Polityka Bezpieczeństwa Informacji Jednostki Organizacyjnej Gminy Lublin

Pełny zakres dostępu do dokumentu – odczyt, modyfikacja:

1. Pełnomocnik ds. Systemu Zarządzania Bezpieczeństwem Informacji Urzędu Miasta Lublin,
2. Inspektor Ochrony Danych Urzędu Miasta Lublin,
3. Administrator Bezpieczeństwa Teleinformatycznego Urzędu Miasta Lublin,

Zakres dostępu do dokumentu – odczyt:

1. Administrator - Kierownik Jednostki Organizacyjnej Gminy Lublin,
2. Inspektor Ochrony Danych Jednostki Organizacyjnej Gminy Lublin,
3. Kierownictwo Jednostki Organizacyjnej Gminy Lublin,
4. Pracownicy Jednostki Organizacyjnej Gminy Lublin,
5. Administratorzy Systemów Informatycznych Jednostki Organizacyjnej Gminy Lublin,
6. Podmioty trzecie zarządzające systemem informatycznym Jednostki Organizacyjnej Gminy Lublin, upoważnione przez Kierownictwo tej Jednostki zakresie adekwatnym do realizowanych przez nie zadań ,
7. Podmioty trzecie, które mają dostęp do danych osobowych zgromadzonych w Jednostkach Organizacyjnej Gminy Lublin na mocy zawartych umów w zakresie adekwatnym do realizowanych przez nie zadań.

Spis treści

1 Cel

1. Cel: Opracowanie, wdrożenie i doskonalenie spójnego i jednolitego systemu zarządzania bezpieczeństwem informacji w Jednostkach Organizacyjnych Gminy Lublin.

2. Dokumentacja Polityki Bezpieczeństwa Informacji jest zbiorem zasad i procedur obowiązującym wszystkie osoby upoważnione przez Kierownika Jednostki Organizacyjnej podczas przetwarzania informacji chronionych.

3. Zarządzanie bezpieczeństwem informacji jest pojęciem obejmującym zasady zarządzania systemem chroniącym dane oraz sposoby reagowania na zagrożenia. Zapewnienie odpowiedniej wiedzy zarządzających Jednostką Organizacyjną oraz siecią informatyczną w zakresie pojawiających się nowych zagrożeń oraz metod ochrony jest kolejnym elementem zapewnienia bezpieczeństwa. Osoby obsługujące systemy przetwarzające dane osobowe są ogniwem zabezpieczeń, na którego skuteczność wpływa również zapewnienie rzetelnej informacji w zakresie sposobu bezpiecznego użytkowania oprogramowania i sprzętu.

4. Zastosowanie niniejszej Polityki Bezpieczeństwa Informacji powinno zapewnić zabezpieczenia adekwatne i proporcjonalne do wyników szacowania ryzyka występującego dla przetwarzanych i przechowywanych danych w Jednostce Organizacyjnej oraz w systemach informatycznych Urzędu Miasta Lublin.

5. Pojęcie „polityki bezpieczeństwa" należy rozumieć jako zestaw procedur, instrukcji, regulaminów oraz praktycznych zaleceń regulujących sposób zbierania, zarządzania, ochrony, modyfikacji, usuwania i przekazywania informacji chronionej. Przez informację chronioną rozumie się w szczególności dane osobowe oraz wszelkie informacje w formie papierowej, elektronicznej i innej, przetwarzane (zbierane, utrwalane, przechowywane, opracowywane, zmieniane, udostępniane i usuwane) w sposób tradycyjny lub w systemach informatycznych, będących własnością Jednostki Organizacyjnej lub Urzędu Miasta Lublin.

6. Polityka Bezpieczeństwa Informacji jest jednocześnie dokumentem określającym zadania osób funkcyjnych, pracowników oraz pracowników i współpracowników podmiotów trzecich, które na mocy zawartych umów mają dostęp do informacji chronionych. Ma ona pomóc w zapewnieniu: poufności, integralności, dostępności oraz rozliczalności przetwarzanych danych osobowych i innych zidentyfikowanych aktywów informacyjnych.

7. W skład Dokumentacji opisującej sposób przetwarzania danych wchodzą wymienione poniżej dokumenty wraz z załącznikami:

   a. Polityka Bezpieczeństwa Informacji Jednostki Organizacyjnej Gminy Lublin,

   b. Regulamin Systemu Informatycznego Jednostki Organizacyjnej Gminy Lublin,

   c. Regulamin Bezpieczeństwa Informacji Jednostki Organizacyjnej Gminy Lublin.

2 Zakres stosowania

1. Niniejszą Politykę Bezpieczeństwa Informacji stosują Jednostki Organizacyjne Gminy Lublin.

2. Politykę Bezpieczeństwa Informacji stosują osoby przetwarzające informacje chronione Jednostki Organizacyjnej, niezależnie od formy zatrudnienia w Jednostce lub formy prawnej wiążącej Jednostkę z tą osobą. W szczególności mogą być to osoby zatrudnione na umowę o pracę, stażyści, praktykanci, wolontariusze oraz osoby realizujące zadania na podstawie podpisanej z Jednostką Organizacyjną umowy cywilnoprawnej, a także pracownicy i współpracownicy podmiotów trzecich, z którymi została zawarta umowa, na mocy której ww. osoby mają dostęp do informacji chronionych, w tym do danych osobowych.

3. Polityka Bezpieczeństwa Informacji dotyczy wszystkich danych osobowych oraz innych informacji podlegających ochronie przetwarzanych w pomieszczeniach Jednostki Organizacyjnej niezależnie od formy ich przetwarzania. Polityka w zakresie danych osobowych odnosi się:

   a. do danych przetwarzanych w zbiorach tradycyjnych, w szczególności kartotekach, skorowidzach, księgach wykazach i w innych zbiorach ewidencyjnych,

   b. do danych osobowych, które mają być do zbioru dołączone,,

   c. do danych przetwarzanych w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych osobowych.

4. Dla skutecznej realizacji Polityki Bezpieczeństwa Informacji, Administrator zapewnia:

   a. szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony,

   b. okresowe szacowanie ryzyka zagrożeń dla zbiorów danych,

   c. okresową ocenę skutków dla ochrony danych osobowych,

   d. kontrolę, monitoring i nadzór nad przetwarzaniem danych osobowych,

   e. monitorowanie zastosowanych środków ochrony,

   f. możliwość realizacji wytycznych zawartych w Kodeksach, o których mowa w art. 40 RODO,

   g. wdrożenie odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku, w tym między innymi w stosownym przypadku:

      - pseudonimizację i szyfrowanie danych osobowych;
      - zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

3 Terminologia

1. Określenia używane w dalszej treści Polityki Bezpieczeństwa Informacji i pozostałej Dokumentacji:
   a. **ABT** – Administrator Bezpieczeństwa Systemów Informatycznych Urzędu Miasta Lublin,
   b. **ADO/Administrator** – Kierownik Jednostki Organizacyjnej Gminy Lublin,
   c. **ADO UML/Administrator UML**– Prezydent Miasta Lublin,
   d. **ASI** – Administrator Systemu Informatycznego Jednostki Organizacyjnej Gminy Lublin (pracownik lub podmiot zewnętrzny),
   e. **BBI UML** – Biuro Bezpieczeństwa Informacji Urzędu Miasta Lublin,
   f. **CPD** – Centrum Przetwarzania Danych Urzędu Miasta Lublin,
   g. **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 ki szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Dane osobowe dzieli się na dane zwykłe i dane wrażliwe – szczególnej kategorii.

