Zarządzenie Nr 4/2019
Dyrektora Zarządu Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu z dnia
14.01.2019r.

w sprawie wprowadzenia Polityki Ochrony Danych Osobowych w Zarządzie Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 ze zm.) oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000 ze zm.) zarządzam co następuje:

§ 1.

Zatwierdzam i wprowadzam Politykę Ochrony Danych Osobowych w Zarządzie Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu w brzmieniu Załącznika do niniejszego Zarządzenia.

§ 2.

Tracą moc zarządzenia Dyrektora Zarządu Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu:

1. Zarządzenie nr 35/2015 Dyrektora Zarządu Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu z dnia 23 czerwca 2015 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji oraz Instrukcji Zarządzania Systemem Informatycznym w Zarządzie Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu,
2. Zarządzenie nr 50/2016 Dyrektora Zarządu Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu z dnia 23 sierpnia 2016 r. w sprawie zmiany Zarządzenia nr 35/2015 z dnia 23 czerwca 2015 r.
3. Zarządzenie nr 81/2017 Dyrektora Zarządu Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu z dnia 12 czerwca 2016 r. w sprawie zmiany Zarządzenia nr 35/2015 z dnia 23 czerwca 2015 r.

§ 3.

Załącznik do niniejszego Zarządzenia stanowi dokumentację wewnętrzną Zarządu Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu i jest wyłączony z publikacji w Biuletynie Informacji Publicznej.

§ 4.

Zarządzenie wchodzi z dniem podjęcia.

DYREKTOR
Krzysztof Szewczyk

POLITYKA OCHRONY DANYCH OSOBOWYCH W ZARZĄDZIE DRÓG KOMUNIKACJI I UTRZYMANIA MIASTA W WAŁBRZYCHU

I. POSTANOWIENIA OGÓLNE

§1

Deklaracja i zastosowanie

1. **Celem** niniejszej Polityki ochrony danych osobowych jest wypełnienie założeń 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, dalej też zwane Rozporządzeniem).
2. Niniejsza Polityka stanowi zbiór wymogów, zasad i regulacji ochrony danych osobowych u **Administratora danych osobowych**, którym jest Dyrektor Zarządu Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu reprezentowany, (dalej jako Administrator).
3. Zasady, działania, kompetencje i zakresy odpowiedzialności opisane w niniejszej Polityce Ochrony Danych Osobowych (Polityka), obowiązują wszystkich pracowników ZDKiUM.
4. Procedury i dokumenty związane z Polityką są weryfikowane i dostosowywane w celu zapewnienia odpowiedniego poziomu bezpieczeństwa. Przeglądy dokumentacji odbywają się nie rzadziej niż raz w roku.
5. Polityka określa środki techniczne i organizacyjne zastosowane przez Administratora dla zapewnienia ochrony danych osobowych oraz tryb postępowania w przypadku stwierdzenia naruszenia zabezpieczenia danych w systemie informatycznym lub w kartotekach papierowych, albo w sytuacji podejrzenia o takim naruszeniu.
6. Polityka została opracowana z uwzględnieniem metod i środków ochrony danych osobowych, których skuteczność w czasie ich zastosowania jest powszechnie uznawana. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania właściwej ochrony wraz z zachowaniem ich dostępności, poufności, integralności i rozliczalności, ze szczególnym uwzględnieniem obowiązujących przepisów prawa dotyczących ochrony danych osobowych.
7. Zakres obowiązywania dokumentu.
   1) Niniejsza Polityka obowiązuje wszystkich pracowników ZDKIUM.

2) Każdy z pracowników ZDKIUM ma obowiązek zapoznania się z treścią niniejszej Polityki i potwierdzić to w stosownym oświadczeniu. Wzór oświadczenia stanowi **załącznik nr 11** do niniejszej Polityki.
3) Polityka dotyczy wyposażenia, systemów, urządzeń przetwarzających informacje w formie elektronicznej i papierowej.
4) Nieprzestrzeganie postanowień zawartych w Polityce może skutkować sankcjami wynikającymi z przepisów prawa pracy.

8. Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest **Administrator Danych Osobowych,** a za nadzór i monitorowanie jej przestrzegania odpowiada: **Inspektor ochrony danych (dalej IOD).**
9. Politykę ochrony danych opracowano na podstawie:
   1) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 ze zm.).
   2) Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000 ze zm.)

§ 2
Określenia użyte w polityce

1. **ZDKiUM** oznacza Zarząd Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu,
2. **Kierownicy komórek organizacyjnych** – należy przez to rozumieć również pracowników Zespołów oraz pracowników na samodzielnych stanowiskach.
3. **Administrator danych osobowych** - „Administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; **Administratorem jest Dyrektor Zarządu Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu** (dalej jako **Administrator**).
4. **Administrator Systemu Informatycznego (ASI)** – rozumie się przez to osobę odpowiedzialną za nadzór nad systemami informatycznymi wykorzystywanymi u Administratora Danych.
5. **organ nadzorczy** – Prezes Urzędu Ochrony Danych Osobowych
6. **dane osobowe** - oznaczają 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, kulturową lub społeczną tożsamość osoby fizycznej;

7. **dane szczególnych kategorii** oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej;
8. **hasło** – rozumie się przez to ciąg znaków alfanumerycznych, znany jedynie użytkownikowi;
9. **identyfikator** – rozumie się przez to, ciąg znaków literowych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
10. **incydent ochrony danych osobowych** – zdarzenie albo seria niepożądanych lub niespodziewanych zdarzeń ochrony danych osobowych stwarzających znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrożenia ochrony danych osobowych;
11. **Inspektor ochrony danych (Inspektor)** – osoba sprawująca nadzór nad przestrzeganiem zasad ochrony danych osobowych wyznaczona przez Administratora;
12. **naruszenie ochrony danych osobowych** - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
13. **obszar przetwarzania danych** – rozumie się przez to budynki i pomieszczenia określone przez administratora danych, tworzące obszar, w którym przetwarzane są dane osobowe i inne informacje prawem chronione. Wzór wykazu budynków i pomieszczeń w których przetwarzane są dane osobowe stanowi **załącznik nr 4** do niniejszej Polityki;
14. **odbiorca danych** – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią; organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
15. **osoba, podmiot danych** - oznacza osobę, której dane dotyczą;

16. **podmiot przetwarzający** - oznacza organizację lub osobę, której Administrator powierzył przetwarzanie danych osobowych.
17. **polityka** oznacza niniejszą Politykę ochrony danych osobowych;
18. **RCPDO lub rejestr** oznacza rejestr czynności przetwarzania danych osobowych;
19. **Rozporządzenie** oznacza rozporządzenie parlamentu europejskiego i rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/we (ogólne rozporządzenie o ochronie danych) (dz.urz. UE l 119, s. 1).
20. **ryzyko** – niepewność osiągnięcia zamierzonych celów;
21. **system informatyczny administratora danych** – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych;
22. **Dokumentacja ochrony danych** – zbiór dokumentów, instrukcji, regulaminów, załączników opisujących sposób przetwarzania i ochrony danych, składający się na politykę ochrony danych osobowych, gromadzonych i nadzorowanych przez IOD.
23. **teletransmisja** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
24. **uwierzytelnienie** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
25. **użytkownik** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło;
26. **zgoda osoby, której dane dotyczą** - oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

§ 3

Zasady ochrony danych

System zarządzania ochroną danych osobowych zgodny z wymaganiami niniejszej Polityki działa z poszanowaniem następujących zasad:

1. w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
2. rzetelnie i uczciwie (rzetelność);
3. w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
4. w konkretnych celach i nie „na zapas" (minimalizacja);

5. nie więcej niż potrzeba (adekwatność);
6. z dbałością o prawidłowość danych (prawidłowość);
7. nie dłużej niż potrzeba (czasowość);
8. zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

§ 4

Cel ochrony danych osobowych i strategie bezpieczeństwa

1. Ochrona danych osobowych w ZDKiUM realizowana jest poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu poniższych celów i zapewnić:
   1) **rozliczalność** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
   2) **integralność** – rozumie się przez to właściwość zapewniającą, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   3) **poufność** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
   4) **dostępność** – gwarantuje, że osoby, które są upoważnione i którym informacje są potrzebne, mają do nich dostęp w odpowiednim miejscu i czasie.
3. Cele i strategie bezpieczeństwa:
   1) zgodność z prawem,
   2) ochrona zasobów informacyjnych i innych aktywów,
   3) uzyskanie i utrzymanie odpowiednio wysokiego poziomu bezpieczeństwa zasobów, rozumiane jako zapewnienie poufności, integralności i dostępności oraz zapewnienie rozliczalności podejmowanych działań,
   4) zapewnienie ciągłości działania procesów i właściwej reakcji na incydenty i naruszenia ochrony danych,
   5) zapewnienie odpowiedniego poziomu wiedzy dotyczącej ochrony danych osobowych wśród pracowników i współpracowników poprzez zapewnienie odpowiednich szkoleń.

II. ZAKRES ODPOWIEDZIALNOŚCI

§ 5

Administrator danych osobowych

1. Administrator stosuje środki techniczne oraz organizacyjne w celu zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzanych danych osobowych, z uwzględnieniem stanu wiedzy technicznej, kosztu wdrożenia, charakteru, zakresu, kontekstu

i celu przetwarzania, ryzyka naruszenia praw lub wolności o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

2. Administrator zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych, określonemu na podstawie przeprowadzonej analizy ryzyka. Instrukcja w sprawie zasad i trybu zarządzania ryzykiem ochrony danych osobowych przetwarzanych w ZDKiUM stanowi **załącznik nr 1** do niniejszej Polityki.
3. We wszystkich umowach, które mogą dotyczyć powierzenia przetwarzania danych, Administrator uwzględnia zapisy zobowiązujące drugą stronę do przestrzegania art. 28 Rozporządzenia oraz obowiązujących przepisów krajowych.
4. Administrator prowadzi dokumentację opisującą sposób przetwarzania danych osobowych oraz sposób ich zabezpieczenia, w szczególności w postaci polityk, procedur, wytycznych oraz formularzy.
5. Administrator dopuszcza do przetwarzania danych osobowych jedynie osoby upoważnione przez administratora, które złożyły oświadczenie o zapoznaniu się z treścią niniejszej Polityki.

§ 6

Inspektor Ochrony Danych

1. Inspektor ochrony danych jest wyznaczany przez Administratora na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 Rozporządzenia, zgodnie z zapisami Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000 ze zm.).
2. Do zadań Inspektora Ochrony Danych należy:
   1) informowanie administratora, pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy Rozporządzenia oraz innych przepisów i doradzanie im w tej sprawie,
   2) monitorowanie przestrzegania Rozporządzenia, innych przepisów o ochronie danych oraz polityk administratora w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
   3) udzielanie na żądanie administratora zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 Rozporządzenia;
   4) współpraca z organem nadzorczym;

5) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 Rozporządzenia, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;

3. Status inspektora ochrony danych.
   1) Administrator zapewnia, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych;
   2) Administrator wspiera inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39 Rozporządzenia, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby i przedsięwzięcia niezbędne do utrzymania właściwego poziomu oraz aktualizacji jego wiedzy fachowej;
   3) Administrator zapewnia, aby inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Inspektor ochrony danych bezpośrednio podlega Administratorowi;
   4) osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw im przysługujących;
   5) Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań;
   6) Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator zapewnia, by takie zadania i obowiązki nie powodowały konfliktu interesów.

§ 7
Administrator Systemu Informatycznego

1. Administrator Systemu Informatycznego odpowiedzialny jest za:
   1) bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
   2) optymalizację wydajności systemu informatycznego, baz danych,
   3) instalację i konfigurację sprzętu sieciowego i serwerowego,
   4) instalację i konfigurację oprogramowania systemowego, sieciowego, oprogramowania baz danych,
   5) konfigurację i administrację oprogramowaniem systemowym sieciowym zabezpieczającym dane chronione przed nieupoważnionym dostępem,

6) współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych,
7) zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego i sieciowego,
8) zarządzanie kopiami awaryjnymi danych, w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
9) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,
10) przyznawanie na wniosek Administratora danych ściśle określonych praw dostępu do informacji w danym systemie,
11) wnioskowanie do Administratora danych w sprawie procedur bezpieczeństwa i standardów zabezpieczeń,
12) zarządzanie licencjami i procedurami ich dotyczącymi,
13) prowadzenie profilaktyki antywirusowej.

§ 8

Kierownicy komórek organizacyjnych oraz pracownicy

1. Każdy kierownik komórki organizacyjnej ZDKiUM, w której przetwarzane są dane osobowe, odpowiedzialny jest za:
   1) zapewnienie, aby bieżące przetwarzanie danych było zgodne z powszechnie obowiązującymi przepisami prawa i aktami wewnętrznymi, w szczególności niniejszą Polityką;
   2) współdziałanie z Inspektorem ochrony danych w zakresie zapewnienia przestrzegania ochrony danych;
   3) występowanie z wnioskiem o nadanie lub odebranie uprawnień do przetwarzania danych osobowych, w tym do ich przetwarzania w systemie informatycznym, jeżeli dane osobowe przetwarzane są w formie elektronicznej,
   4) zgłaszanie Inspektorowi ochrony danych zamiaru tworzenia, modyfikacji lub likwidacji zbioru, za który jest odpowiedzialny;
   5) zgłaszanie Inspektorowi ochrony danych oraz Administratorowi zdarzeń zagrażających bezpieczeństwu danych osobowych.
2. Każdy pracownik ZDKiUM obowiązany jest:
   1) zapoznać się oraz stosować postanowienia niniejszej Polityki;
   2) zapoznać się z obowiązującymi przepisami w zakresie ochrony danych osobowych;
   3) zachować w tajemnicy wszelkie dane osobowe, które pozyskał w trakcie wykonywania obowiązków pracowniczych;

4) przestrzegać stosowanych przez ZDKiUM środków oraz sposobów zabezpieczenia danych osobowych;
5) dbać o bezpieczeństwo danych osobowych, do których ma dostęp.

3. Obowiązek zachowania w tajemnicy danych osobowych, które pracownik pozyskał w trakcie zatrudnienia ZDKiUM, nie gaśnie wraz z rozwiązaniem stosunku pracy.
4. Pracownicy ZDKiUM podlegają wstępnym i okresowym szkoleniom z zakresu ochrony danych osobowych.

