie, tj. ryzyko, dla którego iloczyn prawdopodobieństwa wystąpienia danego zdarzenia oraz jego wpływu wynosi 1 - 4 punktów;

ryzyko wysokie, tj. ryzyko, dla którego prawdopodobieństwo wystąpienia danego zdarzenia wynosi 1, a jego następstwo 5 lub prawdopodobieństwo wystąpienia danego zdarzenia wynosi 5, a jego następstwo 1;
ryzyko średnie, tj. ryzyko, dla którego iloczyn prawdopodobieństwa wystąpienia danego zdarzenia oraz jego wpływu wynosi 6 - 9 punktów;
ryzyko wysokie, tj. ryzyko, dla którego iloczyn prawdopodobieństwa wystąpienia danego zdarzenia oraz jego wpływu wynosi 10 - 16 punktów;
ryzyko bardzo wysokie krytyczne, tj. ryzyko, dla którego iloczyn prawdopodobieństwa wystąpienia danego zdarzenia oraz jego wpływu wynosi 20 - 25 punktów;

Poziom ryzyka	**Postępowanie z ryzykiem**	**Opis działania**
Niski (N) 1-4	akceptowanie (A)	Ryzyko możliwe do zaakceptowania. Akceptacja – ryzyko podlega minimalnemu monitorowaniu. Wartość ryzyka powinna zostać zweryfikowana dopiero przy następnej analizie lub gdy zmienią się warunki mające wpływ na podniesienie wartości ryzyka.
Średni (Ś) 6-9	tolerowanie (T) zapobieganie (Z)	Ryzyko tolerowane. Można zastosować działania zapobiegawcze, ograniczające ryzyko do poziomu akceptowalnego. Ryzyko wymaga monitorowania oraz zaplanowania i podjęcia działań prewencyjnych w określonym dłuższym okresie (w zależności od możliwości np. w ciągu kwartału, półrocza czy roku), przy czym dopuszcza się tolerowanie ryzyka z tego przedziału, gdyby szacowane koszty niezbędnych działań przewyższały korzyści z ograniczenia ryzyka lub właściciel ryzyka podwyższył jego akceptowalny poziom. W sytuacji tolerowania takiego ryzyka właściciel ryzyka powinien monitorować ryzyko i okresowo rozważać potrzebę podjęcia działań ograniczających ryzyko.
Wysoki (W) 10-16 oraz 5, gdy **gdy P = 1 i S = 5 lub P = 5 i S = 1**	zapobieganie (Z) przenoszenie (P) unikanie (U)	Ryzyko nieakceptowalne. Działanie niezwłoczne – ryzyko wymaga niezwłocznego podjęcia działań ograniczających ryzyko, mogących polegać na zapobieganiu, przenoszeniu lub unikaniu.
Bardzo wysokie Krytyczny (BW) 20-25	zapobieganie (Z) przenoszenie (P) unikanie (U)	Poziom ryzyka nietolerowany (krytyczny) wymaga natychmiastowego działania. Działanie niezwłoczne – ryzyko wymaga niezwłocznego podjęcia działań ograniczających ryzyko, mogących polegać na zapobieganiu, przenoszeniu lub unikaniu.

Wzór tabeli szacowania ryzyka dla poszczególnych czynności stanowi załącznik nr 3

14. Ryzykiem akceptowalnym jest ryzyko niskie. Ryzykiem tolerowanym jest ryzyko średnie. Ryzyko wysokie, ryzyko bardzo wysokie - krytyczne przekraczają akceptowalny i tolerowany poziom i wymagają określonego rodzaju reakcji na ryzyko – przeciwdziałania ryzyku.

15. W celu określenia rodzaju reakcji na ryzyko należy przeanalizować:
1) przyczyny ryzyka i możliwe scenariusze rozwoju wydarzeń;
2) skuteczność funkcjonujących mechanizmów kontroli.