      Jako przykład danych zwykłych można wskazać:

      - numery identyfikacyjne: imię, nazwisko, adres zamieszkania, PESEL, NIP, paszport, dowód osobisty,
      - cechy fizyczne: wygląd zewnętrzny, siatkówka oka, linie papilarne,
      - cechy fizjologiczne: grupa krwi,
      - cechy ekonomiczne: status majątkowy, lista zaległości finansowych.
      - środki komunikacji elektronicznej: numer telefonu, adres e-mai.

      Do danych wrażliwych zaliczają się dane dotyczące:

      - pochodzenie rasowe i etniczne,
      - przekonania religijne czy światopoglądowe,
      - przynależność do związków zawodowych czy partii,
      - poglądy polityczne,
      - stan zdrowia,
      - kod genetyczny,
      - dane biometryczne
      - dane o seksualności lub orientacji seksualnej,
      - wyroków skazujących i naruszeń prawa.

h. **Dostępność danych** - rozumie się przez to właściwość zapewniającą, że dane są udostępniane dla upoważnionego podmiotu wtedy, gdy ich potrzebuje do przetwarzania,

i. **Integralność danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,

j. **IOD** – Inspektor Ochrony Danych Jednostki Organizacyjnej Gminy Lublin (pracownik lub podmiot zewnętrzny),

k. **IOD UML** – Inspektor Ochrony Danych Urzędu Miasta Lublin,

l. **Jednostka/Jednostka Organizacyjna** – Jednostka Organizacyjna Gminy Lublin,

m. **KJO** – Kierownik Jednostki Organizacyjnej Gminy Lublin,

n. **KK** – Komórka Jednostki Organizacyjnej Gminy Lublin odpowiedzialna za procesy kadrowe,

o. **KKO** – Kierownik Komórki Organizacyjnej Jednostki Gminy Lublin ,

p. **Kierownictwo Jednostki** – najwyższe kierownictwo Jednostki Organizacyjnej Gminy Lublin,

q. **Naruszenie bezpieczeństwa informacji** – wszelkie zdarzenia lub działania, w tym również niezamierzone, które mogą stanowić przyczynę utraty zasobów, obniżenia wymaganego poziomu poufności, integralności, dostępności informacji lub niezawodności systemów, a także odstępstwa od obowiązujących procedur postępowania, nawet jeżeli nie prowadzą do negatywnych skutków dla organizacji. Zdarzenia lub działania, które mogą prowadzić do naruszenia praw lub wolności osób fizycznych.

r. **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,

s. **Odbiorca danych** – 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 powszechnie obowiązującym, 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. Przy czym przez sformułowanie „ „strona trzecia" rozumie się osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia Administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe,

t. **Osoba upoważniona do przetwarzania danych osobowych** – osoba, która złożyła ADO oświadczenie o zachowaniu w tajemnicy przetwarzanych danych i stosowanych sposobach zabezpieczenia tych danych, posiadająca imienne upoważnienie wydane przez ADO, określające imię i nazwisko osoby upoważnionej, datę

nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych oraz identyfikator, jeżeli dane są przetwarzane w systemie informatycznym,

u. **PML** – Prezydent Miasta Lublin,

v. **PSZBI** – Pełnomocnik ds. Systemu Zarządzania Bezpieczeństwem Informacji Urzędu Miasta Lublin – Sekretarz Miasta,

w. **UML** – Urząd Miasta Lublin,

x. **Podmiot przetwarzający** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora,

y. **Przetwarzanie** - operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,

z. **Poufność danych** - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,

aa. **Regulamin/RSI** – Regulamin Systemu Informatycznego Jednostki Organizacyjnej Gminy Lublin,

bb. **RBI** – Regulamin Bezpieczeństwa Informacji Jednostki Organizacyjnej Gminy Lublin,

cc. **Rozliczalność danych** - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,

dd. **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),

ee. **System CPD** – system informatyczny administrowany przez Wydział Informatyki i Telekomunikacji Urzędu Miasta Lublin,

ff. **System CPD Jednostki** – system informatyczny administrowany przez Jednostkę Organizacyjną i zlokalizowany w CPD,

gg. **System Jednostki** – system informatyczny administrowany przez Jednostkę Organizacyjną i zlokalizowany w niej lub na serwerach innych niż należące do Gminy Lublin (np. serwery rządowe, serwery w chmurze obliczeniowej, i itp.).

hh. **Systemy** – System CPD, System CPD Jednostki oraz System Jednostki,

ii. **Usuwanie danych** – trwałe zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,

jj. **Usługa CPD** – usługa informatyczna administrowana przez WI,

kk. **Usługa CPD Jednostki** – usługa informatyczna administrowana przez Jednostkę Organizacyjną i zlokalizowana w CPD,

ll. **Usługa Jednostki** – usługa informatyczna Jednostki Organizacyjnej administrowana przez Jednostkę i zlokalizowana w niej,

mm. **Ustawa** - ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych,

nn. **Uwierzytelnianie** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,

oo. **Użytkownik CPD** – osoba przetwarzająca dane w Systemie CPD lub Usłudze CPD, niezależnie od formy zatrudnienia lub formy prawnej wiążącej Jednostkę Organizacyjną z tą osobą, w szczególności mogą być to osoby zatrudnione na umowę o pracę, stażyści, praktykanci, osoby realizujące zadania na podstawie umowy cywilnoprawnej,

pp. **Użytkownik/pracownik (w tym podmiotu trzeciego)** - osoba przetwarzająca dane w Systemie Jednostki Organizacyjnej oraz poza nim (np. dokumentacji w formie tradycyjnej), niezależnie od formy zatrudnienia w Jednostce lub formy prawnej wiążącej Jednostkę z tą osobą. W szczególności mogą być to osoby zatrudnione na umowę o pracę, stażyści, praktykanci, osoby realizujące zadania na podstawie podpisanej umowy cywilnoprawnej,

qq. **Zbiór danych** – to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie,

rr. **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.

2. Organizacja systemu zarządzania bezpieczeństwa informacji i zarządzanie bezpieczeństwem informacji odbywa się w odniesieniu do zmieniającego się otoczenia prawnego i technologicznego. Uwzględniane są również wyniki analizy ryzyka i wyniki oceny skutków. W procesy decyzyjne zaangażowane jest Kierownictwo Jednostki Organizacyjnej.

3.2 Procesy zarządzania bezpieczeństwem informacji

W Jednostce Organizacyjnej funkcjonują poniższe procesy zarządzania bezpieczeństwem Informacji:

1. zarządzanie ryzykiem,
2. monitorowanie bezpieczeństwa informacji chronionych poprzez identyfikację incydentów,
3. audyt systemu zarządzania bezpieczeństwem informacji realizowany przez Urząd Miasta Lublin,
4. nadzór nad zgodnością dokumentacji i stosowania zawartych w niej zasad poprzez działania Kierownika Jednostki Organizacyjnej oraz Inspektora Ochrony Danych,
5. zarządzanie dostępem do aktywów informacyjnych oraz systemów informatycznych Jednostki Organizacyjnej,
6. zarządzanie incydentami poprzez identyfikację naruszeń bezpieczeństwa informacji przez wszystkich pracowników Jednostki oraz pracowników i współpracowników podmiotu trzeciego i zastosowanie adekwatnych mechanizmów naprawczych i korygujących,
7. przeprowadzanie oceny skutków.

