ZARZĄDZENIE Nr 17 /2021
Dyrektora Zarządu Dróg, Komunikacji i Utrzymania Miasta
z dnia 16.03.2021 r.

w sprawie zamiany Zarządzenia nr 4/2019 Dyrektora Zarządu Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu z dnia 14 stycznia 2019 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych w Zarządzie Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu

Na podstawie art. 24 ust. 2 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. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.) oraz § 13 ust. 3 pkt 1 Regulaminu Organizacyjnego Zarządu Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu wprowadzonego Zarządzeniem nr 39/2020 Dyrektora zarządu Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu, zarządzam co następuje:

§ 1

W Polityce Ochrony Danych Osobowych w Zarządzie Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu stanowiącej Załącznik do Zarządzenia nr 4/2019 Dyrektora Zarządu Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu z dnia 14 stycznia 2019 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych w Zarządzie Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu, wprowadza się następujące zmiany:

1. Wprowadzam nowy Załącznik nr 1 do Polityki Ochrony Danych Osobowych w Zarządzie Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu, wprowadzonej Zarządzeniem nr 4/2019 Dyrektora Zarządu Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu z dnia 14 stycznia 2019 r. w brzmieniu załącznika do niniejszego Zarządzenia.

§ 2

Zarządzenie wchodzi w życie z dniem podjęcia.

DYREKTOR
Krzysztof Szczerbiak

RADCA PRAWNY
Ilona Gmerek
WPR - 450

Załącznik nr 1
do Polityki Ochrony Danych Osobowych
w Zarządzie Dróg, Komunikacji i Utrzymania
Miasta w Wałbrzychu.

Analiza Ryzyka Ogólnego i Ocena Skutków dla Przetwarzania Danych (DPIA) w Zarządzie Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu

Spis treści

Wstęp....1
Cel szacowania ryzyka....1
Wytyczne wykorzystywane do przeprowadzenia Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA).1
Definicje legalne....1
Oznaczenie uwarunkowań związanych z funkcjonowaniem organizacji – ustalenie kontekstu....2
Wybór metody na cele przeprowadzenia Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA)....3
Klasyfikacja czynności przetwarzania....4
Grupowanie podobnych czynności przetwarzania....7
Szacowanie ryzyka....7
Dokonanie analizy ryzyka....11
Ocena ryzyka dla przetwarzania danych osobowych....13
Plan postępowania z ryzykiem wraz z wtórnym procesem szacowania ryzyka po wdrożeniu zabezpieczeń....14
Akceptacja ryzyka szczątkowego....14
Konsultacje z organem nadzorczym....14
Monitorowanie i przegląd ryzyka....15

Wstęp

Mając na uwadze konieczność uwzględnienia w procesie przetwarzania danych osobowych prawdopodobieństwa i powagi ryzyka naruszenia praw lub wolności osób, których przetwarzanie dotyczy, Administrator niniejszym dokumentem wprowadza w Zarządzie Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu (dalej jako Organizacja) procedurę szacowania ryzyka 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 i organizacyjne, które zapewnią bezpieczeństwo przetwarzanych danych osobowych. Zastosowane środki techniczne i organizacyjne są poddawane cyklicznemu doskonaleniu.

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

Jeżeli za przeprowadzenie procesu szacowania ryzyka odpowiada inna osoba niż Administrator, jest ona odpowiedzialna za przeprowadzenie tego procesu w oparciu o zachowanie obiektywnej postawy względem zidentyfikowanego ryzyka.

§ 1

Cel szacowania ryzyka

1. Administrator przeprowadza proces szacowania ryzyka w zakresie bezpieczeństwa informacji , w tym stanowiących dane osobowe, w celu zidentyfikowania obszarów, które mogą istotnie wpływać na osobę, której przetwarzanie dotyczy. Administrator wdraża podejście oparte na ryzyku, aby zapewnić ochronę praw i wolności osób, których przetwarzanie dotyczy.

2. Na szacowanie ryzyka składa się:

    1) Analiza Ryzyka Ogólnego,

    2) Ocena Skutków Dla Przetwarzania Danych (DPIA).

§ 2

Wytyczne wykorzystywane do przeprowadzenia Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA)

1. Z racji tego, iż Administrator w ramach realizacji praw podstawowych w zakresie ochrony danych osobowych, kieruje się zasadą legalności przetwarzania zgodnego z prawem, opiera proces szacowania ryzyka na następujących podstawach prawnych, normach ISO oraz wytycznych Grupy Roboczej art. 29:

    1) 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;

    2) Norma PN-EN ISO/IEC 27002:2017 (Technika Informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji);

    3) Norma PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-EN ISO/IEC 27001:2017);

    4) Wytyczne Grupy Roboczej art. 29 dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679 z dnia 4 października 2017r.