III. REJESTR CZYNNOŚCI PRZETWARZANIA

§ 9

1. Administrator prowadzi rejestr czynności przetwarzania. Rejestr ten prowadzony jest w formie elektronicznej i papierowej.
2. Rejestr czynności przetwarzania zawiera:
   1) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz inspektora ochrony danych;
   2) nazwę czynności przetwarzania;
   3) określenie komórki organizacyjnej, w której przetwarzane są dane;
   4) określenie celu przetwarzania;
   5) opis kategorii osób, których dane dotyczą oraz kategorii danych;
   6) wskazanie kategorii przetwarzanych danych;
   7) określenie podstawy prawnej przetwarzania;
   8) określenie źródła danych;
   9) wskazanie planowanego terminu usunięcia danych;
   10) nazwę i dane kontaktowe współadministratorów;
   11) nazwę i dane kontaktowe podmiotu przetwarzającego;
   12) opis kategorii odbiorców, który dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach poza Unią Europejską lub w organizacjach międzynarodowych (innych niż podmiot przetwarzający);
   13) nazwę systemu lub oprogramowania;
   14) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa;
   15) wskazanie lokalizacji raportu – jeżeli wymagane jest przeprowadzenie DPIA;
   16) jeżeli dane przekazywane są do państw poza Unię Europejską lub do organizacji międzynarodowych - nazwę tego państwa lub organizacji oraz dokumentację odpowiednich zabezpieczeń;

3. Każda komórka organizacyjna ZDKiUM raz w roku przeprowadza aktualizację Rejestru czynności przetwarzania. Zaktualizowany rejestr należy przekazać Inspektorowi Ochrony Danych do dnia 31 grudnia każdego roku.
4. Wzór Rejestru czynności przetwarzania w ZDKiUM stanowi **załącznik nr 5** do niniejszej Polityki

IV. OCENA SKUTKÓW DLA PRZETWARZANIA DANYCH

§ 10.

1. Administrator dokonuje oceny skutków dla ochrony danych i dokumentuje fakt dokonania tej oceny w przypadkach kiedy zaistnieje, któraś z przesłanek określonych w ust. 2 i 3.
2. Wykonanie oceny skutków dla ochrony danych jest konieczne, jeżeli dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw i wolności osób których dane dotyczą. Dla podobnych operacji przetwarzania wiążących się z podobnym wysokim ryzykiem ocena skutków dla ochrony danych wykonywana jest pojedynczo.
3. Wykonanie oceny skutków dla ochrony danych osobowych wymagana w szczególności:
   1) przetwarzania na dużą skalę szczególnych kategorii danych, o których mowa w art. 9 ust. 1 Rozporządzenia lub danych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10 Rozporządzenia lub
   2) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.
4. Administrator monitoruje wykaz rodzajów przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków dla ochrony danych opublikowany przez Urząd Ochrony Danych Osobowych i dokonuje oceny skutków czynności przetwarzania wskazanych w tym wykazie jako rekomendowanych do poddania tej ocenie.
5. Ocena skutków dla ochrony danych zawiera co najmniej:
   1) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie - prawnie uzasadnionych interesów realizowanych przez administratora;
   2) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celu, w jakim dane zostały pozyskane;
   3) ocenę ryzyka naruszenia praw i wolności osób, których dane dotyczą;
   4) środki planowane w celu minimalizacji ryzyka, w tym zabezpieczenia, środki i mechanizmy bezpieczeństwa zapewniające ochronę danych oraz wykazanie przestrzegania przepisów Rozporządzenia.

6. Administrator dokonuje bieżącego przeglądu czynności przetwarzania, celem weryfikacji, czy przetwarzanie to odbywa się w sposób zgodny z dokonaną oceną skutków dla ochrony danych.
7. Administrator konsultuje się z Urzędem Ochrony Danych Osobowych, jeżeli dokonana ocena skutków dla ochrony danych będzie wskazywała na występowanie wysokiego ryzyka dla praw i wolności pacjentów, jeżeli nie zastosowane zostałyby środki mitygujące ryzyko. Konsultacje z UODO dokonywane są przed rozpoczęciem przetwarzania danych osobowych.

V. POWIERZANIE DANYCH OSOBOWYCH PODMIOTOM ZEWNĘTRZNYM

§ 11.

1. Administrator może korzystać z usług podmiotów zewnętrznych w celu wspierania administratora w jego bieżącej działalności.
2. Administrator korzysta wyłącznie z usług takich dostawców usług, którzy zapewniają odpowiednie gwarancje bezpieczeństwa danych i zgodności przetwarzania danych osobowych z przepisami Rozporządzenia.
3. Administrator zawiera z podmiotem przetwarzającym umowę powierzenia przetwarzania danych lub reguluje okoliczność powierzenia przetwarzania danych innym instrumentem prawnym, w której określone zostają obowiązki podmiotu przetwarzającego wynikające z faktu powierzenia. Wzór umowy powierzenia przetwarzania stanowi **załącznik nr 6** do niniejszej Polityki.
4. W przypadku przekazywania danych do państw poza teren Unii Europejskiej, administrator spełnia dodatkowe warunki, o których mowa w Rozporządzeniu.
5. Inspektor Ochrony Danych prowadzi wykaz podmiotów zewnętrznych z którymi zawarto umowy powierzenia. Wzór wykazu stanowi **załącznik nr 7** do niniejszej Polityki.

VI. PRAWA PODMIOTÓW DANYCH

§ 12.

1. Administrator wypełnia obowiązki informacyjne wobec osób których dane przetwarza, zgodnie z art. 13 i 14 Rozporządzenia.
2. Każdej osobie, której dane są przetwarzane w ZDKiUM przysługuje prawo do kontroli przetwarzania jej danych osobowych, a w szczególności prawo do:
   1) uzyskania wyczerpującej informacji, czy jej dane osobowe są przetwarzane oraz do otrzymania informacji o pełnej nazwie i adresie siedziby Administratora danych

osobowych;uzyskania informacji o celu, podstawie prawnej, zakresie i sposobie przetwarzania danych osobowych;

2) uzyskania informacji, od kiedy są przetwarzane jej dane osobowe oraz podania w powszechnie zrozumiałej formie treści tych danych;
3) uzyskania informacji o źródle, z którego pochodzą dane osobowe jej dotyczące;
4) uzyskania informacji o sposobie udostępniania danych osobowych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym te dane osobowe są udostępniane;
5) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem przepisów prawa albo są już zbędne do realizacji celu, dla którego zostały zebrane

3. Instrukcja w sprawie wypełniania obowiązku informacyjnego oraz zapewnienia realizacji praw podmiotów danych w ZDKiUM stanowi **załącznik nr 2** do niniejszej Polityki.

VII. OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH ORAZ SPOSÓB POSTĘPOWANIA Z NARUSZENIAMI

§ 13

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są informacje to głównie:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
2) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
6) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych,
7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
8) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,

9) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony informacji - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
11) ujawniono istnienie nieautoryzowanych kont dostępu do danych,
12) podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane,
13) naruszono dyscyplinę pracy w zakresie przestrzegania procedur ochrony danych osobowych (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych, itp.).

§ 14

Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.

§ 15

Administrator stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia. Instrukcja w sprawie postępowania w sytuacji naruszenia ochrony danych osobowych w ZDKiUM stanowi **załącznik nr 3** do niniejszej Polityki.

VIII. UDOSTĘPNIANIE DANYCH

§ 16

1. Przetwarzanie, w tym udostępnianie danych osobowych jest prawnie dopuszczalne, jeżeli jest niezbędne dla zrealizowania obowiązku wynikającego z przepisu prawa.
2. Dane osobowe można wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
3. Podmiot występujący o udostępnienie informacji powinien wskazać podstawę prawną upoważniającą go do otrzymania tych danych albo uzasadnioną potrzebę żądania ich udostępnienia. Tylko w takiej sytuacji można dokonać oceny, czy w określonym przypadku

udostępnienie danych jest prawnie dopuszczalne i czy nie będzie ono stanowić naruszenia zasad ochrony danych.

4. Udostępnienie danych może nastąpić jedynie za zgodą Administratora danych.

IX. ŚRODKI TECHNICZNE I ORGANIZACYJNE STOSOWANE DO ZAPEWNIENIA ROZLICZALNOŚCI, INTEGRALNOŚCI, POUFNOŚCI, DOSTĘPNOŚCI

§ 17

Ochrona fizyczna

1. Budynki, w których mieści się Zarząd Dróg Komunikacji i Utrzymania Miasta, w których przetwarzane są dane osobowe są zamykane na klucz po zakończeniu pracy. Budynki są dozorowane.
2. Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych jest dopuszczone tylko w obecności osoby upoważnionej do przetwarzania danych.
3. Pomieszczenia w których przetwarzane są dane osobowe są zamykane na czas nieobecności w nich osób upoważnionych, aby uniemożliwić do nich dostęp osób nieuprawnionych.
4. W przypadku przebywania w pomieszczeniu, w którym przetwarzane są dane osobowe osób postronnych ekran monitora należy ustawić w taki sposób, aby uniemożliwić wgląd w dane.

§ 18

Ochrona organizacyjna

1. Dla zapewnienia bezpieczeństwa danych i informacji zastosowano następujące **środki organizacyjne:**
   1) Administrator danych przyznaje uprawnienia dostępu do przetwarzania danych osobowych w formie pisemnego upoważnienia. Wzór upoważnienia stanowi **załącznik nr 8** do niniejszej Polityki.
   2) Administrator prowadzi ewidencję osób upoważnionych.
   3) Osoby nowozatrudnione przed dopuszczeniem do pracy muszą przejść obowiązkowe szkolenie z zakresu obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane są o podstawowych zagrożeniach związanych z przetwarzaniem danych osobowych.
   4) Szkolenie przeprowadza Inspektor Ochrony Danych.
   5) Potwierdzeniem udziału w szkoleniu jest Karta szkolenia, podpisana przez pracownika i Inspektora ochrony danych. Wzór Karty szkolenia stanowi **załącznik nr 10** do niniejszej Polityki.
   6) Karta szkolenia wpinana jest do dokumentacji ochrony danych,

7) Należy chronić dane przed wszelkim dostępem do nich osób nieuprawnionych.
8) Pomieszczenia w których są przetwarzane dane osobowe muszą być zamykane na klucz.
9) Pobieranie kluczy z portierni w budynku przy ul. Matejki 1 potwierdzane jest podpisem pracownika. Po zakończeniu pracy klucze zdawane są na portierni.
10) Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy. W przypadku, gdy dostęp do pomieszczenia jest wymagany poza godzinami pracy – możliwy jest tylko na podstawie zezwolenia Administratora.
11) Dostęp do pomieszczeń w których są przetwarzane dane osobowe mogą mieć tylko upoważnieni pracownicy.
12) W przypadku pomieszczeń do których dostęp mają również osoby nieupoważnione, mogą one przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności.
13) Szafy w których przechowywane są dane są zamykane na klucz.
14) Szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych a następnie powinny być zamykane.
15) Dane w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych a następnie muszą być chowane do szaf.

2. Dla zapewnienia bezpieczeństwa danych i informacji zastosowano następujące **środki techniczne:**
   1) Dostęp do komputerów na których są przetwarzane dane mają tylko upoważnieni pracownicy.
   2) Monitory komputerów na których przetwarzane są dane są tak ustawione aby osoby nieupoważnione nie miały wglądu w dane.
   3) Po zakończeniu pracy komputery przenośne (np. typu notebook) zawierające dane osobowe powinny być zabezpieczone w zamykanych na klucz szafach.
   4) W wypadku potrzeby wyniesienia komputera przenośnego (np. typu notebook) zawierającego dane osobowe, lub inne informacje chronione dane te muszą zostać zaszyfrowane. Nie należy udostępniać osobom nieupoważnionym tych komputerów.
   5) W przypadku potrzeby przeniesienia danych osobowych pomiędzy komputerami należy dokonać tego z zachowaniem szczególnej ostrożności.
   6) Nośniki użyte do przenoszenia danych należy wyczyścić (skasować nieodwracalnie) aby nie zostały na nich dane osobowe.
   7) W wypadku niemożliwości skasowania danych z nośnika (płyta CD-ROM) należy taką płytę zniszczyć fizycznie.

8) W przypadku wykorzystania do przenoszenia danych dysków, dane należy kasować z tych dysków.
9) Niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną.
10) Błędne lub nieaktualne wydruki i wersje papierowe zawierające dane osobowe lub inne informacje chronione niszczone są za pomocą niszczarki lub w inny mechaniczny sposób uniemożliwiający powtórne ich odtworzenie.
11) Pracownicy zobowiązani są stosować zasadę czystego biurka - wszystkie dokumenty i materiały powinny być po zakończeniu pracy chowane w przeznaczonych do tego szafkach, szufladach.

X. BEZPIECZEŃSTWO TELEINFORMATYCZNE

§ 19

Wykorzystywanie zasobów

1. Do wykonywania obowiązków służbowych związanych z przetwarzaniem danych osobowych dozwolone jest używanie systemów, urządzeń i oprogramowania zgodnie z wymogami Polityki
2. Pracownicy są uprawnieni do korzystania z zasobów teleinformatycznych niezbędnych do wykonywania ich obowiązków.
3. Zakazane jest użytkowanie na terenie obszaru przetwarzania danych lub przy wykonywaniu obowiązków służbowych poza obszarem przetwarzania danych innych niż dopuszczone urządzeń, systemów i oprogramowania bez zgody Administratora Systemu Informatycznego (ASI).
4. Zakazane jest bez zgody ASI:
   1) użytkowanie urządzeń skutkujących połączeniem systemów Administratora danych z sieciami teleinformatycznymi innych podmiotów, w tym publicznymi sieciami teleinformatycznymi,
   2) użytkowanie urządzeń lub oprogramowania mających na celu zakłócenie działania innych systemów, urządzeń lub oprogramowania,
   3) użytkowanie urządzeń lub oprogramowania do testowania bezpieczeństwa lub wykrywania podatności,
   4) użytkowanie urządzeń lub oprogramowania mogących naruszyć bezpieczeństwo innych systemów lub urządzeń,
   5) wprowadzanie zmian konfiguracji urządzeń, systemów lub oprogramowania.

5. Wykorzystanie należących do Administratora urządzeń, systemów i oprogramowania oraz innych zasobów do prywatnych celów pracowników jest dozwolone jedynie na uzasadniony wniosek pracownika i za zgodą Administratora.
6. Zasoby Administratora danych powinny być przechowywane w taki sposób, aby zapobiec możliwości ich kradzieży lub uszkodzenia przez osoby postronne oraz przypadkowe uszkodzenia przez osoby lub czynniki środowiskowe.
7. Wynoszenie aktywów (zasobów i informacji) poza obszar przetwarzania danych możliwe jest za zgodą ADO.
8. Zakazane jest przesyłanie informacji podlegających ochronie na prywatne adresy poczty elektronicznej oraz prowadzenie korespondencji służbowej z wykorzystaniem prywatnego adresu e-mail użytkownika.
9. Zakazane jest używanie prywatnych nośników zewnętrznych (np. typu pendrive) i tworzenie nieautoryzowanych kopii z baz danych
10. Pracownicy są zobowiązani do ochrony zasobów będących własnością innych podmiotów, a powierzonych lub oddanych do dyspozycji Administratorowi danych lub udostępnionych pracownikom na czas wykonywania przez nich czynności służbowych w takim samym stopniu jak w przypadku zasobów będących własnością Administratora danych.
11. Procedury i instrukcje dotyczące bezpieczeństwa teleinformatycznego opracowuje ASI i przechowuje w Dokumentacji ochrony danych.