4 Obowiązki pracowników/użytkowników

1. Kierownik Jednostki Organizacyjnej jest obowiązany zapoznać z treścią Dokumentacji ochrony informacji każdego podległego pracownika/użytkownika przetwarzającego informacje chronione, w szczególności dane osobowe. Pracownicy/użytkownicy są obowiązani zapoznać się z następującymi dokumentami (zwanymi dalej Dokumentacją):
   a. Polityka Bezpieczeństwa Informacji Jednostki Organizacyjnej Gminy Lublin,
   b. Regulamin Bezpieczeństwa Informacji Jednostki Organizacyjnej Gminy Lublin.
2. Za przestrzeganie zasad zapisanych w Dokumentacji odpowiedzialne są wszystkie osoby zaangażowane w przetwarzanie informacji chronionych.
3. Pracownicy/użytkownicy są zobowiązani są do przestrzegania przepisów prawa powszechnie obowiązującego i regulacji wewnętrznych dotyczących ochrony danych osobowych. W tym celu zobowiązani są do:
   a. pisemnego wnioskowania o zaewidencjonowanie nowych zbiorów danych osobowych w Wykazie prowadzonym przez Inspektora Ochrony Danych,
   b. bieżącej oceny funkcjonowania mechanizmów zabezpieczeń i ochrony,
   c. występowania z wnioskami w sprawie wprowadzenia niezbędnych zmian w zakresie ochrony danych osobowych.
4. Jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych osobowych, przewidują dalej idącą ich ochronę, niż to wynika z RODO, czy Ustawy, stosuje się przepisy tych ustaw.

5. Pracownicy/użytkownicy przetwarzający dane osobowe obowiązani są dołożyć należytej staranności w celu ochrony interesu osób, których dane są gromadzone i przetwarzane, a w szczególności należy przestrzegać, aby dane te były:

   a. przetwarzane zgodnie z aktami prawa powszechnie obowiązującego i regulacjami wewnętrznymi,

   b. zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,

   c. merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,

   d. przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania

   oraz by wypełniany był obowiązek informacyjny, w przypadkach wskazanych w przepisach prawa powszechnie obowiązującego.

6. Naruszenie postanowień Polityki Bezpieczeństwa Informacji może skutkować zablokowaniem dostępu pracownika/użytkownika do informacji chronionych i Systemów. W przypadku ciężkich naruszeń, takie działanie może prowadzić do wszczęcia postępowania dyscyplinarnego oraz do rozwiązania bądź wypowiedzenia umowy. W przypadku poniesienia strat w wyniku naruszenia, Jednostka Organizacyjna może dochodzić roszczeń odszkodowawczych na drodze sądowej.

7. Każde naruszenie bezpieczeństwa informacji powinno być niezwłocznie zgłaszane Administratorowi i Inspektorowi Ochrony Danych lub, w przypadku naruszeń bezpieczeństwa dotyczących systemów informatycznych, Administratorowi Systemu Informatycznego.

8. W razie wykrycia naruszenia ochrony informacji chronionych każdy pracownik ma obowiązek postępować zgodnie z procedurami zawartymi w Dokumentacji.

9. Postanowienia pkt 1-8 stosuje się odpowiednio do pracowników i współpracowników podmiotów trzecich, którzy na mocy zawartych umów mają dostęp do zgromadzonych i przetwarzanych danych.

5 Bezpieczeństwo zasobów ludzkich

5.1 Obsada stanowisk odpowiedzialnych za bezpieczeństwo informacji i systemów

1. Osoby mające za zadanie monitorować bezpieczeństwo informacji i systemów informatycznych muszą:

   a. posiadać odpowiednie kompetencje,

   b. przeszkolenie w zakresie zasad Systemu Zarządzania Bezpieczeństwem Informacji.

2. Inspektor Ochrony Danych powinien:

1) posiadać pełną zdolność do czynności prawnych oraz korzystać z pełni praw publicznych,

2) posiadać fachową wiedzę na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO, ustawie i aktach prawa wewnętrznego,

3) wykonywać zadania niezależnie i bez konfliktu interesów,

4) mieć wiedzę w zakresie europejskiego i krajowego prawa ochrony danych oraz praktyk ochrony danych, a także szczegółową wiedzę na temat RODO,

5) posiadać wiedzę na temat systemów informatycznych służących do przetwarzania, a także potrzeb i sposobów zabezpieczania danych osobowych przetwarzanych w Jednostce

i nie może być karany za przestępstwo popełnione z winy umyślnej.

3. Administrator może powierzyć Inspektorowi Ochrony Danych wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania zadań, o których mowa w niniejszej Polityce.

Administrator jest zobowiązany dokonać stosownego zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych zgodnie z wymogami prawa powszechnie obowiązującego o powołaniu Inspektora Ochrony Informacji. Administrator zawiadamia Prezesa Urzędu Ochrony Danych Osobowych o każdej zmianie danych Inspektora oraz jego odwołaniu przez Administratora lub w przypadku jego śmierci.

5.2 Szkolenia osób zaangażowanych w proces przetwarzania informacji

1. Każda osoba zaangażowana w proces przetwarzania informacji w Jednostce Organizacyjnej odbywa szkolenie z zakresu:

   a. zasad bezpieczeństwa informacji,

   b. zagrożenia bezpieczeństwa informacji,

   c. skutków naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialności prawnej,

   d. stosowania środków zapewniających bezpieczeństwo informacji, w tym urządzeń i oprogramowania minimalizującego ryzyko błędów ludzkich.

2. Pracownicy są okresowo szkoleni, nie rzadziej niż 1 raz w roku, z zagadnień bezpieczeństwa informacji i oceniani ze znajomości tematyki bezpieczeństwa informacji. Stażyści, praktykanci, wolontariusze są szkoleni z zakresu bezpieczeństwa informacji przed dopuszczeniem ich do przetwarzania danych osobowych.

3. Szczegółowe zasady dotyczące szkolenia pracowników stosowane są zgodnie z wewnętrznymi regulacjami Jednostki Organizacyjnej.

4. Szkolenia pracowników lub współpracowników podmiotów trzecich, które na mocy zawartej umowy mają dostęp do informacji chronionych, szkoleni są przez Inspektora Ochrony Danych przed zawarciem umowy lub niezwłocznie po jej zawarciu, ale przed dopuszczeniem ich do przetwarzania informacji chronionych.

5.3 Przekazywanie informacji o zmianach w zakresach obowiązków

1. Osoby odpowiedzialne za zarządzanie kadrami w Jednostce Organizacyjnej lub KKO informują niezwłocznie IOD każdej zmianie w zakresie czynności pracowników, która wiąże się ze zmianą zakresu uprawnień do przetwarzania informacji chronionych w Jednostce Organizacyjnej.

2. Kierownik komórki merytorycznej odpowiedzialnej za merytoryczną obsługę umowy informują niezwłocznie IOD o każdej zmianie zakresu informacji chronionych, do których muszą mieć dostęp pracownicy i współpracownicy podmiotu trzeciego, a która wiąże się ze zmianą zakresu uprawnień do przetwarzania informacji chronionych w Jednostce Organizacyjnej.

5.4 Zasady bezpieczeństwa informacji związane z zakończeniem wykonywania obowiązków

1. Cofnięcie upoważnień do przetwarzania informacji chronionych powinno nastąpić niezwłocznie po zakończeniu wykonywania obowiązków pracownika/użytkownika.

