ZARZĄDZENIE NR 59/2018
STAROSTY RACIBORSKIEGO

z dnia 25 maja 2018 r.

w sprawie zasad ochrony danych 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 2018 r. poz. 995), art. 37 ust. 1 lit. a 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. Wprowadzam zasady ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w Starostwie Powiatowym w Raciborzu.

§ 2. Celem Zarządzenia jest ochrona podstawowych praw i wolności osób fizycznych, w szczególności prawa do ochrony danych osobowych.

Rozdział 1.
Podstawowe pojęcia

§ 3. Ilekroć w zarządzeniu jest mowa o:

1) 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 (RODO),
2) PUODO – należy przez to rozumieć Prezesa Urzędu Ochrony Danych Osobowych - organ nadzorczy w rozumieniu rozporządzenia (RODO),
3) Ustawie – należy przez to rozumieć ustawę z dnia 10 maja 2018 roku o ochronie danych osobowych,
4) Starostwie – należy przez to rozumieć Starostwo Powiatowe w Raciborzu,
5) Administratorze Danych – należy przez to rozumieć Starostę Raciborskiego, który decyduje o celach i sposobach przetwarzania danych osobowych w Starostwie,
6) 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,
7) Administratorze Systemu Informatycznego (ASI) – należy przez to rozumieć pracownika zgodnie z zakresem czynności odpowiedzialnego za ciągłość pracy, bezpieczeństwo i rozwój Systemu Informatycznego w Starostwie,
8) dysponencie – należy przez to rozumieć kierownika komórki organizacyjnej odpowiadającego za przetwarzanie danych w aplikacji lub procesie przetwarzania danych osobowych,
9) upoważnionym – należy przez to rozumieć osobę posiadającą upoważnienie do przetwarzania danych osobowych, dla których administratorem jest Starosta Raciborski,
10) użytkowniku – należy przez to rozumieć osobę posiadającą upoważnienie do przetwarzania danych w Systemie Informatycznym Starostwa,
11) danych osobowych – należy przez to rozumieć informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturalną lub społeczną tożsamość osoby fizycznej,
12) przetwarzaniu danych osobowych – należy przez to rozumieć operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany,

taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,

13) poufności danych – należy przez to rozumieć zapewnienie, że dane nie są udostępniane lub ujawniane nieupoważnionym osobom lub podmiotom,

14) integralności danych – należy przez to rozumieć zapewnienie, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

15) dostępności danych – należy przez to rozumieć zapewnienie, że dane są osiągalne i możliwe do wykorzystania na żądanie w założonym czasie, przez upoważnione osoby lub podmioty,

16) rozliczalności – należy przez to rozumieć zapewnienie, że działania osoby lub podmiotu mogą być przypisane tylko tej osobie lub podmiotowi,

17) autentyczności – należy przez to rozumieć zapewnienie, że tożsamość osoby lub podmiotu jest taka, jak deklarowana,

18) niezaprzeczalności – należy przez to rozumieć brak możliwości wyparcia się przez osobę lub podmiot swego uczestnictwa w procesie przetwarzania danych,

19) odbiorcy danych – należy przez to rozmieć każdego, komu udostępnia się dane osobowe, z wyłączeniem: osoby, której dane dotyczą; osoby upoważnionej do przetwarzania danych; przedstawiciela, o którym mowa w art. 27 RODO; podmiotu przetwarzającego, o którym mowa w art. 28 RODO; organów publicznych, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z przepisami prawa,

20) podmiocie przetwarzającym – należy przez to rozumieć podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawartej zgodnie z art. 28 RODO,

21) sieci publicznej – należy przez to rozumieć sieć telekomunikacyjną wykorzystywaną głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych w rozumieniu art. 2 pkt 29 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne,

22) Systemie Informatycznym Starostwa – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych stosowanych w celu przetwarzania danych w Starostwie,

23) aplikacji – należy przez to rozumieć pogram komputerowy, będący częścią Systemu Informatycznego Starostwa służący do przetwarzania danych w określonym dla niego obszarze,

24) administratorze aplikacji – należy przez to rozumieć użytkownika posiadającego uprawnienia do zarządzania aplikacją, odpowiedzialnego za ciągłość pracy i rozwój aplikacji,

25) identyfikatorze użytkownika – należy przez to rozumieć ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę, która jest użytkownikiem systemu informatycznego,

26) identyfikacji użytkownika – należy przez to rozumieć użycie identyfikatora użytkownika w systemie informatycznym w celu weryfikacji jego tożsamości,

27) uwierzytelnieniu – należy przez to rozumieć weryfikowanie przez mechanizmy systemu informatycznego tożsamości użytkownika na podstawie jego identyfikatora,

28) autoryzacji – należy przez to rozumieć weryfikowanie czy dany użytkownik ma prawo dostępu do informacji, do których usiłuje uzyskać dostęp,

29) Active Directory – należy przez to rozumieć usługę systemu informatycznego służącą do uwierzytelniania i autoryzacji użytkowników,

30) incydencie bezpieczeństwa – należy przez to rozumieć pojedyncze zdarzenie lub serię niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań i zagrażają bezpieczeństwu informacji,

31) kierowniku komórki organizacyjnej – należy przez to rozumieć naczelników wydziałów, kierowników referatów, przewodniczących zespołów, pełnomocników biur oraz osoby zatrudnione na samodzielnych stanowiskach pracy,

32) komórce organizacyjnej – należy przez to rozumieć wyodrębniony element struktury Starostwa, realizujący zadania określone w Regulaminie Organizacyjnym, w szczególności: wydział, referat, zespół, biuro oraz samodzielne stanowisko pracy,

33) HelpDesk (Pomoc IT) – należy przez to rozumieć system służący do komunikacji użytkowników z IOD i ASI.

Rozdział 2.
Zakres stosowania

§ 4. 1. Zasady i procedury określone w niniejszym zarządzeniu stosuje się zarówno do danych osobowych przetwarzanych w sposób tradycyjny w księgach, wykazach i innych zbiorach ewidencyjnych, jak i przetwarzanych w systemach informatycznych.

2. Zasady i procedury określone w niniejszym dokumencie stosuje się do wszystkich przetwarzających dane osobowe w Starostwie w szczególności do pracowników i innych osób, które zostały dopuszczone do przetwarzania, np. wolontariuszy, stażystów, praktykantów itd.

3. Zasady i procedury dotyczące przetwarzania danych osobowych przez radnych powiatu raciborskiego określają odrębne regulacje wewnętrzne.

Rozdział 3.
Zapewnienie zgodności przetwarzania danych osobowych z RODO

(przeciwdziałanie ryzyku naruszenia wolności i praw osób, których dane dotyczą)

§ 5. 1. Do realizacji zasad ochrony danych osobowych zalicza się:

1) zasadę legalności przetwarzania - dane osobowe są przetwarzane wyłącznie po spełnieniu jednego z warunków dopuszczalności przetwarzania określonych w art. 6 ust. 1 RODO, a w przypadku szczególnych kategorii danych (tzw. danych wrażliwych) art. 9 i art. 10 RODO,

2) zasadę rzetelności przetwarzania - przetwarzanie rzetelne należy rozumieć jako przetwarzanie uczciwe w stosunku do osób, których dane dotyczą; podejmując dowolne czynności przetwarzania należy respektować prawa i interesy podmiotów danych; należy wziąć pod uwagę, że przetwarzanie może być dokuczliwe dla podmiotu danych i spróbować zminimalizować te uciążliwości; nie można też próbować oszukiwać ani wykorzystywać braku wiedzy lub trudnej sytuacji podmiotu danych,

3) zasadę przejrzystości przetwarzania - należy zapewnić przejrzystą informację podmiotom danych o dotyczącym ich przetwarzaniu; powinny być stworzone dogodne warunki komunikacji umożliwiające zainteresowanym skorzystanie z przyznanych im praw,

4) zasadę ograniczoności celu - dane zbierane są jedynie w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie wolno ich przetwarzać po zebraniu w sposób niezgodny z tymi celami; do celu należy dostosować nie tylko ilość zbieranych danych, ale też zakres ich przetwarzania oraz okres ich przechowywania,

5) minimalizację danych - dane powinny być adekwatne do celu, czyli ograniczone do niezbędnego minimum; metodą urzeczywistnienia tej zasady może być m.in. pseudonimizacja; gdy cel przetwarzania tego nie wymaga, to w ogóle nie należy dokonywać identyfikacji osobowej,

6) prawidłowość danych - dane powinny być prawdziwe (zgodne z prawdą) i w razie potrzeby uaktualniane, należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane,

7) ograniczenie przetwarzania (przechowywanie) - dane wolno przechowywać w formie umożliwiającej identyfikację osoby, której one dotyczą, jedynie przez okres niezbędny dla realizacji celów, w których dane te są przetwarzane,

2. Realizacja obowiązków informacyjnych i zapewnienie przejrzystej komunikacji odbywa się poprzez:

1) przekazywanie informacji podmiotom danych formułowane w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem,

2) uprawdopodobnienie, że informacje są przekazywane osobie, której dane dotyczą; w razie wątpliwości należy zażądać dodatkowych informacji w celu zweryfikowania tożsamości osoby, która się kontaktuje w celu uzyskania informacji,

3) przekazywanie informacji osobie, której dane dotyczą dbając o to, aby informacja ta obejmowała wyłącznie dane jej dotyczące; należy dołożyć starań, by informacja przekazywana jednej osobie nie zdradzała informacji o innych,

4) zbieranie informacji bezpośrednio od osoby, której dotyczą z jednoczesnym przekazaniem tej osobie informacji wskazanych w art. 13 ust. 1 i 2 RODO (klauzule informacyjne przyjęte do stosowania w Starostwie); obowiązek ten należy zrealizować w trakcie pozyskiwania informacji,

5) zbieranie danych z innego źródła niż od osoby, której dotyczą spełniając obowiązek informacyjny w zakresie art. 14 ust. 1 i 2 RODO; należy to zrobić w rozsądnym terminie (do miesiąca) od zebrania informacji, nie później jednak niż przy pierwszej komunikacji z podmiotem danych lub pierwszym udostępnieniem danych,

6) stosowną informację w zakresie art. 13 ust. 1 i 2 lub art. 14 ust. 1 i 2 RODO przekazaną podmiotowi danych w przypadku zmiany celu przetwarzania dokonanym po zebraniu danych, chyba, że został już o tym uprzedzony,

7) zapewnienie dogodnych warunków komunikacji umożliwiających osobom, których dane dotyczą kontakt w celu realizacji przyznanych im praw.