16. Reakcja na ryzyko może obejmować:
1) **zapobieganie (Z)** – polega na obniżeniu poziomu ryzyka (np. poprzez zmianę prawdopodobieństwa wystąpienia określonego zdarzenia lub zmniejszenie skutków jego wystąpienia). Np. zmniejszenie prawdopodobieństwa wystąpienia zdarzenia spowodowanego przerwą w dostawie energii można osiągnąć, włączając w układ zasilania odpowiednią automatykę i niezależne źródła energii (UPS-y, generatory). Zaś zmniejszenie związanych z tym zdarzeniem skutków utraty danych można osiągnąć, modyfikując system wykonywania kopii z wersji, w której kopia wykonywana jest jeden raz na dobę, do postaci, w której kopia jest wykonywana co 15 minut lub w sposób ciągły (na bieżąco) poprzez zastosowanie dodatkowych zabezpieczeń lub modyfikację procedur w sposób pozwalający na zaakceptowanie ryzyka szczątkowego;
2) **tolerowanie ryzyka (T)** – to świadoma i obiektywna decyzja o niewprowadzaniu żadnych zmian w działaniu organizacji (zabezpieczeń), jeżeli poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka;
3) **unikanie ryzyka (U)** – polega na unikaniu przez organizację działań, które powodują powstanie określonych typów ryzyka, np. w przypadku, gdy zidentyfikowane ryzyka są zbyt wysokie lub koszt wdrożenia zabezpieczeń nie jest adekwatny do zysków;
4) **przeniesienie ryzyka (P)** – polega na wykupieniu ubezpieczenia od jakiegoś zdarzenia lub scedowaniu skutków ryzyka na kontrahenta (np. podwykonawcę); należy pamiętać, że przeniesienie ryzyka nie eliminuje go. Trzeba zaznaczyć, że zgodnie z przepisami ogólnego rozporządzenia o ochronie danych wykupienie ubezpieczenia nie wyeliminuje ryzyka niezastosowania się przez dany podmiot do przepisów RODO. Ponadto administrator w sytuacji, kiedy zleca innym podmiotom przetwarzanie danych, to jako podmiot decydujący o zakresie i celach tego przetwarzania, ponosi pełną odpowiedzialność za zgodne z prawem przetwarzanie wskazanych danych;
5) **akceptowanie ryzyka (A)** - (niepodejmowanie żadnych działań do momentu wystąpienia ryzyka – dopuszczalna tylko wtedy, gdy nie ma możliwości ograniczenia ryzyka przez działanie, bądź koszty podjętych działań przekraczają możliwe do uzyskania korzyści).

17. W razie potrzeby można stosować kombinację rodzajów reakcji na ryzyko. Należy mieć na uwadze, że szczególnym przypadkiem jest sytuacja, gdy organizacja nie jest świadoma ryzyka i wobec tego nieświadomie wystawia się na nie w pełnym zakresie.
Na etapie tym, w przypadku, gdy określony rodzaj czynności przetwarzania danych osobowych związany jest z ryzykiem, które przekracza akceptowalny lub tolerowany poziom, administrator lub podmiot przetwarzający musi podjąć decyzję co do dalszego działania/postępowania.
Najrozsądniejszym wyborem jest w takim przypadku podjęcie próby wprowadzenia dodatkowych środków bezpieczeństwa, które umożliwią **obniżenie poziomu ryzyka lub całkowite jego wyeliminowanie.**

18. Na podstawie dokonanej identyfikacji i analizy ryzyka oraz po ustaleniu rodzaju reakcji na ryzyko, sporządzany jest rejestr ryzyk oraz plan postępowania z ryzykiem, są one uaktualniane na bieżąco, wzór rejestru i planu określa załącznik nr 4.

19. Plany postępowania powinny być monitorowane przez osoby wskazane przez kierownictwo oraz inspektora ochrony danych, jeżeli został powołany. W procesie monitorowania ustalamy, czy planowane zabezpieczenia o symulowanej skuteczności w praktyce zostały uruchomione. W wielu przypadkach będzie to wymagało przeprowadzenia testów skuteczności. Powinniśmy w dłuższej perspektywie zaplanować mierzenie skuteczności wdrożonych zabezpieczeń poprzez sprawdzanie, czy właściwie reagują na pojawiające się zagrożenia i próby ich sforsowania.

20. Na podstawie zatwierdzonego Planu postępowania z ryzykiem ochrony danych osobowych przetwarzanych w podmiocie, wyznaczone osoby przez ADO podejmują planowane działania w celu zmniejszenia ryzyka do akceptowalnego lub tolerowanego poziomu.