2. Rozliczenie pracownika z aktywów związanych z przetwarzaniem informacji chronionych w Jednostce Organizacyjnej powinno odbywać się na podstawie stosowanej w Jednostce karty obiegowej.

3. Postanowienia pkt 1-2 stosuje się odpowiednio do pracowników i współpracowników podmiotów trzecich, którzy na mocy zawartych umów mają dostęp do zgromadzonych i przetwarzanych danych oraz wolontariuszy, stażystów, praktykantów.

6 Szacowanie ryzyka dla informacji chronionych i ocena skutków

6.1 Identyfikacja i klasyfikacja informacji chronionych

Zarządzanie aktywami, w tym informacjami chronionymi, jest realizowane w celu zapewnienia wymaganego poziomu bezpieczeństwa informacji. Aktywa to wszystko, co ma wartość dla Jednostki Organizacyjnej, w szczególności aktywa informacyjne to wiedza lub dane. Aktywa chronione dzielimy na dwie grupy: aktywa główne oraz aktywa wspomagające.

1. Aktywa główne:
   a. procesy i działania biznesowe,
   b. informacje.

1. Aktywa wspomagające:
   a. sprzęt,
   b. oprogramowanie,
   c. sieć,
   d. personel,

e. siedziba,

f. struktura organizacyjna.

2. Aktywa są chronione ze względu na wymagania wynikające z:

a. przepisów prawa,

b. regulacji wewnętrznych, z których wynika ochrona właściwych aktywów,

c. zasad bezpieczeństwa wymaganych przez Urząd Miasta Lublin,

d. postanowień umów pomiędzy Jednostką Organizacyjną, a podmiotami zewnętrznymi,

e. warunków licencji.

6.2 Zasady zarządzania aktywami informacyjnymi

1. Zarządzanie aktywami informacyjnymi w Jednostce Organizacyjnej odbywa się zgodnie z zasadami:

1) odpowiedzialności za aktywa: określeni są właściciele wszystkich aktywów oraz jest im przydzielona odpowiedzialność za utrzymanie odpowiednich zabezpieczeń; wdrożenie określonych zabezpieczeń może być delegowane przez właściciela aktywów, jednak pozostaje on nadal odpowiedzialny za adekwatną ochronę aktywów,

2) Identyfikacji aktywów: wszystkie aktywa są zidentyfikowane oraz jest sporządzony i utrzymywany spis wszystkich ważnych aktywów,

3) akceptowalnego użycia aktywów: w Dokumentacji są określone i wdrażane przez Kierownika Jednostki Organizacyjnej zasady dopuszczalnego korzystania z informacji i zasobów związanych z przetwarzaniem informacji, które są wdrożone do stosowania przez Kierownika Jednostki Organizacyjnej,

4) klasyfikacji informacji: określona jest metoda oraz sposób klasyfikacji informacji odzwierciedlający wymagania ochrony informacji na odpowiednim poziomie,

5) oznaczania informacji: stosowane są regulacje wewnętrzne wyznaczające zasady oznaczanie informacji i postępowania z nim.

2. Zarządzanie aktywami informacyjnymi odbywa się zgodnie z zasadami opisanymi w ***Załączniku nr 7 Procedura szacowania ryzyka***. Dla poszczególnych rodzajów informacji chronionych określone są szczegółowe zasady postępowania oraz grupy pracowników posiadające do nich dostęp.

6.3 Szacowanie ryzyka

1. Proces zarządzania ryzykiem w bezpieczeństwie informacji realizuje się zgodnie z wytycznymi normy PN-ISO/IEC 27005:2014.

2. Ryzyko rozpatrujemy w sytuacjach, w których występuje słabość systemu zabezpieczeń dla zasobu chronionego, która może być z pewnym niezerowym prawdopodobieństwem wykorzystana w celu spowodowania strat. Jeżeli nie zidentyfikujemy zagrożenia, słabości lub luki w zabezpieczeniach (zwanych podatnościami), bądź określimy zdarzenie prawdopodobieństwem równym zeru, przyjmujemy, że ryzyko nie występuje dla rozpatrywanej sytuacji dla zasobu chronionego.

3. Wszyscy Pracownicy podczas realizacji zadań biorą pod uwagę ryzyka związane z bezpieczeństwem informacji.

4. Kierownik Jednostki Organizacyjnej jest zobowiązany do:

   a. identyfikacji i klasyfikacji aktywów i zasobów informacyjnych na potrzeby szacowania ryzyka,

   b. identyfikacji scenariuszy wykorzystania podatności na zagrożenie,

   c. szacowania strat dla zasobów użytych w realizacji procesów objętych przeglądem ryzyka,

   d. wykonania oceny skutków zgodnie z art. 35 RODO dla operacji przetwarzania danych osobowych, jeżeli jest wymagana przepisami prawa powszechnie obowiązującego,

   e. wykonania szacowania ryzyka i przeprowadzenia oceny skutków zgodnie z art. 35 RODO, w przypadku wdrożenia nowej technologii (np. nowego systemu informatycznego) w Jednostce Organizacyjnej służącej do przetwarzania danych osobowych,

   f. w razie potrzeby po dokonaniu oceny skutków, przeprowadzenia zgodnie z art. 36 RODO konsultacji z Urzędem Ochrony Danych Osobowych w sytuacji, gdy Kierownik Jednostki Organizacyjnej nie jest w stanie zminimalizować wysokiego ryzyka naruszenia praw lub wolności osób fizycznych.

5. Do zadań Kierownika Jednostki Organizacyjnej należy:

   a. zatwierdzenie Wykazu informacji chronionych Jednostki Organizacyjnej (aktywów informacyjnych Jednostki),

   b. zatwierdzanie Rejestru ryzyka Jednostki Organizacyjnej,

   c. zatwierdzanie planów postępowania z ryzykami,

   d. przeprowadzenia i zatwierdzenia oceny skutków, jeżeli została wykonana.

6. Do zadań Inspektora Ochrony Danych oraz ASI należy:

   g. przygotowanie Wykazu informacji chronionych Jednostki Organizacyjnej wraz z ich klasyfikacją,

   h. przeprowadzenie szacowania ryzyka i przygotowanie wyników szacowania ryzyka w Rejestrze ryzyka,

i. przygotowanie planu postępowania z ryzykami,

j. konsultowanie oceny skutków i wsparcie Kierownika Jednostki Organizacyjnej w jej wykonaniu.

Zarządzanie ryzkiem w bezpieczeństwie informacji odbywa się zgodnie z zasadami zawartymi w ***Załączniku nr 7 Procedura szacowania ryzyka***.

Ocena skutków jest wykonywana zgodnie z metodologią wskazaną przez Urząd Ochrony Danych Osobowych.

6.4 Rodzaje przetwarzanych informacji

W oparciu o wymagania prawne nakładane na ochronę aktywów informacyjnych obejmuje się najważniejsze grupy informacji objęte wymaganiami:

1. dane osobowe,
2. informacje publiczne,
3. informacje finansowe.

6.4.1 Dane osobowe

1. Ochrona danych osobowych realizuje wymogi następujących aktów prawnych:
   a. Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE,
   b. Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781)

   oraz Kodeksów, o których mowa w art. 40 RODO.
2. Informacje do użytku wewnętrznego i przekazywane na zewnątrz Jednostki Organizacyjnej należy chronić pod względem utrzymania odpowiedniego poziomu poufności, integralności i dostępności.
3. Ochrona danych osobowych prowadzona jest zgodnie z niniejszą ***Polityką Bezpieczeństwa Informacji***.