§ 20

Metody i środki uwierzytelniania i autoryzacji oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Zasady ogólne uwierzytelniania i autoryzacji w systemie.
   1) W systemach komputerowych wspomagających czynności merytoryczne, a w szczególności przetwarzających dane osobowe, użytkownicy podlegają uwierzytelnieniu za pomocą identyfikatora użytkownika i autoryzacji za pomocą hasła.
   2) Przy opuszczeniu stanowiska pracy należy zablokować system kombinacją klawiszy [Windows]+[L]
   3) Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wylogować się z systemu.
   4) Przed wyłączaniem komputera należy bezwzględnie:
      a) Zakończyć pracę uruchomionych programów,
      b) Wykonać zakończenie systemu połączone z wylogowywaniem,

5) Niedopuszczalne jest wyłączanie komputera bez zamknięcia wszystkich użytkowanych programów i wylogowania się z systemu.

2. Zasady nadawania identyfikatora.
   1) Identyfikator użytkownika jest unikalny w obrębie systemu, w którym jest stosowany.
   2) Identyfikator użytkownika jest konstruowany z pierwszej litery imienia i nazwiska.
   3) Identyfikator grupowy konstruowany jest na podstawie nazwy grupy.(np. kancelaria 1, kancelaria 2, sekretariat).
   4) Identyfikator użytkownika nie powinien być zmieniany bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielony innej osobie.
3. Zasady zarządzania hasłami
   1) W systemach umożliwiających samodzielną zmianę haseł przez użytkowników, hasło powinno być zmienione przy pierwszym logowaniu do systemu.
   2) Hasło użytkownika jest poufne, jest własnością użytkownika i zna je tylko dany użytkownik. Zabronione jest przekazywanie hasła innym lub w jakikolwiek sposób narażanie na poznanie hasła przez osoby postronne.
   3) Za zachowanie poufności swoich haseł odpowiedzialni są użytkownicy.
   4) Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności.
   5) Dla haseł grupowych użytkownik nie ma prawa udostępniania haseł danej grupy osobom spoza grupy, dla której zostały one utworzone.
   6) Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.
   7) W sytuacji, gdy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, pracownik zobowiązany jest do natychmiastowej zmiany hasła.
   8) Przy wyborze hasła obowiązują zasady:
      a) minimalna długość hasła – 8 znaków,
      b) zakazuje się stosować:
      - haseł, które użytkownik stosował uprzednio w okresie minionego roku,
      - swojej nazwy użytkownika w jakiejkolwiek formie,
      - swojego imienia, drugiego imienia, nazwiska, imion osób z najbliższej rodziny, w jakiejkolwiek formie,
      - ogólnie dostępnych informacji o użytkowniku takich jak: numer telefonu, numer rejestracji samochodu, jego marka, numer dowodu osobistego, nazwa ulicy na której mieszka lub pracuje,
      - przewidzianych w sekwencji znaków klawiatury QWERTY, 12345678, itp.
      c) należy stosować

- hasła zawierające kombinację dużych i małych liter,
- hasła zawierające znaki specjalne,
- hasła, które łatwo zapamiętać,
- hasła szybkie do wprowadzenia,

9) Zmiany hasła nie wolno zlecać innym osobom,
10) Hasła użytkowników uprzywilejowanych (tzn. użytkowników posiadających uprawnienia na poziomie administratorów systemów informatycznych) są zabezpieczone u Administratora w zamkniętej kopercie w metalowej szafie zamykanej na klucz.
11) W przypadku systemów uwierzytelniających za pomocą kart kryptograficznych piny do kart nie mogą być nigdzie zapisywane, a w szczególności nie na kartach lub w ich pobliżu.
12) Karty z kodami PUK pozwalającymi na zmianę PIN kart kryptograficznych winny być przechowywane oddzielnie od odpowiadających im kart kryptograficznych.

4. Zasady nadawania uprawnień w systemie informatycznym.
   1) Przyznawanie zakresu uprawnień powinno być w ścisłym związku z zakresem obowiązków danego pracownika.
   2) Nowe konto dla użytkownika zakładane jest przez Administratora systemu na podstawie **Wniosku o nadanie/odebranie/zmianę uprawnień do pracy w systemie,** podpisanego przez przełożonego pracownika. Wzór wniosku stanowi **załącznik nr 9** do niniejszej Polityki.
   3) W zarządzaniu dostępem obowiązuje zasada, że dostęp użytkownika powinien opierać się na spełnieniu zasady rozliczalności oraz zasady niezaprzeczalności. W przypadku systemów informatycznych obowiązują następujące wymagania:
      a) wymóg jednoznacznej identyfikacji pracownika - tj. w systemach informatycznych każdy użytkownik pracuje wyłącznie na swoim indywidualnym koncie, nie są stosowane konta anonimowe,
      b) wymóg uwierzytelnienia pracownika przy korzystaniu z systemu informatycznego, autoryzacji przyznania praw dostępu do systemów informatycznych.
5. Zasady wyrejestrowywania użytkownika z systemu informatycznego
   1) Wyrejestrowania użytkownika z systemu informatycznego dokonuje Administrator systemu informatycznego na wniosek Kierownika komórki organizacyjnej w której zatrudniony jest pracownik. Kierownik Działu Organizacji, Zarządzania i Kadr informuje administratora systemu informatycznego o dacie rozwiązania umowy z pracownikiem posiadającym uprawnienia. Administrator systemu informatycznego blokuje dostęp do

systemu niezwłocznie po przekazaniu przez Kierownika DOZiK informacji o dacie rozwiązania umowy z pracownikiem.

2) Wyrejestrowanie może mieć charakter czasowy, trwały lub automatyczny.
3) Wyrejestrowanie następuje poprzez:
   a) nieobecność użytkownika w pracy, przez okres wskazany przez Kierownika komórki organizacyjnej.
   b) rozwiązanie stosunku pracy,
   c) wszczęcie postępowania dyscyplinarnego względem osoby upoważnionej do przetwarzania danych
   d) incydentu bezpieczeństwa z udziałem konta nieobecnego w danej chwili użytkownika systemu informatycznego.
4) Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.

6. Zarządzanie uprawnieniami.
   1) Nowy użytkownik systemu może dostać uprawnienia do systemu komputerowego po:
      a) otrzymaniu upoważnienia do przetwarzania danych osobowych,
      b) odbyciu szkolenia w zakresie ochrony danych osobowych,
      c) zapoznaniu się z niniejszą Polityką
   2) Użytkownik systemu nie może uruchamiać innego oprogramowania niż zainstalowane przez Administratora systemu i do którego ma przyznane uprawnienia. Nie może samodzielnie instalować oprogramowania i w jakikolwiek sposób obchodzić zabezpieczenia uniemożliwiające instalację lub uruchomienie innego oprogramowania.
   3) Administrator systemu ma dostęp do całości systemu informatycznego, w tym uprawnienia do nadawania i odbierania uprawnień, zakładania kont użytkowników, zakładania i zmiany haseł.
   4) Użytkownik systemu może mieć dostęp tylko do tych zasobów sieci informatycznej ZDKiUM do której posiada przyznane przez Administratora systemu uprawnienia.
   5) Zmiany uprawnień dokonuje się każdorazowo na wniosek przełożonego użytkownika poprzez złożenie Wniosku o nadanie/odebranie/ zmianę uprawnień do pracy w systemie
   6) Osoby trzecie wykonujące zadanie w sieci ZDKiUM muszą każdorazowo uzyskać pozwolenie ADO. Praca ta musi przebiegać pod nadzorem Administratora systemu.
   7) Każde oprogramowanie konieczne do uruchomienia lub instalacji przez osoby trzecie musi być sprawdzone i zatwierdzone przez Administratora systemu.

§ 21

Tworzenie kopii zapasowych

1. Konfiguracja programów użytkowych powinna zapewnić przechowywanie zbiorów danych na wydzielonym zasobie serwera.
2. Serwer zapewnia automatyczną całościową archiwizację danych w cyklu codziennym lub z odstępem parudniowym w zależności od częstości wprowadzania danych.
3. Czasookres przechowywania kopii zapasowych na zasobach pamięci dyskowej wynosi nie mniej niż pół roku.
4. Każda kopia jest zachowywana z odnotowaniem daty i godziny powstania jako części jej nazwy.
5. Do utworzenia kopii używane są narzędzia przewidziane w serwerach baz danych (SQL Serwer) oraz program do archiwizacji.
6. Nad poprawnością funkcjonowania systemu archiwizacji czuwa Administrator systemu informatycznego.
7. Kopie awaryjne tworzone doraźnie należy usuwać bezzwłocznie po ustaniu ich użyteczności.

§ 22

Ochrona systemu przed wirusami i złośliwym oprogramowaniem

1. Środki ochrony systemu przed wirusami i innym złośliwym oprogramowaniem:
   1) Na każdym stanowisku komputerowym zainstalowane jest oprogramowanie antywirusowe wychwytujące wirusy jak i inne złośliwe oprogramowanie.
   2) Każda odbierana wiadomość przychodząca drogą elektroniczną (jak i załączniki) jest sprawdzana oprogramowaniem antywirusowym.
   3) Każdy nośnik wymienny musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który korzysta z nośnika.
   4) Zabrania się pobierania z internetu plików niewiadomego pochodzenia. Każdy plik pobrany z internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.
   5) W przypadku wykrycia wirusów komputerowych sprawdzane jest:
      a) stanowisko komputerowe na którym wykryto wirus,
      b) wszystkie nośniki wymienne posiadane przez użytkownika pracującego na stanowisku komputerowym
      c) komputery wszystkich osób logujących się na danej stacji.
      d) zasoby i użytkownicy wspólnych grup dzielących zasoby.

§ 23

Sposoby postępowania z dokumentacją elektroniczną

1. Zasady przechowywania dokumentów elektronicznych.
   1) Podczas logowania tworzony jest na pulpicie skrót do zasobu wspólnego właściwego dla danej komórki organizacyjnej
   2) Wszystkie dokumenty elektroniczne danej komórki należy przechowywać na zasobach wspólnych lub w systemie Elektronicznego Obiegu Dokumentów.
   3) Przydział uprawnień do czynności wykonywanych na wspólnych zasobach dokonuje się za pomocą Wniosku o nadanie/odebranie/zmianę uprawnień do pracy w systemie
2. Zasada „Czystego ekranu"
   1) Dokumenty elektroniczne powinny być przechowywane w sposób zapewniający ich bezpieczeństwo.
   2) Dokumenty zawierające dane poufne lub osobowe powinny być wyświetlane na monitorze w sposób uniemożliwiający ich odczyt przez osoby nieuprawnione.
   3) Po zakończeniu pracy na pulpicie oraz w folderach umieszczonych na nim nie wolno przechowywać żadnych dokumentów.
   4) Dokumenty wolno przechowywać na pulpicie tylko podczas bezpośredniej edycji. Po zakończeniu pracy muszą zostać przeniesione na zasób wspólny, a z pulpitu usunięte.

§ 24

Sposoby postępowania z nośnikami mobilnymi i zasady użytkowania komputerów przenośnych

1. Do nośników mobilnych zalicza się: płyty CD, DVD, Bluray, taśmy streamerów, masowe urządzenia magazynujące podłączane pod port USB, FireWire lub inny port wymiany danych komputera, pamięć wewnętrzna komputerów przenośnych, i innych urządzeń taką pamięć posiadających w tym: odtwarzacze mp3, mp4, palmtopy, telefony komórkowe, smartfony, nawigacje satelitarne.
2. Zasady użytkowania nośników mobilnych.
   1) Uprawnienia do użytkowania nośników mobilnych nadawane są za pomocą Wniosku o nadanie/odebranie/zmianę uprawnień do pracy w systemie.
   2) Nośniki USB są imiennie rejestrowane i tylko takie nośniki mogą być skutecznie użytkowane.
   3) Rejestr użytkowników posiadających uprawnienia do przechowywania danych na ośnikach mobilnych prowadzi IOD.
   4) Nośniki mobilne muszą być trwale oznaczone:

a) Środki trwałe posiadające wbudowane nośniki mobilne powinny być oznaczone etykietą zgodnie z oznaczeniami stosowanymi w ZDKiUM,

b) Inne nośniki powinny być oznaczone pieczątką ZDKiUM lub niezmazywalnym markerem „ZDKiUM

3) Nie wolno dokonywać zapisu i odczytu nośników danych innych niż oznaczone z wyjątkiem nośników obrotu danymi podlegających regulacjom odrębnych umów.
4) Dane osobowe powinny być przechowywane na nośnikach mobilnych w sposób bezpieczny. Chronione programem pozwalającym na szyfrowanie.
5) Nośniki wykorzystywane do przenoszenia danych osobowych przed ponownym wykorzystaniem powinny być czyszczone.
6) Niepotrzebne i uszkodzone nośniki mobilne oddawane są do Działu Organizacji, Zarządzania i Kadr.
7) Użytkownik nośników mobilnych podlega wstępnemu i okresowemu szkoleniu z zasad bezpiecznego przechowywania danych na nośnikach, zasad ich udostępniania oraz bezpiecznej pracy na urządzeniach mobilnych przy przetwarzaniu danych osobowych.

3. Zasady użytkowania komputerów przenośnych.
   1) Osoba użytkująca komputer przenośny, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem, przeznaczonym do przetwarzania danych osobowych wskazanym w niniejszej Polityce.
   2) W celu zapobiegania dostępowi do tych danych przez osobę nieuprawnioną należy:
   - Nie zezwalać na użytkowanie komputera osobom nieupoważnionym do dostępu do danych osobowych.
   - W przypadku konieczności przechowywania danych osobowych lub innych poufnych danych na dysku lokalnym należy takie dane zaszyfrować.

§ 25

Zasady korzystania z poczty e – mail

1. Serwer poczty elektronicznej funkcjonuje w wewnętrznej sieci ZDKiUM i zajmuje się dystrybucją wiadomości email w sieci wewnętrznej oraz na serwery zewnętrzne.
2. Wysyłanie poczty elektronicznej działa w oparciu o protokół SMTP.
3. Pobieranie wiadomości z serwera poczty elektronicznej wykonuje się w oparciu o protokół POP 3 lub IMAP
4. Ustawienia serwera wymagają uwierzytelnienia wysyłania wiadomości tj. przed wysłaniem każdej wiadomości pocztowej program pocztowy musi podać dane uwierzytelniające.

5. Konta poczty elektronicznej przydzielane są użytkownikom na podstawie Wniosku o nadanie/odebranie/zmianę uprawnień do pracy w systemie.
6. Konta poczty elektronicznej przydzielane są według klucza: „pierwsza litera imienianazwisko@zdkium.walbrzych.pl"; dla kont grupowych „nazwagrupy@zdkium.walbrzych.pl"
7. Administrator systemu generuje hasła do poczty oraz przeprowadza konfigurację programu pocztowego.
8. Wiadomość pocztowa jest wysyłana i odbierana nieszyfrowanym połączeniem nie wolo jej stosować do przesyłania danych osobowych bez zastosowana szyfrowania załączników.
9. W przypadku wysyłana wiadomości do wielu odbiorców zwłaszcza na adresy prywatne lub do instytucji innych niż administracja publiczna należy używać pola ukrytego.