21. W przypadku rozszerzenia zakresu działania jednostki o nowe zadania bądź ustalenia nowych celów lub zmiany ustalonych zadań i celów w odniesieniu do danych osobowych, albo istotnej zmiany warunków przetwarzania danych osobowych, dokonuje się ponownej identyfikacji ryzyka i oceny jego istotności, w terminie jednego miesiąca od dnia zaistnienia przesłanki uzasadniającej aktualizację. W przypadku zidentyfikowania nowego ryzyka przekraczającego akceptowalny poziom ryzyka, osoby odpowiedzialne za ryzyko określają rodzaj reakcji na ryzyko oraz planowane działania w celu jego zmniejszenia do akceptowalnego poziomu.

22. Osoby wyznaczone przez ADO, raz w roku kalendarzowym, dokonują przeglądu ryzyka, w celu uzyskania informacji, czy:

a) zidentyfikowane zagrożenia nadal występują;
b) pojawiło się nowe zagrożenie;
c) prawdopodobieństwo i wpływ ryzyka zmieniły się;
d) ustalone reakcje na ryzyko są efektywne.

1) Po dokonaniu przeglądu osoby odpowiedzialne we współpracy z IOD dokonują aktualizacji planów postępowania z ryzykiem.
2) Zaktualizowany plan postępowania z ryzykiem ochrony danych osobowych przetwarzanych w podmiocie, przekazuje się administratorowi, celem uzyskania opinii na temat możliwości sfinansowania działań generujących dodatkowe koszty dla podmiotu – zaproponowanych w ramach reakcji na ryzyko.
3) Na podstawie otrzymanej opinii, o której mowa w ppkt. 2), w przypadku braku możliwości sfinansowania działań generujących dodatkowe koszty dla podmiotu w danym roku budżetowym – zaproponowanych w ramach reakcji na ryzyko, Zespół wprowadza zmiany w planie postępowania z ryzykiem ochrony danych osobowych przetwarzanych w podmiocie, o czym informuje osoby funkcyjne, których ta zmiana dotyczy.

23. Pierwsza weryfikacja czy należy przeprowadzić ocenę skutków dla ochrony danych osobowych zgodnie z np. art. 37 RODO oraz Komunikatem Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony oraz wytycznych Grupy Roboczej np. 29 WP 248 rew. 01 17/PL odbywa się zgodnie z załącznikiem nr 1. Następnie ocenie skutków dla ochrony danych poddawane są czynności, których ryzyko naruszenia praw i wolności zostało ustalone na poziomie co najmniej wysokim.

24. W niektórych przypadkach administrator może jednak uznać, że mimo, iż przetwarzanie spełniające tylko np. tylko jedno z wymienionych kryteriów wymienionych w komunikacie PUODO będzie wymagało przeprowadzenia oceny skutków dla ochrony danych.

25. Dokonując oceny skutków dla ochrony danych osobowych ryzyk ocenionych na poziomie wysokim lub bardzo wysokim, należy skonsultować się z IOD w celu uzyskania opinii przed ostateczną akceptacją oszacowanego poziomu.
Konsultacje powinny dotyczyć:
1) Czy słusznie przyjęto wysoki poziom ryzyk, dla których będzie konieczne przeprowadzenie oceny skutków dla ochrony danych;
2) Czy zaleceniem inspektora byłoby przeprowadzenie oceny przez podmiot zewnętrzny;
3) Czy proponowane środki organizacyjne i techniczne, w celu obniżenia poziomu zagrożeń dla praw i wolności podmiotu danych są adekwatne.

26. W procesie oceny skutków dla ochrony danych administrator wykorzystuje:
1) przeprowadzone szacowanie ryzyka ochrony danych osobowych;
2) plan postępowania z ryzkiem;

27. Ocena Skutków Dla Przetwarzania Danych (DPIA) nie jest obowiązkowa w przypadkach:
1) gdy nie jest prawdopodobne, aby operacja przetwarzania może powodować wysokie ryzyko;
2) gdy przeprowadzono już podobną ocenę skutków dla ochrony danych;
3) gdy operację przetwarzania zatwierdzono przed majem 2018 r.;
4) gdy operacja przetwarzania posiada podstawę prawną, która reguluje daną operację przetwarzania;
5) gdy operacja przetwarzania znajduje się w wykazie operacji przetwarzania, które nie podlegają ocenie skutków dla ochrony danych.