6.4.2 Informacje publiczne

1. Ochrona informacji publicznych realizuje wymogi: Ustawy o dostępie do informacji publicznej z dnia 6 września 2001 roku o dostępie do informacji publicznych (Dz. U. z 2019 r. poz. 1429 ze zm.).
2. Informacje publiczne należy chronić pod względem utrzymania odpowiedniego poziomu integralności oraz dostępności.
3. Zasady przetwarzania informacji publicznych są realizowane zgodnie z regulacjami wewnętrznymi, a ochrona jest prowadzona zgodnie z niniejszą ***Polityką Bezpieczeństwa Informacji***.

6.4.3 Informacje finansowe

1. Ochrona informacji finansowych realizuje wymogi następujących aktów prawnych:
   a. Ustawy z dnia 29 września 1994 roku o rachunkowości (Dz. U. z 2019 r. poz. 351 ze zm.).
   b. Ustawy z dnia 27 sierpnia 2009 roku o finansach publicznych (Dz. U. z 2019 r. poz. 869 ze zm.).
   c. Ustawy z dnia 7 września 2001 roku o systemie oświaty (Dz. U. z 2020 r. poz. 1327).
   d. Oraz innych mających zastosowanie w jednostce (do wskazania przez Jednostkę)
2. Zasady przetwarzania informacji finansowych są realizowane zgodnie z regulacjami wewnętrznymi, a ochrona jest prowadzona zgodnie z niniejszą ***Polityką Bezpieczeństwa Informacji.***

6.5 Ocena skutków

1. Jeżeli operacje przetwarzania mogą wiązać się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, przeprowadza się ocenę skutków dla ochrony danych w celu oszacowania w szczególności źródła, charakteru, specyfiki i powagi tego ryzyka. Wyniki oceny uwzględniane są przy określaniu odpowiednich środków, które należy zastosować, by wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z wymogami prawa powszechnie obowiązującego. Jeżeli ocena skutków dla ochrony danych wykaże, że operacje przetwarzania powodują wysokie ryzyko, którego nie może zminimalizować odpowiednimi środkami z punktu widzenia dostępnej technologii i kosztów wdrożenia, przed przetwarzaniem należy skonsultować się z Prezesem Urzędu Ochrony Danych.
2. Przy ocenie skutków należy uwzględnić charakter, zakres, kontekst i cele przetwarzania oraz źródła ryzyka. Ocena skutków powinna w szczególności obejmować planowane środki, zabezpieczenia i mechanizmy mające minimalizować to ryzyko, zapewniać ochronę danych osobowych oraz wykazać przestrzeganie przepisów prawa powszechnie obowiązującego i aktów prawa wewnętrznego.
3. Ocena skutków przeprowadzana jest w szczególności dla operacji przetwarzania:
   a. które ze względu na swój charakter, zakres, kontekst i cele mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych; takie rodzaje operacji przetwarzania obejmują w szczególności operacje, które wiążą się w szczególności z użyciem nowych technologii,
   b. o dużej skali – które służą przetwarzaniu znacznej ilości danych osobowych i które mogą wpłynąć na dużą liczbę osób, których dane dotyczą, oraz które mogą powodować wysokie ryzyko, na przykład (ze względu na swój szczególny charakter), gdy zgodnie ze stanem wiedzy technicznej stosowana jest na dużą skalę nowa technologia – oraz do innych operacji przetwarzania powodujących wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, w szczególności gdy operacje te utrudniają osobom, których dane dotyczą, wykonywanie przysługujących im praw,
   c. w których dane osobowe przetwarza się w celu podjęcia decyzji wobec konkretnej osoby fizycznej po dokonaniu systematycznej, kompleksowej oceny czynników osobowych osób fizycznych na podstawie profilowania tych danych lub po przetworzeniu szczególnych kategorii danych osobowych, danych biometrycznych lub danych osobowych dotyczących wyroków skazujących, naruszeń prawa lub odnośnych,

d. w przypadku monitorowania na dużą skalę miejsc publicznie dostępnych – w szczególności za pomocą urządzeń optyczno-elektronicznych – lub wszelkich innych operacji, względem których Prezes Urzędu Ochrony Danych uznaje, że przetwarzanie może powodować wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, w szczególności dlatego, że operacje te uniemożliwiają osobom, których dane dotyczą, wykonywanie prawa lub korzystania z usługi lub umowy lub mają systematyczny charakter i dużą skalę.

4. Przeprowadzając ocenę skutków odpowiedzieć sobie należy na następujące pytania:

   a. czy przetwarzane dane podlegają profilowaniu (m.in. czy dokonywana jest ocena lub przyznawana jest punktacja na podstawie przewidywań administratora w związku z profilowaniem danych, szczególnie jeżeli prognozowanie dotyczy efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą);

   b. czy przetwarzanie danych obejmuje automatyczne podejmowanie decyzji, które wywierają znaczący wpływ na prawa osoby, której dotyczą;

   c. czy wykonywany jest systematyczny monitoring na dużą skalę miejsc dostępnych publicznie;

   d. czy przetwarzane są dane szczególnych kategorii, o których mowa w art. 9 RODO lub dane dotyczące wyroków skazujących, naruszeń prawa lub związanych z tym środków bezpieczeństwa;

   e. czy zbiory danych podlegają łączeniu;

   f. czy dane osobowe są przetwarzane z wykorzystaniem innowacyjnych technologii lub z wykorzystaniem innowacyjnych środków organizacyjnych, w szczególności dotyczących identyfikacji osób fizycznych z zastosowaniem linii papilarnych lub z wykorzystaniem biometrii

   g. czy dane są przekazywane poza Unię Europejską;

   h. czy dane są przetwarzane na dużą skalę;

   i. czy operacje przetwarzania utrudniają osobom, których dane dotyczą, wykonywanie przysługującym ich praw.

W przypadku pozytywnej odpowiedzi na co najmniej dwa z ww. pytań przeprowadzenie oceny skutków jest obowiązkowe.

5. Przez sformułowanie „przetwarzaniem na dużą skalę" rozumie się przetwarzanie spełniające łącznie następujące przesłanki:

   a. liczba podmiotów danych jest znaczna „liczbowo" lub jako proporcja pewnej populacji,

   b. ilość danych lub zakres różnych danych jest znaczący,

   c. czas przetwarzania jest znaczący,

   d. geograficzny zakres przetwarzanych danych jest szeroki.

6. Ocena skutków nie jest wymagana w przypadku, gdy przetwarzanie nie prowadzi do wysokiego ryzyka naruszenia praw i wolności osób, a zostało już dopuszczone w bardzo podobnym procesie przetwarzania, ma podstawę prawną w prawie Unii Europejskiej lub w państwie członkowskim lub gdy przetwarzanie znajduje się na liście operacji zwolnionych z oceny skutków przez organ nadzorczy, który ustala i podaje do publicznej wiadomości wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych.

7 Ochrona danych osobowych

1. Przetwarzanie danych osobowych, zgodnie z celem działalności, jest możliwe, jeżeli jest to niezbędne do wypełnienia usprawiedliwionych interesów Administratora, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Przetwarzanie jest również dozwolone, gdy osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych lub jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą. W szczególności można przetwarzać dane osobowe, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa, a także gdy jest to niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego.