§ 3

Definicje legalne

Ilekroć w „Analizie Ryzyka Ogólnego i Ocenie Skutków Dla Przetwarzania Danych (DPIA)" mówi się o:

1. **Szacowaniu ryzyka** – rozumie się przez to proces analizy i oceny ryzyka. W procesie szacowania ryzyka w kontekście danych osobowych szacowanie ryzyka uwzględnia ryzyka związane z naruszeniem praw i wolności osób fizycznych, których przetwarzanie dotyczy;
2. **Analizie ryzyka** – rozumie się przez to proces identyfikacji źródeł ryzyka i oszacowania ryzyka;
3. **Ocenie ryzyka** – proces porównywania oszacowanego ryzyka w celu określenia znaczenia ryzyka;
4. **Ryzyku** – rozumie się przez to kombinację prawdopodobieństwa zdarzenia i jego konsekwencji;
5. **Ryzyku szczątkowym** – rozumie się przez to ryzyko pozostające po procesie postępowania z ryzykiem;
6. **Postępowaniu z ryzykiem** – rozumie się przez to proces zmiany poziomu ryzyka poprzez zastosowanie odpowiednich środków technicznych i organizacyjnych;
7. **Akceptacji ryzyka** – rozumie się przez to decyzję Administratora/najwyższego kierownictwa organizacji o tym, aby ryzyko zaakceptować;
8. **Podatności** – rozumie się przez to słabość w strukturze fizycznej, technicznej, organizacyjnej organizacji;
9. **Incydencie** – rozumie się przez to zdarzenie mające lub mogące mieć negatywny wpływ na System Zarządzania Bezpieczeństwem Informacji w organizacji. Incydent może powodować w stosunku do osoby fizycznej, której dane osobowe organizacja przetwarza, szkodę o charakterze majątkowym lub niemajątkowym;
10. **Poufności** – rozumie się przez to właściwość polegająca na tym, że osoba nieupoważniona bądź podmiot nie mają dostępu do danych osobowych, które temu atrybutowi podlegają;
11. **Integralności** – rozumie się przez to właściwość polegająca na tym, że aktywa w postaci informacji/danych osobowych pozostają kompletne;
12. **Dostępności** – rozumie się przez to właściwość polegająca na tym, że aktywa w postaci informacji/danych osobowych pozostają dostępne dla osób upoważnionych/uprawnionych do ich przetwarzania;
13. **Bezpieczeństwie informacji** – rozumie się przez to zachowanie wobec przetwarzanych danych osobowych/informacji takich atrybutów jak poufność, integralność oraz dostępność.

§ 4

Oznaczenie uwarunkowań związanych z funkcjonowaniem organizacji – ustalenie kontekstu

1. W Organizacji określa się, które z uwarunkowań zewnętrznych bądź wewnętrznych mają znaczenie dla szacowania ryzyka.
2. Uwarunkowania zewnętrzne istotnie wpływające na organizację:
    1) relacje z innymi administratorami danych osobowych,
    2) relacje z innymi podmiotami zewnętrznymi,
    3) zasięg terytorialny działalności organizacji,
    4) uwarunkowania prawne organizacji.
3. Uwarunkowania wewnętrzne istotnie wpływające na organizację:

1) struktura i rozmiary organizacji,

2) uwarunkowania formalne wewnętrzne (polityki, regulaminy),

3) sposoby podejmowania decyzji w organizacji względem bezpieczeństwa przepływu danych,

4) kultura organizacji.

4. Organizacja na etapie tworzenia Polityki Ochrony Danych Osobowych przeanalizowała:

1) podstawy legalności przetwarzania danych (w oparciu o przesłanki wynikające z RODO),

2) staranność po stronie organizacji w zakresie spełniania obowiązków informacyjnych oraz realizacji praw osób fizycznych, których dane osobowe dotyczą w oparciu o RODO,

3) cel przetwarzania danych osobowych, chyba, że organizacja działa w imieniu innego administratora (w procesie przetwarzania danych organizacja występuje w roli procesora),

4) zakres przetwarzanych danych kierując się zasadami przetwarzania danych określonymi w RODO,

5) wymagania dotyczące zabezpieczeń organizacyjnych, środków kontroli logicznej procesu przetwarzania, środków ochrony fizycznej danych.

Podstawa prawna:
Zgodnie z art. 24 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.

§ 5

Wybór metody na cele przeprowadzenia Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA)

1. Rozporządzenie ogólne o ochronie danych pozostawia Administratorowi wybór w zakresie zastosowania konkretnej metody szacowania ryzyka.

2. Administrator ma świadomość, iż w procesie szacowania ryzyka może kierować się metodą:

1) **ilościową**: wielkość poniesionych strat próbuje się wyrazić liczbowo, niejednokrotnie w oparciu o dane statystyczne, bądź,

2) **jakościową**: wielkość zagrożenia ocenia się przez pryzmat doświadczenia oraz intuicji osoby szacującej ryzyko (subiektywne odczucie).

3. Administrator ma świadomość, iż szacowanie ryzyka w procesie przetwarzanych danych osobowych powinno opierać się o metodę jakościową - strat związanych z ochroną danych osobowych bardzo często nie sposób wyrazić za pomocą liczb. W związku z powyższym Administrator decyduje się na wykorzystanie metody szacowania ryzyka CRAMM (CCTA Risk Analysis and Management Method).

4. Atrybuty, jakie Administrator przyjmuje w tabeli szacowania ryzyka to:

1) Poufność – osoba nieupoważniona bądź nieupoważniony podmiot nie mają dostępu do danych osobowych. Dane osobowe zgodnie z tym atrybutem nie są ujawniane w nieuprawniony sposób.

2) Integralność – konieczność zapewnienia spójności danych osobowych; atrybut determinujący konieczność ochrony danych osobowych przed przypadkowym ich zniekształceniem w przypadku ich zapisu, odczytu, transmisji bądź magazynowania.