3. Realizacja żądań osób, których dane dotyczą odbywa się w niżej wymienionych przypadkach:

1) jeżeli zainteresowany skorzysta z prawa dostępu do danych (zażąda informacji na temat dotyczącego go przetwarzania) to udziela się mu jej zgodnie z art. 12 ust. 1 i 2 RODO; jeśli podmiot danych tego zażąda, a jest to możliwe, przekazuje się mu także kopię dotyczących go danych; informacji na żądanie udziela się zasadniczo w terminie miesiąca, chyba, że sprawa jest skomplikowana; wtedy przedłużenie terminu następuje zgodnie z art. 12 ust. 3 RODO,

2) jeżeli zainteresowany skorzysta z prawa do sprostowania, to na jego żądanie dokonuje się sprostowania nieprawidłowych danych; prawo to obejmuje też uzupełnienie niekompletnych danych, przy czym kompletność ocenia się z uwzględnieniem celów przetwarzania; o ile to możliwe, to o dokonanym sprostowaniu informuje się odbiorców, którym dane zostały przekazane,

3) jeżeli zainteresowany skorzysta z prawa do usunięcia danych (bycia zapomnianym), to na jego żądanie usuwa się dotyczące go dane, chyba że spełnione są wymogi ich dalszego przetwarzania z art. 17 ust. 3 RODO; o ile to możliwe, to o dokonanym usunięciu informuje się odbiorców, którym dane zostały przekazane; gdy dane zostały upublicznione należy podjąć starania w celu usunięcia wszelkich łączy do tych danych, ich kopii lub replikacji stworzonych przez innych administratorów,

4) jeżeli zainteresowany skorzysta z prawa do ograniczenia przetwarzania, to na jego żądanie należy ograniczyć przetwarzanie do wskazanych czynności, chyba, że zachodzą przesłanki ich dalszego przetwarzania, w szczególności te wymienione w art. 18 ust. 2 RODO; o ile to możliwe, to o dokonanym ograniczeniu informuje się odbiorców, którym dane zostały przekazane,

5) jeżeli zainteresowany skorzysta z prawa do przeniesienia danych, to dostarcza mu się dotyczących go danych w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego; prawo to przysługuje, gdy dane mają postać zapisu elektronicznego i są przetwarzane na podstawie warunku zgody lub realizacji umowy; na żądanie zainteresowanego dane dostarcza się bezpośrednio wskazanemu przez niego podmiotowi,

6) jeżeli zainteresowany skorzysta z prawa sprzeciwu wobec przetwarzania jego danych osobowych, w tym profilowania, powołując się na swoją szczególną sytuację, to należy zaprzestać dalszego przetwarzania dotyczących go danych, chyba, że spełnione są przesłanki dalszego przetwarzania określone w art. 21 ust. 1 RODO,

7) jeżeli zainteresowany skorzysta z prawa sprzeciwu wobec przetwarzania jego danych w celach marketingowych, w tym profilowania, to nie można nie uwzględnić sprzeciwu.

4. Zgoda na przetwarzanie danych osobowych powinna odpowiadać niżej wymienionym warunkom:

1) zgodnie z art. 6 ust. 1 lub 9 ust. 1 RODO jeżeli podstawą przetwarzania danych osobowych jest zgoda osoby, której dane dotyczą to przyzwolenie na przetwarzanie danych powinno być dobrowolne, konkretne, świadome i jednoznaczne; ponadto, powinna spełniać też wymogi rozliczalności i transparentności,

2) zapewnia się prawo do wycofania zgody,

3) nie jest dopuszczalne uzależnienie wykonania usługi niezwiązanej bezpośrednio ze zgodą od jej udzielenia,

4) w przypadku usług społeczeństwa informacyjnego oferowanych dziecku podejmuje się wszelkie niezbędne działania, by uzyskać aprobatę opiekuna.

5. Profilowanie to podejmowanie zautomatyzowanych decyzji wobec indywidualnych osób, w tym profilowanie dopuszczalne jest wyłącznie w przypadkach określonych w art. 22 ust. 3 RODO, w szczególności, gdy zainteresowana osoba wyraziła na to zgodę. Osobie, wobec której są podejmowane zautomatyzowane decyzje lub którą się profiluje zapewnia się prawo do:

1) zakwestionowania tej decyzji,

2) wyrażenia własnego stanowiska w przedmiocie podejmowanych wobec niej decyzji i profilowania,

3) uzyskania interwencji ludzkiej, czyli do indywidualnego rozpatrzenia jej sprawy przez administratora danych,

4) wniesienia sprzeciwu zgodnie z art. 21 ust. 1 i 2 RODO.

6. Udostępnianie danych osobowych odbywa się zgodnie z następującymi wytycznymi:

1) jeśli zgodnie z przepisami prawa administrator danych jest zobowiązany do przekazywana danych osobowych wskazanym podmiotom (np. Urzędowi Skarbowemu lub Zakładowi Ubezpieczeń Społecznych) to upoważnieni pracownicy administratora danych realizują ten wymóg zgodnie z zakresem swoich obowiązków służbowych stosując się ściśle do wskazanych przepisów,

2) jeśli do administratora danych wystąpi z wnioskiem o udzielenie informacji osobowej podmiot, który twierdzi, że jest uprawniony do uzyskania takiej informacji na podstawie przepisów prawa, udostępnienie informacji może nastąpić jedynie po:

   a) zweryfikowaniu podstawy prawnej udostępnienia,

   b) zweryfikowaniu czy składający wniosek jest podmiotem, za który się podaje,

   c) odnotowaniu udostępnienia w ewidencji udostępnień danych osobowych.

3) ewidencję udostępnień danych osobowych prowadzi IOD, zgodnie ze wzorem określonym w Załączniku nr 13 do niniejszego zarządzenia.

4) w przypadku, gdy z wnioskiem o którym mowa w pkt 2) wystąpi uprawniony funkcjonariusz, w szczególności policji, i wnioskujący stwierdzi, że istnieje konieczność niezwłocznego działania udostępnienie informacji może nastąpić po:

   a) wylegitymowaniu funkcjonariusza,

   b) na podstawie pisemnego oświadczenia funkcjonariusza lub za pisemnym pokwitowaniem przez niego uzyskania dokumentów.

5) jeśli złożenie oświadczenia lub pokwitowanie uzyskania danych przez funkcjonariusza nie są możliwe ze względu na okoliczności udostępniania, osoba udostępniająca informacje sporządza na tą okoliczność notatkę służbową. Ewidencjonując udostępnienie IOD opisze w rubryce „Uwagi" ewidencji udostępnień szczególne okoliczności udostępnienia.

6) jeśli do administratora danych wystąpi z wnioskiem o udzielenie informacji osobowej podmiot, który nie jest uprawniony do uzyskania takiej informacji na podstawie przepisów prawa udostępnienie informacji może nastąpić jedynie gdy:

   a) cel przetwarzania nie ulega zmianie;

   b) osobie, której dane mają być udostępnione zostanie umożliwione skorzystanie z prawa sprzeciwu,

   c) nastąpi zweryfikowanie tożsamości podmiotu składającego wniosek,

   d) udostępnienie zostanie odnotowane w ewidencji udostępnień danych osobowych.

7. Przekazywanie danych do państw trzecich lub organizacji międzynarodowych jest zasadniczo zabronione, chyba, że decyzję taką podejmie administrator danych ze względu na szczególne okoliczności. W takim przypadku przekazanie jest dokonywane wyłącznie zgodnie z wymogami określonymi w art. 44-50 RODO. Administrator danych dokłada staranności, by zapewnić stopień ochrony osób fizycznych zagwarantowany w RODO.

8. Współpraca z podmiotami przetwarzającymi prowadzona jest, jeśli wymagają tego okoliczności. Wówczas administrator danych na wniosek kierownika komórki organizacyjnej przy koordynacji IOD, podejmuje decyzję o powierzeniu przetwarzania danych osobowych podmiotowi przetwarzającemu. Przystępując do współpracy należy pamiętać, że:

1) powierzenie danych osobowych podmiotowi przetwarzającemu następuje na podstawie pisemnej umowy przygotowanej przez kierownika komórki organizacyjnej przy współpracy z IOD, określającej w szczególności przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych, kategorie osób, których dane dotyczą, a także obowiązki i prawa administratora danych i podmiotu przetwarzającego.
2) Umowa o której mowa w pkt 2) zawiera w szczególności:
   a) zobowiązanie przetwarzającego do tego, że przetwarzanie danych osobowych będzie się odbywało wyłącznie na udokumentowane polecenie administratora danych,
   b) deklarację przetwarzającego, że osoby upoważnione przez niego do przetwarzania danych osobowych zobowiązały się lub zobowiążą do zachowania w tajemnicy dane osobowe oraz sposób ich zabezpieczenia,
   c) deklarację przetwarzającego, że wdrożył lub wdroży odpowiednie środki techniczne i organizacyjne, aby zapewnić odpowiedni stopień bezpieczeństwa zgodnie z art. 32 RODO,
   d) deklarację przetwarzającego wskazującą, że jeśli korzysta lub będzie korzystać z usług innego podmiotu przetwarzającego, to wypełnia lub wypełni warunki określone w art. 28 ust. 2 i 4 RODO,
   e) zobowiązanie przetwarzającego do pomocy administratorowi danych poprzez odpowiednie środki techniczne i organizacyjne w wywiązaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w pkt 1-7,
   f) zobowiązanie przetwarzającego do usunięcia lub zwrotu wszelkich danych osobowych administratora oraz wszelkich ich istniejących kopii po zakończeniu świadczenia usług, jeśli administrator danych wystąpi z takim żądaniem.
3) Skany zawartych umów z podmiotami przetwarzającymi są przekazywane do IOD w EZD Mdok w celu włączenia do dokumentacji ochrony danych osobowych.

9. Jeśli wymagają tego okoliczności administrator danych na wniosek kierownika komórki organizacyjnej przy współpracy z IOD może podjąć decyzje o wspólnym ustaleniu celów i sposobów przetwarzania danych osobowych z innym administratorem - współadministrowanie.

1) Współadministrowanie jest zawierane w formie umowy pisemnej.
2) Umowa, o której mowa w pkt 1) w przejrzysty sposób:
   a) określa odpowiednie zakresy odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO, w szczególności obowiązków informacyjnych oraz innych obowiązków względem osób, których dane dotyczą,
   b) wskazuje jak osoby, których dane dotyczą mogą kontaktować się w celu uzyskania informacji i realizacji przysługujących im praw.
3) Umowa o której mowa w pkt 1) w zakresie w jakim dotyczy osób, których dane mają być przetwarzane jest udostępniana tym osobom na ich żądanie.

