BURMISTRZ
GMINY I MIASTA
Czerwionka-Leszczyny

ZARZĄDZENIE NR 218/24

BURMISTRZA GMINY I MIASTA CZERWIONKA-LESZCZYNY

z dnia 22 kwietnia 2024 r.

w sprawie wprowadzenia zmiany polityki ochrony danych osobowych w Urzędzie Gminy i Miasta Czerwionka-Leszczyny

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r .o samorządzie gminnym (t.j. Dz. U. z 2023 poz. 40 z późn. zm.) w związku z art. 24 ust 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2);

zarządzam, co następuje:

§1

Wprowadzić „Dokumentację ochrony danych osobowych" w Urzędzie Gminy i Miasta Czerwionka-Leszczyny, w brzmieniu stanowiącym załącznik do niniejszego zarządzenia.

§2

Uchyla się przepis ust. 1 w §1 Zarządzenia nr 203/18 Burmistrza Gminy i Miasta Czerwionka-Leszczyny z dnia 24 maja 2018 r. w sprawie „Polityki Ochrony Danych Osobowych" oraz „Instrukcji zarządzania Ochrony Danych Osobowych" w Urzędzie Gminy i Miasta Czerwionka-Leszczyny.

§3

Wykonanie Zarządzenia powierza się Sekretarzowi Gminy i Miasta Czerwionka-Leszczyny.

§4

Zarządzenie wchodzi w życie z dniem 6 maja 2024 r.

RADCA PRAWNY
mgr Aleksander Żukowski
Kl-2661

INSPEKTOR OCHRONY DANYCH
Wojciech Hoszek

Burmistrz
Gminy i Miasta
Czerwionka-Leszczyny
Wiesław Janiszewski

Załącznik
do Zarządzenia nr 218/24
Burmistrza Gminy i Miasta
Czerwionka-Leszczyny
z dnia 22 kwietnia 2024 r.

DOKUMENTACJA OCHRONY DANYCH OSOBOWYCH

Urząd

Gminy i Miasta

Czerwionka-Leszczyny

ul. Parkowa 9

44-230 Czerwionka-Leszczyny

Spis treści

1 Wstęp

Głównym celem wprowadzenia Systemu Ochrony Danych Osobowych jest zapewnienie przejrzystych zasad, rzetelności i zgodności z prawem procesów przetwarzania danych osobowych.

Wdrożenie Systemu Ochrony Danych Osobowych zgodnego z wymaganiami 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) jest wymogiem prawa.

Jednostka opracowała, wdrożyła, stosuje, monitoruje, przegląda, utrzymuje i doskonali udokumentowany System Ochrony Danych Osobowych w kontekście całościowych działań ustawowych w oparciu o przeprowadzoną i aktualizowaną ocenę ryzyk, które występują w jednostce. Całość podejmowanych działań oraz udokumentowanych polityk i procedur opisanych m.in. w niniejszej Dokumentacji stanowi **Politykę Bezpieczeństwa Danych Osobowych**.

Zasady bezpieczeństwa dotyczą wszystkich procesów związanych z przetwarzaniem danych osobowych realizowanych zarówno w formie tradycyjnej (papierowej) jak i elektronicznej.

Administrator, realizując zapisy niniejszej Dokumentacji, dokłada najwyższej staranności w celu ochrony praw lub wolności osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:

- przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość"),
- zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami („ograniczenie celu"),

- adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych"),
- prawidłowe i w razie potrzeby uaktualniane („prawidłowość"),
- przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane („ograniczenie przechowywania"),
- przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność"),
- przetwarzane w sposób umożliwiający wykazanie przestrzegania ustalonych zasad („rozliczalność").

W celu zapewnienia maksymalnej ochrony danych osobowych, wyznaczono obszary mające istotny wpływ na bezpieczeństwo zasobów Jednostki, są to:

- bezpieczeństwo osobowe,
- bezpieczeństwo systemów i sieci informatycznych,
- bezpieczeństwo danych osobowych gromadzonych w wersji papierowej i elektronicznej,
- bezpieczeństwo zarządzania dostępem do informacji,
- bezpieczeństwo fizyczne pomieszczeń, gdzie przetwarzane są dane osobowe.

W celu zachowania przejrzystości Dokumentacji w wielu miejscach występuje odwołanie do załączników, które stanowią integralną częścią niniejszej dokumentacji. Wszystkie odwołania wyróżniono kolorem zielonym.

2 Definicje

- **Adekwatność** – przetwarzanie danych osobowych w zakresie niezbędnym ze względu na cel zbierania danych;

- **Administrator** – Urząd Gminy i Miasta Czerwionka-Leszczyny z siedzibą przy ul. Parkowej 9, 44-230 Czerwionka-Leszczyny, REGON 000260741, NIP 6422480586, który zapewnia realizację obowiązków: Gminy i Miasta Czerwionka-Leszczyny z siedzibą przy ul. Parkowej 9, 44-230 Czerwionka-Leszczyny, Regon: 276258530, NIP: 642-000-97-26 oraz Burmistrza Gminy i Miasta Czerwionka-Leszczyny z siedzibą przy ul. Parkowej 9, 44-230 Czerwionka-Leszczyny, dalej zwany również Jednostką;
- **Administrator Systemu Informatycznego** (ASI) – osoba (firma) upoważniona przez Administratora do nadzoru i konserwacji systemu informatycznego;
- **Akceptowanie ryzyka** – decyzja, aby podjąć ryzyko;
- **Analiza ryzyka** – proces dążący do poznania charakteru oraz określenia poziomu ryzyka;
- **Apetyt na ryzyko** - poziom ryzyka akceptowalny przez Jednostkę;
- **Bezpieczeństwo informacji** – bezpieczeństwo polegające na zachowaniu poufności, integralności i dostępności informacji oraz innych właściwości, takich jak autentyczność, odpowiedzialność i wiarygodność;
- **Celowość** – dane osobowe mogą być przetwarzane tylko w tych celach, w których zostały zebrane;
- **Czynność przetwarzania** - kompletny proces przetwarzania danych osobowych określony celem przetwarzania danych osobowych,
- **Dane osobowe** – 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;

- **Dane biometryczne** – dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
- **Dane dotyczące zdrowia** – dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej, w tym o korzystaniu z usług opieki zdrowotnej, ujawniające informacje o stanie jej zdrowia;
- **Dane szczególnych kategorii** - dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby;
- **Dokumentacja** – niniejsza Dokumentacja Ochrony Danych Osobowych wraz z dokumentami powiązanymi;
- **Dokumenty powiązane** – wszystkie dokumenty, tj. wykazy, polityki, regulaminy, zasady użytkowania itp. stanowiące uzupełnienie i rozwinięcie zasad opisanych w niniejszym dokumencie;
- **Dostępność** - zapewnienie, by osoby upoważnione miały dostęp do informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne;
- **Hasło dostępu** – ciąg znaków, unikalnych dla każdego użytkownika eksploatującego sprzęt komputerowy oraz korzystającego z zasobów informatycznych przetwarzanych i gromadzonych na serwerze, stacji roboczej lub w programie sieci informatycznej;
- **Identyfikowanie ryzyka** - proces wyszukiwania, rozpoznawania i opisywania ryzyk;
- **Incydent związany z bezpieczeństwem informacji** – pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które mogą, z dużym prawdopodobieństwem, zagrażać operacjom związanym

z działalnością oraz stanowić zagrożenie dla bezpieczeństwa informacji;

- **Inspektor ochrony danych** (IOD) – osoba wyznaczona przez Administratora do nadzoru i koordynowania działań związanych z ochroną danych;
- **Integralność** – zapewnienie dokładności i kompletności informacji;
- **Kod dostępu** – zabezpieczenie urządzenia, np. mobilnego, za pomocą wzoru, kodu PIN lub innego narzędzia autoryzacyjnego w celu uwierzytelnienia użytkownika w systemie;
- **Kryteria ryzyka** - poziomy odniesienia, względem których określa się ważność ryzyka;
- **Login** (nazwa użytkownika) – ciąg znaków alfanumerycznych, unikalnych dla każdego użytkownika korzystającego z zasobów informatycznych przetwarzanych i gromadzonych na serwerze, stacji roboczej lub w sieci informatycznej;
- **Naruszenie ochrony danych osobowych** – 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;
- **Ocena ryzyka** – proces porównywania wyników analizy ryzyka z kryteriami ryzyka w celu stwierdzenia, czy ryzyko i/lub jego wielkość są akceptowalne lub tolerowane;
- **Odbiorca** – osoba fizyczna lub prawna, organ publiczny, jednostka 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;