28. Ocenę skutków dla ochrony danych przeprowadza się przy zastosowania wzoru stanowiącego załącznik nr 5.

29. Jeżeli mimo zastosowania odpowiednich środków technicznych, organizacyjnych i informatycznych, analiza następstw utraty poufności bądź integralności lub dostępności w kontekście czynności przetwarzania sklasyfikowanych do Oceny Skutków Dla Przetwarzania Danych (DPIA) w dalszym ciągu powoduje wysokie ryzyko szczątkowe, Administrator konsultuje się z organem nadzorczym. Administrator ma świadomość, iż ryzyko wysokie nie może podlegać decyzji w formie akceptacji.

30. Zespół na podstawie przeprowadzanych czynności w związku z procesem szacowania ryzyka sporządza raport, który wraz z wnioskami i propozycjami zmian w zakresie stosowanych środków bezpieczeństwa oraz reagowania na zagrożenia. Raport podlega zatwierdzeniu przez administratora.

31. Akceptacja ryzyka przez Administratora następuje poprzez złożenie formalnego oświadczenia o zapoznaniu się z wynikami procesu szacowania ryzyka oraz deklaracji dotyczącej przestrzegania zasad i trybu zarzadzania ryzykiem ochrony danych osobowych - wzór stanowi załącznik nr 6.

czynność z RCP	wartość danych - zasobów	wykaz rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony zgodnie z komunikatem Prezesa UODO z dnia 17 czerwca 2019 r. Wypełnij wybierając 0 - NIE, 1 - TAK												czy ocena skutków -DIPA - jest wymagana kolor zielony NIE, czerowny TAK	art. 35 RODO	czynność zatwierdzona przed wejściem w życie RODO
		1	2	3	4	5	6	7	8	10	11	12	12			
		Ewaluacja lub ocena, w tym profilowanie i przewidywanie (analiza behawioralna) w celach wywołujących negatywne skutki prawne, fizyczne, finansowe lub inne niedogodności dla osób fizycznych	Zautomatyzowane podejmowanie decyzji wywołujących skutki prawne, finansowe lub podobne istotne skutki	Systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie wykorzystujące elementy rozpoznawania cech lub właściwości obiektów, które znajdą się w monitorowanej przestrzeni. Do tej grupy systemów nie są zaliczane systemy monitoringu wizyjnego, w których obraz jest nagrywany i wykorzystywany tylko w przypadku potrzeby analizy incydentów naruszenia prawa	Przetwarzanie szczególnych kategorii danych osobowych i dotyczących wyroków skazujących i czynów zabronionych (danych wrażliwych wg opinii WP 29)	Przetwarzanie danych biometrycznych wyłącznie w celu identyfikacji osoby fizycznej bądź w celu kontroli dostępu	Przetwarzanie danych genetycznych	Dane przetwarzane na dużą skalę, gdzie pojęcie dużej skali dotyczy: liczby osób, których dane są przetwarzane, zakresu przetwarzania, okresu przechowywania danych oraz geograficznego zakresu przetwarzania	Przeprowadzanie porównań, ocena lub wnioskowanie na podstawie analizy danych pozyskanych z różnych źródeł	Przetwarzanie danych dotyczących osób, których ocena i świadczone im usługi są uzależnione od podmiotów lub osób, które dysponują uprawnieniami nadzorczymi i/lub ocennymi	Innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych	przetwarzanie samo w sobie uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy	Przetwarzanie danych lokalizacyjnych		Jeśli występuje jeden z poniższych warunków konieczne jest przeprowadzenia DPIA	
		0	0	0		0	0	0	0	0	0	0	0	0		
		0	0	0		0	0	0	0	0	0	0	0	0		
		0	0	0		0	0	0	0	0	0	0	0	0		
		0	0	0		0	0	0	0	0	0	0	0	0		
		0	0	0		0	0	0	0	0	0	0	0	0		
		0	0	0	0	0	0	0	0	0	0	0	0	0		
		0	0	0		0	0	0	0	0	0	0	0	0		
		0	0	0		0	0	0	0	0	0	0	0	0		
		0	0	0		0	0	0	0	0	0	0	0	0		
		0	0	0		0	0	0	0	0	0	0	0	0		
		0	0	0		0	0	0	0	0	0	0	0	0		
		0	0	0		0	0	0	0	0	0	0	0	0		
		0	0	0		0	0	0	0	0	0	0	0	0		
		0	0	0		0	0	0	0	0	0	0	0	0		
		0	0	0		0	0	0	0	0	0	0	0	0		
		0	0	0		0	0	0	0	0	0	0	0	0		
		0	0	0		0	0	0	0	0	0	0	0	0		
		0	0	0		0	0	0	0	0	0	0	0	0		
		0	0	0		0	0	0	0	0	0	0	0	0		