2. Osoby przetwarzające zgromadzone dane są zobowiązane w szczególności do:

   a. przetwarzania danych zgodnie z aktami prawa powszechnie obowiązującego lub aktami prawa wewnętrznego, w zakresie zgodnym z upoważnieniem podpisanym przez Administratora lub Prezydenta Miasta Lublin,

   b. przechowywania danych osobowych we właściwych zbiorach danych, zgodnie z celem utworzenia zbiorów;

   c. modyfikowania i usuwania danych, zgodnie z wnioskiem złożonym przez osobę, której dane dotyczą oraz ograniczenia przetwarzania danych.

8 Struktura zbiorów danych osobowych przetwarzanych w Jednostce Organizacyjnej określająca zawartość pól informacyjnych

Dokument jest tworzony i utrzymywany przez IOD zgodnie postanowieniami ***Regulaminu Systemu Informatycznego Jednostki Organizacyjnej Gminy Lublin***.

9 Strefy przetwarzania danych osobowych

Dane osobowe są przetwarzane w określonych strefach przetwarzania. Wykaz budynków, pomieszczeń i części pomieszczeń, w których przetwarzane są dane osobowe, jest tworzony i aktualizowany przez IOD zgodnie ze wzorem zawartym w ***Załączniku nr 2 do Polityki Bezpieczeństwa Informacji***.

9.1 Dane osobowe zwykłe i wrażliwe – szczególnej kategorii

1. Przetwarzanie danych wrażliwych jest dopuszczalne wyłącznie po spełnieniu następujących warunków:

   1) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów,

   2) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy; c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze,

3) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,

4) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi.

2. Przesłanką legalności przetwarzania szczególnych kategorii danych osobowych mogą być tylko warunki, o których mowa w art. 9 RODO.

9.2 Organizacja ochrony danych osobowych

1. Administrator Danych Osobowych odpowiada za zakres i bezpieczeństwo przetwarzania danych osobowych w Jednostce Organizacyjnej.

2. Administrator jest odpowiedzialny za przestrzeganie przepisów RODO i musi być w stanie wykazać ich przestrzeganie (tzw. zasada rozliczalności RODO). Administrator zapewnia:

   a. przetwarzanie danych osobowych zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość"),

   b. zbieranie danych osobowych w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami („ograniczenie celu").

   c. adekwatność danych osobowych; dane osobowe powinny być stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych").

   d. prawidłowość danych osobowych i w razie potrzeby ich uaktualnianie; podejmuje wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość").

   e. przechowywanie danych osobowych w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania").

   f. przetwarzanie 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").

3. Administrator zapewnia i stosuje odpowiednie środki informatyczne, techniczne i organizacyjne zapewniając ochronę przetwarzanych danych osobowych odpowiednią do wyników analizy ryzyka, a w szczególności:

   a. podejmuje decyzje o celach i środkach przetwarzanie danych osobowych,

   b. podejmuje decyzje o technicznych i organizacyjnych zabezpieczeniach oraz wdraża zasady i procedury postępowania mające na celu zapewnienie adekwatnego poziomu bezpieczeństwa przetwarzanych danych,

   c. upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnym zakresie, odpowiadającym zakresowi jej obowiązków,

   d. wyznacza Administratora Systemów Informatycznych oraz określa zakres jego zadań i czynności w zakresie ochrony danych osobowych w Systemie Jednostki oraz Systemach CPD Jednostki,

   e. podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia bezpieczeństwa danych osobowych,

   f. prowadzi kontrolę przestrzegania procedur przetwarzania danych osobowych,

   g. zapewnia środki techniczne oraz organizacyjne w celu zapewnienia działań wymaganych przez przepisy prawa dotyczące ochrony danych osobowych;

   h. zapewnia realizację praw osób, których dane osobowe są przetwarzane (m.in. prawo wglądu, poprawiania danych i wniesienia sprzeciwu wobec przetwarzanych danych),

   i. reprezentuje Jednostkę Organizacyjną w postępowaniach przed organami publicznymi oraz w kontaktach z podmiotami trzecimi w sprawach związanych z pozyskiwaniem, przetwarzaniem, ochroną i powierzeniem danych osobowych,

   j. analizuje sprawozdania Inspektora Ochrony Danych, weryfikuje ocenę ryzyka i ocenę skutków związane z przetwarzaniem danych osobowych, a także decyduje o formach przeciwdziałania ewentualnym zagrożeniom,

   k. zapewnia udział osób o odpowiednich kompetencjach i wiedzy (pracowników Administratora i podmiotów zewnętrznych) przy realizacji audytów i weryfikacji systemu ochrony danych osobowych prowadzonego przez Inspektora Ochrony Danych.,

   l. zapewnia bezpieczne usunięcie danych osobowych w przypadku uzasadnionego żądania niezwłocznego usunięcia danych osobowych, bez zbędnej zwłoki.

9.3 Powołanie Inspektora Ochrony Danych

1. Administrator powołuje Inspektora Ochrony Danych, który jest odpowiedzialny za nadzór nad stosowaniem środków organizacyjnych i technicznych, zapewniających ochronę przetwarzanych danych, w szczególności przed

ich udostępnieniem osobom nieupoważnionym, przetwarzaniem z naruszeniem ustawy, kradzieżą, uszkodzeniem lub zniszczeniem.

2. Inspektor Ochrony Danych powinien:

   a. posiadać pełną zdolność do czynności prawnych oraz korzystać z pełni praw publicznych,

   b. posiadać fachową wiedzę na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO, ustawie i aktach prawa wewnętrznego

   c. wykonywać zadania niezależnie i bez konfliktu interesów,

   d. mieć wiedzę w zakresie europejskiego i krajowego prawa ochrony danych oraz praktyk ochrony danych, a także szczegółową wiedzę na temat RODO,

   e. posiadać wiedzę na temat systemów informatycznych służących do przetwarzania, a także potrzeb i sposobów zabezpieczania danych osobowych przetwarzanych

   i nie może być karany za przestępstwo popełnione z winy umyślnej.

3. Kierownik Jednostki Organizacyjnej może powierzyć Inspektorowi Ochrony Danych wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania zadań, o których mowa w niniejszej Polityce.

4. W przypadku powołania Inspektora Ochrony Danych Osobowych Administrator jest zobowiązany dokonać stosownego zgłoszenia zgodnie z wymogami prawa powszechnie obowiązującego. Jego wykreślenie z Rejestru następuje po powiadomieniu Prezesa Urzędu Ochrony Danych Osobowych o jego odwołaniu przez Administratora albo w przypadku jego śmierci.

9.4 Obowiązki Inspektora Ochrony Danych

1. Inspektor Ochrony Danych realizuje obowiązki zgodnie z wymaganiami obowiązującego prawa przy uwzględnieniu ryzyka i oceny skutków związanych z czynnościami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

2. Osoby, których dane są gromadzone i przetwarzane, mogą kontaktować się z Inspektorem Ochrony Danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy przepisów prawa powszechnie obowiązującego i aktów prawa wewnętrznego.

3. Inspektor Ochrony Danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z przepisami prawa powszechnie obowiązującego i regulacjami wewnętrznymi.