§ 26

Zasady usuwania danych z informatycznych nośników zawierających dane osobowe

1. Usuwanie danych z nośnika polega na trwałym, fizycznym ich zniszczeniu wraz z ich nośnikami w stopniu uniemożliwiającym ich odtworzenia przez osoby niepowołane, przy zastosowaniu powszechnie dostępnych metod.
2. W zależności od nośnika na którym przechowywane są dane osobowe, ich usuwanie polega na:
   1) Nośniki optyczne (płyty CD/DVD/BLU-RAY) - należy w taki sposób zniszczyć nośnik, aby uniemożliwić odczytanie danych z płyty. W tym przypadku zalecane jest wykorzystywanie niszczarek spełniających wymagania:
      a) Klasa B – ochrona przeznaczona dla danych poufnych, przeznaczonych dla wąskiego grona odbiorców,
      b) Stopień 3 - nośniki z danymi chronionymi i poufnymi, a także danymi osobowymi, które wymagają większej ochrony – kategoria O-3 dla płyt CD/DVD/BLU-RAY,
      c) Stopień 4: Nośniki z danymi szczególnie chronionymi i poufnymi, a także z danymi osobowymi, które podlegają szczególnej ochronie ochronie – dane szczególnych kategorii – kategoria O- 4 dla płyt CD/DVD/BLU-RAY,
   2) Nośniki elektroniczne (penidrive/karty pamięci/dyski twarde SSD) – obecnie istniejące sposoby niszczenia danych można podzielić na dwie główne grupy metod:
      a) Niszczenie programowe – polegające na wielokrotnym nadpisywaniu danych na nośniku, które uniemożliwiają odczytanie danych. Istnieje specjalnie oprogramowanie dostępne na rynku służące do nadpisywania (definitywnego usuwania) danych.

b) Niszczenie sprzętowe - polegające na trwałym zniszczeniu nośnika za pomocą odpowiednich urządzeń.

3) Nośniki magnetyczne (dyski twarde HDD) – oprócz sposobów niszczenia danych dostępnych dla nośników elektronicznych, istnieje również możliwość demagnetyzacji nośników, jako jednego z rodzajów niszczenia sprzętowego.
4) Przynajmniej raz w roku ASI dokonuje przeglądu informatycznych nośników danych w celu przeznaczenia ich do zniszczenia.
5) Niezależnie od nośnika, na którym są przechowywane dane osobowe przeznaczone zniszczenia, samo ich zniszczenie powinno odbywa się komisyjnie, a z samej operacji jest sporządzany protokół.
6) Komisja w składzie trzech osób (ASI, IOD osoba wyznaczona przez Administratora) powoływana jest Zarządzeniem Dyrektora ZDKiUM.

XI. POSTANOWIENIA KOŃCOWE

§ 27

1. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie aktualnie obowiązujące przepisy prawa w zakresie ochrony danych osobowych.
2. Użytkownicy zobowiązani są do bezwzględnego stosowania postanowień zawartych w niniejszej Polityce. W wypadku odrębnych od zawartych w niniejszej Polityce uregulowań występujących w innych procedurach obowiązujących u Administratora Danych, użytkownicy mają obowiązek stosowania unormowań dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.

XII. SPIS ZAŁĄCZNIKÓW

1. Instrukcja w sprawie zasad i trybu zarządzania ryzykiem ochrony danych osobowych przetwarzanych w ZDKiUM stanowi **załącznik nr 1** do Polityki;
2. Instrukcja wypełniania obowiązku informacyjnego oraz zapewnienia realizacji praw podmiotów danych w Zarządzie Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu stanowi **załącznik nr 2** do Polityki;
3. Instrukcja w sprawie postępowania w sytuacji naruszenia ochrony danych osobowych w Zarządzie Dróg, Komunikacji i Utrzymania Miasta stanowi **załącznik nr 3** do Polityki;
4. Wzór wykazu budynków i pomieszczeń w których przetwarzane są dane osobowe stanowi **załącznik nr 4** do Polityki.
5. Wzór Rejestru czynności przetwarzania danych osobowych stanowi **załącznik nr 5** do Polityki.

6. Wzór umowy powierzenia przetwarzania stanowi **załącznik nr 6** do Polityki;
7. Wykaz podmiotów zewnętrznych, którym powierzono dane osobowe do przetwarzania stanowi **załącznik nr 7** do Polityki.
8. Wzór upoważnienia do przetwarzania danych osobowych stanowi **załącznik nr 8** do Polityki.
9. Wzór wniosku o nadanie/zmianę uprawnień do pracy w systemie stanowi **załącznik nr 9** do Polityki.
10. Wzór karty szkolenia wstępnego/okresowego stanowi **załącznik nr 10** do Polityki
11. Oświadczenie o zapoznaniu się z Polityką ochrony danych w Zarządzie Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu stanowi **załącznik nr 11** do Polityki.

Przedstawione powyżej wzory nie stanowią katalogu zamkniętego dokumentacji składającej się na Politykę ochrony danych osobowych. Każda dodatkowa, nowa procedura, instrukcja czy wytyczna ADO dotycząca obszaru ochrony danych osobowych stanowi integralną część niniejszej Polityki, a ich dodanie nie wymaga jej zmiany.

Załącznik nr **1** do Polityki ochrony danych
w Zarządzie Dróg, Komunikacji
i Utrzymania Miasta w Wałbrzychu

INSTRUKCJA W SPRAWIE ZASAD I TRYBU ZARZĄDZANIA RYZYKIEM DLA OCHRONY DANYCH OSOBOWYCH PRZETWARZANYCH W ZARZĄDZIE DRÓG, KOMUNIKACJI I UTRZYMANIA MIASTA W WAŁBRZYCHU

I. CZĘŚĆ OGÓLNA

§ 1

Określenia użyte Instrukcji w sprawie zasad i trybu zarządzania ryzykiem dla ochrony danych osobowych przetwarzanych w Zarządzie Dróg Komunikacji i Utrzymania Miasta w Wałbrzychu zostały objaśnione § 2 Polityki Ochrony Danych Osobowych w Zarządzie Dróg Komunikacji i Utrzymania Miasta w Wałbrzychu.

§ 2

1. Celem niniejszego dokumentu jest ustalenie metodyki zarządzania ryzykiem bezpieczeństwa danych osobowych przetwarzanych w ZDKiUM z uwzględnieniem ryzyka naruszenia praw lub wolności osób fizycznych, których dane dotyczą.
2. Dokument określa sposób przeprowadzania i dokumentowania procesu szacowania ryzyka.

§ 3

1. Wynikiem przeprowadzonego procesu szacowania ryzyka jest określenie adekwatnych do zagrożeń i prawdopodobieństwa ich wystąpienia, środków technicznych i organizacyjnych, niezbędnych do osiągnięcia akceptowalnego poziomu ryzyka.
2. Zarządzanie ryzykiem ma na celu działania podnoszące poziom bezpieczeństwa ochrony danych osobowych przetwarzanych w ZDKiUM uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych. Oznacza to między innymi, że dane osobowe przetwarzane w ZDKiUM powinny być zabezpieczone przed nieuprawnionymi zmianami, ujawnieniem nieupoważnionym osobom, zniszczeniem, utratą lub uszkodzeniem.
3. Przez pojęcie ochrony danych należy rozumieć zachowanie poufności, integralności, dostępności i rozliczalności.
   Wymienione właściwości, polegają odpowiednio na:

- **poufności** – zapewnieniu, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom;
- **integralności** – zapewnieniu, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- **dostępności** – zapewnieniu bycia osiągalnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot;
- **rozliczalności** – zapewnieniu, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

4. Poprzez zarządzanie ryzykiem bezpieczeństwa ochrony danych osobowych należy rozumieć działania polegające na:

- identyfikacji zasobów;
- określeniu zagrożeń;
- szacowaniu ryzyka;
- postępowaniu z ryzykiem;
- akceptowaniu ryzyka;
- monitorowaniu ryzyka;
- informowaniu o ryzyku.

§ 4

Monitorowanie procesu zarządzania ryzykiem bezpieczeństwa danych osobowych w ZDKiUM i dokumentowanie tych czynności jest elementem wywiązania się z ciążącego na Administratorze Danych Osobowych obowiązku zapewnienia przetwarzania zgodnego z ogólnym rozporządzeniem o ochronie danych.

§ 5

1. Administrator Danych Osobowych zapewnia warunki niezbędne do prawidłowego funkcjonowania procesu zarządzania ryzykiem ochrony danych osobowych przetwarzanych w ZDKiUM.
2. Cały proces szacowania ryzyka ochrony danych osobowych przetwarzanych w ZDKiUM koordynuje i nadzoruje Inspektor Ochrony Danych.
3. Kierownicy komórek organizacyjnych zapewniają i odpowiadają za systematyczną identyfikację zasobów i zagrożeń, przeprowadzenie szacowania ryzyka, ocenę jego istotności i postępowania z ryzykiem ochrony danych osobowych przetwarzanych w ZDKiUM w celu zapewnienia zgodnego z Rozporządzeniem przetwarzania oraz dokumentowanie całego procesu zarządzania ryzykiem, spełniając tym samym wymóg rozliczalności podejmowanych działań.

§ 6

1. Na analizę ryzyka składa się: szacowanie ryzyka, postępowanie z ryzykiem oraz akceptowanie ryzyka.
2. Szacowanie ryzyka ma na celu określenie co może się zdarzyć oraz jak dotkliwe straty mogą powstać i polega na:

- identyfikowaniu zagrożeń;
- analizie ryzyka;
- ocenie ryzyka.

3. W ramach identyfikacji zagrożeń określany jest:

- kontekst;
- identyfikacja zasobów oraz ich istotność;
- identyfikacja zagrożeń dla zasobów;
- identyfikacja istniejących zabezpieczeń;
- identyfikacja podatności
- identyfikacja następstw – skutków.

4. Posiadając zidentyfikowane zasoby, zagrożenia oraz zastosowane zabezpieczenia można przeprowadzić identyfikację podatności na urzeczywistnienie się określonych zagrożeń. Istotne jest, że samo istnienie podatności nie powoduje jeszcze szkody. Jej powstanie jest możliwe dopiero po zaistnieniu zagrożenia, które wykorzysta daną podatność. Analiza

podatności dotyczy aktywów podstawowych – przetwarzanych danych i zastosowanych do przetwarzania urządzeń – jak i wspierających – sprzęt, oprogramowanie, sieć komputerowa, pracownicy, siedziba, organizacja.

5. Dokonanie analizy ryzyka polega na:
- oszacowaniu następstw ze szczególnym uwzględnieniem możliwości naruszenia praw lub wolności osób fizycznych;
- oszacowaniu prawdopodobieństwa incydentu;
- określeniu poziomu ryzyka.

8. Oceniając następstwa urzeczywistnienia się zagrożeń, w przypadku danych osobowych, należy uwzględnić – poza innymi czynnikami – także dotkliwe, przewidziane w RODO kary finansowe, które mogą być nakładane przez organ nadzorczy na administratora i podmioty przetwarzające w przypadku niewywiązywania się przez nie z nałożonych obowiązków właściwej ochrony danych. Szacowanie następstw dla określonych zagrożeń powinno uwzględniać zarówno materialny, jak i niematerialny charakter.
9. Przyjmuje się, że zasadniczym rodzajem reakcji na ryzyko jest działanie lub przeniesienie ryzyka. Przeniesienie oznacza przekazanie ryzyka podmiotowi zewnętrznemu, np. : powierzenie przetwarzania danych osobowych w drodze umowy przy zastosowaniu zasad zgodnych z RODO. Działanie może obejmować w szczególności ustanowienie nowych lub zintensyfikowanie istniejących mechanizmów kontroli, a także działania o innym charakterze (np. przeszkolenie pracowników, wprowadzenie zmian organizacyjnych, wystąpienie o dodatkowe środki finansowe, wprowadzenie dodatkowych wymogów informacyjnych, podjęcie lub nasilenie działań kontrolnych itp.).

§ 7

1. Proces szacowania ryzyka, przeprowadzony w sposób określony powyżej, kończy jego ocena i ustalenie planu postępowania z ryzykiem.
2. Coroczne szacowanie ryzyka należy przeprowadzić dla określonych zasobów. W zależności od zmiany realizowanych zadań, celu, sposobu przetwarzania oraz rodzaju danych zasoby te mogą ulegać zmianie lub obejmować inny zakres danych osobowych.

II. CZĘŚĆ SZCZEGÓŁOWA

§ 8

1. Każda komórka organizacyjna ZDKiUM, przeprowadza co najmniej raz na 12 miesięcy inwentaryzację zasobów i oszacowanie ryzyka dla własnych zasobów. Ponadto należy dokonywać przeglądów inwentaryzacji zasobów, biorąc pod uwagę zmiany:
   - w organizacji
   - w celach i procesach
   - zidentyfikowanych zagrożeń
   - skuteczności wdrożonych zabezpieczeń
   - zewnętrznych zdarzeń, takich jak zmiany prawa lub stosownych regulacji, zmiany wynikające z umów oraz zmiany o charakterze społecznym.

§ 9

1. Podczas szacowania ryzyka należy przeanalizować zagrożenia wraz z ich wewnętrznymi i zewnętrznymi uwarunkowaniami.
2. Określenie prawdopodobieństwa wystąpienia ryzyka polega na ocenie możliwości wystąpienia danego zdarzenia. Do określenia prawdopodobieństwa stosowana jest

następująca skala ocen: 1 – niskie, 2 – mało prawdopodobne, 3 – średnie, 4 – prawdopodobne, 5 – prawie pewne.

3. Określenie wpływu ryzyka polega na ocenie przewidywanego stopnia konsekwencji wystąpienia zagrożeń dla bezpieczeństwa danych osobowych w tym skutków dla osób fizycznych i podjęcia działań w celu ich zminimalizowania. Do określenia wpływu używana jest następująca skala ocen: 1 – nieznaczny, 2 – mały, 3 – średni, 4 – poważny, 5 – katastrofalny.
6. Zasady oceny wpływu ryzyka oraz prawdopodobieństwa jego wystąpienia określa **załącznik Nr 1 do Instrukcji.**
7. Na podstawie dokonanej oceny prawdopodobieństwa wystąpienia ryzyka oraz wpływu jego wystąpienia określa się poziom istotności danego ryzyka. Ustala się następujące możliwe poziomy istotności ryzyka:

- **ryzyko wysokie**, tj. ryzyko, dla którego iloczyn prawdopodobieństwa wystąpienia danego zdarzenia oraz jego wpływu wynosi 15–25 punktów;
- **ryzyko średnie**, tj. ryzyko, dla którego iloczyn prawdopodobieństwa wystąpienia danego zdarzenia oraz jego wpływu wynosi 8–12 punktów;
- **ryzyko niskie**, tj. ryzyko, dla którego iloczyn prawdopodobieństwa wystąpienia danego zdarzenia oraz jego wpływu wynosi 1–6 punktów.