Rozdział 4.
Zasady przetwarzania danych osobowych

§ 6. 1. Osoba, która dokonuje operacji przetwarzania danych osobowych zobowiązana jest do ścisłego przestrzegania obowiązujących przepisów z zakresu ochrony danych osobowych, a w szczególności do:

1) przetwarzania danych osobowych tylko w zakresie posiadanego upoważnienia,
2) nie udostępniania i nie umożliwiania dostępu do danych osobowych osobom nieupoważnionym,

3) prawidłowego zabezpieczania danych osobowych przed zabraniem, uszkodzeniem lub zniszczeniem,

4) informowania osób, których dane dotyczą o ich prawach w sposób przyjęty w Starostwie, w szczególności poprzez udostępnianie klauzul informacyjnych, wywieszenie w pomieszczeniach biurowych, na tablicach ogłoszeń i udostępnianie w Biuletynie Informacji Publicznej,

5) niezwłocznego informowania ASI jednocześnie informując kierownika komórki organizacyjnej o wszelkich zauważonych incydentach stwarzających zagrożenie dla bezpieczeństwa przetwarzania danych osobowych w Systemie Informatycznym Starostwa (w systemie HelpDesk (Pomoc IT)),

6) niezwłocznego informowania IOD jednocześnie informując kierownika komórki organizacyjnej o wszelkich zauważonych nieprawidłowościach mających wpływ na bezpieczeństwo przetwarzania danych osobowych (w systemie HelpDesk (Pomoc IT)).

Rozdział 5.
Obszar przetwarzania danych osobowych

§ 7. 1. Obszarem przetwarzana danych osobowych są budynki Starostwa w lokalizacjach:

1) Plac Stefana Okrzei 4,

2) Plac Stefana Okrzei 4a,

3) ul. Opolska 5,

4) ul. Gamowska 3a.

2. Szczegółowy opis obszarów przetwarzania znajduje się w załączniku nr 5 do niniejszego zarządzenia.

3. Przetwarzanie danych osobowych ma miejsce wyłącznie w pomieszczeniach Starostwa i pomieszczeniach podmiotów, z którymi zawarto umowy powierzenia przetwarzania danych.

4. Dane osobowe, dla których zawarto umowy powierzenia przetwarzania danych przetwarzane są w lokalizacji określonej w pisemnej umowie.

5. Przebywanie w pomieszczeniach, o których mowa w ust.1 i 2 osób nieuprawnionych do przetwarzania danych osobowych, jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych.

6. Pomieszczenia, w których przetwarzane są dane osobowe są zamykane i chronione na czas nieobecności w nich osób upoważnionych do przetwarzania danych osobowych, w sposób uniemożliwiający dostęp do nich osób trzecich.

7. Pomieszczenia, w których przechowywane są bazy informatyczne lub kopie baz danych oraz pomieszczenie ASI podlegają szczególnej ochronie i są wyposażone w instalację kontroli dostępu i instalację alarmową.

Rozdział 6.
Komputery przenośne i praca poza siedzibą administratora

§ 8. 1. Wynoszenie poza obszar przetwarzania danych dokumentów zawierających dane osobowe jest dopuszczalne jedynie za zgodą bezpośredniego przełożonego oraz wiedzą IOD.

2. Wynoszenie poza obszar przetwarzania danych komputerów służących do przetwarzania danych osobowych jest możliwe tylko po uzyskaniu upoważnienia od Administratora Danych i wyrażeniu zgody przez bezpośredniego przełożonego i IOD. Wzór zgody został określony w załączniku nr 14 do niniejszego zarządzenia.

3. Urządzenia zawierające dane osobowe wynoszone poza obszar przetwarzania danych należy chronić przed uszkodzeniami fizycznymi. Należy też bezwzględnie przestrzegać zaleceń producentów dotyczących ochrony sprzętu. W szczególności należy pamiętać, że urządzenia elektroniczne mogą ulec uszkodzeniu w skutek działanie silnego pola elektromagnetycznego i chronić je przed takim oddziaływaniem.

4. Urządzenia przenośne, nośniki danych oraz dokumenty wynoszone poza obszar przetwarzania danych nie powinny być pozostawiane bez nadzoru. W szczególności zabrania się pozostawiania urządzeń i dokumentów zawierających dane osobowe bez odpowiedniego zabezpieczenia w miejscach publicznych, pokojach hotelowych oraz w samochodach.

5. Wykorzystywanie urządzeń przenośnych, nośników danych oraz dokumentów zawierających dane osobowe w miejscach publicznych jest dozwolone, o ile otoczenie, w którym znajduje się osoba upoważniona do przetwarzania danych osobowych, stwarza warunki minimalizujące ryzyko utraty, zniszczenia lub zapoznania się z danymi przez osoby nieupoważnione.

6. Niedozwolone jest udostępnianie urządzeń przenośnych i nośników danych należących do administratora danych osobom nieupoważnionym, w tym domownikom i osobom bliskim użytkownika. Użytkownik obowiązany jest zachować w tajemnicy wobec wszystkich osób, w tym wobec domowników i osób bliskich identyfikator i hasło, których podanie jest konieczne do rozpoczęcia pracy na komputerze przenośnym administratora danych lub chroniącym dostęp do nośników danych.

7. ASI w razie potrzeby wskazuje w dokumencie powierzenia komputera przenośnego osobie upoważnionej do przetwarzania danych osobowych konieczność i częstotliwość sporządzania kopii zapasowych danych przetwarzanych na komputerze przenośnym.

Rozdział 7.
Organizacja przetwarzania danych osobowych

§ 9. 1. Do zadań Administratora Danych należy w szczególności:

1) podejmowanie decyzji o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązujących przepisach prawa, zmian w organizacji Starostwa oraz technik zabezpieczenia danych osobowych,
2) upoważnianie poszczególnych pracowników do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi ich obowiązków,
3) wyznaczenie Inspektora Ochrony Danych i jego zastępcy na czas nieobecności oraz Administratorów Systemu Informatycznego,
4) podejmowanie odpowiednich działań w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych.

2. Do zadań Inspektora Ochrony Danych należy realizacja zadań w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych, a w szczególności:

1) sprawowanie nadzoru nad wdrożeniem stosownych środków fizycznych, organizacyjnych i technicznych – w celu zapewnienia bezpieczeństwa danych,
2) sprawowanie bieżące nadzoru nad funkcjonowaniem systemu zabezpieczeń danych osobowych,
3) przeprowadzanie wewnętrznych audytów (sprawdzeń) przestrzegania przepisów o ochronie danych osobowych,
4) aktualizowanie dokumentacji z zakresu ochrony danych osobowych oraz przestrzegania określonych w niej zasad,
5) nadzorowanie udostępnianych danych osobowych odbiorcom danych i innym podmiotom,
6) zapoznawanie się na bieżąco z przepisami dotyczącymi ochrony danych osobowych i wytycznymi organu nadzorczego w tej dziedzinie oraz dbanie o dostosowanie działalności Starostwa do aktualnych wymogów,
7) zatwierdzanie dokumentów lub odpowiednich klauzul w dokumentach dotyczących ochrony danych osobowych,
8) prowadzenie dokumentacji z zakresu ochrony danych osobowych,
9) przeprowadzanie szkoleń osób upoważnionych do przetwarzania danych osobowych z przepisów o ochronie,
10) prowadzenie rejestru upoważnień do przetwarzania danych osobowych zgodnie ze wzorem określonym w załączniku nr 10 do niniejszego zarządzenia,
11) prowadzenie rejestru czynności przetwarzania danych osobowych przetwarzanych przez Administratora Danych zgodnie ze wzorem określonym w załączniku nr 2 do niniejszego zarządzenia,
12) realizowanie procedury postępowania naruszenia lub podejrzenia naruszenia ochrony danych osobowych,
13) bieżąca aktualizacja załączników do niniejszego zarządzenia.

3. Do Administratora Systemu Informatycznego należy realizacja zadań w zakresie zarządzania i bieżącego nadzoru nad Systemem Informatycznym Starostwa, a w szczególności:

1) zarządzanie systemem informatycznym posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora,
2) przydzielanie każdemu użytkownikowi identyfikatora oraz hasła dostępu do Systemu Informatycznego Starostwa oraz dokonywanie ewentualnych modyfikacji uprawnień, a także blokowanie i usuwanie konta użytkowników zgodnie z zasadami określonymi w instrukcji zarządzania systemem informatycznym, na podstawie upoważnienia wydanego przez Administratora Danych,
3) prowadzenie w systemie elektronicznym rejestru użytkowników upoważnionych do przetwarzania danych w Systemie Informatycznym Starostwa, zgodnie ze wzorem określonym w załączniku nr 15 do niniejszego zarządzenia,
4) niezwłoczne wyrejestrowywanie użytkownika z Systemu Informatycznego Starostwa na podstawie karty obiegowej pracownika w związku z zakończeniem umowy o pracę,
5) przeciwdziałanie dostępowi osób niepowołanych do Systemu Informatycznego Starostwa, w tym w szczególności do aplikacji, w których przetwarzane są dane osobowe,
6) nadzorowanie działań mechanizmów uwierzytelniania i autoryzacji użytkowników w Systemie Informatycznym Starostwa,
7) informowanie IOD i współdziałanie z nim przy usuwaniu skutków naruszenia zasad bezpieczeństwa przetwarzania danych osobowych w Systemie Informatycznym Starostwa,
8) prowadzenie dokumentacji naruszeń bezpieczeństwa (incydentów) w Systemie Informatycznym Starostwa,
9) sprawowanie nadzoru nad wykonywaniem napraw, konserwacji oraz likwidacji urządzeń komputerowych,
10) wykonywanie kopii zapasowych, ich przechowywanie oraz testowanie poprawności pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii Systemu Informatycznego Starostwa,
11) podejmowanie działań służących zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

4. Do zadań dysponenta należy realizacja zadań w zakresie nadzoru nad prawidłowym procesem przetwarzania danych osobowych, bazą danych osobowych lub aplikacją służącą do przetwarzania danych osobowych, zgodnie z wykazem procesów przetwarzania danych osobowych, dla których administratorem jest Starosta Raciborski, a w szczególności:

1) zgłaszanie do IOD zamiaru zmian w procesach przetwarzania danych osobowych, za które odpowiada,
2) opiniowanie wniosków o udzielenie upoważnienia użytkownikowi do przetwarzania danych w procesach przetwarzania danych osobowych i decydowanie o poziomie uprawnień do przetwarzania danych osobowych w tych procesach,
3) opiniowanie wniosków o udzielenie upoważnienia użytkownikowi do przetwarzania danych w aplikacji i decydowanie o poziomie uprawnień do przetwarzania danych osobowych w tej aplikacji, w tym uprawnieniu do administrowania aplikacją,
4) zarządzanie kopiami bazy danych i aplikacji:
   a) zlecanie ASI wysłanie bazy danych do naprawy w serwisie zewnętrznym (w systemie HelpDesk (Pomoc IT)),
   b) zlecanie ASI przywrócenie bazy danych z kopii bezpieczeństwa (w systemie HelpDesk Pomoc IT)),
5) wyznaczanie administratorów aplikacji.