3) Dostępność – zasób w postaci danych osobowych jest możliwy do wykorzystania na żądanie w konkretnym czasie przez osobę bądź podmiot upoważniony/uprawniony w zakresie dostępu do danych.

§ 6

Klasyfikacja czynności przetwarzania

1. Administrator, w pierwszej kolejności dzieli czynności przetwarzania (określone w Rejestrze czynności przetwarzania) na te, które wymagają Oceny Skutków dla Przetwarzania Danych (DPIA) oraz te, względem których Administrator wykonuje Analizę Ryzyka Ogólnego.

2. Kryterium, według którego Administrator dokonuje wstępnej klasyfikacji z uwzględnieniem kontekstu przetwarzania danych jest 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 wytyczne Grupy Roboczej art. 29 WP 248 rew.01 17/PL dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie może powodować wysokie ryzyko do celów rozporządzenia 2016/679 tj.:

   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.**

Podstawa prawna:

Zgodnie z wymogami Komunikatu 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

3. Powyższe wytyczne znajdują źródło w art. 35 ust. 3 RODO:

   „Ocena skutków dla ochrony danych, o której mowa w ust. 1, jest wymagana w szczególności w przypadku:

a) *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;*

b) *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; lub*

c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie."

Podstawa prawna:

Zgodnie z art. 35 ust. 3 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.

a także w wytycznych Grupy Roboczej art. 29 WP 248 rew.01 17/PL dotyczących oceny skutków dla ochrony danych i pomagające ustalić, czy przetwarzanie może powodować wysokie ryzyko do celów rozporządzenia 2016/679 tj.:

1) **Ocena lub punktacja:** w tym profilowanie i prognozowanie w szczególności na podstawie „aspektów dotyczących efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą" (motywy 71 i 91).

2) **Automatyczne podejmowanie decyzji o skutku prawnym lub podobnie znaczącym skutku:** przetwarzanie mające na celu podjęcie decyzji w sprawie osób, których dane dotyczą, wywołujących „skutki prawne wobec osoby fizycznej" lub decyzji, które „w podobny sposób istotnie na nią wpływają" (art. 35 ust. 3 lit. a)). Zagrożenie: przetwarzanie mogące prowadzić do wykluczenia lub dyskryminacji osób fizycznych. Przetwarzanie mające niewielki wpływ na osoby fizyczne lub niemające na nie żadnego wpływu nie spełnia tego konkretnego kryterium.

3) **Systematyczne monitorowanie:** przetwarzanie wykorzystywane do obserwacji, monitorowania lub kontrolowania osób, których dane dotyczą, w tym danych gromadzonych za pośrednictwem sieci lub ramach „systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie" (art. 35 ust. 3 lit. c)). Zagrożenie: osoby, których dane dotyczą, nie są świadome tego, kto gromadzi ich dane i w jaki sposób z nich korzysta. Ponadto osoby fizyczne mogą nie być w stanie uniknąć takiego rodzaju przetwarzania w przestrzeni publicznej (lub przestrzeni publicznie dostępnej).

4) **Dane wrażliwe lub dane o charakterze wysoce osobistym:** obejmują szczególne kategorie danych osobowych określone w art. 9 oraz dane osobowe dotyczące wyroków skazujących za przestępstwo lub naruszeń prawa zdefiniowane w art. 10.

5) **Dane przetwarzane na dużą skalę:** przy ustalaniu, czy przetwarzanie danych odbywa się na dużą skalę, Administrator wespół z Inspektorem Ochrony Danych bierze pod uwagę w szczególności następujące czynniki:

   a) liczbę osób, których dane dotyczą – wyrażoną jako konkretna wartość albo jako odsetek populacji odniesienia;

   b) ilość danych lub zakres poszczególnych przetwarzanych pozycji danych;

   c) czas trwania lub trwałość czynności przetwarzania danych;

   d) zakres geograficzny czynności przetwarzania.

6) **Dopasowywanie lub łączenie zbiorów danych:** zbiory pochodząc z co najmniej dwóch operacji przetwarzania danych przeprowadzonych w różnych celach lub przez różnych administratorów danych w sposób wykraczający poza uzasadnione oczekiwania osób, których dane dotyczą.

7) **Dane dotyczące osób wymagających szczególnej opieki, których dane dotyczą:** przetwarzanie tego rodzaju danych stanowi jedno z kryteriów ze względu na zwiększoną nierównowagę sił między osobami, których

dane dotyczą, a administratorem danych, co oznacza, że osoby fizyczne mogą mieć trudności z wyrażeniem zgody na przetwarzanie swoich danych lub z wyrażeniem sprzeciwu wobec ich przetwarzania, lub mogą mieć trudności z korzystaniem z przysługujących im praw. Do osób wymagających szczególnej opieki, których dane dotyczą, zalicza się dzieci, pracowników, bardziej wrażliwe grupy społeczne wymagające szczególnej ochrony oraz w każdą sytuację, gdy można stwierdzić brak równowagi między stanowiskiem osoby, której dane dotyczą, a stanowiskiem administratora.

8) **Innowacyjne wykorzystanie lub stosowanie nowych rozwiązań technologicznych lub organizacyjnych:** takich jak połączenie technologii rozpoznającej odcisk palca i twarz w celu poprawy fizycznej kontroli dostępu. Zastosowanie takiej technologii może wiązać się z nowymi formami gromadzenia i wykorzystania danych, co może stwarzać ryzyko naruszenia praw i wolności osób fizycznych. Ocena skutków dla ochrony tych danych pomoże Administratorowi zrozumieć ryzyko i je wyeliminować.