- **Ograniczenie przetwarzania** – oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
- **Organ nadzorczy** - niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51 RODO;
- **Podmiot przetwarzający** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;
- **Postępowanie z ryzykiem** – proces modyfikowania ryzyka, wyboru i wdrażania działań mających na celu zmodyfikowanie ryzyka do poziomu mieszczącego się w Apetycie na ryzyko;
- **Poufność** – właściwość, że informacja nie jest dostępna ani ujawniana nieupoważnionym osobom, instytucjom lub procesom;
- **Pracownik** – osoba wykonująca polecenia Administratora na podstawie zawartej umowy, bez względu na rodzaj zawartej umowy, przez pracownika rozumiemy np.: pracownika wykonującego pracę na podstawie umowy o pracę, osobę wykonującą pracę na podstawie umowy cywilnoprawnej, praktykanta, stażystę, wolontariusza, zleceniobiorcę itp., pracownikiem nie jest Przedsiębiorca świadczący usługi na rzecz Administratora;
- **Przedsiębiorca** – osoba fizyczna lub prawna prowadząca działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą;
- **Przetwarzanie** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
- **Pseudonimizacja** – przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane

dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

- **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2);
- **Ryzyka** - wpływ niepewności na cele, możliwość wystąpienia dowolnego zdarzenia, które może prowadzić do naruszenia praw lub wolności osób, których dane Jednostka przetwarza. Ryzyko jest efektem materializacji zagrożenia przy wykorzystaniu podatności występujących dla poszczególnych Czynności przetwarzania;
- **Ryzyko szczątkowe** – ryzyko pozostające po zastosowaniu działań określonych w postępowaniu z ryzykiem;
- **Sieć informatyczna** – struktura składająca się z serwerów, stacji roboczych, osprzętu sieciowego, połączonych ze sobą za pomocą mediów transmisji w celu wymiany danych lub współdzielenia zasobów;
- **Strona trzecia** – osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, Administrator, podmiot przetwarzający czy osoby, które – z upoważnienia Administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;
- **Szacowanie ryzyka** – całościowy proces identyfikacji ryzyka, analizy ryzyka i oceny ryzyka;
- **System Zarządzania Bezpieczeństwem Informacji (SZBI)** - przyjęty przez Administratora zbiór procedur, polityk i instrukcji, którego celem jest zapewnienie odpowiedniego poziomu bezpieczeństwa informacji zgodnego ze zidentyfikowanymi

i oszacowanymi ryzykami, zakres SZBI określają odrębne przepisy i normy;

- **Szczególne kategorie danych** – dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne i dane biometryczne, przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej;
- **Usuwanie danych osobowych** – niszczenie danych osobowych lub taka ich modyfikacja, która nie pozwala na ustalenie tożsamości osoby, której dane dotyczą;
- **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
- **Użytkownik** – osoba obsługująca stanowisko komputerowe w zakresie udzielonych uprawnień;
- **Właściciel procesu** - Pracownik Jednostki odpowiedzialny za organizację i przebieg procesu Czynności przetwarzania;
- **Właściciel ryzyka** - osoba lub podmiot rozliczalna i uprawniona do zarządzania ryzykiem;
- **Zarządzanie ryzykiem** – skoordynowane działania w celu kierowania i kontroli organizacji z uwzględnieniem ryzyka;
- **Zbiór danych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
- **Zdarzenie związane z bezpieczeństwem informacji** – określone wystąpienie pewnego stanu systemu, usługi lub sieci wskazujące na prawdopodobne naruszenie polityki bezpieczeństwa informacji lub awarie zabezpieczeń, lub też wcześniej nieznanej sytuacji, która może być istotna ze względów bezpieczeństwa;
- **Zgoda osoby, której dane dotyczą** – 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 Zakres odpowiedzialności i obowiązków

3.1 Obowiązki i odpowiedzialność Administratora

Zważywszy na to, że o tym kto jest administratorem danych osobowych decyduje przede wszystkim rodzaj i charakter nadanych przez prawo kompetencji z obszaru spraw publicznych oraz wyznaczone ustawowo zadania w zakresie działalności jednostki samorządu terytorialnego, w ramach realizowanych zadań możemy wyróżnić kilku administratorów:

- Urząd Gminy i Miasta Czerwionka-Leszczyny z siedzibą przy ul. Parkowej 9, 44-230 Czerwionka-Leszczyny,
- Gmina i Miasto Czerwionka-Leszczyny z siedzibą przy ul. Parkowej 9, 44-230 Czerwionka-Leszczyny,
- Burmistrz Gminy i Miasta Czerwionka-Leszczyny z siedzibą przy ul. Parkowej 9, 44-230 Czerwionka-Leszczyny,

dla nich wszystkich zasady postępowania określa niniejsza Dokumentacja.

Administrator, uwzględniając charakter, zakres, kontekst i cele przetwarzania danych osobowych oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, wdraża odpowiednie środki organizacyjne i techniczne, aby przetwarzanie odbywało się zgodnie z prawem i aby móc to wykazać. Ponadto ustala cel i sposoby oraz zakres przetwarzanych danych osobowych pod kątem ich adekwatności, zapewnia kontrolę nad tym, jakie dane, kiedy i przez kogo zostały zgromadzone oraz komu i kiedy zostały przekazane (rozliczalność). W celu spełnienia tych wymogów Administrator wprowadza do użytku Polityki, Instrukcje, Procedury oraz inne dokumenty opisane w niniejszej Dokumentacji. Administrator odpowiada za zastosowanie adekwatnych środków technicznych zapewniających zdolność ciągłego zapewnienia

poufności, integralności, dostępności i odporności systemów przetwarzania danych osobowych.

Administrator wyznacza **I**nspektora **O**chrony **D**anych, który nadzoruje przestrzeganie zasad ochrony danych osobowych (zastosowanie odpowiednich środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych). Szczegółowy zakres IOD określono w punkcie 3.2.

Administrator wyznacza **A**dministratora **S**ystemów **I**nformatycznych, którego zadania zostały określone w punkcie 3.3. Jeśli ASI nie został wyznaczony na stałe, zakres jego obowiązków może być realizowany przez inne osoby lub podmioty jednak zawsze musi zostać zachowana zasada rozliczalności.

Ponadto Administrator:

- określa zakres uprawnień dostępu Pracownika do zasobów informacyjnych,
- wystawia upoważnienia do przetwarzania danych osobowych,
- kontroluje zgodność przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
- nadzoruje i aktualizuje dokumentację ochrony danych osobowych,
- nadzoruje przestrzeganie zasad ochrony danych osobowych,
- prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych,
- prowadzi ewidencję wszystkich dokumentów powiązanych z dokumentacją bezpieczeństwa danych osobowych,
- nadzoruje treść podpisywanych umów, szczególnie w przypadku przekazywania danych osobowych zleceniobiorcom,
- zabezpiecza dane osobowe przed dostępem osób nieupoważnionych,
- dokonuje analizy przyczyn i skutków sytuacji, które naruszyły bezpieczeństwo danych oraz przygotowuje aktualizacje dokumentacji w związku z wystąpieniem ww. sytuacji oraz nowych zagrożeń,
- zapewnia kontrolę nad tym jakie dane, kiedy i przez kogo zostały wprowadzone do systemu oraz komu zostały przekazane,

- odnotowuje w Rejestrze realizacji praw osób uprawnionych realizację praw osób, których dane dotyczą zrealizowanych na wniosek tych osób,
- w razie potrzeby dokonuje okresowej oceny skutków dla ochrony danych.

3.2 Obowiązki Inspektora Ochrony Danych

Do obowiązków IOD należy między innymi:

- udział we wszystkich pracach dotyczących ochrony danych osobowych,
- informowanie Administratora, podmiotów przetwarzających oraz Pracowników o ich obowiązkach w zakresie ochrony danych,
- monitorowanie przestrzegania przepisów oraz ustanowionych zasad dotyczących przetwarzania danych, w tym podziału obowiązków,
- monitorowanie podejmowanych działań w zakresie zwiększania świadomości osób upoważnionych do przetwarzania danych,
- udzielanie zaleceń co do oceny skutków dla ochrony danych,
- nadzorowanie realizacji oceny skutków dla ochrony danych,
- współpraca z organem nadzorczym,
- nadzór nad dokumentacją ochrony danych osobowych i jej aktualizacja,
- uwzględnianie w wykonywaniu swoich obowiązków charakteru, zakresu, kontekstu i celu przetwarzania,
- przygotowanie upoważnień do przetwarzania danych osobowych,
- prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
- prowadzenie rejestru czynności przetwarzania,
- prowadzenie rejestru kategorii czynności przetwarzania,
- opiniowanie projektów umów powierzenia przetwarzania danych osobowych,
- przeprowadzanie okresowych audytów zasad przetwarzania danych osobowych przez Pracowników,

- weryfikacja podmiotów przetwarzających pod kątem spełniania wymagań w zakresie ochrony danych osobowych,
- udział w projektach związanych z bezpieczeństwem informacji.