5. Do zadań administratora aplikacji należy realizacja zadań w zakresie zarządzania aplikacją na podstawie uprawnień nadanych mu przez dysponenta aplikacji, a w szczególności:

1) nadawanie uprawnień użytkownikom do modułów i funkcji aplikacji zgodnie z ich upoważnieniem,
2) zgłaszanie do IOD uwag dotyczących przetwarzania w aplikacji danych osobowych,

3) zgłaszanie do ASI problemów technicznych występujących w trakcie działania aplikacji oraz konieczności zainstalowania nowej wersji aplikacji wraz z instrukcją obsługi dla użytkowników,

4) informowanie ASI (w systemie HeplDesk (Pomoc IT)) i współdziałanie przy usuwaniu skutków stwierdzenia naruszenia zabezpieczeń aplikacji.

6. Upoważniony zobowiązany jest do przestrzegania następujących zasad:

1) przetwarza dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez administratora danych w upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków; rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych,

2) zachowuje w tajemnicy treść danych osobowych oraz sposób ich zabezpieczenia. Upoważniony jest zobowiązany do zachowania powyższych tajemnic przez cały okres zatrudnienia u administratora danych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji,

3) stosuje przepisy prawa w zakresie ochrony danych osobowych oraz zasady określnych niniejszym zarządzeniem,

4) stosuje się do wydawanych przez administratora danych, IOD oraz innych przedłożonych procedur, wytycznych oraz poleceń służbowych mających na celu zapewnienie zgodnego z prawem przetwarzania danych osobowych,

5) zabezpiecza dane przed ich utratą, nieautoryzowanym zmienieniem lub ujawnieniem osobom nieupoważnionym.

7. Użytkownik korzysta z systemu informatycznego administratora danych w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu informatycznego, oprogramowania i nośników. Zakres dostępu do danych osobowych w systemie informatycznym przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie. Użytkownik zobowiązany jest do przestrzegania następujących zasad:

1) zgłasza do administratora aplikacji uwagi dotyczące przetwarzania w aplikacji danych osobowych,

2) zgłasza do administratora aplikacji problemy techniczne występujące w trakcie działania aplikacji.

Rozdział 8.
Dostęp do danych osobowych

§ 10. 1. Do przetwarzania danych osobowych, dla których administratorem jest Starosta Raciborski dostęp może mieć wyłącznie osoba spełniająca następujące warunki:

1) została przeszkolona przez IOD w zakresie obowiązujących przepisów o ochronie danych osobowych i uzyskała zaświadczenie, o którym mowa w załączniku nr 12 do niniejszego zarządzenia lub posiada inny dokument stwierdzający odbycie takiego przeszkolenia,

2) przed przystąpieniem do wykonywania czynności związanych z przetwarzaniem danych osobowych złożyła oświadczenie, o którym mowa w załączniku nr 11 do niniejszego zarządzenia,

3) posiada upoważnienie wydane przez Administratora Danych zgodne ze wzorem określonym w załączniku nr 9 do niniejszego zarządzenia.

2. Upoważnienie, o którym mowa w ust. 1 pkt 3 wydawane jest:

1) pracownikom Starostwa zatrudnionym na podstawie umowy o pracę, wyboru i powołania – na wniosek bezpośredniego przełożonego,

2) osobom nie będącym pracownikami Starostwa, w szczególności odbywającym staż, praktykę lub wykonującym czynności określone w innej umowie – na wniosek kierownika komórki organizacyjnej Starostwa sprawującego nadzór nad realizacją powierzonych zadań,

3. Wniosek, o którym mowa w ust. 2 pkt 1 opiniowany jest przez dysponentów procesów przetwarzania danych osobowych i aplikacji służących do ich przetwarzania.

4. Oświadczenie, o którym mowa w ust. 2 pkt 2 przechowywane jest w Wydziale Organizacyjnym na stanowisku pracy ds. zarządzania personelem.

Rozdział 9.
Procesy przetwarzania danych osobowych

§ 11. Wykaz elektroniczny procesów przetwarzania danych osobowych w Starostwie znajduje się w załączniku nr 1 do niniejszego zarządzania.

Rozdział 10.
Rejestr czynności przetwarzania danych osobowych

§ 12. Wzór rejestru czynności przetwarzania danych osobowych służących do realizacji zadań w Starostwie znajduje się w załączniku nr 2 do niniejszego zarządzenia.

Rozdział 11.
Programy (aplikacje) służące do przetwarzania danych osobowych

§ 13. Wzór wykazu aplikacji stosowanych w Starostwie do przetwarzania danych osobowych znajduje się w załączniku nr 3 do niniejszego zarządzenia.

Rozdział 12.
Rejestracja procesów (czynności) przetwarzania danych osobowych

§ 14. 1. Kierownik komórki organizacyjnej zobowiązany jest do zgłoszenia IOD, w formie pisemnej, zamiaru realizacji nowego zadania / projektu / czynności, w którym może zachodzić proces przetwarzania danych osobowych.

2. Dla nowego zadania, w którym zachodzi proces przetwarzania danych osobowych, IOD wraz z kierownikiem komórki organizacyjnej opracowuje kartę czynności (procesu) przetwarzania danych, zgodnie z określonym wzorem w załączniku nr 4 do niniejszego zarządzenia.

3. Dysponenci procesów przetwarzania danych osobowych zobowiązani są do zgłoszenia IOD, w formie pisemnej, zamiaru dokonania zmian w zakresie informacji przetwarzanych w podlegających im procesach.

4. Zmiany w procesie przetwarzania danych osobowych, IOD wraz z kierownikiem komórki organizacyjnej nanoszą na karcie przetwarzania tego procesu.

5. Dla nowego lub zmienionego procesu przetwarzania danych osobowych IOD:

1) aktualizuje „Rejestr czynności procesu przetwarzania ...” określony w załączniku nr 2 do niniejszego zarządzenia,

2) aktualizuje „Obszary przetwarzania ...” określone w załączniku nr 5 do niniejszego zarządzenia,

3) aktualizuje „Ocenę poziomów ryzyka dla procesów przetwarzania danych osobowych ...” określoną w załączniku nr 6 do niniejszego zarządzenia,

6. Jeżeli ocena ryzyka wskaże ryzyko wysokie, a przetwarzanie nie jest obowiązkiem wynikającym z przepisu prawa lub nie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej, to IOD: ·proponuje zrezygnowanie z działania, ·przeprowadza „Ocenę skutków operacji przetwarzania dla ochrony danych zgodnie z art. 35 RODO” określoną w załączniku nr 7 do niniejszego zarządzenia.

7. Kierownicy komórek organizacyjnych wnioskują o udzielenie uprawnień użytkownikom do przetwarzania danych osobowych w nowym procesie.

8. Upoważnienia użytkownikom do przetwarzania danych w nowym procesie nadaje się zgodnie z zapisami w § 10 ust. 2 i 3 niniejszego zarządzenia.

9. ASI aktualizuje procedury wykonywania kopii systemu o nowy proces przetwarzania danych.

10. O rozpoczęciu zbierania informacji w nowym procesie przetwarzania osobowych decyduje dysponent który sprawdza czy:

1) użytkownicy posiadają aktualne upoważnienia z odpowiednim poziomem uprawnień,

2) dostęp przetwarzania danych w procesie posiadają tylko upoważnieni użytkownicy,

3) zastosowane zostały zasady zabezpieczenia danych zgodnie z §16 i §17 niniejszego zarządzenia.

Rozdział 13.
Identyfikacja zagrożeń bezpieczeństwa danych osobowych

§ 15. W Starostwie identyfikuje się następujące zagrożenia bezpieczeństwa przetwarzanych danych osobowych:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. pożar, zalanie pomieszczeń, katastrofa budowlana, niepożądana ingerencja ekipy remontowej, włamanie do budynku,

2) niewłaściwe parametry środowiska, zakłócające pracę urządzeń komputerowych (nadmierna wilgotność lub bardzo wysoka temperatura, oddziaływanie pola elektromagnetycznego i inne),

3) awarie sprzętu lub oprogramowania, zarówno losowe, jak i spowodowane przez niewłaściwe działanie użytkowników i serwisantów,

4) zastosowanie niewłaściwych metod zabezpieczenia systemu informatycznego lub brak dostosowania poziomu zabezpieczeń do aktualnego poziomu wyzwań technologicznych,

5) działania przestępcze mające na celu przejęcie lub zniszczenie danych osobowych (np. ataki internetowe),

6) podejmowanie pracy w systemie z przełamaniem lub zaniechaniem stosowania procedur ochrony danych, np. praca osoby, która nie jest upoważniona do przetwarzania, pozostawienie serwisantów bez nadzoru, a także przyzwolenie na naprawę sprzętu zawierającego dane poza siedzibą administratora danych,

7) naruszenia zasad i procedur określonych w dokumentacji ochrony danych osobowych przez osoby upoważnione do przetwarzania danych osobowych, będące skutkiem nieprzestrzegania procedur ochrony danych, w tym zwłaszcza, wprowadzanie zmian do systemu informatycznego administratora danych i instalowanie programów bez wiedzy i zgody ASI,

8) ujawnienie osobom nieupoważnionym danych osobowych, jak też procedur ochrony danych stosowanych u administratora danych (poprzez umożliwienie wglądu lub przekazania danych i dokumentacji),

9) naruszenie bezpieczeństwa danych przez nieautoryzowane ich przetwarzanie lub zgoda na takie działania przez inne osoby (np. udostępnienie identyfikatora i hasła innemu użytkownikowi),

10) niezgodne z procedurami zakończenie pracy lub opuszczenie stanowiska pracy (nieprawidłowe wyłączenie komputera, niezablokowanie wyświetlenia treści pracy na ekranie komputera przed tymczasowym opuszczeniem stanowiska pracy, pozostawienie po zakończeniu pracy nieschowanych do zamykanych na klucz szaf dokumentów zawierających dane osobowe, niezamknięcie na klucz pokoju po jego opuszczeniu, nieoddanie klucza w wyznaczonym miejscu),

11) przetwarzanie danych osobowych w celach niezgodnych z ich przeznaczeniem.

Rozdział 14.
Zasady zabezpieczenia danych osobowych przetwarzanych w sposób tradycyjny

§ 16. 1. Dokumenty zawierające dane osobowe przechowywane są w pomieszczeniach biurowych, w meblach zamykanych na klucz.