4. Inspektor Ochrony Danych zobowiązany jest w szczególności do:

a) informowania Administratora oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy powszechnie obowiązujących przepisów prawa oraz aktów prawa wewnętrznego w zakresie ochrony danych osobowych i doradzanie im w tej sprawie,

b) nadzorowania i monitorowania przestrzegania przepisów prawa o ochronie danych oraz aktów prawa wewnętrznego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu Administratora i podmiotów trzecich uczestniczącego w operacjach przetwarzania oraz powiązanych z tym audytów,

c) udziału w ocenie skutków dla ochrony danych zgodnie z art. 35 RODO oraz monitorowanie wykonania zaleceń opracowanych w wyniku wykonania oceny,

d) współpracy z organem nadzorczym,

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

f) weryfikacji zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie, co najmniej raz na kwartał rok sprawozdania dla Administratora lub częściej jeśli wyniki analizy ryzyka wskazują na taką konieczność,

g) przygotowywania do 15 grudnia każdego roku Planu sprawdzeń (audytów) na następny rok i przedstawienie go Administratorowi, a po akceptacji jego realizację; plan sprawdzeń jest określeniem harmonogramu weryfikacji systemu ochrony danych osobowych i w okresie pięciu lat sprawdzenia powinny łącznie objąć:

   - zabezpieczenia: organizacyjne i techniczne zbiorów danych osobowych,
   - system informatyczny służący do przetwarzania danych osobowych,
   - kompletność zidentyfikowanych zbiorów danych osobowych,
   - przesłanki legalności przetwarzania danych osobowych,
   - przesłanki legalności przetwarzania danych szczególnie chronionych,
   - zakres i cel przetwarzania danych,
   - merytoryczna poprawność danych i ich adekwatność do celu przetwarzania,
   - obowiązek informacyjny,
   - profilowanie,
   - przekazywanie danych do państwa trzeciego, w tym do krajów spoza Unii Europejskiej,

- powierzenie przetwarzania danych osobowych (w tym zakres i poprawność konstruowania umów powierzenia przetwarzania danych),
- zabezpieczenia danych: organizacyjne i techniczne,
- zgodność dokumentacji przetwarzania danych osobowych z obowiązującymi przepisami prawa powszechnie obowiązującego i stosowanymi w Jednostce Organizacyjnej zabezpieczeniami, technologiami, systemami i itp.,

obowiązek ten realizowany jest zgodnie z ***Załącznikiem nr 3 do PBI – Procedurą sprawdzeń,***

h) opracowania i aktualizowania Polityki Bezpieczeństwa Danych Osobowych oraz współudział w opracowaniu i aktualizowaniu Polityki Bezpieczeństwa Systemów Informatycznych wraz z dokumentami związanymi z przetwarzaniem danych osobowych,

i) wspieranie administratora w realizacji przygotowywaniu odpowiedzi na żądania osób, których dane dotyczą, uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma miejsce, uzyskanie dostępu do nich wraz z zakresem właściwych informacji o danych osobowych,

j) informowania o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania osób, które wystąpiły z takim żądaniem,

k) prowadzenia i aktualizacji Rejestru czynności przetwarzania, zgodnie ze wzorem zawartym w ***Załączniku nr 8 do PBI,***

l) prowadzenia i aktualizacji Rejestru kategorii przetwarzania (w przypadku, gdy ma to zastosowanie), z zgodnie ze wzorem zawartym **w Załączniku nr 10 do PBI,**

m) prowadzenia i aktualizacji Rejestru naruszeń bezpieczeństwa, zgodnie ze wzorem **wskazanym w Załączniku nr 9 do PBI,**

n) przygotowania i przekazywania do podpisu do Administratora zgłaszania o naruszeniu ochrony danych osobowych do organu nadzorczemu oraz zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych – zgodnie z postanowieniami art. 33 i 34 RODO,

o) prowadzenia i aktualizacji Rejestru umów powierzenia przetwarzania danych, zgodnie ze wzorem wskazanym w ***Załączniku nr 4 do PBI,***

p) nadzorowania i monitorowania procesu profilowania,

q) opiniowania umów zawieranych z podmiotami trzecimi w zakresie ich zgodności z przepisami prawa powszechnie obowiązującego i wewnętrznego w zakresie ochrony danych osobowych i w porozumieniu z Kierownikiem

Komórki Organizacyjnej zakresu dostępu podmiotu trzeciego do danych osobowych udzielanego na mocy zawieranej umowy (w tym umów powierzenia przetwarzania),

r) uzgadniania z pracownikami i współpracownikami podmiotów trzecich przed zawarciem umowy lub niezwłocznie po jej zawarciu zasad dostępu do danych osobowych gromadzonych przez Jednostkę Organizacyjną oraz zasad dostępu do nich i ich przetwarzania,

s) nadzorowania i monitorowania realizacji obowiązku informacyjnego, zgodnie z wymogami RODO,

t) prowadzenia Rejestru zgłoszonych sprzeciwów dotyczących przetwarzania danych osobowych i wniosków o zaprzestanie lub ograniczenie przetwarzania danych,

u) informowanie Administratora o wystąpieniu incydentu,

v) przygotowania wzorów klauzul informacyjnych i umów powierzenia przetwarzania danych oraz dystrybucja ich do komórek organizacyjnych,

w) gromadzenia potwierdzenia (dotyczy formy papierowej) wywiązania się z obowiązku informacyjnego oraz weryfikacji prawidłowości gromadzenia potwierdzeń w systemach informatycznych,

x) prowadzenia Ewidencji upoważnień do przetwarzania danych osobowych oraz dokumentacji związanej z udzielaniem upoważnień, zgodnie ze wzorem zawartym w ***Załączniku nr 5 do PBI,***

y) przygotowywania upoważnień do przetwarzania danych osobowych zgodnie ze wzorem zawartym w ***Załączniku nr 6 do PBI.***

z) wspierania Administratora w wykazaniu jednej z przesłanek przetwarzania danych osobowych, o których mowa w art. 6–11 RODO,

aa) wykonania szacowania ryzyka i oceny skutków przed wprowadzeniem nowej technologii w Jednostce Organizacyjnej (np. nowego systemu informatycznego, w którym przetwarzane będą dane osobowe) wraz z administratorem systemu i właścicielem zasobu.

5. Szczegółowy zakres zadań realizowanych przez Inspektora Ochrony Danych określony jest w jego zakresie obowiązków.

6. W przypadku, gdy w Dokumentacji nie określono wzorów dla prowadzenia określonych rejestrów, ewidencji czy też innych dokumentów Inspektor Ochrony Danych prowadzi ją zgodnie z opracowanymi przez siebie wzorami.

7. Inspektor Ochrony Danych jest uprawniony w szczególności do:
   a) wstępu do pomieszczeń, w których przetwarzane są dane osobowe,
   b) wstępu do pomieszczeń, w których gromadzone są informacji o przetwarzaniu danych osobowych,
   c) odbierania wyjaśnień od osób przetwarzających dane osobowe,

d) dokumentowania ustaleń i dokonywania innych czynności niezbędnych do wykonania jego zadań wynikających z RODO, Ustawy, aktów prawa wewnętrznego i zakresu jego obowiązków/zakresu umowy o świadczenie usług.

Szczegółowy zakres uprawnień Inspektora Ochrony Danych określa RODO i Ustawa.