3.3 Obowiązki Administratora Systemu Informatycznego

Do obowiązków ASI należy między innymi:

- nadzorowanie przestrzegania zasad ochrony danych osobowych,
- sprawowanie nadzoru i koordynacja prac w zakresie eksploatacji, monitorowania i praw dostępu do zasobów informatycznych gromadzonych i przetwarzanych w systemie informatycznym,
- zabezpieczenie danych osobowych przed dostępem osób nieupoważnionych,
- prowadzenie ewidencji przydzielonych Użytkownikom loginów i praw dostępu,
- sprawowanie nadzoru nad wykonywaniem kopii bezpieczeństwa danych zgromadzonych w systemie informatycznym,
- analiza przyczyn i skutków sytuacji, które naruszyły bezpieczeństwo danych oraz przygotowanie aktualizacji dokumentacji w związku z pojawieniem się ww. sytuacji oraz nowych zagrożeń,
- właściwa konfiguracja systemu zapewniająca jego bezpieczeństwo,
- nadawanie Użytkownikom uprawnień do zasobów informatycznych zgodnie z dyspozycją Administratora,
- nadzór nad oprogramowaniem i sprzętem oraz bieżąca konserwacja i naprawy,
- regularne testowanie, mierzenie i ocena skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

3.4 Odpowiedzialność Pracowników

Do obowiązków Pracowników należy między innymi:

- przestrzeganie zapisów niniejszej Dokumentacji wraz z dokumentami powiązanymi,
- informowanie Administratora, IOD lub ASI o nienaturalnych sytuacjach w funkcjonowaniu systemu informatycznego,
- przekazywanie Administratorowi, IOD lub ASI sugestii i propozycji rozwiązań poprawiających poziom bezpieczeństwa przetwarzania danych osobowych,
- przetwarzanie danych wyłącznie na polecenie Administratora i w zakresie określonym w Upoważnieniu,
- w przypadku naruszenia zasad ochrony danych osobowych podjęcie bez zbędnej zwłoki działań zmierzających do ograniczenia skutków tego incydentu w oparciu o Procedurę postępowania z naruszeniami ochrony danych osobowych.

4.2 Dopuszczalne operacje na danych

Dane osobowe mogą być przetwarzane w ramach następujących operacji:

- **zbieranie** - wszelkie działania mające na celu uzyskanie danych osobowych bezpośrednio od osoby, której dane dotyczą (np. poprzez wypełnienie formularza elektronicznego), lub pośrednio (np. przez zakup bazy danych),
- **utrwalanie** - zapisanie danych osobowych na określonym nośniku, np. w pamięci komputera, na pendrivie, na papierze, na zdjęciu,
- **porządkowanie** - zbudowanie pewnej struktury z zebranych danych osobowych w oparciu o określone kryterium, np. kryterium alfabetyczne, kryterium wieku, kryterium płci etc.; wszelkie operacje, które służą usprawnieniu korzystania z uporządkowanych zbiorów

danych, np. ułatwienie wyszukiwania danych osobowych przez opatrywanie tagami,

- **przechowywanie** - wszelkie działania, które służą zachowaniu utrwalonych danych osobowych i pozwalają zapoznać się z danymi osobowymi w dowolnym momencie; dane osobowe mogą być przechowywane na wszelkich dostępnych nośnikach, w tym również w tzw. chmurach,
- **modyfikowanie**- zmiana treści danych osobowych, np. poprzez zmianę adresu, poprawienie błędnego imienia, dopasowanie treści danych osobowych do zmieniających się okoliczności, np. automatyczna zmiana wieku danej osoby w systemie w związku z upływem czasu,
- **pobieranie** - wykonanie kopii danych osobowych na jednym nośniku z innego nośnika, za pośrednictwem sieci telekomunikacyjnej; może to być np. pobranie danych osobowych z serwera na komputer osobisty,
- **przeglądanie** - zapoznawanie się z treścią danych osobowych jednej po drugiej,
- **wykorzystywanie** - użycie danych osobowych do założonego celu,
- **dopasowywanie** lub **łączenie** - czynność polegająca na sprawdzeniu, czy w dwóch różnych zbiorach znajdują się dane osobowe tej samej osoby i czy są one ze sobą spójne; scalanie danych osobowych jednej osoby, które są zamieszczone w różnych zbiorach, np. danych o aktywności w Internecie, jak również scalanie danych osobowych różnych osób pod względem określonego kryterium,
- **ograniczanie**, **usuwanie** - oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania; usunięcie treści danych z określonego nośnika bez niszczenia nośnika, czyli np. usunięcie adresu e-mail z bazy newslettera, skasowanie nagrania z kamery,
- **ujawnianie poprzez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnianie** - dowolna forma przekazania danych osobowych innej osobie, np. poprzez wysłanie pocztą, kurierem,

e-mailem, przez komunikator internetowy; zamieszczenie danych osobowych w miejscu publicznym, np. na ogólnie dostępnej stronie internetowej, do której ma dostęp nieograniczona liczba użytkowników; na forum internetowym.

4.3 Dopuszczenie do przetwarzania osób spoza Jednostki

Umowy umożliwiające dostęp podwykonawców lub kontrahentów do danych osobowych, w szczególności gdy dane zostają zabierane poza strefę bezpieczną, bazują na formalnych zapisach zawierających wszystkie istotne wymogi bezpieczeństwa. Generalną zasadą jest stosowanie klauzul poufności oraz ściśle określonych zasad dostępu do zasobów Jednostki. Jeśli jest to uzasadnione zasady przetwarzania danych osobowych powinny zostać określone w Umowie powierzenia przetwarzania danych osobowych. Umowy powierzenia przetwarzania danych osobowych są rejestrowane w Wykazie umów powierzenia.

Jeśli w zakresie wykonywanych prac zleconych nie dochodzi do przeniesienia danych osobowych poza systemy i sprzęt będące pod nadzorem Administratora oraz dane nie opuszczają stref bezpiecznych określonych w dokumencie Opis stref bezpiecznych, osoba wykonująca te prace może zostać dopuszczona do przetwarzania danych osobowych na zasadach określonych w punkcie 4.1.

4.4 Przetwarzanie danych osobowych na zlecenie innego administratora

Administrator jako Podmiot przetwarzający (Procesor) prowadzi rejestr kategorii czynności przetwarzania danych powierzonych przez przez innych administratorów. Rejestr kategorii czynności prowadzi Inspektor Ochrony Danych wg wzoru Rejestr kategorii czynności przetwarzania.

4.5 Klauzule poufności

Klauzule poufności, dotyczące bezpieczeństwa danych osobowych będących w posiadaniu Administratora, są stosowane we wszystkich umowach cywilno -prawnych zawieranych przez Jednostkę.

4.6 Postępowanie w sytuacji naruszenia bezpieczeństwa

W przypadku naruszenia zasad ochrony danych osobowych Administrator bez zbędnej zwłoki podejmuje działania zmierzające do oceny skutków tego naruszenia dla praw lub wolności osób fizycznych i postępuje zgodnie z Procedurą postępowania z naruszeniami ochrony danych osobowych.

4.7 Inwentaryzacja aktywów

Wszystkie ważne aktywa z punktu widzenia bezpieczeństwa informacji zostały zinwentaryzowane wg lokalizacji i właściciela. Księgi inwentarzowe są prowadzone przez z Wydział finansowo-budżetowy. Procesy przetwarzania danych osobowych zostały zidentyfikowane i opisane w dokumencie Rejestr czynności przetwarzania, którego wzór stanowi załącznik do Dokumentacji. Systemy informatyczne (programy, usługi) wykorzystywane w procesach przetwarzania danych osobowych zostały zinwentaryzowane w dokumencie Wykaz systemów informatycznych, którego wzór stanowi załącznik do Dokumentacji. Rejestr czynności przetwarzania oraz Wykaz systemów informatycznych są prowadzone i okresowo aktualizowane przez Inspektora Ochrony Danych. Wszystkie aktywa informacyjne oraz aktywa związane z przetwarzaniem informacji mają swoich właścicieli, tj. osoby lub komórki organizacyjne za nie odpowiedzialne. Zasady możliwego do zaakceptowania korzystania z aktywów informacyjnych i aktywów związanych z przetwarzaniem informacji są określone w dokumentach powiązanych z Dokumentacją.