2. Pomieszczenia biurowe, o których mowa w ust. 1 są:

1) przed rozpoczęciem pracy - sprawdzane, czy nie ma śladów włamania lub uszkodzenia; takiemu samemu sprawdzeniu podlegają meble biurowe, w których przechowywane są dokumenty zawierające dane osobowe,

2) w trakcie godzin pracy - zamykane na czas nieobecności osoby zatrudnionej przy przetwarzaniu danych osobowych,

3) po zakończeniu pracy – sprawdzane, czy nie pozostały niezabezpieczone dokumenty zawierające dane osobowe, czy meble biurowe i szafy zostały zamknięte, czy dokumenty w pojemniku z makulaturą zostały zniszczone w stopniu uniemożliwiającym identyfikację danych osobowych.

3. Osoby nieupoważnione przebywają w pomieszczeniach biurowych tylko w obecności osoby zatrudnionej przy przetwarzaniu danych.

4. Dostęp do danych osobowych posiada tylko osoba upoważniona.

5. Zasady postępowania z kluczami od pomieszczeń i mebli biurowych określają odrębne przepisy.

Rozdział 15.
Zabezpieczenie danych przetwarzanych w systemie informatycznym

§ 17. 1. W Starostwie z uwagi na fakt, że urządzenia systemu teleinformatycznego służącego do przetwarzania danych osobowych połączone są z siecią publiczną, stosuje się wysoki poziom bezpieczeństwa teleinformatycznego.

2. Bezpieczeństwo teleinformatyczne na poziomie wysokim zapewnia się przez:

1) środki prawne - spełnienie wymogów określonych w RODO i ustawie, a w szczególności:

a) został wyznaczony IOD nadzorujący przestrzeganie zasad ochrony przetwarzanych danych osobowych,

b) został wyznaczony ASI nadzorujący przestrzeganie zasad bezpieczeństwa w systemie informatycznym,

c) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych,

d) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych,

e) zostały opracowane i wdrożone zasady ochrony danych osobowych,

f) została opracowana i wdrożona instrukcja zarządzania systemem informatycznym.

2) środki ochrony fizycznej danych:

a) bazy danych osobowych przechowywane są w pomieszczeniach zabezpieczonych drzwiami zwykłymi wyposażonymi w minimum dwa zamki klasy B,

b) bazy danych osobowych przechowywane są w pomieszczeniach, w których okna zabezpieczone są za pomocą rolet antywłamaniowych,

c) pomieszczenia, w których przechowywane są bazy danych osobowych oraz pomieszczenia podlegające szczególnej ochronie (§7 ust. 7), wyposażone są w systemem kontroli dostępu i instalację alarmową,

d) dostęp do pomieszczeń, w których przechowywane są bazy danych osobowych poza godzinami pracy nadzorowany jest przez podmiot zewnętrzny, świadczący na rzecz Starostwa usługi ochrony mienia,

e) kopie zapasowe/archiwalne baz danych osobowych przechowywane są w zamkniętej niemetalowej szafie – w zamkniętej kasecie posiadającej certyfikat producenta w zakresie odporności mechanicznej, wodnej i termicznej,

f) pomieszczenia, w których przechowywane są bazy danych osobowych zabezpieczone są przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy,

g) kopie robocze dokumentów zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów,

3) środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej:

a) dostęp do bazy danych osobowych, która przetwarzana jest na wydzielonej stacji komputerowej/ komputerze przenośnym zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła BIOS,

b) zastosowano urządzenia typu UPS, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania,

c) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,

d) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem karty procesorowej oraz kodu PIN lub tokena (dla komputerów spełniających warunki techniczne),

e) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem technologii biometrycznej (dla komputerów spełniających warunki techniczne),

f) zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych,

g) zastosowano system rejestracji dostępu do bazy danych osobowych,

h) zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji,

i) dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia,

j) zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej,

k) zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity,

l) do ochrony dostępu do sieci komputerowej użyto sprzętowego systemu Firewall, IPS, GAV, z aktualnymi licencjami producenta,

4) środki ochrony w ramach narzędzi programowych i baz danych:

a) dostęp do Systemu Informatycznego Starostwa mają użytkownicy posiadający identyfikator i hasło dostępu nadane przez ASI na podstawie upoważnienia wydanego przez administratora danych,

b) wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach bazy danych osobowych,

c) zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanej bazy danych osobowych,

d) dostęp do bazy danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,

e) zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym baz danych osobowych dla poszczególnych użytkowników systemu informatycznego,

f) zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do Systemu Informatycznego Starostwa i aplikacji obsługujących bazy danych osobowych,

g) zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe,

h) zastosowano mechanizm automatycznej blokady dostępu do stanowiska komputerowego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika,

5) środki organizacyjne:

a) osoby pracujące przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych i w zakresie zabezpieczeń,

b) przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego,

c) osoby pracujące przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy,

d) monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane,

e) kopie zapasowe baz danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco,

f) użycie komputerów przenośnych służących do przetwarzania danych osobowych poza terenem Starostwa jest możliwe tylko po uzyskaniu zgody administratora danych i IOD. Wzór wniosku stanowi załącznik nr 14 do niniejszego zarządzenia.

Rozdział 16.
Postępowanie w sytuacji naruszenia zasad ochrony danych osobowych

§ 18. 1. W razie stwierdzenia przez osobę przetwarzającą dane osobowe naruszenia zasad ich ochrony lub podejrzenia takiego naruszenia zobowiązana jest ona do:

1) natychmiastowego powiadomienia o zdarzeniu swojego bezpośredniego przełożonego, który kolejno informuje IOD,

2) zabezpieczenia miejsca zdarzenia (obraz z monitora, dokumentacja fotograficzna),

3) fizycznego odłączenia urządzenia i segmentów sieci, które mogłyby umożliwić dostęp do danych osobom nieupoważnionym.

2. IOD po otrzymaniu zawiadomienia o naruszeniu zasad ochrony danych osobowych lub podejrzenia takiego naruszenia przeprowadza niezwłocznie postępowanie wyjaśniające w celu ustalenia czy naruszenie ochrony danych osobowych miało miejsce (tzw. sprawdzenie doraźne).

3. Sprawdzenie doraźne może zostać wszczęte przez IOD także z własnej inicjatywy, gdy w inny sposób niż w skutek zawiadomienia powźmie informację o naruszeniu lub możliwym naruszeniu ochrony danych osobowych.

4. W przypadku stwierdzenia naruszenia ochrony danych osobowych IOD :

1) w porozumieniu z odpowiednim kierownikiem komórki organizacyjnej podejmuje niezwłoczne, możliwe do wprowadzenia na bieżąco, działania zapobiegające dalszemu naruszaniu ochrony danych osobowych,

2) w porozumieniu z odpowiednim kierownikiem komórki organizacyjnej stosuje niezwłoczne, możliwe do wprowadzenia na bieżąco, środki eliminujące lub zmniejszające ryzyko naruszenia praw lub wolności osoby, której dane dotyczą,

3) sporządza raport w terminie 14 dni od dnia naruszenia ochrony danych osobowych, a następnie niezwłocznie przekazuje administratorowi danych – Staroście.

5. Raport naruszenia ochrony danych osobowych zawiera w szczególności:

1) rodzaj zaistniałego zdarzenia,

2) dokładny czas uzyskania informacji o naruszeniu ochrony danych osobowych,

3) opis okoliczności naruszenia ochrony danych osobowych,

4) opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazuje kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,

5) opis możliwych konsekwencji naruszenia ochrony danych osobowych,

6) ocenę czy jest prawdopodobne, że naruszenie skutkowało ryzykiem lub wysokim ryzykiem naruszenia wolności lub praw osób fizycznych,

7) wskazanie zastosowanych lub proponowanych działań zaradczych, ze szczególnym uwzględnieniem takich, które zmierzają do zminimalizowania ewentualnych negatywnych skutków naruszenia.

6. W razie naruszenia ochrony zabezpieczenia danych osobowych przetwarzanych w systemie informatycznym IOD wspólnie z ASI podejmują działania:

1) wylogowania użytkownika podejrzanego o naruszenie zabezpieczenia ochrony danych,

2) zmiany hasła na koncie użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownego włamania,

3) zapisania wszelkich informacji związanych z danym zdarzeniem a szczególnie czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych lub czas samodzielnego wykrycia tego faktu,

4) wygenerowania i wydrukowania (jeżeli zasoby systemu na to pozwalają) wszystkich możliwych dokumentów i raportów, które mogą pomóc w ustaleniu okoliczności zdarzenia. Należy opatrzyć je datą i podpisem.

5) sprawdzenia:

a) stanu urządzeń wykorzystywanych do przetwarzania danych osobowych,

b) zawartości zbioru danych,

c) sposobu działania programu,

d) jakości komunikacji w sieci telekomunikacyjnej,

6) wykluczenia możliwości obecności wirusów komputerowych,

7) przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali szkód i sposobu dostępu do danych osoby niepowołanej.

Rozdział 17.
Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu

§ 19. 1. Jeśli administrator danych ustali, że jest prawdopodobne, że naruszenie ochrony danych osobowych stwierdzone w trybie określonym w §18 ust. 1 skutkowało ryzykiem naruszenia wolności lub praw osób fizycznych nakazuje IOD przygotowanie projektu zgłoszenia naruszenia organowi nadzorczemu (PUODO).

2. Zgłoszenie naruszenia ochrony danych osobowych zawiera, w szczególności:

1) informacje zawarte w raporcie, zgodnie z § 20 ust. 2.

2) wskazanie imienia i nazwiska oraz danych kontaktowych IOD, jako osoby właściwej do kontaktu w sprawie. W szczególnych przypadkach, po konsultacji z administratorem danych, do kontaktu w sprawie może być wskazana inna osoba niż IOD,

3) zgłoszenie naruszenia ochrony danych osobowych, administrator danych zatwierdza i przekazuje organowi nadzorczemu bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia,

4) jeżeli dotrzymanie terminu wskazanego w pkt 3) jest niemożliwe administrator danych do zgłoszenia dołącza wyjaśnienie przyczyn opóźnienia. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić od razu, administrator danych udziela tych informacji sukcesywnie, bez zbędnej zwłoki.

Rozdział 18.
Zawiadomienie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych

§ 20. 1. Jeśli administrator danych ustali, że stwierdzone naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia wolności lub praw osób fizycznych i nie da się zastosować środków eliminujących to wysokie ryzyko, nakazuje IOD przygotowanie projektu zawiadomienia o naruszeniu dla wszystkich osób, których danych naruszenie dotyczy.