9) **Gdy samo przetwarzanie „uniemożliwia osobom, których dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy":** Obejmuje to operacje przetwarzania, których celem jest umożliwienie osobom, których dane dotyczą, uzyskania dostępu do usługi lub zawarcia umowy, zmiana tego dostępu lub odmówienie dostępu.

Podstawa prawna:
Zgodnie z wymogami wytycznymi Grupy Roboczej art. 29 WP 248 rew.01 17/PL dotyczącymi oceny skutków dla ochrony danych oraz pomagającymi ustalić, czy przetwarzanie może powodować wysokie ryzyko do celów rozporządzenia 2016/679, s. 10 - 13

4. Administrator przyjmuje zasadę, że przetwarzanie spełniające dwa kryteria z zakresu Komunikatu Prezesa Urzędu Ochrony Danych z 17 czerwca 2019r., będzie skutkowało koniecznością przeprowadzenia Oceny Skutków dla Przetwarzania Danych (DPIA).

5. Administrator przy podejmowaniu decyzji, które z operacji przetwarzania będzie poddawał Analizie Ryzyka Ogólnego, a które Ocenie Skutków dla Przetwarzania Danych (DPIA) posiłkuje się dodatkowo wytycznymi Grupy Roboczej art. 29 WP 248 rew.01 17/PL dotyczącymi oceny skutków dla ochrony danych i pomagającymi ustalić, czy przetwarzanie może powodować wysokie ryzyko do celów rozporządzenia 2016/679.

6. Administrator może uznać, iż przetwarzanie wyczerpujące tylko jedno z przywołanych kryteriów będzie wymagało przeprowadzenia oceny skutków dla ochrony danych.

7. Administrator może równocześnie stwierdzić, iż przetwarzanie wyczerpuje więcej niż dwa kryteria, ale mimo to nie przeprowadza oceny skutków dla ochrony danych. W takim przypadku Administrator uzasadnia i dokumentuje powody, dla których nie przeprowadzono oceny skutków dla ochrony danych.

Zgodnie z art. 35 ust. 4 RODO:

> *„Organ nadzorczy ustanawia i podaje do publicznej wiadomości wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych na mocy ust. 1. Organ nadzorczy przekazuje te wykazy Europejskiej Radzie Ochrony Danych, o której mowa w art. 68.".*

Administrator, w procesie podejmowania decyzji o klasyfikacji operacji przetwarzania do Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA) bierze pod uwagę wytyczne Urzędu Ochrony Danych Osobowych w tym zakresie.

Podstawa prawna:
Zgodnie z art. 35 ust. 4 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.

8. 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 2018r.,

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.

Podstawa prawna:

Zgodnie z wymogami wytycznymi Grupy Roboczej art. 29 WP 248 rew.01 17/PL dotyczącymi oceny skutków dla ochrony danych oraz pomagającymi ustalić, czy przetwarzanie może powodować wysokie ryzyko do celów rozporządzenia 2016/679, s. 15

9. **„Klasyfikacja Czynności Przetwarzania do Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA)"** – dokument nr: SZBI-PAW-SZAC-Zał. 1 stanowiący Załącznik nr 1 do Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA), określa czynności przetwarzania względem których należy przeprowadzić analizę ryzyka ogólnego oraz czynności przetwarzania, względem których należy przeprowadzić ocenę skutków.

§ 7

Grupowanie podobnych czynności przetwarzania

1. Zgodnie z art. 35 ust. 1 RODO dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem Administrator przeprowadza pojedynczą ocenę.

2. Administrator grupuje podobne operacje przetwarzania dla Analizy ryzyka ogólnego (ARO) oraz Oceny Skutków Przetwarzania Danych (DPIA) uwzględniając kontekst ich przetwarzania w oparciu o następujące kryterium:

   1) **ARO-Gr.1** - dane osobowe związane z pracownikami,

   2) **ARO-Gr.2** - dane osobowe związane z usługami "na zewnątrz" (np. czynności dla społeczeństwa, programy dofinansowania itd...),

   3) **ARO-Gr.3** - dane osobowe związane z usługami "do wewnątrz" (np. kontrahenci, usługodawcy itp...),

   4) **DPIA-Gr.1** - dane osobowe związane z pracownikami,

   5) **DPIA-Gr.2** - dane osobowe związane z usługami "na zewnątrz" (np. czynności dla społeczeństwa, programy dofinansowania itd...).

3. Przedmiotowe grupowanie podobnych operacji przetwarzania znajduje odzwierciedlenie w „Grupowaniu podobnych czynności przetwarzania do Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA)" – dokumencie nr: SZBI-PAW-SZAC-Zał. 2 stanowiącym Załącznik nr 2 do Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA).

§ 8

Szacowanie ryzyka

1. Proces szacowania ryzyka Administrator poprzedza identyfikacją aktywów organizacji, zagrożeń dla aktywów, zabezpieczeń stosowanych w organizacji, podatności (prawdopodobieństwa) oraz następstw (skutków).

2. **Organizacja identyfikuje aktywa** i dzieli je na aktywa podstawowe i aktywa wspierające.