4.8 Granica obszaru bezpiecznego

Szczegółowy wykaz lokalizacji, budynków i pomieszczeń wykorzystywanych do przetwarzania danych osobowych wraz z zastosowanymi zabezpieczeniami znajduje się w dokumencie Opis stref bezpiecznych.

Dostęp do pomieszczeń służących do przetwarzania danych osobowych podlega kontroli, a zasady dostępu do nich zostały określone w Polityce kluczy.

4.9 Rejestrowanie czynności przetwarzania

Szczegółowy rejestr czynności przetwarzania danych osobowych został opisany w załączniku Rejestr czynności przetwarzania.

4.10 Realizacja obowiązku informacyjnego

Podczas pozyskania danych lub pierwszego kontaktu z podmiotem danych Administrator przekazuje informacje niezbędne do wypełnienia obowiązku informacyjnego określonego w art 13 lub 14 RODO.

4.11 Realizacja praw osób, których dane dotyczących

Administrator realizuje prawa osób, których dane dotyczą, określone w artykułach 15-21 RODO na podstawie pisma złożonego do administratora. Przykładowe wzory pisma stanowią załączniki: Wniosek o sprostowanie danych, Wniosek o wykonanie czynności na danych oraz Sprzeciw wobec przetwarzania. Każde żądanie osoby, której dane dotyczą oraz związana z nim decyzja Administratora zostają odnotowane w Rejestrze realizacji praw osób uprawnionych.

4.12 Prawo do sprostowania danych

Osoba, której dane dotyczą, ma prawo żądania od Administratora niezwłocznego sprostowania swoich nieprawidłowych danych. Osoba, której

dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych (z uwzględnieniem celów przetwarzania), w tym poprzez przedstawienie dodatkowego oświadczenia. Żądanie zostaje wyrażone z chwilą złożenia Wniosku o sprostowanie danych.

4.13 Prawo dostępu przysługujące osobie, której dane dotyczą

Każda osoba jest uprawniona do uzyskania od Administratora informacji czy przetwarza jej dane osobowe. Jeżeli Administrator przetwarza dane osobowe osoby zwracającej się z zapytaniem, przysługuje jej prawo dostępu do tych danych. Informacje i dane są udostępniane osobie zainteresowanej na podstawie Wniosku o wykonanie czynności na danych.

4.14 Prawo do bycia zapomnianym

Każda osoba, której dane przetwarza Administrator, ma prawo żądania od Administratora niezwłocznego usunięcia jej danych, jeśli występują okoliczności określone w artykule 17 ust. 1 RODO. Prawo do bycia zapomnianym jest realizowane na podstawie Wniosku o wykonanie czynności na danych.

4.15 Ograniczenie przetwarzania

Osoba, której dane dotyczą, ma prawo żądać ograniczenia przetwarzania jej danych w następujących przypadkach:

- gdy kwestionuje prawidłowość tych danych, do czasu zweryfikowania danych przez Administratora;
- przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się ich usunięciu;
- Administrator nie potrzebuje już tych danych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
- osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie

Administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

Administrator wykonuje prawo do ograniczenia przetwarzania na podstawie Wniosku o wykonanie czynności na danych.

4.16 Prawo do przenoszenia danych

Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie, nadającym się do odczytu maszynowego, dane osobowe jej dotyczące, które dostarczyła Administratorowi, jeżeli:

a) przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO lub na podstawie umowy w myśl art. 6 ust. 1 lit. b) RODO; oraz

b) przetwarzanie odbywa się w sposób zautomatyzowany.

Wykonując prawo do przenoszenia danych osoba ma prawo żądania, by dane osobowe zostały przesłane przez Administratora bezpośrednio innemu Administratorowi, o ile jest to technicznie możliwe. Prawo to jest realizowane po złożeniu przez osobę zainteresowaną Wniosku o wykonanie czynności na danych.

4.17 Sprzeciw wobec przetwarzania

Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych; w związku z wykonywaniem zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi; w tym profilowania na podstawie ww. podstawy. 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. Sprzeciw wobec przetwarzania danych osobowych oraz jego rozstrzygnięcie Administrator realizuje na podstawie Sprzeciwu wobec przetwarzania.

4.18 Udostępnianie danych osobowych

1. Jednostka udostępnia dane osobowe odbiorcom tylko w uzasadnionych przypadkach i w oparciu o podstawę prawną.
2. Administrator prowadzi rejestr odbiorców, którym dane osobowe zostały udostępnione, dacie i zakresie udostępnienia oraz udostępniającym Pracowniku. Rejestr może być prowadzony w dowolnej formie umożliwiającej uzyskanie ww informacji, przykład rejestru stanowi załącznik Rejestr udostępnień.

4.19 Okres przechowywania danych osobowych

Administrator określa okres w jakim będzie przechowywał dane osobowe uwzględniając:

- cel w jakim dane zostały pozyskane,
- podstawę prawną pozyskania danych,
- kontekst, w jakim cel został określony,
- czas realizacji celu,
- ryzyko naruszenia dóbr i wolności osób, których dane podlegają przetwarzaniu,
- zakres przetwarzanych danych,
- adekwatność przetwarzanych danych.
- prawnie uzasadniony interes realizowany przez Administratora.

Okres retencji danych został ustalony na podstawie „Instrukcji archiwizacji" obowiązującej w Jednostce i podany w Rejestrze czynności przetwarzania. Zasady postępowania z danymi oraz okresowej weryfikacji czasu retencji określono w Procedurze retencji danych osobowych.

5 Ocena ryzyka przy przetwarzaniu

Ocena ryzyka ma na celu określenie ryzyka wynikającego z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych przesyłanych,

przechowywanych lub przetwarzanych w inny sposób. Analiza ryzyka powinna zostać przeprowadzona przed rozpoczęciem przetwarzania danych osobowych, po zmianach organizacyjnych w procesach przetwarzania danych osobowych, po zmianie kontekstu lub zmianach narzędzi służących do przetwarzania danych osobowych. Przeprowadza się okresowe przeglądy zasad postępowania z ryzykiem, nie rzadziej niż raz do roku. Szczegółowe zasady zastosowanej metody oceny i analizy ryzyka zostały opisane w Procedurze oceny ryzyka i postępowania z ryzykiem. Wynikiem przeprowadzonej oceny ryzyka jest Raport z oceny ryzyka, na podstawie którego Administrator podejmuje decyzję o dalszym postępowaniu ze zidentyfikowanymi i ocenionymi ryzykami. Ustalone dalsze czynności zostały określone w dokumencie Raport z oceny ryzyka i zatwierdzone przez Administratora.

6 Ocena skutków dla ochrony danych

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 lub wolności osób fizycznych, Administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Sposób dokonania oceny został zawarty w Instrukcji oceny skutków.

7 Wykaz dokumentów powiązanych

Wykaz dokumentów powiązanych z Dokumentacją:

1. Ewidencja osób upoważnionych do przetwarzania danych osobowych – WZÓR
2. Imienne upoważnienie do przetwarzania danych osobowych – WZÓR
3. Oświadczenie osoby upoważnionej – WZÓR

4. Instrukcja oceny skutków
5. Opis stref bezpiecznych
6. Polityka czystego biurka i czystego ekranu
7. Polityka kluczy
8. Upoważnienie do posiadania kluczy i kodów – WZÓR
9. Procedura oceny ryzyka i postępowania z ryzykiem
10. Zatwierdzenie wyników oceny ryzyka – WZÓR
11. Procedura postępowania z naruszeniami ochrony danych osobowych
12. Kalkulacja oceny ryzyka naruszenia - Wzór
13. Protokół z naruszenia ochrony danych osobowych - Wzór
14. Rejestr naruszeń – WZÓR
15. Rejestr czynności przetwarzania – WZÓR
16. Rejestr kategorii czynności przetwarzania – WZÓR
17. Rejestr udostępnień – WZÓR
18. Sprzeciw wobec przetwarzania – WZÓR
19. Wniosek o wykonanie czynności na danych – WZÓR
20. Wniosek o sprostowanie danych – WZÓR
21. Rejestr realizacji praw osób uprawnionych – WZÓR
22. Wykaz umów powierzenia – WZÓR
23. Umowa powierzenia przetwarzania danych osobowych – WZÓR
24. Wykaz systemów informatycznych – WZÓR

Burmistrz
Gminy i Miasta
Czerwionka-Leszczyny
Wiesław Janiszewski

.....
(data i podpis Administratora)

Załączniki do Dokumentacji Ochrony Danych Osobowych stanowiącej załącznik do Zarządzenia nr 218/24 Burmistrza Gminy i Miasta Czerwionka-Leszczyny z dnia 22 kwietnia 2024 r.

