ZARZĄDZENIE NR 77/2019
STAROSTY RACIBORSKIEGO

z dnia 5 czerwca 2019 r.

w sprawie zasad szacowania ryzyka w operacjach przetwarzania danych osobowych w Starostwie Powiatowym w Raciborzu

Na podstawie art. 35 ust. 2 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (t.j.: Dz. U. z 2019 r. poz. 511), art. 35 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady Unii Europejskiej 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 (RODO)

zarządzam, co następuje:

§ 1. 1. Mając na uwadze konieczność uwzględnienia w procesie przetwarzania danych osobowych prawdopodobieństwa i powagi ryzyka naruszenia praw lub wolności osób, których przetwarzanie dotyczy, wprowadzam w Starostwie Powiatowym w Raciborzu obowiązek szacowania ryzyka w stosunku do aktualnie prowadzonych, jak i planowanych operacji przetwarzania danych osobowych.

2. Wprowadzam w życie zasady szacowania ryzyka w operacjach przetwarzania danych osobowych w Starostwie Powiatowym w Raciborzu.

Rozdział 1.
Podstawowe pojęcia

§ 2. Ilekroć w Zarządzeniu jest mowa o:

1) **Starostwie** – należy przez to rozumieć Starostwo Powiatowe w Raciborzu;
2) **Administratorze Danych** – należy przez to rozumieć Starostę Raciborskiego, który decyduje o celach i sposobach przetwarzania danych osobowych w Starostwie;
3) **Inspektorze Ochrony Danych** (IOD) – należy przez to rozumieć osobę, której Administrator Danych powierzył realizację zadania w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych zgodnie z art. 39 RODO;
4) **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;
5) **PUODO** – należy przez to rozumieć Prezesa Urzędu Ochrony Danych Osobowych - organ nadzorczy w rozumieniu RODO;
6) **Grupie Roboczej Art. 29** - należy przez to rozumieć zespół roboczy ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych - niezależny podmiot o charakterze doradczym, powołany na mocy art. 29 RODO;
7) **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;
8) **analizie ryzyka** – rozumie się przez to proces identyfikacji źródeł ryzyka i oszacowania ryzyka;
9) **ocenie ryzyka** – proces porównywania oszacowanego ryzyka w celu określenia znaczenia ryzyka;
10) **ryzyku** – rozumie się przez to kombinację prawdopodobieństwa zdarzenia i jego konsekwencji;
11) **ryzyku szczątkowym** – rozumie się przez to ryzyko pozostające po procesie postępowania z ryzykiem;
12) **postępowaniu z ryzykiem** – rozumie się przez to proces zmiany poziomu ryzyka poprzez zastosowanie odpowiednich środków technicznych i organizacyjnych;
13) **akceptacji ryzyka** – rozumie się przez to decyzję Administratora Danych o tym, aby ryzyko zaakceptować;
14) **podatności** – rozumie się przez to słabość w strukturze fizycznej, technicznej, organizacyjnej Starostwa;

15) **incydencie** – rozumie się przez to zdarzenie mające lub mogące mieć negatywny wpływ na bezpieczeństwo informacji w Starostwie. Incydent może powodować w stosunku do osoby fizycznej, której dane osobowe Starostwo przetwarza, szkodę o charakterze majątkowym lub niemajątkowym;

16) **poufności** – rozumie się przez to właściwość polegającą na tym, że osoba nieupoważniona bądź podmiot nie mają dostępu do danych osobowych, które temu atrybutowi podlegają;

17) **integralności** – rozumie się przez to właściwość polegającą na tym, że aktywa w postaci informacji/danych osobowych pozostają kompletne;

18) **dostępności** – rozumie się przez to właściwość polegającą na tym, że aktywa w postaci informacji/danych osobowych pozostają dostępne dla osób upoważnionych/uprawnionych do ich przetwarzania;

19) **bezpieczeństwie informacji** – rozumie się przez to zachowanie wobec przetwarzanych danych osobowych/informacji takich atrybutów jak poufność, integralność oraz dostępność.

Rozdział 2.
Cel szacowania ryzyka

§ 3. 1. Administrator Danych przeprowadza proces szacowania ryzyka w zakresie bezpieczeństwa informacji w celu zidentyfikowania obszarów, które mogą istotnie wpływać na osobę, której przetwarzanie dotyczy. Administrator Danych 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).

Rozdział 3.
Wytyczne wykorzystywane do przeprowadzenia Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA)

§ 4. Z racji tego, iż Administrator Danych w ramach realizacji praw podstawowych w zakresie ochrony danych osobowych, kieruje się zasadą legalności przetwarzania zgodnego z prawem, opiera proces szacowania ryzyka na następujących normach ISO oraz wytycznych Grupy Roboczą Art. 29:

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

2) 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);

3) 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.