Arkusz identyfikacji zagrożeń dla bezpieczeństwa danych osobowych w			
powyżej wpisz nazwę Twojej jednostki organizacyjnej			
Instrukcja wypełnienia arkusza Spośród wymienionych przykładowych zagrożeń wybierz od 10 do 15 wg Ciebie najistotniejszych dla bezpieczeństwa danych w Twojej jednostce wybierając TAK			
Lp.	**Zagrożenia**	**wybierz TAK, jeśli zagrożenie występuje**	**Uwagi**
1.	Nieprawidłowe zabezpieczenie budynku, brak zamków w drzwiach, systemu zarządzania dostępem, systemu alarmowego, monitoringu wizyjnego itp.	NIE	
2.	Nieprawidłowe zabezpieczenie pomieszczeń - brak zamków w drzwiach do biur, systemu zarządzania dostępem itp.	NIE	
3.	Brak mebli posiadających odpowiednie zabezpieczenia do przechywania dokumentów/nośników	NIE	
4.	Usytuowanie obiektu w zwartej zabudowie/w pobliżu innych budynkow, które mogą wpływać na obiekt (pożar, wybuch gazu, itp.)	NIE	
5.	Usytuowanie instalacji wodno-kanalizacyjnej, gazowej, innej w pomieszczeniach serwerowni/archiuwum/kancelarii OIN	NIE	
6.	Zły stan techniczny budynku i pomieszczeń	NIE	
7.	Zły stan techniczny instalacji sanitarnej, gazowej, ciepłowniczej, wodno-kanalizacyjnej, informatycznej	NIE	
8.	Brak zabezpieczenia elektromagnetycznego dla systemów informatycznych	NIE	
9.	Brak szkolenia lub nieświadomość pracowników w zakresie fizycznego zabezpieczenia pomieszczeń i informacji/danych	NIE	
10.	Zniszczenie, uszkodzenie dokumentów/urządzeń z danymi w wyniku pożaru, zawalenia budynku/pomieszczenia/zalania na skutek opadów atmosfertycznych, awarii sieci wodno-kanalizacyjnej, powodzi	NIE	
11.	Kradzież, utrata, zagubienie, itp. nośnika danych, sprzętu IT, komputera, smartfona, itp. na których znajdują się informacje/dane	NIE	
12.	Kradzież, utrata, zagubienie, itp. dokumentów w wersji tradycyjnej, w których znajdują się informacje/dane	NIE	
13.	Wyciek,skopiowanie, itp. informacji/danych w wersji tradycyjnej papierowej	NIE	
14.	Wyciek, skopiowanie itp. informacji/danych z niezabezpieczonych: nośników, sprzętu IT, komputera	NIE	