WYKAZ DOKUMENTÓW POWIĄZANYCH

Nr załącznika	Nazwa dokumentu
1.	Ewidencja osób upoważnionych do przetwarzania danych osobowych – **WZÓR**
2.	Imienne upoważnienie do przetwarzania danych osobowych – **WZÓR**
3.	Oświadczenie osoby upoważnionej – **WZÓR**
4.	Instrukcja oceny skutków
5.	Opis stref bezpiecznych
6.	Polityka czystego biurka i czystego ekranu
7.	Polityka kluczy
8.	Upoważnienie do posiadania kluczy i kodów – **WZÓR**
9.	Procedura oceny ryzyka i postępowania z ryzykiem
10.	Zatwierdzenie wyników oceny ryzyka – **WZÓR**
11.	Procedura postępowania z naruszeniami ochrony danych osobowych
12.	Kalkulacja oceny ryzyka naruszenia - **Wzór**
13.	Protokół z naruszenia ochrony danych osobowych - **Wzór**
14.	Rejestr naruszeń – **WZÓR**
15.	Rejestr czynności przetwarzania – **WZÓR**
16.	Rejestr kategorii czynności przetwarzania – **WZÓR**
17.	Rejestr udostępnień – **WZÓR**
18.	Sprzeciw wobec przetwarzania – **WZÓR**
19.	Wniosek o wykonanie czynności na danych – **WZÓR**
20.	Wniosek o sprostowanie danych – **WZÓR**
21.	Rejestr realizacji praw osób uprawnionych – **WZÓR**
22.	Wykaz umów powierzenia – **WZÓR**
23.	Umowa powierzenia przetwarzania danych osobowych – **WZÓR**
24.	Wykaz systemów informatycznych – **WZÓR**

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Imię i nazwisko osoby upoważnionej	Komórka organizacyjna	Stanowisko	Nr imiennego upoważnienia	Czynności przetwarzania danych	Data nadania uprawnień	Uprawnienia w systemach IT [tak/nie]	Data odebrania uprawnień *(zwolnienia)*	Uwagi
1.									
2.									
3.									
4.									
5.									
6.									
7.									
8.									
9.									
10.									

Załącznik nr 2 do Dokumentacji Ochrony Danych Osobowych stanowiącej załącznik do Zarządzenia nr 218/24 Burmistrza Gminy i Miasta Czerwionka-Leszczyny z dnia 22 kwietnia 2024 r.

IMIENNE UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Upoważnienie

nr ../202..

Na podstawie Art. 29 i 32 ust. 4 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)

Upoważniam:

Pani/Pan:	
Wydział:	
Stanowisko:	
Upoważnienie do przetwarzania danych w systemach informatycznych	☐ Tak ☐ Nie
do przetwarzania danych osobowych w związku z wykonywaniem powierzonych obowiązków służbowych.	
Upoważnienie obejmuje następujące czynności przetwarzania danych:	
Dopuszczalne operacje na danych:	
☐ zbieranie, utrwalanie ☐ porządkowanie ☐ dopasowywanie lub łączenie ☐ wykorzystywanie	☐ modyfikowanie ☐ przeglądanie ☐ pobieranie ☐ ograniczanie, usuwanie lub niszczenie
☐ ujawnianie poprzez przesyłanie, rozpowszechnianie lub innego rodzaju udostępnianie	

Niniejsze upoważnienie obejmuje przetwarzanie danych osobowych w dowolnej formie (kartoteki, ewidencje, rejestry, spisy, dane w formie elektronicznej itp.).

Niniejsze upoważnienie traci moc najpóźniej z dniem odwołania albo rozwiązania lub wygaśnięcia umowy o pracę lub innej podstawy prawnej współpracy pomiędzy osobą upoważnioną a Administratorem. W przypadku posiadania wcześniej wydanych upoważnień niniejsze upoważnienie odwołuje wszystkie uprzednio wydane upoważnienia.

Jednocześnie zobowiązuję Panią/a do zachowania w tajemnicy przetwarzanych danych osobowych oraz sposobu ich zabezpieczenia w trakcie trwania upoważnienia oraz po jego wygaśnięciu.

Czerwionka-Leszczyny, ...
(miejscowość i data)

.....
(podpis Administratora)

Zapoznałem/am się z treścią upoważnienia i przyjmuję je bez zastrzeżeń.

.....
(data i podpis os. upoważnionej)

Sporządził:

Załącznik nr 3 do Dokumentacji Ochrony Danych Osobowych stanowiącej załącznik do Zarządzenia nr 218/24 Burmistrza Gminy i Miasta Czerwionka-Leszczyny z dnia 22 kwietnia 2024 r.

OŚWIADCZENIE OSOBY UPOWAŻNIONEJ

Oświadczam, że zapoznałam/em się z przepisami dotyczącymi ochrony danych osobowych i zobowiązuję się do przestrzegania:

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);
2. Dokumentacji Ochrony Danych Osobowych.

Jednocześnie zobowiązuję się do:

1. Zapewnienia ochrony danym osobowym przetwarzanym w zbiorach Administratora, zabezpieczenia przed udostępnianiem osobom trzecim i nieuprawnionym, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem.
2. Po ustaniu stosunku pracy / współpracy zachowania w tajemnicy przez okres 10 lat wszelkich informacji pozyskanych w trakcie pracy / współpracy u Administratora.
3. W momencie ustania stosunku pracy / współpracy zwrócenia lub zniszczenia/skasowania wszelkich posiadanych kopii i rejestrów danych osobowych udostępnionych przez Administratora.

.....
Imię i nazwisko

.....
(data i podpis os. upoważnionej)

INSTRUKCJA OCENY SKUTKÓW DLA OCHRONY DANCYH

1. 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 lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.
2. Dokonując oceny skutków dla ochrony danych, administrator konsultuje się z inspektorem ochrony danych, jeżeli został on wyznaczony.
3. Raport z oceny skutków dla ochrony danych zawiera co najmniej:
   - systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
   - ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
   - ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w punkcie 1; oraz
   - środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.
4. Oceniając – w szczególności do celów oceny skutków dla ochrony danych – skutki operacji przetwarzania wykonywanych przez administratora lub podmiot przetwarzający, uwzględnia się przestrzeganie przez takiego administratora lub taki podmiot przetwarzający zatwierdzonych kodeksów postępowania.
5. W stosownych przypadkach administrator zasięga opinii osób, których dane dotyczą, lub ich przedstawicieli w sprawie zamierzonego przetwarzania, bez uszczerbku dla ochrony interesów handlowych lub publicznych lub bezpieczeństwa operacji przetwarzania.
6. W razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z operacji przetwarzania, administrator dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych.

Burmistrz
Gminy i Miasta
Czerwionka-Leszczyny
Wiesław Janiszewski

.....

(data i podpis Administratora)

Załącznik nr 8 do Dokumentacji Ochrony Danych Osobowych stanowiącej załącznik do Zarządzenia nr 218/24 Burmistrza Gminy i Miasta Czerwionka-Leszczyny z dnia 22 kwietnia 2024 r.

UPOWAŻNIENIE DO POSIADANIA KLUCZY I KODÓW

Nr upoważnienia ..../202...

Powierzam Pani/Panu .....

zatrudnionej/mu na stanowisku .....

komplet kluczy, w skład którego wchodzą klucze do następujących budynków/pomieszczeń:

1. .....
2. .....
3. .....
4. .....
5. .....

☐ Ponadto przydzielam Pani/Panu kod cyfrowy do systemu alarmowego, który należy zachować w ścisłej tajemnicy i wykorzystywać zgodnie z przeznaczeniem.

Upoważnienie nadaje się na czas zatrudnienia na zajmowanym stanowisku lub do odwołania.

Czerwionka-Leszczyny,.....
(data)

.....
(podpis Administratora)

Oświadczenie pracownika

Oświadczam, że przyjmuję pełną odpowiedzialność za powierzone:

TAK* / NIE* – klucze

TAK* / NIE* – kod cyfrowy do systemu alarmowego

i zobowiązuję się do ich wykorzystywania jedynie w celach realizacji powierzonych mi zadań.

.....
(data i podpis pracownika)

** niepotrzebne skreślić*

Załącznik nr 10 do Dokumentacji Ochrony Danych Osobowych stanowiącej załącznik
do Zarządzenia nr 218/24 Burmistrza Gminy i Miasta Czerwionka-Leszczyny z dnia 22 kwietnia 2024 r.

ZATWIERDZENIE WYNIKÓW OCENY RYZYKA

Zatwierdzam wyniki przeprowadzonej oceny ryzyka wraz z planem postępowania z ryzykiem zawarte w pliku „Raport z oceny ryzyka i postępowanie z ryzykiem".