2. Zawiadomienie, o którym mowa w pkt 1) powinno być napisane jasnym i prostym językiem oraz zawierać, w szczególności:

a) opis charakteru naruszenia,

b) opis możliwych konsekwencji naruszenia,

c) wskazanie zastosowanych lub planowanych działań zaradczych, ze szczególnym uwzględnieniem takich, które mogą zminimalizować ewentualne negatywne skutki naruszenia,

d) wskazanie imienia i nazwiska oraz danych kontaktowych IOD, jako osoby właściwej do kontaktu w sprawie. W szczególnych przypadkach, po konsultacji z administratorem danych osobowych, do kontaktu w sprawie może być wskazana inna osoba niż IOD.

3. Zawiadomienie o naruszeniu ochrony danych osobowych, administrator danych zatwierdza i przekazuje niezwłocznie wszystkim osobom, których danych naruszenie dotyczy.

4. Jeżeli administrator danych oceni, że realizacja wymogów określonych w pkt 1-3) wymagałoby niewspółmiernie dużego wysiłku, w szczególności niewspółmiernie dużego wysiłku wymagałoby nawiązanie bezpośredniego, indywidualnego kontaktu z osobami, których danych naruszenie dotyczy, może podjąć decyzje o przekazaniu informacji zainteresowanym poprzez wydanie publicznego komunikatu lub o zastosowaniu innego podobnego środka, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Rozdział 19.
Dokumentacja naruszenia ochrony danych osobowych

§ 21. 1. IOD prowadzi dokumentację naruszenia ochrony danych osobowych.

2. W skład dokumentacji o naruszenia ochrony danych osobowych wchodzą:

1) raport dla Administratora Danych,

2) zgłoszenie do organu nadzorczego,

3) zawiadomienia do osób, których dane dotyczą,

4) wszelkie inne dokumenty, w tym notatki służbowe, pliki, zdjęcia i inne dowody zebrane w trakcie przeprowadzania czynności wyjaśniających pozwalające ustalić okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

3. Dokumentacja naruszenia ochrony danych osobowych pozostaje do wglądu organu nadzorczego.

Rozdział 20.
Postanowienia końcowe

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

§ 23. Zobowiązuję kierowników komórek organizacyjnych do pełnienia nadzoru nad pracownikami w zakresie stosowania przepisów prawa dotyczących ochrony danych osobowych oraz zasad wprowadzonych niniejszym zarządzeniem.

§ 24. Zobowiązuję wszystkie osoby dopuszczone do przetwarzania danych osobowych w Starostwie Powiatowym w Raciborzu do dostosowania swojego postępowania do wymogów wynikających z niniejszego zarządzenia.

§ 25. Zmiana treści załączników nie powoduje konieczności zmiany niniejszego zarządzenia.

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

2. Nadzór nad wykonaniem zarządzenia sprawować będzie Inspektor Ochrony Danych.

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

§ 27. Traci moc Zarządzenie Nr 65/2017 Starosty Raciborskiego z dnia 22.05.2017r. w sprawie zasad ochrony danych osobowych przetwarzanych w Starostwie Powiatowym w Raciborzu.

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

Starosta

Ryszard Winiarski

Załącznik Nr 1
do Zarządzenia Nr 59/2018
Starosty Raciborskiego
z dnia 25 maja 2018r.

WYKAZ PROCESÓW PRZETWARZANIA DANYCH
OSOBOWYCH W STAROSTWIE POWIATOWYM W RACIBORZU

Lp.	Nazwa procesu	Komórka organizacyjna odpowiedzialna za proces przetwarzania danych osobowych	Dysponent procesu
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

Aktualny WYKAZ PROCESÓW PRZETWARZANIA DANYCH OSOBOWYCH
znajduje się systemie elektronicznym Inspektora Ochrony Danych

Starosta

Ryszard Winiarski

Załącznik Nr 2
do Zarządzenia Nr 59/2018
Starosty Raciborskiego
z dnia 25 maja 2018r.

REJESTR CZYNNOŚCI PROCESU PRZETWARZANIA DANYCH OSOBOWYCH

NAZWA PROCESU

I. PODSTAWOWE INFORMACJE O PROCESIE

Lp.	Rodzaj informacji	Treść informacji	Uwagi
1.	Administrator Danych Inspektor Ochrony Danych	Wskazanie administratora danych osobowych oraz wszelkich współadministratorów. Nazwę lub imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych.	
2.	Cel przetwarzania	Wskazanie celu przetwarzania danych osobowych w procesie	
3.	Podstawa legalności przetwarzania	Podstawa prawna prowadzenia zasobu. Jeden z warunków z art. 6 ust. 1 RODO lub art. 9-10 dla szczególnych (wrażliwych) kategorii danych.	
4.	Zakres przetwarzanych danych.	Kategorie osób, których dane dotyczą oraz kategorie danych osobowych dotyczących tych osób.	
5.	Kategorie odbiorców danych.	Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych.	
6.	Przekazywanie danych do państwa trzeciego lub organizacji międzynarodowej	Nazwa państwa trzeciego lub organizacji międzynarodowej. Informacja o dokumentacji odpowiednich zabezpieczeń zgodnie z ar. 49 ust. 1 RODO.	
7.	Czas przechowywania danych	Planowane terminy usunięcia poszczególnych kategorii danych.	
8.	Sposób zabezpieczenia dostępu do tradycyjnej części zasobu (jeśli dotyczy).	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa	

II. OCENA POZIOMU RYZYKA

Lp.	Rodzaj działania - czynność polega na lub obejmuje	Ocena
1.	Ocena lub punktacja w tym profilowanie, lub prognozowanie (na podstawie danych osobowych)	
2.	Podejmowanie automatycznych decyzji mających skutki prawne lub w podobny sposób istotnie wpływające na sytuację osoby, której dane dotyczą	
3.	Systematyczne monitorowanie, przez które rozumie się przetwarzanie danych w celu obserwowania, monitorowania lub kontroli osób, których dane dotyczą	
4.	Przetwarzanie danych wrażliwych – dane wskazane w art. 9 RODO, ale też dane dotyczące komunikacji elektronicznej, dane o lokalizacji i dane finansowe	
5.	Przetwarzanie danych na dużą skalę	
6.	Porównywanie lub łączenie zbiorów danych	
7.	Przetwarzanie danych osób wymagających szczególnej ochrony, np. pracowników, dzieci, pacjentów czy osób starszych	
8.	Innowacyjne użycie lub zastosowanie technologicznych lub organizacyjnych rozwiązań, np. połączenie identyfikacji odciskiem palca oraz mechanizmu rozpoznawania twarzy w celu uzyskania dostępu do pomieszczeń, tzw. Internet rzeczy, itp.	
9.	Transgraniczny transfer danych poza Unię Europejską	
10.	Uniemożliwianie korzystania z praw osobom których dane dotyczą z usługi lub umowy	
11.	Suma	
12.	Ocena skutków	

UWAGA: Jeżeli w pkt. 10 wykazano więcej niż jedną czynność to Grupa Robocza sugeruje przeprowadzenie oceny skutków dla ochrony danych osobowych. Jednak nie trzeba jej dokonywać, gdy przetwarzanie jest obowiązkiem wynikającym z przepisu prawa lub jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej.

III. OCENA SKUTKÓW DLA OCHRONY DANYCH

Lp.	Wymagane elementy oceny	Treść informacji
1.	Systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora; ocenę lub punktację w tym profilowanie, lub prognozowanie (na podstawie danych osobowych).	
2	Ocena, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów.	
3	Wskazanie środków zaplanowanych w celu zaradzenia ryzyku, w tym zabezpieczeń oraz środków i mechanizmów bezpieczeństwa mających zapewnić ochronę danych osobowych i wykazać przestrzeganie wymagań RODO.	
4	Ocena ryzyka naruszenia praw lub wolności osób, których dane dotyczą.	

UWAGA: jeżeli ocena ryzyka w pkt. 4 wykaże, że przetwarzanie powodowałoby wysokie ryzyko naruszenia wolności lub praw osób, których dane dotyczą, a środki zaradcze wskazane w pkt. 3 nie pozwalają na jego zminimalizowanie to należy zrezygnować z danego typu operacji lub rozpocząć uprzednie konsultacje z organem nadzorczym zgodnie z art. 36 RODO.

Starosta

Ryszard Winiarski

Załącznik Nr 3
do Zarządzenia Nr 59/2018
Starosty Raciborskiego
z dnia 25 maja 2018r.

WYKAZ APLIKACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Nazwa aplikacji Wykaz modułów	Dysponent (Komórka organizacyjna)	Administrator aplikacji/modułu (Osoba, stanowisko)	Wymagany identyfikator i hasło użytkownika	Wymagane upoważnienie do przetwarzania
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

Aktualny WYKAZ APLIKACJI DO PRZETWARZANIA DANYCH OSOBOWYCH
znajduje się systemie elektronicznym Inspektora Ochrony Danych

Starosta

Ryszard Winiarski

Załącznik nr 4
do Zarządzenia Nr 59/2018
Starosty Raciborskiego
z dnia 25 maja 2018r.

1. Karta czynności przetwarzania ma odnosić się do charakteru, zakresu, kontekstu i celów przetwarzania danych osobowych.
2. Głównymi wartościami ochrony danych osobowych jest ochrona praw i wolności osób, których dane dotyczą.
3. Definicje

powiat raciborski zielona oaza kultur	**KARTA CZYNNOŚCI (PROCESU) PRZETWARZANIA DANYCH** **STAROSTWO POWIATOWE W RACIBORZU** 47-400 RACIBÓRZ Pl. STEFANA OKRZEI 4 tel. (32) 45 97 300, (centrala) fax. (32) 415 87 36	Komórka organizacyjna odpowiedzialna za czynność przetwarzania ***ST - Starosta Raciborski***

I. NAZWA PROCESU / USŁUGI

Kliknij tutaj, aby wprowadzić tekst.

II. PRZETWARZANIE DANYCH OSOBOWYCH

1. CEL PRZETWARZANIA

Proszę podać wszystkie cele realizowane w tym procesie.

2. KATEGORIE OSÓB, KTÓRYCH DANE DOTYCZĄ

Proszę podać wszystkie kategorie osób, których dane przetwarzane są w tym procesie.

3. KATEGORIE DANYCH OSOBOWYCH

DANE ZWYKŁE

- ☐ nazwiska i imiona
- ☐ imiona rodziców
- ☐ data urodzenia
- ☐ miejsce urodzenia
- ☐ adres zamieszkania lub pobytu
- ☐ numer ewidencyjny PESEL
- ☐ Numer Identyfikacji Podatkowej
- ☐ miejsce pracy
- ☐ zawód
- ☐ wykształcenie
- ☐ seria i numer dowodu osobistego
- ☐ numer telefonu
- ☐ adres e-mail

DANE WRAŻLIWE

- ☐ pochodzenie rasowe lub etniczne
- ☐ poglądy polityczne
- ☐ przekonania religijne lub światopoglądowe
- ☐ przynależność do związków zawodowych
- ☐ dane genetyczne i dane biometryczne

przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej

- ☐ dane dotyczące zdrowia
- ☐ dane dotyczące seksualności

lub orientacji seksualnej

- ☐ dane dotyczące wyroków skazujących

oraz naruszeń prawa lub powiązanych środków bezpieczeństwa

INNE: Inne dane przetwarzane w tym procesie. Jeśli występują.
Dane zbierane dla realizacji dodatkowego celu
Proszę podać kategorie danych i cel ich przetwarzania. Jeżeli występuje.