8. Ryzykiem akceptowalnym jest ryzyko niskie. Ryzyko średnie i ryzyko wysokie przekracza akceptowalny poziom ryzyka. Ryzyko przekraczające akceptowalny poziom ryzyka wymaga określenia rodzaju reakcji na ryzyko – przeciwdziałania ryzyku.
9. W celu określenia rodzaju reakcji na ryzyko należy przeanalizować:

- przyczyny ryzyka i możliwe scenariusze rozwoju wydarzeń,
- skuteczność funkcjonujących mechanizmów kontroli.

10. Reakcja na ryzyko może obejmować:

- **działanie** – reakcje mające na celu wyeliminowanie danego ryzyka lub uwarunkowań z nim związanych w celu ochrony przed skutkami osób fizycznych;
- **łagodzenie** – zmniejszanie prawdopodobieństwa lub skutków niekorzystnego zdarzenia do akceptowalnego poziomu;
- **przeniesienie** – próba transferu skutków wystąpienia ryzyka na inny podmiot;
- **akceptację** – aktywną (stworzenie planu działań na wypadek wystąpienia ryzyka) lub bierną (niepodejmowanie żadnych działań do momentu wystąpienia ryzyka – dopuszczalna tylko wtedy, gdy nie ma możliwości ograniczenia ryzyka przez działanie, bądź koszty podjętych działań przekraczają możliwe do uzyskania korzyści).

11. W razie potrzeby można stosować kombinację rodzajów reakcji na ryzyko.

§ 10

1. Na podstawie dokonanej inwentaryzacji zasobów i szacowania ryzyka oraz po ustaleniu rodzaju reakcji na ryzyko, Kierownicy komórek organizacyjnych wypełniają Rejestr szacowania ryzyka ochrony danych osobowych. Wzór formularza rejestru określa **załącznik Nr 2 do Instrukcji.**
2. Rejestr szacowania ryzyka ochrony danych osobowych przekazuje się Inspektorowi Ochrony Danych do dnia 31 grudnia każdego roku.
3. Inspektor dokonuje analizy otrzymanych rejestrów szacowania ryzyka ochrony danych osobowych.
4. Inspektor na podstawie otrzymanych rejestrów szacowania ryzyka ochrony danych osobowych oraz przeprowadzonej analizy, sporządza Zbiorczy rejestr szacowania ryzyka ochrony danych osobowych przetwarzanych w ZDKiUM, który przedstawia Dyrektorowi ZDKiUM do 30 kwietnia każdego roku.

5. Zatwierdzony Zbiorczy rejestr szacowania ryzyka ochrony danych osobowych przetwarzanych w ZDKiUM wraz z aktualizacjami zostaje włączony do Dokumentacji ochrony danych.

§ 11

Na podstawie zatwierdzonego Zbiorczego rejestru szacowania ryzyka ochrony danych osobowych przetwarzanych w ZDKiUM, Kierownicy komórek organizacyjnych podejmują planowane działania w celu zmniejszenia ryzyka do akceptowalnego poziomu.

§ 12

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

§ 13

Kierownicy komórek organizacyjnych na bieżąco oceniają skuteczność działań podejmowanych w celu zmniejszenia ryzyka do akceptowalnego poziomu.

Załącznik nr 1 do Instrukcji w sprawie zasad i trybu zarządzania ryzykiem ochrony danych osobowych przetwarzanych w Zarządzie Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu

PRAWDOPODOBIEŃSTWO WYSTĄPIENIA RYZYKA

Prawdopodobieństwo wiąże się z niepewnością wystąpienia ewentualnego zdarzenia. Szacowanie prawdopodobieństwa jest kwestią subiektywnej oceny. Przy szacowaniu prawdopodobieństwa wystąpienia ryzyka uwzględnia się:
1) statystyki dotyczące podobnych zdarzeń;
2) atrakcyjność aktywu;
3) czynniki środowiskowe;
4) rodzaje podatności;
5) istniejące zabezpieczenia.
Oszacowanie prawdopodobieństwa wystąpienia danego ryzyka powinno nastąpić na podstawie jakościowo-ilościowej oceny, wg poniższej tabeli:

Prawdopodobieństwo wystąpienia ryzyka	Opis szczegółowy	Wartość punktowa prawdopodobieństwa
Niskie	Do tej pory takie zdarzenie nie wystąpiło w ZDKiUM lub może zaistnieć jedynie w wyjątkowych okolicznościach raz w roku	1
Mało prawdopodobne	Zdarzenie występuje co najmniej raz na pół roku	2
Średnie	Zdarzenie występuje co najmniej raz na kwartał	3
Prawdopodobne	Zdarzenie występuje co najmniej raz w miesiącu	4
Prawie pewne	Zdarzenie występuje co najmniej raz w tygodniu	5

WPŁYW(SKUTEK)WYSTĄPIENIA RYZYKA

Wpływ, czyli co się wydarzy w przypadku zmaterializowania ryzyka, związany jest z określeniem sytuacji po wystąpieniu ryzyka, a następnie określenie możliwych skutków zwłaszcza dla naruszenia praw lub wolności osób fizycznych. Określenia potencjalnych skutków wystąpienia danego ryzyka dokonuje się w oparciu o jakościowo – ilościową ocenę, wg poniższej tabeli:

Wpływ ryzyka	**Opis szczegółowy**	**Wartość punktowa skutków**
Nieznaczny	- rozwiązanie problemu będzie wymagało znikomego nakładu czasu i/lub zasobów, – znikomy wpływ na realizację celów i zadań, – możliwe jedynie krótkotrwałe zakłócenia w działalności ZDKiUM, – brak trwałej szkody, – brak skutków prawnych, – skutek finansowy w zakresie poniżej 5.000 zł, – brak wpływu na bezpieczeństwo pracowników, – brak wpływu na wizerunek jednostki, – brak naruszenia praw lub wolności osób fizycznych.	1
Mały	- rozwiązanie problemu będzie wymagało znikomego nakładu czasu i/lub zasobów, – mały wpływ na realizację celów i zadań, – możliwe jedynie niewielkie zakłócenia w działalności ZDKiUM, – brak trwałej szkody, – brak skutków prawnych, – skutek finansowy w zakresie 5.000-20.000 zł, – brak wpływu na bezpieczeństwo pracowników, – niewielki wpływ na wizerunek jednostki – negatywne opinie bez udziału mediów, – naruszenia praw lub wolności osób fizycznych przez niewielkie opóźnienie w realizacji praw wynikających z RODO.	2
Średni	- rozwiązanie problemu będzie wymagało umiarkowanego nakładu czasu i/lub zasobów, – średni wpływ na realizację celów i zadań, – umiarkowany poziom zakłóceń w działalności ZDKiUM, – usuniecie skutków będzie wymagało czasu, – umiarkowane konsekwencje prawne,	3

	– skutek finansowy w zakresie powyżej 20.000-50.000 zł, – brak wpływu na bezpieczeństwo pracowników, – średni wpływ na wizerunek jednostki – negatywne opinie w mediach lokalnych i regionalnych, – naruszenie praw lub wolności osób fizycznych przez opóźnienia w realizacji praw wynikających z RODO – umiarkowana skala	
Poważny	- rozwiązanie problemu będzie wymagało dużego nakładu czasu i/lub zasobów oraz podjęcia decyzji przez kierownictwo wyższego szczebla o sposobie wyjścia z zaistniałej sytuacji, – poważny wpływ na realizację zadania, w tym poważne zagrożenie terminu jego realizacji jak i osiągnięcia celu, – poważne zakłócenia w działalności ZDKiUM, – usunięcie skutków będzie bardzo trudne, – poważne konsekwencje prawne, – straty finansowe w zakresie powyżej 50.000-100.000 zł, – zagrożenie bezpieczeństwa pracowników, – zagrożenie bezpieczeństwa zasobów (np. utrata danych, nieuprawniony dostęp), – poważny wpływ na wizerunek jednostki – negatywne opinie w mediach krajowych, – naruszenie praw lub wolności osób fizycznych przez brak realizacji praw wynikających z RODO, – konsekwencje dla osób fizycznych (motyw 85 RODO) – umiarkowana skala.	4
Katastrofalny	- rozwiązanie problemu będzie wymagało dużego nakładu czasu i zasobów oraz podjęcia decyzji na poziomie strategicznym, – brak realizacji kluczowych zadań i celów, – paraliż działalności ZDKiUM, – skutki będą nieodwracalne, – bardzo poważne i rozległe konsekwencje prawne, – naruszenie bezpieczeństwa pracowników (ujemne konsekwencje dla ich życia i zdrowia), – straty finansowe w zakresie powyżej 100.000 zł, – utrata dobrego wizerunku jednostki w środowisku oraz w opinii publicznej – negatywne opinie w mediach międzynarodowych, – naruszenie praw lub wolności osób fizycznych przez brak realizacji praw wynikających z RODO, – konsekwencje dla osób fizycznych (motyw 85 RODO) – duża skala	5

ISTOTNOŚĆ RYZYKA

Określenie prawdopodobieństwa (P) i wpływu ryzyka (W) w pięciostopniowej skali, umożliwia ustalenie współczynnika istotności ryzyka (IR) – jako iloczynu (wyrażonych punktowo) prawdopodobieństwa wystąpienia ryzyka (P) oraz potencjalnego wpływu jego wystąpienia (W):

IR = P x W

gdzie:

IR – współczynnik istotności ryzyka
P – prawdopodobieństwo wystąpienia ryzyka
W – potencjalny wpływ ryzyka

Przyjęty dla obliczenia współczynnika istotności ryzyka wzór zakłada, że poziom zagrożenia w każdym wypadku zależy zarówno od prawdopodobieństwa wystąpienia ryzyka, jak i od wpływu jego wystąpienia. Wskazuje więc, że ryzyko bardzo prawdopodobne, ale wywołujące skutki niewielkie, wpływ może mieć podobny stopień istotności, jak ryzyko mało prawdopodobne, ale o poważnym przewidywanym wpływie.

Z uwagi na pięciostopniową skalę zarówno prawdopodobieństwa (P), jak wpływu wystąpienia ryzyka (W) współczynnik istotności danego ryzyka może przyjąć wartość od 1 do 25. Po przeprowadzonej analizie, wartości przyporządkowane, zarówno wpływowi jak i prawdopodobieństwu ryzyka, należy przenieść na mapę ryzyka. Mapę punktowej oceny istotności ryzyka „5x5", przedstawiono poniżej:

Wpływ						
Katastrofalny 1	5	10	15	20	25	
Poważny 2	4	8	12	16	20	
Średni 3	3	6	9	12	15	
Mały 4	2	4	6	8	10	
Nieznaczny 5	1	2	3	4	5	
	Niskie 1	**Mało prawdopodobne 2**	**Średnie 3**	**Prawdopodobne 4**	**Prawie pewne 5**	**Prawdopodobieństwo**

Wpływ	Prawdopodobieństwo	Istotność
1 - nieznaczny 2 - mały 3 - średni 4 - poważny 5 - katastrofalny	1 - Niskie 2 – Mało prawdopodobne 3 – Średnie 4 - Prawdopodobne 5 – Prawie pewne	niska - 1–6 średnia - 8–12 wysoka - 15–25

Ocena istotności ryzyka

Istotność ryzyka obliczona według wzoru umożliwia dokonanie oceny i hierarchizacji ryzyka.

Dla oceny istotności ryzyka stosuje się trzystopniową skalę obejmującą następujące poziomy:

- **WYSOKI** – jest to ryzyko o wartości 15–25, które istotnie wpływa na kluczową działalność jednostki, uniemożliwia realizację jej zadań i celów, rodzi straty finansowe,

- **ŚREDNI** – jest to ryzyko o wartości 8–12, które potencjalnie wpływa na kluczową działalność jednostki, jest zagrożeniem dla realizacji zadań i celów, zagraża powstaniem strat finansowych,

- **NISKI** – jest to ryzyko o wartości 1–6, które nie ma wpływu na kluczową działalność jednostki, nie uniemożliwia realizacji zadań i osiągania celów.

Istotność	Wartość punktowa	Przesłanki
Niska	1-6	Ryzyko możliwe do zaakceptowania. Akceptacja - ryzyko podlega minimalnemu monitorowaniu. Wartość ryzyka powinna zostać zweryfikowana dopiero przy następnej analizie lub gdy zmienią się warunki mające wpływ na podniesienie wartość ryzyka.
Średnia	8-12	Ryzyko nieakceptowane. Działanie ograniczające ryzyko do poziomu akceptowalnego. Należy rozważyć możliwość przeniesienia ryzyka na inny podmiot. Ryzyko wymaga monitorowania oraz zaplanowania i podjęcia działań prewencyjnych w określonym dłuższym okresie czasu(w zależności od możliwości np. w ciągu kwartału, półrocza czy roku), przy czym dopuszcza się akceptację ryzyka z tego przedziału, gdyby szacowane koszty niezbędnych działań przewyższały korzyści z ograniczenia ryzyka lub właściciel ryzyka podwyższył jego akceptowalny poziom. W sytuacji akceptacji takiego ryzyka właściciel ryzyka powinien monitorować ryzyko i okresowo rozważać potrzebę podjęcia działań ograniczających ryzyko.

Wysoka	15-25	Ryzyko nieakceptowane. Działanie niezwłoczne – ryzyko wymaga niezwłocznego podjęcia działań ograniczających ryzyko. Należy rozważyć możliwość przeniesienia ryzyka na inny podmiot lub jeśli jest to możliwe wycofania się z realizacji zadania powodującego ryzyko.

Załącznik nr 2 do Instrukcji w sprawie zasad i trybu zarządzania ryzykiem ochrony danych osobowych przetwarzanych w Zarządzie Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu

Analiza ryzyka w obszarze przetwarzania danych osobowych w komórce organizacyjnej .....

LP.	Właściciel zasobu (Dział/Zespół Samodzielne stanowisko)	Identyfikacja ryzyka							Analiza ryzyka			Zarządzanie ryzykiem	
		Nazwa zasobu	Forma	Miejsce przechowywania	Wartość/Istotność aktywów	Zagrożenia	P/I/D/R	Obecnie stosowane zabezpieczenia	Stopień zagrożenia / Prawdopodobieństwo wystąpienia zagrożenia	Poziom podatności / Wpływ/skutek wystąpienia ryzyka	Istotność ryzyka	Metoda przeciwdziałania ryzyku	Termin wdrożenia działań
1													
2													
3													
4													
5													
6													
7													
8													
9													
10													
11													
12													

Aktualne na dzień:

Sporządził:

.....
Kierownika komórki organizacyjnej

Załącznik nr 2 do Polityki ochrony danych
w Zarządzie Dróg, Komunikacji
i Utrzymania Miasta w Wałbrzychu

INSTRUKCJA W SPRAWIE WYPEŁNIANIA OBOWIĄZKU INFORMACYJNEGO ORAZ ZAPEWNIENIA REALIZACJI PRAW PODMIOTÓW DANYCH W ZARZĄDZIE DRÓG, KOMUNIKACJI I UTRZYMANIA MIASTA W WAŁBRZYCHU

§ 1

Postanowienia ogólne

1. Określenia użyte Instrukcji w sprawie wypełniania obowiązku informacyjnego oraz zapewnienia realizacji praw podmiotów danych w Zarządzie Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu zostały objaśnione w § 2 Polityki Ochrony Danych Osobowych w Zarządzie Dróg Komunikacji i Utrzymania Miasta w Wałbrzychu.
2. W przypadku gdy przetwarzanie odbywa się w celu wypełnienia obowiązku prawnego, któremu podlega administrator, lub jeżeli jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej, podstawę przetwarzania danych osobowych powinien stanowić przepis prawa.
3. W przypadku gdy przetwarzanie odbywa się w celu wykonania umowy, podstawę przetwarzania powinna stanowić umowa, której stroną jest osoba, której dane dotyczą, lub działania na żądanie osoby, której dane dotyczą, przed zawarciem umowy
4. W przypadku gdy podstawą przetwarzania danych osobowych jest zgoda osoby, której dane dotyczą Administrator powinien być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na operację przetwarzania.
5. Jeżeli osoba, której dane dotyczą, wyrażą zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
6. W oświadczeniu o wyrażeniu zgody należy wskazać przynajmniej tożsamość administratora oraz zamierzone cele przetwarzania danych osobowych.
7. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.