Lp.	Data przeprowadzenia oceny ryzyka	Osoba nadzorująca wykonanie oceny	Podpis Administratora
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

Załącznik nr 12 do Dokumentacji Ochrony Danych Osobowych stanowiącej załącznik do Zarządzenia nr 218/24
Burmistrza Gminy i Miasta Czerwionka-Leszczyny z dnia 22 kwietnia 2024 r.

KALKULACJA OCENY RYZYKA NARUSZENIA

LP.	KRYTERIUM		OCENA	UZASADNIENIE
1.	**Charakter i wrażliwość danych** **należy określić, czy dane osobowe, których dotyczy naruszenie mają szczególne znaczenie dla osoby, której dane dotyczą, a ich ujawnienie niesie za sobą poważne konsekwencje* ** np.: dane związane z życiem zawodowym (mniej wrażliwe), dane związane z życiem prywatnym (bardziej wrażliwe), EROD: "ujawnienie imienia i nazwiska oraz adresu danej osoby prawdopodobnie nie wyrządzi jej szkody w normalnej sytuacji. Jednak jeżeli imię i nazwisko oraz adres rodzica adopcyjnego zostaną ujawnione rodzicowi biologicznemu, może mieć to bardzo poważne konsekwencje zarówno dla rodzica adopcyjnego, jak i dziecka"*			
2.	**Rodzaj danych** **należy ocenić rodzaj danych osobowych, których dotyczy naruszenie, także w kontekście kategorii danych osobowych*	dane zwykłe		
		szczególne kategorie danych osobowych		
		dane dotyczące wyroków skazujących i czynów zabronionych		
3.	**Łatwość identyfikacji osoby** **należy ocenić czy osoba / podmiot, który wszedł w posiadanie danych osobowych będzie w stanie dokonać identyfikacji osoby, której dane dotyczą*			
4.	**Konsekwencje** **należy zidentyfikować jakie są konsekwencje naruszenia dla osoby, której dane dotyczą*	Utrata kontroli nad własnymi danymi osobowymi		
		Ograniczenie możliwości realizowania praw z art. 15-22 RODO		
		Ograniczenie możliwości realizowania praw		
		Dyskryminacja		
		Kradzież lub sfałszowanie tożsamości		
		Strata finansowa		
		Naruszenie dobrego imienia		
		Utrata poufności danych osobowych chronionych tajemnicą zawodową		
		Nieuprawnione odwrócenie pseudonimizacji		
		Niemożliwość świadczenia usługi / realizacji umowy		
		inne **jeżeli występują konsekwencje inne niż wskazane powyżej, należy je dodatkowo zidentyfikować*		
		inne **jeżeli występują konsekwencje inne niż wskazane powyżej, należy je dodatkowo zidentyfikować*		
		inne **jeżeli występują konsekwencje inne niż wskazane powyżej, należy je dodatkowo zidentyfikować*		
		inne **jeżeli występują konsekwencje inne niż wskazane powyżej, należy je dodatkowo zidentyfikować*		
		inne **jeżeli występują konsekwencje inne niż wskazane powyżej, należy je dodatkowo zidentyfikować*		
		inne **jeżeli występują konsekwencje inne niż wskazane powyżej, należy je dodatkowo zidentyfikować*		
5.	**Podmiot niezaufany** ** należy określić czy podmiot, który uzyskał / mógł uzyskać dostęp do danych osobowych jest podmiotem niezaufanym (tj. innym niż zaufany)* **podmiot zaufany to taki, z którym Administrator Danych pozostaje w stałych stosunkach, może znać stosowane u niego procedury, historię, inne szczegóły go dotyczące np. podmiot przetwarzający, z którym mamy podpisaną umowę powierzenia przetwarzania danych osobowych*			
6.	**Cechy szczególne osoby** **należy wziąć pod uwagę czy osoby, których danych osobowych dotyczy naruszenie należą do grup osób wymagających szczególnej opieki i / lub można stwierdzić brak równowagi między stanowiskiem osoby, której dane dotyczą, a stanowiskiem Administratora Danych*	osoby starsze (pow. 60 r.ż.)		

		dzieci (pon. 16 r.ż.)		
		osoby niepełnosprawne		
		inne *jeżeli występują grupy inne niż wskazane powyżej, należy je dodatkowo zidentyfikować		
		inne *jeżeli występują grupy inne niż wskazane powyżej, należy je dodatkowo zidentyfikować		
		inne *jeżeli występują grupy inne niż wskazane powyżej, należy je dodatkowo zidentyfikować		
7.	**Brak publicznej dostępności danych** *należy określić czy dane osobowe, których dotyczy naruszenie nie są dostępne w ogólnodostępnych źródłach informacji np. CEIDG, portale społecznościowe, KRS, strony internetowe			
8.	**Aktualność danych** *należy określić czy dane osobowe, których dotyczy naruszenie są aktualne oraz poprawne merytorycznie			

WYNIK KALKULACJI

*niezależnie od wyniku kalkulacji, końcowa ocena naruszenia może się od niego różnić ze względu na dodatkowe czynniki (podnoszące lub obniżające ryzyko) brane pod uwagę przy ustalaniu oceny końcowej naruszenia stanowiącej część Protokołu z naruszenia ochrony danych osobowych

Brak ryzyka (do 19%)
Ryzyko (20%-49%)
Ryzyko wysokie (50%-100%)

#DZIEL/0!	#DZIEL/0!

PROTOKÓŁ Z NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Protokół nr . . . . .

Inspektor Ochrony Danych	
Osoba zgłaszająca naruszenie (imię, nazwisko, stanowisko)	
Osoby prowadzące czynności sprawdzające (imiona, nazwiska, stanowiska)	
Osoby udzielające informacji na temat naruszenia (imiona, nazwiska, stanowiska)	
Informacje na temat naruszenia ujawnione w toku czynności sprawdzających:	

Data i miejsce naruszenia	

Kategorie osób, których danych dotyczy naruszenie

☐ potencjalnych pracowników
☐ pracowników / współpracowników
☐ klientów
☐ kontrahentów
☐ innych osób (należy określić jakie to osoby): ...

Kategorie danych osobowych, których dotyczy naruszenie

Dane osobowe zwykłe

☐ imię
☐ nazwisko
☐ numer telefonu
☐ adres mailowy
☐ adres zamieszkania
☐ adres zameldowania
☐ adres korespondencyjny
☐ PESEL*
☐ NIP
☐ inne dane (należy określić jakie to kategorie danych): ...

**należy pamiętać, że występowanie numeru PESEL wraz z innymi danymi pozwalającymi na identyfikację osoby fizycznej (np. imię, nazwisko) powoduje w opinii Prezesa Urzędu Ochrony Danych Osobowych wystąpienie wysokiego ryzyka naruszenie praw i wolności osób fizycznych*

Szczególne kategorie danych osobowych

☐ pochodzenie rasowe lub etniczne
☐ poglądy polityczne
☐ przekonania religijne lub światopoglądowe
☐ przynależność do związków zawodowych
☐ dane genetyczne
☐ dane biometryczne
☐ dane dotyczące zdrowia
☐ seksualność lub orientację seksualną

PROTOKÓŁ Z NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Kategorie danych osobowych podlegające szczególnej ochronie

☐ wyroki skazujące
☐ czyny zabronione lub powiązane środki bezpieczeństwa

Przybliżona liczba osób, których dotyczy naruszenie	

Opis naruszenia

Naruszenie polegało na:

☐ zgubienie lub kradzież nośnika/urządzenia
☐ dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji
☐ korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy
☐ nieuprawnione uzyskanie dostępu do informacji
☐ nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń
☐ złośliwe oprogramowanie ingerujące w poufność, integralność lub dostępność danych
☐ uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing)
☐ nieprawidłowa anonimizacja danych osobowych w dokumencie
☐ nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora
☐ niezamierzona publikacja
☐ dane osobowe wysłane do niewłaściwego odbiorcy
☐ ujawnienie danych niewłaściwej osoby
☐ ustne ujawnienie danych osobowych

Charakter naruszenia

☐ naruszenie dotyczące poufności danych
☐ naruszenie dotyczące integralności danych
☐ naruszenie dotyczące dostępności danych

Przyczyna naruszenia

☐ wewnętrzne działanie niezamierzone
☐ wewnętrzne działanie zamierzone
☐ zewnętrzne działanie niezamierzone
☐ zewnętrzne działanie zamierzone