   1) Do aktywów podstawowych organizacja zalicza:

      a) **informacje** - obejmują dane osobowe, które organizacja przetwarza w związku z prowadzoną działalnością; informacje niezbędne do ociągnięcia celów organizacji,

      b) **operacje przetwarzania**: czynności w procesie przetwarzania danych osobowych, które organizacja jest zobowiązana podejmować/utrzymywać, by osiągać cele strategiczne jednostki przy jednoczesnym zapewnieniu bezpieczeństwa przetwarzanych informacji w organizacji.

2) Do aktywów wspierających organizacja zalicza:

a) **sprzęt** - obejmuje przenośne oraz stacjonarne urządzenia komputerowe, urządzenia serwerowe, urządzenia peryferyjne (drukarki czy wymienny napęd dyskowy),

b) **nośniki danych (papierowe) zawierające dane osobowe** - dokumentacja zawierająca treści o charakterze osobowym,

c) **nośniki danych (elektroniczne)** - z racji swojego przeznaczenia mogą być podłączone do urządzenia komputerowego w celu przygotowania danych osobowych do przetwarzania (pendrive, płyta CD, DVD, BD z podziałem na (ROM$^{(tylko\ odczyt)}$ / R$^{(jednokrotny\ zapis)}$ / RW$^{(wielokrotny\ zapis)}$), wymienny dysk twardy),

d) **oprogramowanie** - obejmuje wszystkie programy, dzięki którym bądź w oparciu o nie organizacja przetwarza dane osobowe. W zakresie oprogramowania uwzględnia się system operacyjny, oprogramowanie uzupełniające usługi systemu operacyjnego, oprogramowanie służące do obsługi poczty elektronicznej czy bazy danych, standardowe i dedykowane aplikacje biznesowe np. oprogramowanie księgowe, oprogramowanie służące do obsługi Klientów, pracowników organizacji.

e) **okablowanie** - sieć, którą należy rozumieć przez pryzmat urządzenia używanego do połączenia wielu komputerów i elementów systemu informacyjnego,

f) **personel** – osoby zaangażowane w proces przetwarzania danych osobowych oraz obsługę systemu informacyjnego. Do personelu zaliczamy kierownictwo, osoby upoważnione do przetwarzania danych, osoby, którym nadano uprawnienia do pracy w programach dziedzinowych bazodanowych, osoby, które mają w zakresie swoich obowiązków mają między innymi konieczność utrzymania systemu informacyjnego oraz twórców oprogramowania,

g) **lokalizację** - siedziba, ale również środowisko zewnętrzne. Siedziba organizacji odnosi się do budynków, jakie organizacja zajmuje oraz wszystkich obszarów przetwarzania wewnątrz budynków. Siedziba jest istotna ze względu na jej położenie geograficzne, obszar miejski, przestrzeń publiczną.

Podstawa prawna:
Zgodnie z wymogami normy PN-ISO/IEC 27005:2014-01 Zał. B

3. Organizacja identyfikuje zagrożenia i dzieli je na:

1) **zniszczenia fizyczne**:

a) pożar,
b) zalanie,
c) zanieczyszczenie,
d) poważny wypadek,
e) zniszczenie urządzeń lub nośników,

f) pył, korozja, wychłodzenie.

2) **zjawiska naturalne**:

a) zjawiska klimatyczne,
b) zjawiska sejsmiczne,
c) zjawiska wulkaniczne,
d) zjawiska pogodowe,

e) powódź.

3) **utrata podstawowych usług**:

a) awaria systemu klimatyzacji lub dostaw wody,
b) utrata dostaw prądu,

c) awaria urządzenia telekomunikacyjnego.

4) **zakłócenia spowodowane promieniowaniem**:

a) promieniowanie elektromagnetyczne,
b) promieniowanie cieplne,

c) impuls elektromagnetyczny.

5) **naruszenia bezpieczeństwa informacji**:

a) przechwycenie sygnałów na skutek zjawiska interferencji,
b) szpiegostwo zdalne,
c) podsłuch,
d) kradzież nośników lub dokumentów,
e) kradzież urządzenia,
f) odtworzenie z powtórnie wykorzystanych lub wyrzuconych nośników,
g) ujawnienie,
h) dane z niewiarygodnych źródeł,
i) manipulowanie urządzeniem,
j) sfałszowanie oprogramowania,

k) detekcja umiejscowienia.

6) **awarie techniczne**:

a) awaria urządzenia,
b) niewłaściwe funkcjonowanie urządzeń,
c) przeciążenie systemu informacyjnego,
d) niewłaściwe funkcjonowanie oprogramowania,

e) naruszenie zdolności utrzymania systemu informacyjnego.

7) **nieautoryzowane działania**:

a) nieautoryzowane użycie urządzeń,
b) nieuprawnione kopiowanie oprogramowania,
c) użycie fałszywego lub skopiowanego oprogramowania,
d) zniekształcenie danych,

e) nielegalne przetwarzanie danych.

8) **naruszenia bezpieczeństwa funkcji**:

a) błąd użytkowania,
b) naruszenie praw,
c) fałszowanie praw,
d) odmowa działania,

e) naruszenie dostępności personelu.