§ 2

Cel i zakres Polityki

1) Celem Polityki jest ustalenie sposobu realizacji przez Administratora obowiązków informacyjnych wobec osób których dane dotyczą oraz umożliwienia korzystania z przysługujących im praw.
2) Polityka określa zasady i procedury realizacji następujących praw osób, których dane dotyczą, w tym:

1) udzielenie informacji – spełnienie obowiązku informacyjnego;
2) zapewnienie dostępu do danych osobowych;
3) sprostowanie i uzupełnienie danych osobowych;
4) usunięcie danych osobowych („prawo do bycia zapomnianym");
5) ograniczenie przetwarzania danych osobowych;
6) sprzeciw;
7) przenoszenie danych;

§ 3

Zasady realizacji praw osób których dane dotyczą

1. Osobą odpowiedzialną za zapewnienie realizacji praw jest Inspektor. Do zadań Inspektora w tym zakresie należy w szczególności:
   1) przyjmowanie i zarządzanie żądaniami osób, których dane dotyczą,
   2) pomoc przy udzielaniu odpowiedzi na ww. żądania,
   3) koordynowanie i zapewnienie prawidłowości realizacji praw przez Administratora.
2. Żądanie osoby, której dane dotyczą, może zostać zgłoszone w formie ustnej w siedzibie Administratora, ul. Matejki 1, 58-300 Wałbrzych, pisemnie lub elektronicznie na adres iodo@zdkium.walbrzych.pl
3. Ilekroć osoba, której dane dotyczą, zgłosi Administratorowi żądanie realizacji danego prawa, w przypadku zaistnienia uzasadnionych wątpliwości w zakresie tożsamości tej osoby, Administrator uprawniony jest do żądania dodatkowych informacji od osoby, której dane dotyczą, w celu potwierdzenia jej tożsamości.
4. Administrator udziela odpowiedzi na każde zgłoszone żądanie realizacji prawa bez zbędnej zwłoki, jednakże nie później niż w terminie jednego miesiąca od dnia otrzymania danego żądania, z zastrzeżeniem ust. 7. Odpowiedzi udziela się w tej samej formie, w której żądanie zostało zgłoszone, chyba że osoba, której dane dotyczą, zażąda udzielenia odpowiedzi w innej formie.
5. W wyjątkowych sytuacjach, tj. z uwagi na skomplikowany charakter żądania lub liczbę żądań w danym okresie, Administrator jest uprawniony do przedłużenia terminu realizacji żądania o kolejne dwa miesiące. W takim przypadku informuje on o tym osobę, której dane dotyczą, nie później niż w terminie jednego miesiąca od dnia otrzymania żądania, z podaniem przyczyny przedłużenia.
6. W przypadku gdy żądanie jest oczywiście nieuzasadnione lub nadmierne, Administrator może odmówić działań lub pobrać za nie opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Administrator dokumentuje fakt, że żądanie ma oczywiście nieuzasadniony lub nadmierny charakter. W przypadku, o którym mowa w zdaniu pierwszym, Administrator informuje o tym osobę, której dane dotyczą, niezwłocznie, jednakże nie później niż w terminie jednego miesiąca od dnia otrzymania żądania, uzasadniając swoją decyzję oraz informując o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.
7. W przypadku gdy nie ma podstaw do realizacji żądania osoby, której dane dotyczą, Administrator informuje o tym osobę, której dane dotyczą, w terminie, o którym mowa w ust. 4 powyżej, wskazując powody niepodejmowania działań oraz informując o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.
8. Administrator informuje o sprostowaniu, uzupełnieniu, usunięciu lub ograniczeniu przetwarzania danych osobowych każdego odbiorcę, któremu ujawniono dane osobowe,

chyba że byłoby to niemożliwe lub wymagające niewspółmiernie dużego wysiłku. W przypadku zaistnienia któregokolwiek z tych wyjątków, Administrator sporządza notatkę ze stosownym uzasadnieniem.

§ 4

Udzielanie informacji w przypadku pozyskiwania danych bezpośrednio od osób, których dane dotyczą

1. W przypadku pozyskiwania danych osobowych bezpośrednio od osoby, której te dane dotyczą Administrator przekazuje osobie następujące informacje:
   1) swoją tożsamość i dane kontaktowe,
   2) dane kontaktowe inspektora ochrony danych,
   3) cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;
   4) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
   5) gdy ma to zastosowanie - informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi Rozporządzenia wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz informację o sposobach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia.
   6) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
   7) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
   8) jeżeli przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą - informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
   9) informacje o prawie wniesienia skargi do organu nadzorczego;
   10) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
   11) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz - przynajmniej w tych przypadkach - istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
2. Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 1 pkt. 6 - 11.
3. Administrator przekazuje informacje o których mowa w ust. 1 w zwięzłej, przejrzystej, zrozumiałej oraz łatwo dostępnej formie, a także jasnym i prostym językiem.
4. Administrator przekazuję informacje, o których mowa w ust. 1, podczas pozyskiwania danych osobowych poprzez:

1) wprowadzenie bezpośrednio do formularza wniosku składanego przez osobę fizyczną, umowy, lub w innych dokumentów do których osoba fizyczna wprowadza swoje dane osobowe,
2) załączenie do pisma kierowanego do osoby fizycznej,
3) umieszczenie na tablicach informacyjnych, w przestrzeni ogólnodostępnej dla osób fizycznych,
4) umieszczenie na stronie internetowej, Biuletynie Informacji Publicznej,
5) wprowadzenie do dokumentacji w sprawie zamówienia publicznego,

5. Ust. 1-5 nie mają zastosowania, gdy – i w zakresie, w jakim – osoba, której dane dotyczą, dysponuje już tymi informacjami.
6. Administrator wykonujący zadanie publiczne nie przekazuje informacji, o których mowa w ust. 2 jeżeli zmiana celu przetwarzania służy realizacji zadania publicznego i niewykonanie obowiązku, o którym mowa ust. 2 jest niezbędne dla realizacji celów, o których mowa w art. 23 ust. 1 Rozporządzenia oraz przekazanie tych informacji:
   1) uniemożliwi lub znacząco utrudni prawidłowe wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z realizacji tego zadania publicznego lub
   2) naruszy ochronę informacji niejawnych.
7. W przypadku, o którym mowa w ust. 6, Administrator zapewnia odpowiednie środki służące ochronie interesu lub podstawowych praw i wolności osoby, której dane dotyczą,
8. Administrator jest obowiązany poinformować osobę, której dane dotyczą, na jej wniosek, bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca od dnia otrzymania wniosku, o podstawie nieprzekazania informacji, o których mowa ust. 2.

§ 5

Udzielanie informacji w przypadku pozyskiwania danych w sposób inny niż bezpośrednio od osób, których dane dotyczą

1. W przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której te dane dotyczą Administrator przekazuje osobie następujące informacje:
   1) swoją tożsamość i dane kontaktowe,
   2) dane kontaktowe inspektora ochrony danych,
   3) cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;
   4) kategorie odnośnych danych osobowych;
   5) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
   6) gdy ma to zastosowanie - informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi Rozporządzenia wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz informację o sposobach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia.
   7) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
   8) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

9) jeżeli przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą - informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
10) informacje o prawie wniesienia skargi do organu nadzorczego;
11) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie - czy pochodzą one ze źródeł publicznie dostępnych;
12) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz - przynajmniej w tych przypadkach - istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

2. Informacje o których mowa w ust. 1 Administrator podaje:
   1) w rozsądnym terminie po pozyskaniu danych osobowych - najpóźniej w ciągu miesiąca - mając na uwadze konkretne okoliczności przetwarzania danych osobowych
   2) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą - najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub
   3) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy - najpóźniej przy ich pierwszym ujawnieniu.
3. Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 1 od pkt 7 -12.
4. Administrator przekazuje informacje o których mowa w ust. 1 w zwięzłej, przejrzystej, zrozumiałej oraz łatwo dostępnej formie, a także jasnym i prostym językiem.
5. Administrator przekazuję informacje, o których mowa w art 1 w możliwie najkrótszym terminie, nie dłuższym niż 30 (trzydzieści) dni od dnia pozyskania danych osobowych, z zastrzeżeniem następujących przypadków:
   1) jeżeli pozyskane dane osobowe mają służyć komunikacji z osobą, której dane dotyczą - informacje przekazywane są najpóźniej przy pierwszej komunikacji z tą osobą;
   2) jeżeli pozyskane dane osobowe mają być ujawnione innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.
6. Ust. 1-5 nie mają zastosowania, gdy – i w zakresie, w jakim:
   1) osoba, której dane dotyczą, dysponuje już tymi informacjami;
   2) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem zastosowania przez administratora odpowiednich warunków i zabezpieczeń, o których mowa w art. 89 ust.1 Rozporządzenia, lub o ile obowiązek, o którym mowa w ust. 1 niniejszego paragrafu, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie;
   3) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane w przepisach prawnych przewidującymi odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą; lub
   4) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w przepisach prawnych, w tym ustawowym obowiązkiem zachowania tajemnicy.

7. W zakresie nieuregulowanym w ust. 6 administrator wykonujący zadanie publiczne nie przekazuje informacji, o których mowa w ust. 1 i 3, jeżeli służy to realizacji zadania publicznego i niewykonanie obowiązku, o którym mowa w ust 1 i 3 jest niezbędne dla realizacji celów, o których mowa w art. 23 ust. 1 Rozporządzenia, oraz przekazanie tych informacji:
   1) uniemożliwi lub znacząco utrudni prawidłowe wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z realizacji tego zadania publicznego lub
   2) naruszy ochronę informacji niejawnych.
8. W przypadku, o którym mowa w ust. 7, administrator zapewnia odpowiednie środki służące ochronie interesu lub podstawowych praw i wolności osoby, której dane dotyczą.
9. Administrator jest obowiązany poinformować osobę, której dane dotyczą, na jej wniosek, bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca od dnia otrzymania wniosku, o podstawie nieprzekazania informacji, o których mowa w ust. 1 i 3.

§ 6

Zapewnienie dostępu do danych osobowych

1. Na wniosek osoby, której dane dotyczą, Administrator udostępnia dotyczące jej dane osobowe oraz przekazuje następujące informacje:
   1) cele przetwarzania;
   2) kategorie odnośnych danych osobowych;
   3) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
   4) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
   5) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
   6) informacje o prawie wniesienia skargi do organu nadzorczego;
   7) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą - wszelkie dostępne informacje o ich źródle;
   8) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 Rozporządzenia oraz - przynajmniej w tych przypadkach - istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
2. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w art. 46 Rozporządzenia związanych z przekazaniem.
3. Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się w powszechnie stosowanej formie elektronicznej.
4. Prawo do uzyskania kopii, o której mowa w ust. 3, nie może niekorzystnie wpływać na prawa i wolności innych.

5. Administrator wykonujący zadanie publiczne nie przekazuje informacji, o których mowa w ust. 1-3 jeżeli służy to realizacji zadania publicznego i niewykonanie obowiązków, o których mowa w ust. 1-3 jest niezbędne dla realizacji celów, o których mowa w art. 23 ust. 1 Rozporządzenia, oraz wykonanie tych obowiązków:
   1) uniemożliwi lub znacząco utrudni prawidłowe wykonanie zadania publicznego, a interes lub podstawowe prawa lub wolności osoby, której dane dotyczą, nie są nadrzędne w stosunku do interesu wynikającego z realizacji tego zadania publicznego lub
   2) naruszy ochronę informacji niejawnych.
6. W przypadku gdy wykonanie obowiązków, o których mowa w ust. 1 i 3 Rozporządzenia wymaga niewspółmiernie dużego wysiłku związanego z wyszukaniem danych osobowych, administrator wykonujący zadanie publiczne wzywa osobę, której dane dotyczą, do udzielenia informacji pozwalających na wyszukanie tych danych. Przepis art. 64 ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego stosuje się odpowiednio.
7. W przypadkach, o których mowa w ust. 1 i 2, administrator zapewnia odpowiednie środki służące ochronie interesu lub podstawowych praw i wolności osoby, której dane dotyczą.
8. Administrator jest obowiązany poinformować osobę, której dane dotyczą, na jej wniosek, bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca od dnia otrzymania wniosku, o podstawie niewykonania obowiązków, o których mowa w ust. 1-3.

§ 7

Sprostowanie i uzupełnienie danych osobowych

1. Administrator dokłada wszelkich starań aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.
2. Na wniosek osoby, której dane dotyczą Administrator ma obowiązek niezwłocznego sprostowania jej danych osobowych, które są nieprawidłowe.
3. Z uwzględnieniem celów przetwarzania, Administrator umożliwia osobie której dane dotyczą uzupełnienie niekompletnych danych osobowych poprzez przedstawienie dodatkowego oświadczenia.
4. Administrator informuje o sprostowaniu danych osobowych każdego odbiorcę, któremu ujawnił dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagało niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba tego zażąda.

§ 8

Usunięcie danych („prawo do bycia zapomnianym")

1. Na żądanie osoby, której dane dotyczą Administrator ma obowiązek bez, zbędnej zwłoki usunąć dotyczące jej dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:
   1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane
   2) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
   3) osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 Rozporządzenia wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 Rozporządzenia wobec przetwarzania;
   4) dane osobowe były przetwarzane niezgodnie z prawem;

5) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;
6) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1.Rozporządzenia,

2. Jeżeli administrator upublicznił dane osobowe, a na mocy ust. 1 ma obowiązek usunąć te dane osobowe, to - biorąc pod uwagę dostępną technologię i koszt realizacji - podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.
3. Administrator informuje o usunięciu danych osobowych każdego odbiorcę, któremu ujawnił dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagało niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba tego zażąda.
4. Ust. 1, 2 i 3 nie mają zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:
   1) do korzystania z prawa do wolności wypowiedzi i informacji;
   2) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy przepisów prawa któremu podlega Administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
   3) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3 Rozporządzenia.
   4) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 Rozporządzenia, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub
   5) do ustalenia, dochodzenia lub obrony roszczeń.