4. ZGODNOŚĆ PRZETWARZANIA Z PRAWEM

DANE ZWYKŁE
Art. 6 ust. 1 RODO

- ☐ **Zgoda osoby**
- ☐ **Wykonywanie umowy**
- ☐ **Wykonywanie obowiązku prawnego**

Jeśli wykonywanie obowiązku prawnego to proszę podać przepis prawa.

- ☐ **Ochrona żywotnych interesów osoby**
- ☐ **Wykonywanie zadania w interesie publicznym**
- ☐ **Prawnie uzasadnione interesy**

DANE WRAŻLIWE
Art. 9 ust. 2 RODO

Jeśli są przetwarzane dane wrażliwe to proszę podać przesłankę z Art. 2 ust. 2 RODO

5. KATEGORIE ODBIORCÓW

a) podmioty przetwarzające

Proszę podać nazwy i adresy podmiotów przetwarzających. Jeśli występują.

b) odbiorcy danych

Proszę podać nazwy odbiorców danych. Jeśli występują.

c) strony trzecie

Proszę podać nazwy stron trzecich. Jeśli występują.

d) organy publiczne, które mogą otrzymywać dane osobowe

Proszę podać nazwy organów publicznych. Jeśli otrzymują dane osobowe.

6. PRZEKAZANIA DANYCH DO PAŃSTWA TRZECIEGO LUB ORGANIZACJI MIĘDZYNARODOWEJ

☐ TAK ☐ NIE

Proszę opisać. Jeśli występuje.

7. CYKL ŻYCIA DANYCH I KATEGORIE OPERACJI PRZETWARZANIA

a) ZBIERANIE DANYCH

- ☐ od osoby, której dane dotyczą
- ☐ z innego źródła

Jeśli z innego źródła to proszę podać skąd.

b) UTRWALANIE DANYCH

- ☐ komputer użytkownika
- ☐ przydzielony zasób na serwerze Starostwa
- ☐ baza danych aplikacji lokalnej lub sieciowej
- ☐ baza danych aplikacji internetowej
- ☐ zasób internetowy (chmura danych)
- ☐ baza danych EZD (MDOK)
- ☐ nośnik zewnętrzny (dysk, pendrive, CD/DVD)
- ☐ nośnik papierowy (kopia, wydruk)

INNE: Kliknij tutaj, aby wprowadzić tekst.

c) ORGANIZOWANIE I PORZĄDKOWANIE

- ☐ klasyfikacja wg JRWA
- ☐ nadanie unikalnego numeru

☐ struktura folderów i plików systemu Windows

☐ struktura folderów systemu EZD (MDOK)

☐ teczki i segregatory

INNE: Kliknij tutaj, aby wprowadzić tekst.

d) PRZECHOWYWANIE DANYCH

☐ tak jak zostały utrwalone

☐ w inny sposób

Jeśli w inny sposób to proszę podać w jaki.

e) ADAPTOWANIE DANYCH

☐ TAK ☐ NIE

Kliknij tutaj, aby wprowadzić tekst.

f) MODYFIKOWANIE DANYCH

☐ TAK ☐ NIE

Kliknij tutaj, aby wprowadzić tekst.

g) POBIERANIE DANYCH

☐ TAK ☐ NIE

Kliknij tutaj, aby wprowadzić tekst.

h) PRZEGLĄDANIE DANYCH

☐ TAK ☐ NIE

Kliknij tutaj, aby wprowadzić tekst.

i) UJAWNIANIE DANYCH

☐ poczta - list zwykły

☐ poczta - list polecony

☐ poczta - potwierdzenie odbioru

☐ e-mail - zwykły

☐ e-mail - szyfrowany

☐ EPUAP

☐ kurier

☐ strona internetowa

☐ forum internetowe

☐ komunikator internetowy

☐ protokół komunikacyjny (FTP)

☐ szyfrowany tunel VPN

INNE: Proszę podać inny sposób ujawniania. Jeśli występuje.

j) DOPASOWYWANIE DANYCH

☐ TAK ☐ NIE

Proszę opisać. Jeśli występuje.

k) ŁĄCZENIE DANYCH

☐ TAK ☐ NIE

Proszę opisać. Jeśli występuje.

l) OGRANICZANIE PRZETWARZANIA DANYCH

☐ TAK ☐ NIE

Kliknij tutaj, aby wprowadzić tekst.

m) USUWANIE DANYCH

☐ TAK ☐ NIE

Kliknij tutaj, aby wprowadzić tekst.

n) NISZCZENIE DANYCH

☐ TAK ☐ NIE

Kliknij tutaj, aby wprowadzić tekst.

o) PROFILOWANIE

☐ ocena lub punktacja ☐ NIE

☐ prognozowanie

☐ zautomatyzowane decyzje

☐ inne profilowanie

Jeśli inne profilowanie to proszę podać jakie.

p) MONITOROWANIE

☐ śledzenie w internecie ☐ NIE

☐ śledzenie w sieci telekomunikacyjnej

☐ świadczenie usług telekomunikacyjnych

☐ ocena lub punktacja

☐ monitoring wizyjny

☐ inne monitorowanie

Jeśli inne monitorowanie to proszę podać jakie.

q) PRZETWARZANIE NA DUŻĄ SKALĘ

☐ TAK ☐ NIE

Kliknij tutaj, aby wprowadzić tekst.

r) INNE RODZAJE OPERACJI PRZETWARZANIA DANYCH OSOBOWYCH

Kliknij tutaj, aby wprowadzić tekst.

8. CZAS PRZECHOWYWANIA

Proszę podać czas przechowywania i podstawę jego ustalenia.

9. OGÓLNY OPIS ŚRODKÓW BEZPIECZEŃSTWA

Ochrona w komórce organizacyjnej

☐ strefy bezpieczeństwa

☐ system alarmowy

☐ ochrona drzwi i okien

☐ zamykane szafy i biurka

☐ czyste biurko

☐ prawidłowe ustawienie monitorów

Inne środki ochrony. Jeśli występują.

Organizacyjne (wypełnia ABI)

Kliknij tutaj, aby wprowadzić tekst.

Techniczne (wypełnia ASI)

Kliknij tutaj, aby wprowadzić tekst.

III. AKTYWA

a) personel

☐ decydenci

☐ pracownicy - urzędnicy

☐ pracownicy - obsługa

☐ stażyści

☐ praktykanci

☐ inne umowy cywilno-prawne

INNE: Inny personel. Jeśli występuje.

b) sprzęt

☐ serwery (ASI)

☐ komputery stacjonarne

- ☐ komputery przenośne
- ☐ drukarki
- ☐ kopiarki
- ☐ skanery
- ☐ faxy
- ☐ telefony

INNE: Inny sprzęt. Jeśli występuje.

c) siedziba

- ☐ Racibórz, Plac Stefana Okrzei 4
- ☐ Racibórz, Plac Stefana Okrzei 4a
- ☐ Racibórz, ul. Gamowska 3a
- ☐ Racibórz, ul. Opolska 5
- ☐ Racibórz, ul. Reymonta 8b

Proszę podać dokładną lokalizację przetwarzania (piętro, pokój)

d) oprogramowanie

- ☐ edytor tekstu
- ☐ arkusz kalkulacyjny
- ☐ przeglądarka internetowa
- ☐ program pocztowy
- ☐ program dziedzinowy (dedykowany)
- ☐ system operacyjny (ASI)
- ☐ antywirus (ASI)
- ☐ firewall (ASI)
- ☐ zarządzanie kontami (ASI)
- ☐ oprogramowanie monitorujące (ASI)

Programy dziedzinowe

Proszę wybrać program dziedzinowy z listy. Jeśli jest używany.

INNE: Inne oprogramowanie. Jeśli występuje.

e) sieć *(wypełnia ASI)*

Kliknij tutaj, aby wprowadzić tekst.

f) Forma (kontekst) danych

- ☐ baza danych w wersji elektronicznej
- ☐ dokumenty elektroniczne
- ☐ akta sprawy
- ☐ umowy
- ☐ akta osobowe
- ☐ decyzje administracyjne
- ☐ orzeczenia sądowe

INNE: Inne dokumenty. Jeśli występują.

g) zbiory danych

Jeżeli dane są przetwarzane w zbiorze to proszę podać jego numer i nazwę.

Data:	**Opracował:** Kliknij, aby wprowadzić tekst.

Starosta

Ryszard Winiarski

Załącznik Nr 5
do Zarządzenia Nr 59/2018
Starosty Raciborskiego
z dnia 25 maja 2018r.

OBSZARY PRZETWARZANIA DANYCH OSOBOWYCH
W STAROSTWIE POWIATOWYM W RACIBORZU

Plac Stefana Okrzei 4

1. Nazwa procesu przetwarzania danych
piętro, nr pokoju
2. .....
3. .....
4. .....

Plac Stefana Okrzei 4a

1. Nazwa procesu przetwarzania danych
piętro, nr pokoju
2. .....
3. .....
4. .....

Ulica Opolska 5

1. Nazwa procesu przetwarzania danych
piętro, nr pokoju
2. .....
3. .....
4. .....

Ulica Gamowska 3a

1. Nazwa procesu przetwarzania danych
piętro, nr pokoju
2. .....
3. .....
4. .....

Starosta

Ryszard Winiarski

Załącznik Nr 6
do Zarządzenia Nr 59/2018
Starosty Raciborskiego
z dnia 25 maja 2018r.

OCENA POZIOMÓW RYZYKA DLA PROCEÓW PRZETWARZANIA DANYCH OSOBOWYCH
(zgodnie z wytycznymi Grupy Roboczej 29 - WP 248/2017)

	NAZWA PROCESU	Rodzaj działania - czynność polega na lub obejmuje											
		Ocena lub punktacja w tym profilowanie, lub prognozowanie (na podstawie danych osobowych)	Podejmowanie automatycznych decyzji mających skutki prawne lub w podobny sposób istotnie wpływającena sytuację osoby, której dane dotyczą	Systematyczne monitorowanie, przez które rozumie się przetwarzanie danych w celu obserwowania, monitorowania lub kontroli osób, których dane dotyczą	Przetwarzanie danych wrażliwych – dane wskazane w art. 9 RODO, ale też dane dotyczące komunikacji elektronicznej, dane o lokalizacji i dane finansowe	Przetwarzanie danych na dużą skalę	Porównywanie lub łączenie zbiorów danych	Przetwarzanie danych osób wymagających szczególnej ochrony, np. pracowników, dzieci, pacjentów czy osób starszych	organizacyjnych rozwiązań, np. połączenie identyfikacji odciskiem palca oraz mechanizmu rozpoznawania twarzy w celu uzyskania dostępu do pomieszczeń, tzw. Internet rzeczy, itp.	Iransgraniczny transfer danych poza Unię Europejską	Suma	Ocena skutków
Lp.	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
1.												
2.												