Lp.	Zagrożenia	wybierz TAK, jeśli zagrożenie występuje	Uwagi
15.	Kopiowanie informacji/danych na prywatny nośnik danych np. Pendrive wbrew przyjętym politykom wewnętrznym	NIE	
16.	Kopiowanie informacji/danych na służbowy niezabezpieczony hasłem nośnik danych np. Pendrive	NIE	
17.	Błędna konfiguracja systemu lub oprogramowania (niezgodnie z przyjętymi politykami)	NIE	
18.	Użycie lub zainstalowanie nielegalnego oprogramowania - niezgodnie z przyjętymi politykami i zasadami	NIE	
19.	Awaria sprzętu informatycznego	NIE	
20.	Awaria oprogramowania	NIE	
21.	Brak aktualizacji oprogramowania: antywirusowego, operacyjnego, użytkowego, innego	NIE	
22.	Omyłkowe przyznanie użytkownikom uprawnień administratora	NIE	
23.	Przechwycenie danych przez nieprawidłowe zabezpieczenie sprzętu bądź WiFi lub podczas teletransmisji	NIE	
24.	Brak szyfrowania nośników danych, sprzętu informatycznego w szczególności wykorzystywanego poza jednostką lub w trakcie pracy zdalnej	NIE	
25.	Zainstalowanie szkodliwego lub nielegalnego oprogramowania przez użytkownika STI	NIE	
26.	Włamanie do sieci, systemu - atak hakerski	NIE	
27.	Niewłaściwe zabezpieczenie przechowywanych dokumentów (poza szafami, sejfami, pomieszczeniami)	NIE	
28.	Zbyt długie przechowywanie danych w wersji papierowej lub elektronicznej	NIE	
29.	Niewłaściwe lub brak niszczenia elektronicznych nośników informacji oraz dokumentacji papierowej	NIE	
30.	Brak niszczarek: dokumentów tradycyjnych, elektronicznych nośników danych	NIE	
31.	Brak urządzeń podtrzymujących zasilanie urządzeń informatycznych lub awaria zasilania	NIE	
32.	Pozostawienie niezabezpieczonych pomieszczeń, szaf, gdzie znajdują się urządzenia, nośniki lub dokumentacja tradycyjna zawierająca informacje, dane osobowe	NIE	
33.	Dostęp do pomieszczeń, gdzie przetwarzane są dane dla osób nieuprawnionych: klientów, kurierów itd.	NIE	
34.	Niezgodne z przepisami zabezpieczenie przeciwpożarowe	NIE	

Lp.	Zagrożenia	wybierz TAK, jeśli zagrożenie występuje	Uwagi
35.	Zbieranie błędnych danych, stosowanie nieaktualnych druków i formularzy	NIE	
36.	Przetwarzanie zbyt szerokiego zakresu danych	NIE	
37.	Przetwarzanie danych bez podstawy prawnej, niezgodnie z celem określonym w przepisach prawa, po wygaśnięciu celu przetwarzania	NIE	
38.	Stosowanie nieaktualnych przepisów	NIE	
39.	Brak procedury reagowania na incydenty i naruszenia	NIE	
40.	Brak wsparcia specjalisty od przepisów ODO niewyznaczenie IOD	NIE	
41.	Brak skutecznej kontroli dostawców usług w czasie trwania umowy	NIE	
42.	Brak zapisów w umowie z dostawcami usług w zakresie serwisu, wsparcia, bieżącej obsługi programu	NIE	
43.	Niewłaściwe realizowanie obowiązków informacyjnych	NIE	
44.	Brak procedur realizowania praw osób, których dane dotyczą	NIE	
45.	Brak wyznaczenia osoby/firmy/podmiotu odpowiedzialnej za ciągłość działania systemów informatycznych	NIE	
46.	Wykorzystanie prywatnego sprzętu informatycznego do celów służbowych	NIE	
47.	Nieumiejętne posługiwanie się oprogramowaniem i sprzętem infromatycznym, błąd użytkownika	NIE	
48.	Brak szkolenia personelu, niewystarczająca wiedza dot. ochrony danych oraz informacji	NIE	
49.	Brak skutecznego nadzoru nad bezpieczeństwem informacji przez osoby odpowiedzialne za ciągłość działania systemu	NIE	
50.	Niefrasobliwe rozmowy personelu dotyczące informacji i danych	NIE	
51.	Zbyt małe zaangażowanie w proces zabezpieczania danych najwyższego kierownictwa/pracowników	NIE	
52.	Przesyłanie pocztą elektroniczną niezaszyfrowanych danych	NIE	
53.	Udostępnianie danych podmiotom lub osobom nieuprawnionym/upoważnionym	NIE	
54.	Celowe działanie pracownika na szkodę organizacji	NIE	
55.	Dopuszczanie do przetwarzania osób nieupoważnionych	NIE	
56.	Brak nadzoru na sprzętem komputerowym/mobilnym podczas pracy zdalnej lub pracy poza strefą przetwarzania danych	NIE	
57.	Brak nadzoru nad dokumentacją tradycyjną podczas pracy zdalnej lub pracy poza strefą przetwarzania danych	NIE	