§ 9

Ograniczenie przetwarzania danych osobowych

1. Na żądanie osoby, której dane dotyczą Administrator ma obowiązek ograniczenia przetwarzania dotyczących jej danych osobowych, w następujących przypadkach:
   1) osoba której dane dotyczą, kwestionuje prawidłowość danych osobowych - na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;
   2) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
   3) administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
   4) osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 Rozporządzenia wobec przetwarzania - do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.
1. Jeżeli na mocy ust. 1 Administrator ograniczył przetwarzanie, takie dane osobowe może przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.
2. Przed uchyleniem ograniczenia przetwarzania Administrator informuje o tym osobę, której dane dotyczą, która żądała ograniczenia na mocy ust. 1.

3. Administrator informuje o ograniczeniu przetwarzania danych osobowych każdego odbiorcę, któremu ujawnił dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagało niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba tego zażąda.

§ 10

Przenoszenie danych

1. Administrator umożliwia osobie której dane dotyczą realizację prawa do przenoszenia danych, w tym: otrzymania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi, jeżeli:
   1) przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą lub na podstawie umowy, której stroną jest osoba której dane dotyczą oraz
   2) przetwarzanie odbywa się w sposób zautomatyzowany.
2. Wykonując prawo do przenoszenia danych na mocy ust. 1, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.
3. Wykonanie prawa, o którym mowa w ust. 1 niniejszego artykułu, pozostaje bez uszczerbku dla prawa do usunięcia danych. Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.
4. Prawo, o którym mowa w ust. 1, nie może niekorzystnie wpływać na prawa i wolności innych.

§ 11

Sprzeciw wobec przetwarzania danych

1. W przypadku przetwarzania danych osobowych opartego na art. 6 ust. 1 lit. e) lub f) Rozporządzenia (w tym profilowania) osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw - z przyczyn związanych z jej szczególną sytuacją - wobec przetwarzania dotyczących jej danych osobowych.
2. W przypadku wniesienia sprzeciwu, o którym mowa w ust. 1 Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.
3. Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie, o którym mowa w ust. 1, oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji.
4. Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 Rozporządzenia osoba, której dane dotyczą, ma prawo wnieść sprzeciw - z przyczyn związanych z jej szczególną sytuacją - wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

§ 12

Postanowienia końcowe

W celu zapewnienia właściwego wypełniania obowiązków informacyjnych wobec osób fizycznych oraz umożliwienia realizowania uprawnień tych osób, Kierownicy komórek organizacyjnych są zobowiązani do zapewnienia przestrzegania zapisów niniejszej Instrukcji przez podległych pracowników.

Załącznik nr **3** do Polityki ochrony danych
w Zarządzie Dróg, Komunikacji
i Utrzymania Miasta w Wałbrzychu

INSTRUKCJA W SPRAWIE POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH W ZARZĄDZIE DRÓG KOMUNIKACJI I UTRZYMANIA MIASTA W WAŁBRZYCHU

§ 1

Określenia użyte Instrukcji w sprawie postępowania w sytuacji naruszenia ochrony danych osobowych w Zarządzie Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu zostały objaśnione w § 2 Polityki Ochrony Danych Osobowych w Zarządzie Dróg Komunikacji i Utrzymania Miasta w Wałbrzychu.

§2

1. Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
2. Zdarzenia zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia ochrony danych osobowych zostały określone w rozdziale § 14 i 15 Polityki Ochrony Danych Osobowych w Zarządzie Dróg Komunikacji i Utrzymania Miasta w Wałbrzychu.

§ 3

1. W przypadku wystąpienia okoliczności wskazujących na możliwość naruszenia ochrony danych, o którym mowa w § 2 pracownicy ZDKiUM zobowiązani są do natychmiastowego reagowania w sposób określony w ust. 2 - 3.
2. W sytuacji wskazującej na naruszenie ochrony danych osobowych należy:
   1) zabezpieczyć dane osobowe przed dalszą podatnością na naruszenie;
   2) poinformować Inspektora ochrony danych oraz swojego bezpośredniego przełożonego;
   3) jeśli naruszenie dotyczy danych osobowych przetwarzanych w systemie informatycznym należy zgłosić ten fakt również Administratorowi systemu informatycznego.
3. Osoba stwierdzająca naruszenie zobowiązana jest do:
   1) zaniechania wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia osób, o których mowa w ust. 2
   2) podjęcia czynności zmierzających do zabezpieczenia miejsca zdarzenia, zabezpieczenia ewentualnych dowodów naruszenia i minimalizacji zaistniałych szkód.
4. W przypadku wystąpienia naruszenia Administrator powołuje Zespół ds. oceny skutków naruszenia w następującym składzie:
   1) Kierownik komórki organizacyjnej w której doszło do naruszenia ochrony danych osobowych

2) Inspektor ochrony danych
3) Administrator systemu informatycznego - jeśli naruszenie dotyczy danych osobowych przetwarzanych w Systemie informatycznym,

5. Zespół, o którym mowa w ust. 1 dokonuje oceny, czy naruszenie skutkuje lub może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych, a jeśli tak dokonuje oceny tego ryzyka.
6. Oceny ryzyka naruszenia praw lub wolności osób fizycznych Zespół dokonuje nie później niż w terminie 24 godzin od stwierdzenia naruszenia i przekazuje niniejszą ocenę Administratorowi.

§ 4

1. W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Urzędowi ochrony danych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, stwierdzonego na podstawie oceny przeprowadzonej przez Zespół o którym mowa w § 3 ust. 1. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
2. Zgłoszenie, o którym mowa w ust. 7, musi co najmniej:
   1) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
   2) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   3) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
   4) opisywać środki zastosowane lub proponowane przez Administratora w celu zapobiegania naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach - środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
3. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.
4. Administrator dokumentuje w Rejestrze wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz środki zastosowane w celu zminimalizowania jego negatywnych skutków.
5. Wzór Rejestru stanowi **załącznik nr 1** do niniejszej Instrukcji.

§ 5

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, stwierdzone na podstawie oceny przeprowadzonej przez Zespół o którym mowa w § 3 ust. 1, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
2. Zawiadomienie, o którym mowa w ust. 1 niniejszego paragrafu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w § 4 ust. 2 pkt 2 – 4.
3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:

1) Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
2) Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1
3) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Załącznik do Instrukcji w sprawie postępowania w sytuacji naruszenia ochrony danych osobowych w Zarządzie Dróg, Komunikacji i Utrzymania Miasta

Rejestr Naruszeń Ochrony Danych Osobowych w Zarządzie Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu

L.p.	Naruszenie (stypizowany opis naruszenia)	Data i godzina zgłoszenia podejrzenia naruszenia	Data oraz godzina stwierdzenia naruszenia	Data naruszenia/okres, którego dotyczy	Kategoria i ilość osób, których dotyczy naruszenie	Zakres danych i/lub kategorie danych, których dotyczy naruszenie	Osoba/ źródło informacji o zdarzeniu	Miejsce naruszenia	Okoliczności naruszenia - opis charakteru naruszenia, analiza zdarzenia, przyczyny wystąpienia	Opis skutków/konsekwencji naruszenia	Osoba/ jednostka odpowiedzialna za naruszenie	Podjęte działania - opis środków zastosowanych lub proponowanych do wdrożenia w celu zaradzenia naruszeniu, w tym środki zastosowane w celu zminimalizowania jego negatywnych skutków	Rezultat działań naprawczych	Osoba odpowiedzialna za wdrożenie działań naprawczych	Czy zachodzi obowiązek poinformowania Urzędu Ochrony Danych Osobowych (Jeśli tak - data i godzina zgłoszenia; w przypadku wystąpienia opóźnienia w powiadomieniu – wyjaśnienie przyczyn opóźnienia)	Czy poinformowano organy ścigania (data zawiadomienia)	Czy zachodzi obowiązek poinformowania osoby/osób, których naruszenie dotyczy oraz sposób przekazania informacji wraz opisem zaleceń dla podmiotów danych	Monitoring działań naprawczych
1.																	
2.																	
3.																	
4.																	
5.																	

Załącznik nr **4** do Polityki ochrony danych
w Zarządzie Dróg, Komunikacji
i Utrzymania Miasta w Wałbrzychu

WYKAZ BUDYNKÓW I POMIESZCZEŃ, W KTÓRYCH SĄ PRZETWARZANE, PRZECHOWYWANE ORAZ NISZCZONE DANE OSOBOWE:

Zarząd Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu zajmuje pomieszczenia zlokalizowane w .....

1. **Główny Specjalista ds. Inwestycji** zajmuje pomieszczenie/a nr ..... na..... piętrze. Dane osobowe przetwarzane są w systemie tradycyjnym i informatycznym. Dokumentacja zawierająca dane osobowe przechowywana jest: .....

2. **Dział Drogowy** zajmuje pomieszczenie/a nr ..... na..... piętrze. Dane osobowe przetwarzane są w systemie tradycyjnym i informatycznym. Dokumentacja zawierająca dane osobowe przechowywana jest: .....

3. **Dział Organizacji, Zarządzania i Kadr** zajmuje pomieszczenie/a nr ..... na..... piętrze. Dane osobowe przetwarzane są w systemie tradycyjnym i informatycznym. Dokumentacja zawierająca dane osobowe przechowywana jest: .....

4. **Zespół ds. Przetargów i Umów** zajmuje pomieszczenie/a nr ..... na..... piętrze. Dane osobowe przetwarzane są w systemie tradycyjnym i informatycznym. Dokumentacja zawierająca dane osobowe przechowywana jest: .....

5. **Zespól Radców Prawnych** zajmuje pomieszczenie/a nr ..... na..... piętrze. Dane osobowe przetwarzane są w systemie tradycyjnym i informatycznym. Dokumentacja zawierająca dane osobowe przechowywana jest: .....

6. **Główny Specjalista ds. Kontroli** zajmuje pomieszczenie/a nr ..... na..... piętrze. Dane osobowe przetwarzane są w systemie tradycyjnym i informatycznym. Dokumentacja zawierająca dane osobowe przechowywana jest: .....

7. **Inspektor Ochrony Danych** zajmuje pomieszczenie/a nr ..... na..... piętrze. Dane osobowe przetwarzane są w systemie tradycyjnym i informatycznym. Dokumentacja zawierająca dane osobowe przechowywana jest: .....

8. **Główny Specjalista ds. BHP i P.poż** zajmuje pomieszczenie/a nr ..... na..... piętrze. Dane osobowe przetwarzane są w systemie tradycyjnym i informatycznym. Dokumentacja zawierająca dane osobowe przechowywana jest: .....

9. **Dział Komunikacji Zbiorowej** zajmuje pomieszczenie/a nr ..... na..... piętrze. Dane osobowe przetwarzane są w systemie tradycyjnym i informatycznym. Dokumentacja zawierająca dane osobowe przechowywana jest: .....

10. **Dział Utrzymania Miasta** zajmuje pomieszczenie/a nr ..... na..... piętrze. Dane osobowe przetwarzane są w systemie tradycyjnym i informatycznym. Dokumentacja zawierająca dane osobowe przechowywana jest: .....

11. **Dział Finansowo-Księgowy** zajmuje pomieszczenie/a nr ..... na..... piętrze. Dane osobowe przetwarzane są w systemie tradycyjnym i informatycznym. Dokumentacja zawierająca dane osobowe przechowywana jest .....

12. **Serwerownia** zajmuje pomieszczenia /a nr pomieszczenie/a nr ..... na..... piętrze. Dane osobowe przetwarzane są w informatycznym. .....

13. **Pomieszczenia szaf krosowniczych** zajmują pomieszczenia /a nr pomieszczenie/a nr ..... na..... piętrze. Dane osobowe przetwarzane są w informatycznym. Zabezpieczenia .....

Załącznik nr 5 do Polityki ochrony danych w Zarządzie Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu

Rejestr czynności przetwarzania w Zarządzie Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu

Nazwa i dane kontaktowe administratora	
Nazwa	
Adres	
Email	
Telefon	
Dane kontaktowe Inspektora Ochrony Danych	
Email	
Telefon	

LP.	Nazwa czynności przetwarzania	Komórka organizacyjna	Cel przetwarzania	Kategorie osób	Kategorie danych	Podstawa prawna	Źródło danych	Planowany termin usunięcia kategorii danych *(jeżeli jest to możliwe)*	Nazwa współadministratora i dane kontaktowe *(jeśli dotyczy)*	Nazwa podmiotu przetwarzajacego i dane kontakowe *(jeśli dotyczy)*	Kategorie odbiorców *(innych niż podmiot przetwarzajacy)*	Nazwa systemu lub oprogramowania	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1 *(jeżeli jest to możliwe)*	DPIA (jeśli tak, lokalizacja raportu)	Transfer do kraju trzeciego lub org. międzynarodowej	
															Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń
			Art.. 30 ust. 1 pkt b	Art.. 30 ust. 1 pkt c	Art.. 30 ust. 1 pkt c			Art.. 30 ust. 1 pkt f	Art.. 30 ust. 1 pkt a	Art.. 30 ust. 1 pkt d	Art.. 30 ust. 1 pkt d		Art.. 30 ust. 1 pkt g		Art. 30 ust. 1 pkt e	Art. 30 ust. 1 pkt e
1																
2																
3																

Załącznik nr 6 do Polityki ochrony danych
w Zarządzie Dróg, Komunikacji
i Utrzymania Miasta w Wałbrzychu

UMOWA
O POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w dniu ..... w .....

pomiędzy:

.....

reprezentowaną przez:

_____

zwanym dalej **„Administratorem Danych"**

a

_____, wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd _____., nr KRS _____ REGON _____, NIP _____, reprezentowaną przez:

_____ na podstawie, zwaną dalej **„Podmiotem przetwarzającym"**,

łącznie zwane **„Stronami"**

§ 1
Powierzenie przetwarzania danych osobowych

1. W celu wykonania umowy Nr..... z dnia ..... (dalej – „Umowa") zawartej pomiędzy ....., Administrator Danych powierza Podmiotowi przetwarzającemu przetwarzanie danych osobowych w trybie art. 28 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", dalej „rozporządzenie",
2. Przetwarzanie danych przez Podmiot przetwarzający obejmuje dane osobowe ze zbiorów:
   1) .....
   2) .....
2. Podmiot przetwarzający jest uprawniony do wykonywania, w szczególności takich operacji na powyższych danych osobowych jak: .....
3. Przetwarzanie przez Podmiot przetwarzający powierzonych danych osobowych będzie trwało..... w okresie realizacji Umowy.
4. Podmiot przetwarzający zobowiązuje się do przetwarzania powierzonych danych osobowych wyłącznie w celu i zakresie oraz w sposób i przez czas określony w ust. 1 – 4.
5. Podmiot przetwarzający oświadcza, że nie będzie przetwarzał powierzonych danych osobowych

w państwie trzecim, tj. w państwie nienależącym do Europejskiego Obszaru Gospodarczego.