UWAGA: Jeżeli w pkt. 10 wykazano więcej niż jedną czynność to Grupa Robocza sugeruje przeprowadzenie oceny skutków dla ochrony danych osobowych.
Jednak nie trzeba jej dokonywać, gdy przetwarzanie jest obowiązkiem wynikającym z przepisu prawa lub jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej.

Starosta

Ryszard Winiarski

Załącznik Nr 7
do Zarządzenia Nr 59/2018
Starosty Raciborskiego
z dnia 25 maja 2018r.

OCENA SKUTKÓW OPERACJI PRZETWARZANIA DLA OCHRONY DANYCH ZGODNIE Z ART. 35 RODO

NAZWA PROCESU (CZYNNOŚCI)

Lp.	Wymagane elementy oceny	Treść informacji
1.	Systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora; ocenę lub punktację w tym profilowanie, lub prognozowanie (na podstawie danych osobowych).	
2.	Ocena, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów.	
3.	Wskazanie środków zaplanowanych w celu zaradzenia ryzyku, w tym zabezpieczeń oraz środków i mechanizmów bezpieczeństwa mających zapewnić ochronę danych osobowych i wykazać przestrzeganie wymagań RODO.	
4.	Ocena ryzyka naruszenia praw lub wolności osób, których dane dotyczą.	

UWAGA: jeżeli ocena ryzyka w pkt. 4 wykaże, że przetwarzanie powodowałoby wysokie ryzyko naruszenia wolności lub praw osób, których dane dotyczą, a środki zaradcze wskazane w pkt. 3 nie pozwalają na jego zminimalizowanie to należy zrezygnować z danego typu operacji lub rozpocząć uprzednie konsultacje z organem nadzorczym zgodnie z art. 36 RODO.

Starosta

Ryszard Winiarski

Załącznik nr 8
do Zarządzenia Nr 59/2018
Starosty Raciborskiego
z dnia 25 maja 2018r.

WNIOSEK O WYDANIE UPOWAŻNIENIA
DO PRZETWARZANIA DANYCH OSOBOWYCH I DOSTĘP DO SYSTEMU INFORMATYCZNEGO

Aktualizacja upoważnienia nr
Wydanie upoważnienia do: - przetwarzania danych osobowych **X**
Wydanie upoważnienia do: - dostępu do systemu informatycznego **X**

Imię i nazwisko pracownika:
Komórka organizacyjna :
Stanowisko:

.....
Podpis wnioskującego

Dysponenci (Komórki organizacyjne):

Przetwarzanie danych osobowych
Pracownik

Lp.	Uzasadnienie potrzeby posiadania uprawnienia do przetwarzania danych osobowych. Wypełnia bezpośredni przełożony								Opinia w sprawie celowości uzyskania uprawnienia do przetwarzania danych osobowych w procesie. Wypełnia kierownik komórki organizacyjnej Starostwa odpowiedzialny za przetwarzanie danych osobowych w procesie.		
	Nazwa procesu przetwarzania danych osobowych	Rodzaj uprawnienia						Uzasadnienie	Dysponent procesu przetwarzania danych osobowych	Opinia	Podpis
		Oglądanie	**Zbieranie**	**Edycja**	**Wykorzystywanie**	**Usuwanie**	**Niszczenie**				
1.											
2.											
3.											
4.											
5.											
6.											

Dostęp do systemu informatycznego

Pracownik

Lp.	Uzasadnienie potrzeby posiadania dostępu Wypełnia bezpośredni przełożony								Opinia w sprawie celowości nadania hasła Wypełnia kierownik komórki organizacyjnej Starostwa/Dysponent programu		
	Wykaz programów, do których konieczne jest uzyskanie zgody na dostęp	Rodzaj dostępu						Uzasadnienie	Dysponent programu	Opinia	
		Oglądanie	Wprowadzanie	Edycja	Usuwanie	Wydruki	Administrator				
1.											
2											
3.											
4.											
5.											
6.											
7.											
8.											
9.											
10.											

Starosta

Ryszard Winiarski

Załącznik Nr 9
do Zarządzenia Nr 59/2018
Starosty Raciborskiego
z dnia 25 maja 2018r.

U P O W A Ż N I E N I E Nr

z dnia

Aktualizacja upoważnienia nr:

Stanowisko:

Komórka organizacyjna:

Pan (i)

otrzymuje upoważnienie

I. do wykonywania operacji przetwarzania danych osobowych w procesach	O	Z	E	W	U	N

O-oglądanie, Z-zbieranie, E-edycja, W-wykorzystywanie, U-usuwanie, N-niszczenie

II. do wykonywania operacji przetwarzania w systemach informatycznych:	O	W	E	U	W	A

O-oglądanie, W-wprowadzanie, E-edycja, U-usuwanie, W-wydruki, A-administracja

Niniejsze upoważnienie ważne jest w czasie zatrudnienia w Starostwie Powiatowym w Raciborzu.
Upoważnienie aktualizowane utraciło ważność.
Upoważnienie nie może być przeniesione na inne osoby

. . . . . .
STAROSTA RACIBORSKI

Powyższe upoważnienie przyjmuję do wiadomości i ścisłego przestrzegania

Racibórz .....
/data i podpis upoważnionego/

Starosta

Ryszard Winiarski

Załącznik Nr 10
do Zarządzenia Nr 59/2018
Starosty Raciborskiego
z dnia 25 maja 2018r.

REJESTR UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH

UPOWAŻNIENIA AKTUALNE NA DZIEŃ:

Lp	Imię i nazwisko	Stanowisko Komórka organizacyjna Wydano upoważnienie do:	Numer upoważnienia	Data wydania	Data cofnięcia	Podstawa cofnięcia	Uwagi
1	2	3	4	5	6	7	8

Aktualny REJESTR UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH znajduje się systemie elektronicznym Inspektora Ochrony Danych.

Starosta

Ryszard Winiarski

Załącznik Nr 11
do Zarządzenia Nr 59/2018
Starosty Raciborskiego
z dnia 25 maja 2018r.

Pracownik
Stanowisko
Komórka organizacyjna

OŚWIADCZENIE

Oświadczam, że zapoznałem/zapoznałam się z obowiązującymi w Starostwie Powiatowym w Raciborzu zasadami ochrony danych osobowych określonych w

……..

Są one dla mnie zrozumiałe i zobowiązuję się do:

1. stosowania się do ich zapisów;
2. zachowania w tajemnicy danych osobowych, do których mam lub będę miał/a dostęp w związku z wykonywaniem powierzonych mi czynności;
3. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych o których mowa w pkt. 2;
4. zachowania danych osobowych i sposobów ich zabezpieczenia w tajemnicy także po zakończeniu realizacji powierzonych mi czynności, zmiany stanowiska, a także ustania stosunku zatrudnienia;

Przyjmuję do wiadomości, iż za postępowanie sprzeczne z powyższymi zobowiązaniami mogę zostać pociągnięty/a do odpowiedzialności, w szczególności mogę podlegać odpowiedzialności karnej.

Racibórz, dn.....

.....
czytelny podpis

Starosta

Ryszard Winiarski

Załącznik Nr 12
do Zarządzenia Nr 59/2018
Starosty Raciborskiego
z dnia 25 maja 2018r.

Pracownik
Stanowisko
Komórka organizacyjna

ZAŚWIADCZENIE

o szkoleniu z zakresu ochrony danych osobowych

Zaświadczam, że Pan/Pani . . . . . w dniu . . . . został/została przeszkolony/przeszkolona z przepisów 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).

Prowadzący szkolenie

Data i podpis osoby szkolonej

Starosta

Ryszard Winiarski

Załącznik Nr 13
do Zarządzenia Nr 59/2018
Starosty Raciborskiego
z dnia 25 maja 2018r.

REJESTR UDOSTĘPNIONYCH DANYCH OSOBOWYCH
I PODMIOTÓW, KTÓRYM UDOSTĘPNIONO DANE OSOBOWE

Administrator danych: **STAROSTA RACIBORSKI**

Lp.	Nazwa zbioru danych	Odbiorca danych	Data udostępnienia	Podstawa prawna udostępnienia	Zakres udostępnionych danych	Osoba udostępniająca

Aktualny WYKAZ APLIKACJI DO PRZETWARZANIA DANYCH OSOBOWYCH
znajduje się systemie elektronicznym Inspektora Ochrony Danych

Starosta

Ryszard Winiarski

Załącznik Nr 14
do Zarządzenia Nr 59/2018
Starosty Raciborskiego
z dnia 25 maja 2018r.

Racibórz, dn. …….

……
(imię i nazwisko)

……
(stanowisko, jednostka organizacyjna)

Proszę o wyrażenie zgody na użytkowanie urządzenia służącego do przetwarzania danych osobowych, dla których administratorem jest Starosta Raciborski, poza obszarem przetwarzania danych osobowych Starostwa Powiatowego w Raciborzu.

Rodzaj urządzenia	**Nr inw.**
…….	……...

Wyszczególniony sprzęt jest niezbędny do wykonania następujących zadań służbowych:

……...

……...

.....
wnioskodawca

Wyrażam zgodę / Nie wyrażam zgody

.....
Inspektor Ochrony Danych

Wyrażam zgodę / Nie wyrażam zgody

.....
Bezpośredni przełożony

Starosta

Ryszard Winiarski

Załącznik Nr 15
do Zarządzenia Nr 59/2018
Starosty Raciborskiego
z dnia 25 maja 2018r.

REJESTR UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH W SYSTEMIE INFORMATYCZNYM STAROSTWA

UPOWAŻNIENIA AKTUALNE NA DZIEŃ:

Lp	**Imię, nazwisko, identyfikator**	**Stanowisko Komórka organizacyjna Wydano upoważnienie do:**	**Numer upoważnienia**	**Data wydania**	**Data cofnięcia**	**Podstawa cofnięcia**	**Uwagi**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**

Aktualny REJESTR UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH W SYSTEMOE INFORMATYCZNYM STAROSTWA znajduje się systemie elektronicznym Inspektora Ochrony Danych.

Starosta

Ryszard Winiarski