Lp.	Zagrożenia	wybierz TAK, jeśli zagrożenie występuje	Uwagi
58.	Korzystanie w celach prywatnych ze służbowej poczty elektronicznej	NIE	
59.	Korzystanie w celach służbowych z prywatnej poczty elektronicznej	NIE	
60.	Brak stosowania opcji „kopia ukryta" w korespondencji elektronicznej skutkującej ujawnieniem adresów e-mail wszystkich odbiorców	NIE	
61.	Wyrzucenie dokumentów zawierających dane do śmieci bez zniszczenia	NIE	
62.	Ujawnienie przez pracownika loginu i hasła lub sposobu logowania do systemu lub programu	NIE	
63.	Wykorzystywanie tego samego hasła w wielu systemach oraz wykorzystywanie tego samego hasła do celów prywatnych i służbowych	NIE	
64.	Używanie haseł dostępowych do systemów, sieci, programów o zbyt małej jakości - układu liter, cyfr i znaków specjalnych	NIE	
65.	Brak kopii zapasowych informacji/danych	NIE	
66.	Zlokalizowanie kopii zapasowej w tej samej lokalizacji lub na tym samym sprzęcie co główna baza danych	NIE	
67.	Utrata kopii zapasowej lub jej nieprawidłowe wykonanie	NIE	
68.	Brak okresowych testów kopii zapasowych	NIE	
69.	Brak procedury przywracania ciągłości działania systemu w przypadku awarii urządzeń, zaszyfrowania serwerów, itp.	NIE	
70.	Wynoszenie informacji/danych bez zgody kierownictwa poza jednostkę	NIE	
71.	Otwieranie korespondecncji mailowej oraz załączników od nieznanego nadawcy	NIE	
72.	Upublicznienie nagrania z monitoringu wizyjnego lub udostępnienie bez podstawy prawnej	NIE	
73.	Uruchomienie w komputerze zewnętrznego nośnika informacji o nieznanym pochodzeniu	NIE	
74.	Uruchomienie znalezionego laptopa i podłączenie go do sieci internetowej	NIE	
75.	Brak umowy powierzenia przetwarzania danych lub niewłaściwe wykonanie jej postanowień	NIE	
76.	Zastosowanie socjotechnik wobec użytkowników w celu wyłudzenia informacji/danych/danych logowania/dostępu do zasobów	NIE	
77.	Udostępnienie hasła do sieci WiFi	NIE	
78.	Kradzież z włamaniem do obiektu, pomieszczenia i zabór komputera, nośnika innego urządzenia lub dokumentów tradycyjnych zawierających informacje, dane osobowe	NIE	

Lp.	Zagrożenia	wybierz TAK, jeśli zagrożenie występuje	Uwagi
79.	Instalowanie oprogramowania bez wiedzy lub akceptacji informatyka/wbrew zasdom przyjętym w dokumentacji wewnętrznej	NIE	
80.	Korzystanie w celach służbowych z ogólnodostępnej publicznej zewnętrznej sieci WiFi	NIE	
81.	Nieprzestrzeganie zasady poufności informacji	NIE	
82.	Niewłaściwe zarządzanie treściami publikowanymi przez redagującego serwis społecznościowy lub strony internetowe	NIE	
83.	Naruszenie prawa lub zasad współżycia społecznego przez osoby korzystające z serwisów społecznościowych	NIE	
84.		NIE	
85.		NIE	
86.		NIE	
87.		NIE	
88.		NIE	
89.		NIE	
90.		NIE	
91.		NIE	
92.		NIE	
93.		NIE	
94.		NIE	
95.		NIE	

Imię i nazwisko wypełniającego

Ryzyko związane z poufnością, dostępnością i integralnością przetwarzanych danych osobowych w czynności:

Test RCP 2										
Nr	Zidentyfikowane ryzyko	atrybuty			Skutki ryzyka	Aktualne środki ograniczające ryzyko techniczne i organizacyjne	Aktualne środki ograniczające ryzyko informatyczne	Skutek	Prawdopodobieństwo	Wartość ryzyka	Reakcja na ryzyko
		poufność	integralność	dostępność							
1	test ryzyka 2										
2	test ryzyka 2	P									
			I								
				D							
3	test ryzyka 1	P									
			I								
				D							

W przypadku ewaluacji ryzyka na poziomie wysokim i bardzo wysokim – przygotować projekt planu postępowania z ryzykiem pod kątem działań naprawczych/zapobiegawczych, wskazując opis i cel działania, podmiot odpowiedzialny za monitorowanie działania oraz planowany termin zakończenia działania. Plan postepowania z ryzykiem powinien zostać opracowany dla każdego ryzyka określonego na poziomie wysokim i bardzo wysokim.