Rozdział 4.
Oznaczenie uwarunkowań związanych z funkcjonowaniem Starostwa – ustalenie kontekstu

§ 5. 1. Określa się, które z uwarunkowań zewnętrznych bądź wewnętrznych mają znaczenie dla szacowania ryzyka w Starostwie.

2. Uwarunkowania zewnętrzne istotnie wpływające na Starostwo:

1) relacje z innymi administratorami danych osobowych;

2) relacje z innymi podmiotami zewnętrznymi;

3) zasięg terytorialny działalności Starostwa;

4) uwarunkowania prawne Starostwa.

3. Uwarunkowania wewnętrzne istotnie wpływające na Starostwo:

1) struktura i rozmiary Starostwa;

2) uwarunkowania formalne wewnętrzne (polityki, regulaminy);

3) sposoby podejmowania decyzji w Starostwie względem bezpieczeństwa przepływu danych.

4. W Starostwie na etapie tworzenia polityki (zasad) ochrony danych przeanalizowano:

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

2) staranność po stronie Starostwa 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 Starostwo działa w imieniu innego administratora danych (w procesie przetwarzania danych Starostwo 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.

Rozdział 5.
Wybór metody przeprowadzenia Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA)

§ 6. 1. Administrator Danych do szacowania ryzyka wykorzystuje metodę CRAMM (CCTA Risk Analysis and Management Method).

2. Metoda, o której mowa w ust. 1 jest metodą jakościową, gdzie wielkość zagrożenia ocenia się przez pryzmat doświadczenia oraz intuicji osoby szacującej ryzyko (subiektywne odczucie).

3. Atrybuty, jakie Administrator Danych 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.

Rozdział 6.
Klasyfikacja czynności przetwarzania

§ 7. 1. Administrator Danych, w pierwszej kolejności dzieli czynności przetwarzania danych osobowych (określone w Załączniku Nr 2 do Zarządzenia Nr 59/2018 Starosty Raciborskiego z dnia 25 maja 2018r. w sprawie zasad ochrony danych w Starostwie Powiatowym w Raciborzu) na te, które wymagają Oceny Skutków dla Przetwarzania Danych (DPIA) oraz te, względem których Administrator Danych wykonuje Analizę Ryzyka Ogólnego.

2. Kryterium, według którego Administrator Danych dokonuje wstępnej klasyfikacji z uwzględnieniem kontekstu przetwarzania danych są 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 naruszenia praw i wolności osób fizycznych, których przetwarzanie dotyczy zgodnie z RODO 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 RODO);

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 RODO). 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 RODO). 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 RODO oraz dane osobowe dotyczące wyroków skazujących za przestępstwo lub naruszeń prawa zdefiniowane w art. 10 RODO;

5) dane przetwarzane na dużą skalę: przy ustalaniu, czy przetwarzanie danych odbywa się na dużą skalę, Administrator Danych 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 pochodzące 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 danych;

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 danych 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.

3. Administrator Danych przyjmuje zasadę, że przetwarzanie spełniające dwa kryteria, będzie skutkowało koniecznością przeprowadzenia Oceny Skutków dla Przetwarzania Danych (DPIA).

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

5. Administrator Danych może równocześnie stwierdzić, iż przetwarzanie wyczerpuje więcej niż dwa kryteria, ale mimo to nie przeprowadza oceny skutków dla ochrony danych. W takim przypadku Administrator Danych uzasadnia i dokumentuje powody, dla których nie przeprowadzono oceny skutków dla ochrony danych. Zgodnie z art. 35 ust. 4 RODO, Administrator Danych, 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.

6. Ocena Skutków Dla Przetwarzania Danych (DPIA) nie jest obowiązkowa w przypadkach gdy:

1) nie jest prawdopodobne, aby operacja przetwarzania może powodować wysokie ryzyko;

2) przeprowadzono już podobną ocenę skutków dla ochrony danych;

3) operację przetwarzania zatwierdzono przed majem 2018r.;

4) operacja przetwarzania posiada podstawę prawną, która reguluje daną operację przetwarzania;

5) operacja przetwarzania znajduje się w wykazie operacji przetwarzania, które nie podlegają ocenie skutków dla ochrony danych.

7. „Klasyfikacja Czynności Przetwarzania do Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA)" – stanowiąca Załącznik nr 1 do niniejszego zarządzenia, określa czynności przetwarzania, względem których należy przeprowadzić analizę ryzyka ogólnego oraz czynności przetwarzania, względem których należy przeprowadzić ocenę skutków.

Rozdział 7.
Grupowanie podobnych czynności przetwarzania

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

2. Administrator Danych 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)" – stanowiącym Załącznik nr 2 do niniejszego zarządzenia.