§ 2
Zasady przetwarzania powierzonych danych osobowych

1. Podmiot przetwarzający zobowiązuje się wykonać wszelkie czynności wynikające z niniejszej umowy o powierzenie przetwarzania danych osobowych i przepisów o ochronie danych osobowych z najwyższą starannością.
2. W przypadku wystąpienia zagrożeń mogących mieć wpływ na odpowiedzialność Administratora Danych za przetwarzanie powierzonych danych osobowych, Podmiot przetwarzający zobowiązuje się niezwłocznie podjąć działania w celu ich usunięcia oraz natychmiast zawiadomić o nich Administratora Danych.
3. Administrator Danych wyraża zgodę na ewentualne dalsze powierzenie przez Podmiot przetwarzający innemu podmiotowi przetwarzającemu przetwarzania danych osobowych. Może to nastąpić na podstawie pisemnej umowy, na mocy której zostaną nałożone te same obowiązki jak w niniejszej umowie o powierzenie przetwarzania danych osobowych. O zamiarze dalszego powierzenia Podmiot przetwarzający każdorazowo poinformuje Administratora Danych. W przypadku niewyrażenia przez Administratora Danych sprzeciwu w terminie 14 dni od dnia otrzymania informacji umowa może zostać zawarta. Po zawarciu umowy Podmiot przetwarzający jest zobowiązany poinformować o tym fakcie Administratora Danych podając dane podmiotu, któremu powierzył przetwarzanie danych. W przypadku nie wywiązania się przez inny podmiot przetwarzający ze spoczywających na nim obowiązków ochrony danych osobowych, pełną odpowiedzialność wobec Administratora Danych za ich wypełnienie ponosi przetwarzający.

§ 3
Zabezpieczenie powierzonych danych osobowych

1. Podmiot przetwarzający zapewnia, że wdroży odpowiednie środki techniczne i organizacyjne by przetwarzanie danych osobowych spełniało wymogi określone w obowiązujących przepisach prawa i chroniło prawa osób, których dane dotyczą.
2. Podmiot przetwarzający zobowiązuje się w szczególności do:
   1) przetwarzania danych wyłącznie na udokumentowane polecenie Administratora Danych; za udokumentowane polecenie uznaje się zadania nałożone na Podmiot przetwarzający w Umowie,
   2) podjęcia wszelkich środków aby zapewnić bezpieczeństwo przetwarzania danych osobowych zgodnie z wymogami nałożonymi na mocy art. 32 rozporządzenia,
   3) dopuszczenia do przetwarzania danych osobowych wyłącznie osób posiadających wydane przez niego upoważnienie i zapoznanych przez niego z przepisami o ochronie danych osobowych,
   4) zapewnienia aby osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania danych osobowych w tajemnicy,
   5) pomagania Administratorowi Danych poprzez odpowiednie środki techniczne i organizacyjne wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III a także z obowiązków określonych w art. 32-36 rozporządzenia,
   6) udostępniania Administratorowi Danych wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w art. 28 rozporządzenia,

7) prowadzenia rejestru kategorii czynności przetwarzania, o którym mowa w art. 30 ust. 2 rozporządzenia, jeżeli jest wymagane na mocy rozporządzenia.

3. Podmiot przetwarzający zobowiązuje się bez zbędnej zwłoki zgłosić Administratorowi Danych:
   1) stwierdzenie naruszenia ochrony danych osobowych, zawierające co najmniej informacje, o których mowa w art. 33 ust. 3 rozporządzenia,
   2) otrzymanie żądania od osoby, której dane przetwarza, w zakresie przetwarzania dotyczących jej danych osobowych,
   3) wszczęcie u Podmiotu przetwarzającego, przez organ właściwy ds. ochrony danych osobowych, kontroli sposobu przetwarzania powierzonych danych osobowych.

§ 4
Nadzór nad wykonaniem Umowy o powierzenie przetwarzania danych osobowych

1. Administrator Danych jest uprawniony do audytu wykonywania przez Podmiot przetwarzający obowiązków określonych w niniejszej Umowie o powierzenie przetwarzania danych osobowych.
2. Podmiot przetwarzający umożliwia Administratorowi Danych lub audytorowi upoważnionemu przez Administratora przeprowadzenie audytów, w tym inspekcji. W szczególności Podmiot przetwarzający:
   1) zapewni wstęp do pomieszczeń, w których Podmiot przetwarzający przetwarza powierzone dane osobowe,
   2) przekaże pisemne lub ustne wyjaśnienia w celu ustalenia stanu faktycznego,
   3) umożliwi przeprowadzenie oględzin dokumentów, a także urządzeń, nośników oraz systemów informatycznych służących do przetwarzania powierzonych danych.
2. Z czynności sporządza się protokół, którego jeden egzemplarz doręcza się kontrolowanemu.
3. W przypadku stwierdzenia uchybień w zakresie wykonywania niniejszej umowy o powierzenie przetwarzania danych osobowych lub przepisów o ochronie danych osobowych, Administratorowi Danych przysługuje prawo do żądania natychmiastowego wstrzymania przetwarzania danych osobowych i wyznaczenia Podmiotowi przetwarzającemu terminu na usunięcie uchybień.

§ 5
Odpowiedzialność Podmiotu przetwarzającego

Podmiot przetwarzający zobowiązuje się do naprawienia szkody wyrządzonej Administratorowi Danych w wyniku naruszenia danych osobowych z winy Podmiotu przetwarzającego. W szczególności zobowiązuje się do pokrycia kar zapłaconych przez Administratora Danych, poniesionych przez Administratora Danych, kosztów procesu i zastępstwa procesowego, a także odszkodowania na rzecz osoby, której naruszenie dotyczyło.

§ 6
Wygaśnięcie Umowy

1. Umowa o powierzenie wygasa z dniem wykonania, rozwiązania za wypowiedzeniem lub bez wypowiedzenia lub odstąpienia od Umowy, o której mowa w § 1 ust. 1 niniejszej umowy o powierzenie przetwarzania danych osobowych.
2. Po zakończeniu świadczenia usług związanych z przetwarzaniem danych osobowych Podmiot przetwarzający zobowiązuje się niezwłocznie, nie później niż w terminie 3 dni usunąć lub zwrócić Administratorowi Danych wszelkie dane osobowe oraz skutecznie

usunąć wszelkie istniejące kopie, chyba że przepisy prawa nakazują przechowywanie danych.
Z czynności usunięcia lub zwrotu należy sporządzić pisemny protokół. Powierzenie trwa do czasu wykonania tych czynności.

§ 7
Postanowienia końcowe

1. Wszelkie zmiany i uzupełnienia Umowy o powierzenie dokonywane będą w formie pisemnej pod rygorem nieważności.
2. W sprawach nieuregulowanych zastosowanie znajdują przepisy o ochronie danych osobowych.
3. W przypadku sporów wynikających z realizacji Umowy o powierzenie Strony poddają jej rozstrzygnięciu przez sąd właściwy ze względu na siedzibę Administratora Danych.
4. Niniejszą umowę sporządzono w .... jednobrzmiących egzemplarzach, ... dla Administratora Danych i ..... dla Podmiotu przetwarzającego.

ADMINISTRATOR DANYCH PODMIOT PRZETWARZAJĄCY

Załącznik nr 7 do Polityki ochrony danych
w Zarządzie Dróg, Komunikacji
i Utrzymania Miasta w Wałbrzychu

WYKAZ PODMIOTÓW ZEWNĘTRZNYCH

którym powierzono dane do przetwarzania
Wykaz firm /zleceniobiorców /wykonawców, z którymi realizacja umów/porozumień/zamówień zobowiązuje lub umożliwia dostęp do informacji zawierających dane osobowe

L.p.	Nazwa podmiotu	Zakres świadczonych usług	Numer/ data umowy	Uwagi (czy w umowie są zapisy dot. powierzenia przetwarzania danych osobowych czyt zawarto umowę powierzenia przetwarzania danych)
1.				
2.				

Załącznik nr **8** do Polityki ochrony danych
w Zarządzie Dróg, Komunikacji
i Utrzymania Miasta w Wałbrzychu

Wałbrzych, dnia 2018 r.

Nr. upoważnienia

Upoważnienie do przetwarzania danych osobowych

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1) i Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000).

upoważniam

Panią/Pana.....

zatrudniona/-y na stanowisku .....

do wykonywania następujących operacji na danych osobowych będących w dyspozycji Zarządu Dróg, Komunikacji i Utrzymania Miasta - Działu ....., zawartych w zbiorach:

Nazwa zbioru danych	Nazwa operacji przetwarzania													
	ZBIERANIE	UTRWALANIE	ORGANIZOWANIE	PORZĄDKOWANIE	PRZECHOWYWANIE	ADAPTOWANIE	MODYFIKOWANIE	POBIERANIE	PRZEGLĄDANIE	WYKORZYSTYWANIE	UJAWNIANIE - PRZESYŁANIE , ROZPOWSZECHNIANIE,UDOSTĘPNIANIE	DOPASOWYWANIE	ŁĄCZENIE	OGRANICZANIE	USUWANIE LUB NISZCZENIE

Upoważnienie jest udzielone do dnia .....

Załącznik nr 9 do Polityki ochrony danych
w Zarządzie Dróg, Komunikacji
i Utrzymania Miasta w Wałbrzychu

WNIOSEK
O NADANIE / ODEBRANIE/ ZMIANĘ* UPRAWNIEŃ W SYSTEMIE INFORMATYCZNYM

Nowy użytkownik	Modyfikacja uprawnień	Odebranie uprawnień w systemie informatycznym

Imię i nazwisko użytkownika oraz numer upoważnienia do przetwarzania danych:	**Wydział / Zespół/ Samodzielne stanowisko**

Opis i zakres uprawnień użytkownika w systemie informatycznym	
Data wystawienia:	Podpis bezpośredniego przełożonego użytkownika systemu:

Adnotacje Administratora Systemu Informatycznego	
Nadany identyfikator:	Uwagi:
Data nadania uprawnień	Podpis Administratora Systemu Informatycznego:

* niepotrzebne skreślić

Załącznik nr **10** do Polityki ochrony danych w Zarządzie Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu

Karta szkolenia wstępnego/okresowego z zakresu ochrony danych osobowych

Imię i nazwisko osoby odbywającej szkolenie:

.....

Stanowisko:

.....

W ramach szkoleniach poruszone zostały następujące tematy i zagadnienia:

Zasady przetwarzania i ochrony danych osobowych :

1. Dostęp do danych osobowych miały osoby posiadające upoważnienie do przetwarzania danych.
2. Każdy z pracowników powinien zachować szczególną ostrożność przy przenoszeniu danych.
3. Każdy z pracowników powinien chronić dane przed dostępem do nich osób nieupoważnionych.
4. Pomieszczenia, w których są przetwarzane dane osobowe, powinny być zamykane na klucz.
5. Dostęp do kluczy posiadają tylko upoważnieni pracownicy.
6. Dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy. W sytuacji, gdy jest wymagany poza godzinami pracy – możliwy jest tylko na podstawie zezwolenia administratora danych.
7. Dostęp do pomieszczeń, w których są przetwarzane dane osobowe, mogą mieć tylko upoważnieni pracownicy.
8. W przypadku pomieszczeń, do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności.
9. Szafy, w których przechowywane są dane, powinny być zamykane na klucz.
10. Klucze do tych szaf posiadają tylko upoważnieni pracownicy.
11. Szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych, a następnie powinny być zamykane.
12. Dane w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny do wykonania czynności służbowych, a następnie muszą być chowane do

szaf.

13. Dostęp do komputerów, na których są przetwarzane dane, mają tylko upoważnieni pracownicy.
14. Monitory komputerów, na których przetwarzane są dane, są tak ustawione, aby osoby nieupoważnione nie miały wglądu w dane.
15. W razie potrzeby wyniesienia komputera przenośnego (np. typu notebook) zawierającego dane osobowe lub inne informacje chronione, komputer taki musi być odpowiednio zabezpieczony, a dane zaszyfrowane. Nie należy udostępniać osobom nieupoważnionym komputerów przenośnych.
16. W razie potrzeby przeniesienia danych osobowych pomiędzy komputerami należy zrobić to z zachowaniem szczególnej ostrożności. Nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie), aby nie zostały na nich dane osobowe.
17. W przypadku wykorzystania do przenoszenia danych dysków, dane należy kasować z tych dysków.
18. Niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną.
19. Błędne lub nieaktualne wydruki i wersje papierowe zawierające dane osobowe lub inne informacje chronione niszczone są za pomocą niszczarki lub w inny mechaniczny sposób uniemożliwiający powtórne ich odtworzenie.

Odpowiedzialność

Za prawidłowe przetwarzanie danych oraz zapewnienie im odpowiedniej ochrony odpowiada każdy pracownik ZDKiUM, na swoim stanowisku pracy.

Naruszenie ochrony danych

1. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia danych osobowych to głównie:
   1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
   2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura,
   3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,

4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów, lub inny komunikat o podobnym znaczeniu,
5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
6) naruszenie lub próba naruszenia integralności systemu lub bazy danych,
7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
8) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie,
9) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń,
10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony informacji – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu itp.,
11) ujawniono istnienie nieautoryzowanych kont dostępu do danych,
12) podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane,
13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych itp.)

2. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych, tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.

Uwagi:

.....

.....

(data i podpis osoby, której udzielono instruktażu)

.....

(podpis Inspektora Ochrony Danych)

.....

(miejscowość, data)

Załącznik nr **11** do Polityki ochrony
danych w Zarządzie Dróg,
Komunikacji i Utrzymania Miasta w Wałbrzychu

.....
(imię i nazwisko pracownika)

.....
(Dział/Zespół/stanowisko)

OŚWIADCZENIE

Oświadczam, że zapoznałem się z treścią Polityki Ochrony Danych w Zarządzie Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu wprowadzoną Zarządzeniem nr .....Dyrektora Zarządu Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu z dnia .....

Jednocześnie oświadczam, że zobowiązuję się przestrzegać zasad ochrony danych osobowych obowiązujących w Zarządzie Dróg, Komunikacji i Utrzymania Miasta w Wałbrzychu podczas wykonywania obowiązków służbowych, w tym zobowiązuję się do:

- dołożenia wszelkich starań przy wykonywaniu powierzonych mi obowiązków w celu ochrony danych osobowych i informacji prawem chronionych,
- przetwarzania danych osobowych zgodnie z obowiązującymi w tym zakresie przepisami prawa i regulacjami wewnętrznymi,
- do zabezpieczenia przetwarzanych danych w tym: udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa, nieuprawnioną zmianą lub zniszczeniem, utratą, uszkodzeniem,
- zachowania w tajemnicy, w okresie zatrudnienia jak i po jego ustaniu, wszelkich informacji o danych osobowych uzyskanych w trakcie dokonywania operacji związanych z ich przetwarzaniem oraz informacji o ich zabezpieczeniu.

.....
(podpis osoby składającej oświadczenie)