Ocena naruszenia

Ocena ryzyka z kalkulacji

☐ brak ryzyka
☐ ryzyko
☐ wysokie ryzyko

Końcowa ocena

Naruszenie kwalifikowane jest jako:

☐ nieskutkujące ryzykiem naruszenia praw lub wolności osób fizycznych
☐ skutkujące ryzykiem naruszenia praw lub wolności osób fizycznych

PROTOKÓŁ Z NARUSZENIA OCHRONY DANYCH OSOBOWYCH

☐ skutkujące wysokim ryzykiem naruszenia praw lub wolności osób fizycznych

Uzasadnienie

Powiadomienie organu nadzorczego
Naruszenie kwalifikowane jest jako:
☐ niewymagające powiadomienia organu nadzorczego
☐ wymagające powiadomienia organu nadzorczego

Uzasadnienie

Zawiadomienie osoby, której dane dotyczą
Naruszenie kwalifikowane jest jako:
☐ niewymagające zawiadomienia osoby, której dane dotyczą
☐ wymagające zawiadomienia osoby, której dane dotyczą

Uzasadnienie

Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa dotychczas stosowanych

Środki bezpieczeństwa zastosowane lub proponowane w celu zminimalizowana ryzyka ponownego wystąpienia naruszenia

Środki zastosowane lub proponowane w celu zaradzenia naruszeniu i zminimalizowania negatywnych skutków dla osób, których dane dotyczą

.....

(data i podpis Administratora)

REJESTR NARUSZEŃ

Lp.	Data	Rodzaj naruszenia	Okoliczności naruszenia	Liczba osób dotkniętych naruszeniem	Skutki naruszenia	Podjęte działania zaradcze	Obowiązek zgłoszenia organowi?	Obowiązek zawiadomienia osoby?	Osoba odpowiedzialna za działania zaradcze

REJESTR CZYNNOŚCI PRZETWARZANIA

Administrator	Urząd Gminy i Miasta Czerwionka-Leszczyny 44-230 Czerwionka-Leszczyny ul. Parkowa 9 Regon: 000526854, NIP: 642-310-39-57
Dane kontaktowe Administratora	• listownie na adres: ul. Parkowa 9, 44-230 Czerwionka-Leszczyny, • telefonicznie: 32 429 59 11, 32 431 17 60 • osobiście w godzinach pracy urzędu, • e-mail: sekretariat@czerwionka-leszczyny.com.pl
Inspektor Ochrony Danych	
Dane kontaktowe IOD	iod@czerwionka-leszczyny.pl

Rejestr zawiera czynności:

REJESTR CZYNNOŚCI PRZETWARZANIA

Nazwa czynności przetwarzania	
Identyfikator czynności przetwarzania	
Współadministrator	
Właściciel procesu	
Cel przetwarzania	
Opis kategorii osób	
Opis kategorii danych osobowych	
Kategorie odbiorców	
Przekazanie danych	
Termin usunięcia	
Opis środków bezpieczeństwa	
Podstawa prawna przetwarzania	
Oznaczenie klauzuli informacyjnej (jeśli dotyczy)	
Uwagi	

Załącznik nr 16 do Dokumentacji Ochrony Danych Osobowych stanowiącej załącznik do Zarządzenia nr 218/24
Burmistrza Gminy i Miasta Czerwionka-Leszczyny z dnia 22 kwietnia 2024 r.

REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA

Lp.	Administrator	Przedstawiciel Administratora lub Podmiotu Przetwarzającego	Inspektor Ochrony Danych	Kategorie przetwarzań	Przekazania danych osobowych do państwa trzeciego ...	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.	Data zawarcia umowy	Data wygaśnięcia umowy	Osoba do kontaktu	Prawo kontroli	Termin usunięcia	Informacja zwrotna o usunięciu danych	Podpowierzenia
1													
2													
3													
4													
5													
6													
7													
8													
9													
10													
11													
12													
13													
14													
15													
16													
17													
18													
19													
20													
21													
22													
23													
24													
25													

REJESTR UDOSTĘPNIEŃ

Lp.	Odbiorca danych (nazwa, adres)	Data udostępnienia	Imię i nazwisko osoby, której dane zostały udostępnione	Zakres udostępnienia	Osoba udostępniająca
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

Załącznik nr 18 do Dokumentacji Ochrony Danych Osobowych stanowiącej załącznik do Zarządzenia nr 218/24 Burmistrza Gminy i Miasta Czerwionka-Leszczyny z dnia 22 kwietnia 2024 r.

SPRZECIW WOBEC PRZETWARZANIA

Imię i nazwisko*: .....

* Jeżeli imię i nazwisko są niewystarczające w celu jednoznacznego zidentyfikowania osoby, należy podać dodatkowy identyfikator (np. PESEL, nr dowodu osobistego itp.)

Sprzeciw wobec przetwarzania danych

Na podstawie Artykułu 21 ust. 1 RODO wnoszę sprzeciw wobec przetwarzania moich danych osobowych opartego na art. 6 ust 1 lit. e) lub f), w tym profilowania na podstawie tych przepisów.

UZASADNIENIE:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

(data i podpis)

Decyzja Administratora

.....

UZADADNIENIE:

.....

.....

.....

.....

.....

.....

.....

(data i podpis Administratora)

Załącznik nr 19 do Dokumentacji Ochrony Danych Osobowych stanowiącej załącznik do Zarządzenia nr 218/24 Burmistrza Gminy i Miasta Czerwionka-Leszczyny z dnia 22 kwietnia 2024 r.

WNIOSEK O WYKONANIE CZYNNOŚCI NA DANYCH

Imię i nazwisko*: .....

* Jeżeli imię i nazwisko są niewystarczające w celu jednoznacznego zidentyfikowania osoby, należy podać dodatkowy identyfikator (np. PESEL, nr dowodu osobistego itp.)

	Wniosek o udostępnienie informacji
☐	*Zwracam się z wnioskiem o udzielenie informacji, czy Administrator przetwarza moje dane osobowe.*
☐	*Zwracam się z wnioskiem o udostępnienie informacji o przetwarzanych danych osobowych, celu przetwarzania, kategoriach danych osobowych, odbiorcach, okresie przechowywania lub kryteriach jego określenia.*

	Wniosek o bycie zapomnianym
☐	*Żądam niezwłocznego usunięcia dotyczących mnie danych osobowych.*

	Wniosek o ograniczenie przetwarzania
☐	*Żądam ograniczenia przetwarzania moich danych osobowych.*

	Wniosek o przeniesienie danych
☐	*Zwracam się z wnioskiem o przekazanie mi dostarczonych przeze mnie danych osobowych w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego.*
☐	*Żądam przesłania dotyczących mnie danych osobowych bezpośrednio do:* .....

.....

(data i podpis Wnioskodawcy)

Załącznik nr 20 do Dokumentacji Ochrony Danych Osobowych stanowiącej załącznik do Zarządzenia nr 218/24 Burmistrza Gminy i Miasta Czerwionka-Leszczyny z dnia 22 kwietnia 2024 r.

WNIOSEK O SPROSTOWANIE DANYCH

Imię i nazwisko*: .....

* Jeżeli imię i nazwisko są niewystarczające w celu jednoznacznego zidentyfikowania osoby, należy podać dodatkowy identyfikator (np. PESEL, nr dowodu osobistego itp.)

Żądanie sprostowania danych

Żądam sprostowania lub uzupełnienia moich danych osobowych w zakresie:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Załącznik: .....

.....