Rozdział 8.
Szacowanie ryzyka

§ 9. 1. Proces szacowania ryzyka Administrator Danych poprzedza identyfikacją aktywów Starostwa, zagrożeń dla aktywów, zabezpieczeń stosowanych w Starostwie, podatności (prawdopodobieństwa) oraz następstw (skutków).

2. Po identyfikacji aktywa dzieli się na aktywa podstawowe i aktywa wspierające.

1) Do aktywów podstawowych zalicza się:

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

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

2) Do aktywów wspierających zalicza się:

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 ROM, wymienny dysk twardy);

d) oprogramowanie - obejmuje wszystkie programy, dzięki którym bądź w oparciu o nie Starostwo 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 Starostwa;

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 w zakresie swoich obowiązków mają między innymi konieczność utrzymania systemu informacyjnego oraz twórców oprogramowania;

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

3. Po identyfikacji zagrożenia dzieli się 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.

4. Po identyfikacji zastosowane zabezpieczenia klasyfikuje się w Rejestrze Czynności Przetwarzania Danych Osobowych stanowiącym Załącznik Nr 2 do Zarządzenia Nr 59/2018 Starosty Raciborskiego z dnia 25 maja 2018r. w sprawie zasad ochrony danych w Starostwie Powiatowym w Raciborzu. Administrator Danych 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. Identyfikacja podatności (prawdopodobieństwa) wystąpienia zdarzenia następuje zgodnie z poniższą skalą:

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

6. Identyfikacja skutków wystąpienia zdarzenia następuje zgodnie z poniższą skalą:

SKUTEK	SKALA	OPIS NASTĘPSTW
zdarzenie wywołuje katastrofalny skutek	4	·strata finansowa powyżej 100 000 zł dla Starostwa, ·strata finansowa dla osoby fizycznej, której przetwarzanie dotyczy na tyle katastrofalna w skutkach, że powoduje utratę podstawowych potrzeb jak poczucie bezpieczeństwa, ·strata osobista dla osoby fizycznej, której przetwarzanie

		dotyczy na tyle katastrofalna w skutkach, że powoduje utratę uznania (dyskryminacja, kradzież tożsamości, naruszenie dobrego imienia), ·kara finansowa nałożona przez organ nadzorczy wysokości 100 000 zł, ·zakaz przetwarzania danych nałożony decyzją administracyjną przez organ nadzorczy, ·strata wizerunkowa Starostwa – brak zaufania ze strony osób, które Starostwo obsługuje w ramach wykonywanych zadań publicznych, ·orzeczenie wyroku skazującego w zakresie przetwarzania danych przez Starostwo.
zdarzenie wywołuje bardzo znaczący skutek	3	·strata finansowa powyżej 50 000 zł dla Starostwa, ·strata finansowa dla osoby fizycznej, której przetwarzanie dotyczy na tyle znacząca w skutkach, że powoduje utratę podstawowych potrzeb jak poczucie bezpieczeństwa, ·strata osobista dla osoby fizycznej, której przetwarzanie dotyczy na tyle znacząca w skutkach, że powoduje utratę uznania (dyskryminacja, kradzież tożsamości, naruszenie dobrego imienia), ·kara finansowa nałożona przez organ nadzorczy powyżej 50 000 zł, ·zakaz przetwarzania danych nałożony decyzją administracyjną przez organ nadzorczy, ·strata wizerunkowa Starostwa– brak zaufania ze strony osób, które Starostwo obsługuje w ramach wykonywanych zadań publicznych.
zdarzenie wywołuje znaczący skutek	2	·strata finansowa powyżej 3 000 zł dla Starostwa, ·strata finansowa dla osoby fizycznej, której przetwarzanie dotyczy na tyle znacząca w skutkach, że powoduje utratę podstawowych potrzeb jak poczucie bezpieczeństwa, ·strata osobista dla osoby fizycznej, której przetwarzanie dotyczy na tyle znacząca w skutkach, że powoduje utratę uznania (dyskryminacja, kradzież tożsamości, naruszenie dobrego imienia), ·kara finansowa nałożona przez organ nadzorczy powyżej 3 000 zł, ·zakaz przetwarzania danych nałożony decyzją administracyjną przez organ nadzorczy, ·strata wizerunkowa Starostwa– brak zaufania ze strony osób, które Starostwo obsługuje w ramach wykonywanych zadań publicznych.
zdarzenie wywołuje niewielki skutek	1	·strata finansowa poniżej 3 000 zł dla Starostwa, ·strata finansowa dla osoby fizycznej, której przetwarzanie dotyczy wywołuje niewielki skutek, ·strata osobista dla osoby fizycznej, której przetwarzanie wywołuje niewielki skutek, ·organ nadzorczy daje upomnienie i wzywa do naprawienia braków formalnych (przy założeniu, że Starostwo wypełnia wskazania organu nadzorczego), ·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 osobistym,

		·zaufanie osób, które Starostwo obsługuje w ramach wykonywanych zadań publicznych nie doznaje żadnego uszczerbku.