Plan Postępowania z ryzykiem

(przykład)

	Opis ryzyka	**Właściciel ryzyka**	**Kwalifikacja ryzyka**	**Odpowiedzialny za realizację planu postępowania z ryzykiem**	**Poziom ryzyka po wprowadzeniu działań zaradczych**	**Termin realizacji**	**Określenie działań**
1	Niewłaściwe zabezpieczenie przechowywanych dokumentów	Administrator	wysokie	Administrator	ŚREDNI	Proces ciągły	• pracownicy posiadają upoważnienia oraz odebrano od nich oświadczenia o zachowaniu danych w poufności • przeszkolono pracowników z ochrony danych • strefa przetwarzania zabezpieczona systemem alarmu oraz monitoringu wizyjnego, • egzekwowanie polityki czystego biurka

OCENA SKUTKÓW DLA OCHRONY DANYCH (DPIA)

czynność przetwarznia	podstawa prawna	cel przetwarzania, w tym uzasadnieniy interes administratora	ocena, czy operacje przetwarznia sa niezbedne oraz proporcjonalne do celów	kategorie osób, których dane są przetwarzane	kategorie danych osobowych	retnecja danych	odbiorcy danych i podmioty przetwarzające	odbiorcy w państwach trzeciech	czy osoba, której dane dotyczą ma możliwosc realizacji prawa, o których mowa w rodz. III RODO

OCENA SKUTKÓW DLA OCHRONY DANYCH (DPIA)

czy realizowany jest obowiązek infromacyjny o którym mowa w art.. 12,13,14 RODO	opis planowanych operacji	wynik ocena ryzyka naruszenia praw lub wolności osób, których dane dotyczą	ryzyka występujące w procesie	dotychasowe środki zastosowane do zabepieczenia danych	zalecenia IOD oraz ewentualne konsultacja z pracownikami	środki planowane w celu zaradzenia ryzyku	ocena ryzyka po zastosowaniu środków w celu zarządzania ryzykiem


decyzja administratora

OŚWIADCZENIE ADMINISTRATORA

Oświadczam, iż zapoznałem się z wynikami procesu szacowania ryzyka. Informacje dotyczące ryzyka po zastosowaniu odpowiednich zabezpieczeń są mi znane i przejmuję odpowiedzialność za zidentyfikowane ryzyko oraz ewentualne konsekwencje utrzymywania tego ryzyka, jako jego właściciel, w zakresie swoich kompetencji.

Ponadto deklaruje, że:

1. Przestrzegam zasad i trybu zarządzania ryzykiem ochrony danych osobowych przetwarzanych w podmiocie w zakresie, w jakim mają one wpływ na pełnione przeze mnie obowiązki;
2. Nadzoruję swoich pracowników pod kątem przestrzegania zasad i trybu zarządzania ryzykiem ochrony danych osobowych przetwarzanych w podmiocie w zakresie, w jakim mają one wpływ na pełnione przez nich obowiązki; prowadzę i dokonuję przeglądu właściwych rejestrów ryzyka i monitoruję podjęcie odpowiednich działań w celu zarządzania najważniejszymi rodzajami ryzyk, które ustalono trakcie szacowania;
3. Niezwłocznie podejmuję działania w celu wdrożenia uzgodnionych zaleceń audytu wewnętrznego i zewnętrznego (np. NIK) oraz raportów stron trzecich;
4. Pracownicy są aktywnie zachęcani do identyfikacji i zarządzania ryzykiem oraz informowania administratora o nowych ryzykach i istotnych kwestiach związanych z bezpieczeństwem danych osobowych.

.....

data i podpis Administratora