Podstawa prawna:
Zgodnie z wymogami normy PN-ISO/IEC 27005:2014-01 Zał. C

4. Organizacja identyfikuje zabezpieczenia zastosowane w organizacji w ten sposób, iż klasyfikuje je w Rejestrze Czynności Przetwarzania stanowiącym załącznik nr 1 do Polityki Bezpieczeństwa Informacji. Administrator uwzględnia stosowane zabezpieczenia w rejestrze czynności przetwarzania z uwagi na konieczność dostosowania wymogów formalnych do art. 30 RODO (opis technicznych i organizacyjnych środków bezpieczeństwa).

5. Organizacja identyfikuje podatność (prawdopodobieństwo) wystąpienia zdarzenia w organizacji zgodnie z poniższą skalą:

PRAWDOPODOBIEŃSTWO	SKALA	CZĘSTOTLIWOŚĆ WYSTĄPIENIA ZDARZENIA
Zdarzenie niemal pewne	4	zdarzenie występuje lub mogłoby wystąpić co najmniej raz w tygodniu
Zdarzenie wysoce prawdopodobne	3	zdarzenie występuje lub mogłoby wystąpić co najmniej raz w miesiącu
Zdarzenie mało prawdopodobne	2	zdarzenie występuje lub mogłoby wystąpić co najmniej raz na kwartał
Zdarzenie prawie nieprawdopodobne	1	zdarzenie nie występuje lub występuje raz w roku

6. Organizacja identyfikuje skutek wystąpienia zdarzenia w organizacji zgodnie z poniższą skalą, a także zgodnie z kontekstem przetwarzania [w zależności, czy organizacja podejmuje Analizę Ryzyka Ogólnego (ARO) czy Ocenę Skutków (DPIA)]:

SKUTEK	SKALA	OPIS NASTĘPSTW
zdarzenie wywołuje katastrofalny skutek	4	• strata finansowa powyżej 100,000 zł dla organizacji, • strata finansowa dla osoby fizycznej, której przetwarzanie dotyczy na tyle **katastrofalna w skutkach**, że powoduje utratę podstawowych potrzeb jak poczucie bezpieczeństwa (np. przetwarzanie takich danych, których naruszenie skutkuje powzięciem pożyczki na podmiot danych, podpisaniem umowy w imieniu podmiotu danych bądź zaciągnięcie innego rodzaju zobowiązań o charakterze gospodarczym w imieniu podmiotu danych), • strata o charakterze niemajątkowym dla osoby fizycznej, której przetwarzanie dotyczy na tyle **katastrofalna w skutkach**, że powoduje np. utratę uznania, dyskryminację, kradzież/sfałszowanie tożsamości, naruszenie dobrego imienia, utratę kontroli nad własnymi danymi osobowymi, ograniczenie praw, nieuprawnione odwrócenie pseudonimizacji, czy wszelkie inne katastrofalne szkody społeczne dla podmiotu danych, • strata wizerunkowa organizacji – brak zaufania ze strony osób, które organizacja obsługuje w ramach wykonywanych zadań publicznych.
zdarzenie wywołuje bardzo znaczący skutek	3	• strata finansowa powyżej 50,000 zł dla organizacji, • strata finansowa dla osoby fizycznej, której przetwarzanie dotyczy **na tyle znacząca w skutkach**, że powoduje utratę podstawowych potrzeb jak poczucie bezpieczeństwa (np. przetwarzanie takich danych, których naruszenie skutkuje powzięciem pożyczki na podmiot danych, podpisaniem umowy w imieniu podmiotu danych bądź zaciągnięcie innego rodzaju zobowiązań o charakterze gospodarczym w imieniu podmiotu danych), • strata o charakterze niemajątkowym dla osoby fizycznej, której przetwarzanie dotyczy **na tyle znacząca w skutkach**, że powoduje np. utratę uznania, dyskryminację, kradzież/sfałszowanie tożsamości, naruszenie dobrego imienia, utratę kontroli nad własnymi danymi osobowymi, ograniczenie praw, nieuprawnione odwrócenie pseudonimizacji, czy wszelkie inne katastrofalne szkody społeczne dla podmiotu danych, • strata wizerunkowa organizacji – brak zaufania ze strony osób, które organizacja obsługuje w ramach wykonywanych zadań publicznych.

SKUTEK	SKALA	OPIS NASTĘPSTW
zdarzenie wywołuje znaczący skutek	2	• strata finansowa powyżej 3000 zł dla organizacji, • strata o charakterze majątkowym dla osoby fizycznej, której przetwarzanie dotyczy, która **może spowodować znaczącą** dla osoby fizycznej utratę podstawowych potrzeb jak poczucie bezpieczeństwa (np. przetwarzanie takich danych, których naruszenie może skutkować powzięciem pożyczki na podmiot danych, podpisaniem umowy w imieniu podmiotu danych bądź zaciągnięcie innego rodzaju zobowiązań o charakterze gospodarczym w imieniu podmiotu danych), • strata o charakterze niemajątkowym dla osoby fizycznej, której przetwarzanie dotyczy **może spowodować znaczącą** np. utratę uznania, dyskryminację, kradzież/sfałszowanie tożsamości, naruszenie dobrego imienia, utratę kontroli nad własnymi danymi osobowymi, ograniczenie praw, nieuprawnione odwrócenie pseudonimizacji, czy wszelkie inne katastrofalne szkody społeczne dla podmiotu danych, • skutek powodujący możliwość wystąpienia straty wizerunkowej organizacji tj. braku zaufania ze strony osób, które organizacja obsługuje w ramach wykonywanych zadań publicznych.
zdarzenie wywołuje niewielki skutek	1	• strata finansowa poniżej 3000 zł dla organizacji, • zdarzenie wywołuje **niewielki skutek** o charakterze majątkowym dla osoby fizycznej, której przetwarzanie dotyczy, • zdarzenie wywołuje **niewielki skutek** o charakterze niemajątkowym dla osoby fizycznej, której przetwarzanie dotyczy, • skutek nie powodujący utraty zaufania ze strony osób fizycznych, względem których jednostka wykonuje zadania publiczne.
zdarzenie nie powoduje skutku (nie występuje)	0	• nie ma straty finansowej, • po stronie osoby fizycznej, której przetwarzanie dotyczy **nie występuje ani szkoda o charakterze majątkowym, ani niemajątkowym**, • zaufanie osób, które organizacja obsługuje w ramach wykonywanych zadań publicznych nie doznaje żadnego uszczerbku.