(data i podpis Wnioskodawcy)

REJESTR REALIZACJI PRAW OSÓB UPRAWNIONYCH

Lp.	Imię i nazwisko osoby uprawnionej	Zakres wniosku / sprzeciwu	Data złożenia wniosku / sprzeciwu	Sposób realizacji praw	Podpis osoby realizującej prawa	Uwagi

WYKAZ UMÓW POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	**Oznaczenie Podmiotu Przetwarzającego (Procesora)** (nazwa, adres, nr NIP)	**Umowa powierzenia** (tak/zapisy w umowie głównej)	**Data zawarcia / data obowiązywania**	**Cel powierzenia**
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Umowa powierzenia przetwarzania danych osobowych,

zawarta w dniu ..... r. pomiędzy:

Gminą i Miastem Czerwionka-Leszczyny z siedzibą przy ul. Parkowej 9, 44-230 Czerwionka-Leszczyny, Regon: 276258530, NIP: 642-000-97-26,

reprezentowaną przez:

Burmistrza -

zwaną w dalszej części umowy **„Zamawiającym"**, a

xx

zwanym w dalszej części umowy **Procesorem,** a wraz ze Zleceniodawcą **- Stronami**

- zwana dalej Umową

§ 1

1. **Zamawiający i Procesor** oświadczają, że w dniu <DATA> zawarli umowę <ZAKRES>, zwaną dalej Umową Główną.
2. **Zamawiający** oświadcza, że jest Administratorem w rozumieniu 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), zwanego dalej Rozporządzeniem, w stosunku do danych powierzonych **Podmiotowi przetwarzającemu (Procesorowi).**

§ 2

1. **Zamawiający** powierza Procesorowi w trybie art. 28 Rozporządzenia dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie. **Procesor** może przetwarzać dane osobowe przekazane przez **Zamawiającego** wyłącznie w celu i zakresie zgodnym z niniejszą Umową i Umową Główną, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
2. W celu wykonania obowiązków wynikających z niniejszej Umowy **Procesor** może przetwarzać dane pracowników, dane klientów, kontrahentów, interesantów, petentów. Zakres danych obejmuje imię, nazwisko, stanowisko, nazwa firmy, adres, dane kontaktowe. Rodzaj powierzonych danych obejmuje tzw. dane zwykle, nie obejmuje tzw. szczególnych kategorii danych oraz danych osobowych dotyczących wyroków skazujących i czynów zabronionych. Procesor w zakresie realizacji celu jest uprawniony do wykonywania następujących operacji na danych: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, przeglądanie, usuwanie lub niszczenie wedle wyboru Zamawiającego. Przetwarzanie powierzonych danych osobowych odbywać się w formie papierowej lub przy wykorzystaniu systemów informatycznych. Z uwagi na cel powierzenia przetwarzania danych osobowych, przetwarzanie danych będzie miało charakter cykliczny/sporadyczny/jednorazowy.
3. Powierzone przez **Zamawiającego** dane osobowe będą przetwarzane przez **Procesora** wyłącznie w celu realizacji Umowy Głównej.

4. **Procesor** może powierzyć przetwarzanie danych osobowych podmiotowi trzeciemu (podwykonawcy) po uzyskaniu uprzedniej, wyrażonej w formie pisemnej pod rygorem nieważności, zgody **Zamawiającego** na powierzenie podwykonawcy dalszego przetwarzania danych osobowych w określonym celu i zakresie. Wykaz podwykonawców zawiera Załącznik 1 do Umowy.
5. W przypadku skorzystania z podwykonawcy, **Procesor** zobowiązany jest do zapewnienia, iż podwykonawca przetwarzał będzie dane osobowe wyłącznie w celu i w zakresie opisanym w Umowie zawartej przez podwykonawcę z **Procesorem**, przy czym cel i zakres przetwarzania nie będzie szerszy niż wynikający z niniejszej Umowy oraz podwykonawca zobowiązany będzie do zachowania wszelkich wymagań oraz warunków przetwarzania danych osobowych wynikających z niniejszej Umowy i Rozporządzenia.
6. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Zamawiającego, chyba że obowiązek taki nakłada na Procesora Prawo Unii lub prawo państwa członkowskiego, któremu podlega **Procesor**. W takim przypadku przed rozpoczęciem przetwarzania **Procesor** poinformuje **Zamawiającego** o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.

§ 3

1. **Procesor** jest zobowiązany do przestrzegania przepisów Rozporządzenia.
2. **Procesor** oświadcza, że wdrożył środki techniczne i organizacyjne, mające na celu zabezpieczenie powierzonych danych osobowych stosownie do wymagań, określonych w artykule 28, 29 i 30 ust 2, 3 i 4 oraz w artykule 32 Rozporządzenia. **Procesor** zapewni zachowanie odpowiednich środków technicznych i organizacyjnych przez cały okres obowiązywania umowy, a także po jej zakończeniu tak, aby przetwarzanie danych osobowych spełniało wymogi Rozporządzenia i chroniło prawa osób, których dane dotyczą.

§ 4

1. **Procesor** zobowiązuje się do nadzoru nad przestrzeganiem zasad ochrony i przetwarzania danych lub wyznacza do tego Inspektora Ochrony Danych lub pełnomocnika. Procesor zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
2. **Procesor** zobowiązuje się do dopuszczania do przetwarzania danych wyłącznie osób, posiadających upoważnienie nadane przez **Procesora**, które przeszły szkolenie z zasad przetwarzania danych osobowych oraz zobowiązały się do przestrzegania tych zasad i zachowania tajemnicy.
3. **Procesor** w miarę możliwości pomaga **Zamawiającemu** poprzez odpowiednie środki techniczne i organizacyjne wywiązać się obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III Rozporządzenia.

4. **Procesor** w razie potrzeby i posiadania stosownych informacji pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36 Rozporządzenia.
5. **Procesor** udostępnia **Zamawiającemu** wszelkie informacje niezbędne do wykazania spełnienia obowiązków, określonych w artykule 28 Rozporządzenia oraz umożliwia **Zamawiającemu** lub audytorowi upoważnionemu przez **Zamawiającego** przeprowadzanie audytów, w tym inspekcji, i bierze w nich udział.
6. Procesor po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki, nie później niż w ciągu 24 godzin od stwierdzenia naruszenia, przekazuje Zamawiającemu wszystkie niezbędne informacje na adres e-mail: iod@czerwionka-leszczyny.pl oraz dokonuje zgłoszenia telefonicznego na numer +48 575 515 035.

§ 5

1. **Procesor** odpowiada za szkody jakie powstały wobec **Zamawiającego** lub osób trzecich w wyniku niezgodnego z Umową i Umową Główną przetwarzania danych osobowych. Odpowiedzialność, o której mowa w niniejszym ustępie wynika z przepisów ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2019 poz. 1781) oraz przepisów ogólnych wskazanych w kodeksie cywilnym.
2. **Procesor** gwarantuje, że powierzone dane nie będą przetwarzane poza Unią Europejską.
3. **Zamawiający** zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez **Procesora** przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.
4. **Zamawiający** poinformuje **Procesora** o terminie planowanej kontroli z wyprzedzeniem co najmniej 7 dni (słownie: siedmiu dni). Powiadomienie o kontroli będzie określało zakres i przedmiot kontroli oraz wskazanie osób upoważnionych do prowadzenia kontroli w imieniu Administratora.
5. **Zamawiający** realizować będzie prawo kontroli w godzinach pracy **Procesora**.
6. Z kontroli zostanie sporządzony protokół podpisany przez obie Strony, którego jeden egzemplarz zatrzyma **Procesor**.
7. **Procesor** może wnieść zastrzeżenia do protokołu z kontroli w ciągu 7 dni roboczych od daty jego podpisania, przez Strony.
8. **Procesor** zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie ustalonym z **Zamawiającym**.
9. **Procesor** udostępnia **Zamawiającemu** wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.
10. **Procesor** po zakończeniu przetwarzania danych osobowych zobowiązany jest do niezwłocznego przekazania posiadanych danych **Zamawiającemu** oraz usunięcia posiadanych kopii z systemu informatycznego.
11. **Procesor** zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych, otrzymanych od **Zamawiającego** i od współpracujących z nim osób oraz danych uzyskanych w

jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej, dalej zwanych danymi poufnymi.

12. **Procesor** oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody **Zamawiającego** w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

§ 6

1. Niniejsza Umowa wygasa z chwilą wygaśnięcia Umowy Głównej.
2. **Zamawiający** może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy **Procesor**:
   a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
   b) przetwarza dane osobowe w sposób niezgodny z umową;
   c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody **Zamawiającego**.

§ 7

Zmiana niniejszej Umowy może nastąpić tylko w formie pisemnego aneksu pod rygorem nieważności.

§ 8

W sprawach nieuregulowanych niniejszą Umową mają zastosowanie przepisy Rozporządzenia oraz kodeksu cywilnego i inne właściwe przepisy prawne.

§ 9

Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

Procesor	Zamawiający
.....	.....

Załączniki:

Załącznik 1: Wykaz podprocesorów (dalszych podmiotów przetwarzających)

Załącznik 1

do Umowy powierzenia z dnia .....

WYKAZ PODPROCESORÓW

(dalszych podmiotów przetwarzających)

Zamawiający wyraża zgodę na podpowierzenie przetwarzania danych osobowych następującym podmiotom:

Lp.	Dane podmiotu	Cel powierzenia	Zakres danych
1.			
2.			

Każda zmiana podprocesora wymaga pisemnej zgody Zamawiającego udzielonej przed dopuszczeniem podmiotu do przetwarzania danych.

Procesor

.....

Zamawiający

.....

WYKAZ SYSTEMÓW INFORMATYCZNYCH

Czynność przetwarzania	Systemy informatyczne i programy wykorzystywane do przetwarzania danych osobowych	Osoba odpowiedzialna za system/program

.....

(data i podpis Administratora)