Rozdział 9.
Dokonanie analizy ryzyka

§ 10. 1. Wykorzystuje się następujący wzór analizy ryzyka w zakresie wykonywania:

1) Analizy Ryzyka Ogólnego,

2) Oceny Skutków Dla Przetwarzania Danych (DPIA).

WZÓR ANALIZY RYZYKA:
$R = P^{x} S$

WARTOŚĆ	OPIS	ZAKRES
R	poziom wyliczanego ryzyka	
P	wartość przypisana prawdopodobieństwu materializacji zagrożenia niezrealizowania założonych celów przez Starostwo	1 - zdarzenie 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. Przyjmuje się następujący zakres macierzy:

			SKUTEK				
			0	**1**	**2**	**3**	**4**
PRAWDOPODOBIEŃSTWO	Zdarzenie 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. Starostwo 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 Danych 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. Przyjmuje się 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 Danych 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 Danych nie jest w stanie zredukować ryzyka do poziomu przynajmniej średniego mimo, że przewidział wprowadzenie środków bezpieczeństwa.

5. Wyniki analizy szacowania ryzyka zawarte są w macierzach:

1) ryzyka analizy ryzyka ogólnego, stanowiącej Załącznik nr 3 do niniejszego zarządzenia;

2) ryzyka oceny skutków dla przetwarzania danych, stanowiącej Załącznik nr 4 do niniejszego zarządzenia.

Rozdział 10.
Ocena ryzyka dla przetwarzania danych osobowych

§ 11. 1. Na ocenę ryzyka składają się następujące elementy:

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 Danych decyzja wobec zidentyfikowanego ryzyka;

9) zalecenia wobec zidentyfikowanego ryzyka.

2. Administrator Danych 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) – Starostwo nie wprowadza żadnych zmian w zakresie zidentyfikowanego ryzyka (najczęściej do przyjęcia na poziomie niskim);

3) unikanie ryzyka – polega na unikaniu przez Starostwo 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)" – stanowiącej Załącznik nr 5 do niniejszego zarządzenia.

Rozdział 11.
Plan postępowania z ryzykiem wraz z wtórnym procesem szacowania ryzyka po wdrożeniu zabezpieczeń

§ 12. 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)" – stanowiącym Załącznik nr 6 do niniejszego zarządzenia.

Rozdział 12.
Akceptacja ryzyka szczątkowego

§ 13. Akceptacja ryzyka przez Administratora Danych następuje poprzez złożenie formalnego „Oświadczenia właściciela ryzyka" – stanowiącego Załącznik nr 7 do niniejszego zarządzenia.

Rozdział 13.
Konsultacje z organem nadzorczym

§ 14. 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 Danych konsultuje się z organem nadzorczym. Administrator Danych ma świadomość, iż ryzyko wysokie nie może podlegać decyzji w formie akceptacji.

Rozdział 14.
Monitorowanie i przegląd ryzyka

§ 15. 1. Administrator Danych deklaruje chęć utrzymania założonego poziomu bezpieczeństwa danych osobowych przetwarzanych w Starostwie 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 trzy lata;

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 Danych uwzględnia fakt, iż prowadzanie Analizy Ryzyka Ogólnego i Oceny Skutków Dla Przetwarzania Danych (DPIA) jest procesem ciągłym, a nie jednorazowym.

Rozdział 15.
Postanowienia końcowe

§ 16. Zobowiązuję pracowników Starostwa do zapoznania się z treścią niniejszego zarządzenia i jego stosowanie.

§ 17. 1. Załączniki do zarządzenia stanowią dokumentację wewnętrzną Starostwa Powiatowego w Raciborzu i nie podlegają publikacji w Biuletynie Informacji Publicznej na podstawie wdrożonych założeń Zintegrowanego Systemu Zarządzania opartego na wymaganiach normy ISO 9001:2015 w Starostwie Powiatowym w Raciborzu (pkt 7.5.3 Nadzór nad udokumentowanymi informacjami).

2. Zmiana treści załączników nie powoduje konieczności zmiany niniejszego zarządzenia.

§ 18. 1. Wykonanie zarządzenia powierzam wszystkim pracownikom Starostwa.

2. Nadzór nad wykonaniem zarządzenia sprawować będę osobiście.

3. Zarządzenie zostanie podane do wiadomości pracowników Starostwa poprzez umieszczenie jego tekstu w Intranecie.

§ 19. Zarządzenie wchodzi w życie z dniem podpisania i podlega publikacji w Bazie Rejestrów Urzędowych na stronie internetowej www.bip.powiatraciborski.pl.

Starosta

Grzegorz Swoboda