§ 9

Dokonanie analizy ryzyka

1. Organizacja wykorzystuje następujący wzór analizy ryzyka w zakresie wykonywania:

   1) Analizy Ryzyka Ogólnego,

   2) Oceny Skutków Dla Przetwarzania Danych (DPIA).

WZÓR ANALIZY RYZYKA:

$R = P \times S$

WARTOŚĆ	OPIS	ZAKRES
R	poziom wyliczanego ryzyka	
P	wartość przypisana prawdopodobieństwu materializacji zagrożenia niezrealizowania założonych celów przez organizację	1 - zdarzenie prawie nieprawdopodobne, 2 - zdarzenie mało prawdopodobne, 3 - zdarzenie wysoce prawdopodobne, 4 - zdarzenie niemal pewne.
S	Skutki zdarzenia	0 – zdarzenie nie powoduje skutku (nie występuje), 1 – zdarzenie wywołuje niewielki skutek, 2 – zdarzenie wywołuje znaczący skutek, 3 – zdarzenie wywołuje bardzo znaczący skutek,- 4 - zdarzenie wywołuje katastrofalny skutek.

2. Organizacja przyjmuje następujący zakres macierzy:

			SKUTEK				
			0	1	2	3	4
PRAWDOPODOBIEŃSTWO	Zdarzenie prawie nieprawdopodobne	1	0	1	2	3	4
	Zdarzenie mało prawdopodobne	2	0	2	4	6	8
	Zdarzenie wysoce prawdopodobne	3	0	3	6	9	12
	Zdarzenie niemal pewne	4	0	4	8	12	16

3. Organizacja przyjmuje klasyfikację działań w związku ze zidentyfikowanym ryzykiem w kontekście czynności przetwarzania sklasyfikowanych do Analizy Ryzyka Ogólnego:

POZIOM	SKALA WARTOŚCI	OPIS
Ryzyko NISKIE	od 0 do 4	Ryzyko akceptowane, które nie wymaga dalszego postępowania. Zaniechanie działań względem ryzyka akceptowalnego.
Ryzyko ŚREDNIE	od 6 do 9	Administrator podejmuje decyzję w zakresie: obniżanie ryzyka poprzez wdrażanie odpowiednich środków technicznych i organizacyjnych; pozostawienie ryzyka i niepodejmowanie dalszych działań; unikanie ryzyka poprzez niepodejmowanie działań, które stały się źródłem ryzyka; przeniesienie ryzyka na inny podmiot w zakresie odpowiedzialności za zarządzanie ryzykiem. Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga okresowego monitorowania
Ryzyko WYSOKIE	od 12 do 16	Poziom ryzyka nieakceptowany – wymaga bezwzględnej reakcji – cel: zredukowanie podatności

4. Organizacja przyjmuje klasyfikację działań w związku ze zidentyfikowanym ryzykiem w kontekście czynności przetwarzania sklasyfikowanych do Oceny Skutków Dla Przetwarzania Danych (DPIA):

POZIOM	SKALA WARTOŚCI	OPIS
Ryzyko NISKIE	od 0 do 4	Ryzyko akceptowane, które nie wymaga dalszego postępowania. Zaniechanie działań względem ryzyka akceptowalnego.
Ryzyko ŚREDNIE	od 6 do 9	Administrator podejmuje decyzję w zakresie: obniżanie ryzyka poprzez wdrażanie odpowiednich środków technicznych i organizacyjnych; pozostawienie ryzyka i niepodejmowanie dalszych działań; unikanie ryzyka poprzez niepodejmowanie działań, które stały się źródłem ryzyka; przeniesienie ryzyka na inny podmiot w zakresie odpowiedzialności za zarządzanie ryzykiem. Poziom ryzyka nieakceptowany – działanie może zostać przesunięte w czasie, ale wymaga okresowego monitorowania
Ryzyko WYSOKIE	od 12 do 16	Wymaga bezwzględnej reakcji – cel: zredukowanie podatności Konsultacja z organem nadzorczym konieczna w momencie, kiedy Administrator nie jest w stanie zredukować ryzyka do poziomu przynajmniej średniego mimo, że przewidział wprowadzenie środków bezpieczeństwa.

5. Wyniki analizy szacowania ryzyka zawarte są w:

   1) macierzy ryzyka **analizy ryzyka ogólnego** tj.: „Macierzy ryzyka do Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA)" – dokumencie nr: SZBI-PAW-SZAC-Zał. 3 stanowiącym Załącznik nr 3 do Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA) oraz

   2) macierzy ryzyka **oceny skutków dla przetwarzania danych** tj.: „Macierzy ryzyka do Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA)" – dokumencie nr: SZBI-PAW-SZAC-Zał. 3 stanowiącym Załącznik nr 3 do Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA).

§ 10

Ocena ryzyka dla przetwarzania danych osobowych

1. Ocena ryzyka składa się z następujących elementów:

   1) określenie grupy czynności przetwarzania, dla której zostało zidentyfikowane ryzyko,

   2) aktyw, dla którego zostało zidentyfikowane ryzyko,

   3) kategoria zagrożenia,

   4) rodzaj zagrożenia,

   5) atrybut, dla którego zidentyfikowano ryzyko,

   6) poziom ryzyka przed wprowadzeniem działań naprawczych wraz ze skalą ryzyka po wstępnym procesie,

   7) szacowania ryzyka,

   8) podjęta przez Administratora decyzja wobec zidentyfikowanego ryzyka,

   9) zalecenia wobec zidentyfikowanego ryzyka.

2. Administrator może podjąć cztery rodzaje decyzji wobec zidentyfikowanego ryzyka, a mianowicie:

1) redukcja ryzyka (modyfikowanie ryzyka) – polega na obniżeniu poziomu ryzyka poprzez na przykład zastosowanie dodatkowych zabezpieczeń,

2) akceptacja ryzyka (zachowanie ryzyka) – organizacja nie wprowadza żadnych zmian w zakresie zidentyfikowanego ryzyka (najczęściej do przyjęcia na poziomie niskim),

3) unikanie ryzyka – polega na unikaniu przez organizację działań determinujących powstanie określonych typów ryzyka,

4) dzielenie (transfer) ryzyka – polega na przeniesieniu ryzyka najczęściej poprzez scedowanie skutków ryzyka na podmiot zewnętrzny.

3. Ocena ryzyka dla przetwarzania danych osobowych zawarta jest w „Ocenie ryzyka dla przetwarzania danych osobowych do Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA)" – dokumencie nr: SZBI-PAW-SZAC-Zał. 4 stanowiącym Załącznik nr 4 do Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA).

§ 11

Plan postępowania z ryzykiem wraz z wtórnym procesem szacowania ryzyka po wdrożeniu zabezpieczeń

1. Plan postępowania z ryzykiem określa:

1) określenie grupy czynności przetwarzania, dla której zostało zidentyfikowane ryzyko,

2) aktyw, dla którego zostało zidentyfikowane ryzyko,

3) kategorię zagrożenia,

4) rodzaj zagrożenia,

5) atrybut, dla którego zidentyfikowano ryzyko,

6) zalecenia wobec zidentyfikowanego ryzyka,

7) komórkę organizacyjną odpowiedzialną za wprowadzenie zaleceń,

8) termin realizacji wdrożenia zaleceń,

9) poziom ryzyka po wprowadzeniu działań naprawczych (wtórny proces szacowania ryzyka) wraz ze skalą ryzyka po wprowadzeniu tychże działań,

10) właściciela ryzyka.

2. Plan postępowania z ryzykiem wraz z wtórnym procesem szacowania ryzyka zawarty jest w „Planie postępowania z ryzykiem wraz z wtórnym procesem szacowania ryzyka po wdrożeniu zabezpieczeń do Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA)" – dokumencie nr: SZBI-PAW-SZAC-Zał. 5 stanowiącym Załącznik nr 5 do Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA).

§ 12

Akceptacja ryzyka szczątkowego

Akceptacja ryzyka przez Administratora następuje poprzez złożenie formalnego oświadczenia, którego treść stanowi zawartość „Oświadczenia właściciela ryzyka" – dokumentu nr: SZBI-PAW-SZAC-Zał. 6 stanowiącym Załącznik nr 6 do Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA).

§ 13

Konsultacje z organem nadzorczym

Jeżeli mimo zastosowania odpowiednich środków technicznych lub organizacyjnych, 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.

Podstawa prawna:
Zgodnie z art. 36 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.

§ 14

Monitorowanie i przegląd ryzyka

1) Administrator deklaruje chęć utrzymania założonego poziomu bezpieczeństwa danych osobowych przetwarzanych w organizacji poprzez:
    1) przeprowadzanie nie rzadziej niż raz na rok przeglądów ryzyk,
    2) przeprowadzanie nie rzadziej niż raz na 6 miesięcy przeglądów stanu bezpieczeństwa,
    3) przeprowadzanie oceny skutków względem już poddanych przeglądowi w zakresie praw i wolności czynności przetwarzania, nie rzadziej, niż raz na rok,
    4) przeprowadzanie oceny skutków dla nowych kategorii przetwarzania czy zastosowania nowoczesnych technologii przetwarzania, przed rozpoczęciem ich przetwarzania z uwzględnieniem ochrony danych w fazie projektowania oraz domyślnej ochrony danych,
    5) stosowanie procedur postępowania w przypadku wystąpienia incydentu,
    6) przeprowadzanie cyklicznie szkoleń z zakresu ochrony danych osobowych,
    7) ustalenie odpowiedzialności za ciągły proces minimalizacji ryzyka.
2) Administrator uwzględnia fakt, iż prowadzenie Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA) jest procesem ciągłym, a nie jednorazowym.