9.5 Sposób udzielania upoważnień do przetwarzania danych osobowych

1. Do przetwarzania danych osobowych mogą być dopuszczone tylko osoby upoważnione przez Administratora, który w zależności od potrzeb jednostki może opracować procedurę nadawania upoważnień do przetwarzania danych osobowych uwzględniającą sposób nadawania uprawnień do systemów teleinformatycznych. Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana przestrzegać następujących zasad:

   a. przed rozpoczęciem przetwarzania należy złożyć oświadczenie o zapoznaniu się z dokumentacją ochrony danych osobowych,

   b. dane osobowe można przetwarzać wyłącznie w zakresie ustalonym indywidualnie przez Kierownika Jednostki Organizacyjnej oraz Prezydenta Miasta Lublin zawartym w upoważnieniu i tylko w celu wykonywan[illegible] obowiązków służbowych,

   c. przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia, a także po ustaniu stosunku pracy lub odwołania z pełnionej funkcji, przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres realizacji umowy, a także po zakończeniu jej realizacji,

   d. stosowanie określonych przez Administratora procedur oraz wytycznych mających na celu przetwarzanie danych zgodnie z obowiązującym prawem,

   e. zabezpieczenie danych osobowych przed udostępnieniem osobom nieupoważnionym.

2. Sposób nadawania adekwatnych uprawnień w systemach jest opisany w ***Regulaminie Systemu Informatycznego Jednostki Organizacyjnej Gminy Lublin.*** Za realizację procedury nadawania uprawnień odpowiedzialny *jest* IOD oraz ASI, którym należy zgłaszać zapotrzebowanie na zmia[illegible] zakresu upoważnień do przetwarzania danych osobowych oraz uprawnień do systemów.

3. Zakres dostępu do danych gromadzonych w Systemie Jednostki przypisany jest do niepowtarzalnych identyfikatorów użytkownika, niezbędnych do pracy w systemach oraz aplikacjach, do których Użytkownik otrzymał stosowne uprawnienia na podstawie podpisanego upoważnienia do przetwarzania danych.

4. W aktach osobowych pracownika przechowuje się egzemplarz oryginalny upoważnienia do przetwarzania danych osobowych podpisany własnoręcznie przez pracownika, co jednocześnie jest potwierdzeniem, że pracownik przyjął treść upoważnienia do wiadomości,

5. Rozwiązanie stosunku pracy lub odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych. Zakończenie współpracy z podmiotem trzecim powoduje wygaśnięcie upoważnienia do przetwarzania danych udzielonych pracownikom i współpracownikom tego podmiotu.

6. W przypadku naruszenia przez pracownika/użytkownika przepisów lub zasad postępowania może podlegać on odpowiedzialności służbowej i karnej.

7. Upoważnienia do przetwarzania danych osobowych udzielane są również wolontariuszom, praktykantom, stażystom. Oryginał upoważnienia przechowywany jest w Jednostce. Zakończenie stażu, praktyki, wolontariatu powoduje wygaśniecie upoważnienia.

8. Upoważnienia do przetwarzania danych osobowych udzielane są również pracownikom podmiotów trzecich, które na mocy zawartych umów otrzymują dostęp do danych zgromadzonych przez Jednostkę Organizacyjną lub którym powierzono przetwarzanie danych osobowych. Postanowienia pkt 1-3 stosuje się odpowiednio, z zastrzeżeniem że upoważnienia te przechowywane są w Jednostce.

9.6 Zbieranie danych osobowych

1. Dane osobowe przetwarzane w Jednostce Organizacyjnej mogą być pozyskiwane bezpośrednio od osób, których te dane dotyczą. W przypadku zbierania danych osobowych nie od osoby, której te dane dotyczą, należy zapewnić, że istnieje podstawa prawna przetwarzania danych.

2. Pozyskiwanie danych osobowych ze źródeł wymienionych w pkt 1 oraz innych źródeł jest dopuszczalne wyłącznie w granicach określonych odpowiednimi przepisami prawa.

3. Przetwarzanie i przechowywanie danych osobowych powinno odbywać się w postaci umożliwiającej identyfikację osób, których dotyczą.

4. Przetwarzanie i przechowywanie danych osobowych powinno odbywać się nie dłużej niż jest to niezbędne do realizacji celu przetwarzania.

5. Dane osobowe, które są zbierane powinny być merytorycznie poprawne.

6. Zakres danych osobowych, które są zbierane, powinien być adekwatny w stosunku do celu, w jakim dane zostały zebrane.

7. Zebrane dane po ich wykorzystaniu mogą być przechowywane w przypadku, gdy uprzednio zostaną poddane procesowi anonimizacji, czyli procesowi, który ma na celu uniemożliwienie identyfikacji osób, których dotyczą dane.

8. Zebrane dane po ich wykorzystaniu mogą być przechowywane w przypadku, gdy odpowiedni przepis prawa wymaga ich archiwizacji przez określony czas.

9. Przetwarzanie danych osobowych kandydata do pracy jest możliwe podczas procesu rekrutacji wyłącznie po uzyskaniu jego pisemnego oświadczenia zawierającego zgodę na przetwarzanie jego danych osobowych w celu

przeprowadzenia procesu rekrutacyjnego lub przyszłych procesów rekrutacyjnych. W przypadku wymagań wynikających z zapisów odpowiednich przepisów prawa, po zakończeniu procesu rekrutacji dokumenty zawierające dane osobowe kandydatów do pracy są archiwizowane zgodnie z zapisami tych przepisów.

9.7 Zgody na przetwarzanie danych osobowych

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.

1. Zgoda powinna być dobrowolna.
2. Zgoda nie jest uważana za dobrowolną, gdy:
   a. istnieje wyraźny brak równowagi między osobą, której dane dotyczą, a administratorem, w szczególności gdy administrator jest organem publicznym i dlatego jest mało prawdopodobne, by w tej konkretnej sytuac zgodę wyrażono dobrowolnie we wszystkich przypadkach.
   b. nie można jej wyrazić z osobna na różne operacje przetwarzania danych osobowych, mimo że w danym przypadku byłoby to stosowne,
   c. od zgody uzależnione jest wykonanie umowy – w tym świadczenie usługi – mimo że do jej wykonania zgoda nie jest niezbędna.

9.8 Obowiązek informacyjny

1. Administrator zobowiązany jest na etapie gromadzenia danych (niezależnie od tego, czy zbiera je bezpośredniego od osób, których one dotyczą, czy też pozyskania ich od podmiotu trzeciego) powiadomić osoby, których dane gromadzi o przysługujących im prawach oraz przekazać informacje o zasadach i celu przetwarzania danych osobowych (wypełnienie „obowiązków informacyjnych" wskazanych w art. 12, 13, 14, 22 i 25 RODO).
2. Zgodnie z art. 13 ust. 1 i 2 RODO, do niezbędnych elementów informacyjnych zaliczyć należy podanie:
   a. nazwy i adresu Administratora oraz adresu poczty elektronicznej i numeru faksu i telefonu oraz gdy ma to zastosowanie, tożsamości i danych kontaktowych przedstawiciela Administratora,
   b. danych kontaktowych Inspektora Ochrony Danych, jeżeli został powołany,
   c. celu przetwarzania danych osobowych oraz podstawy prawnej przetwarzania,
   d. informacji o odbiorcach danych osobowych lub o kategoriach odbiorców,
   e. informacji o zamiarze transferu danych osobowych do państwa trzeciego, ze szczególnym uwzględnieniem:
      - przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej,

- stwierdzenia lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony lub - w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO - wzmianki o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych,

f. okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteriach ustalania tego okresu;

g. informacji 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;

h. jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO – informacji o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,

i. informacji o prawie wniesienia skargi do organu nadzorczego;

j. informacji 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;

k. informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, 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.

3. W przypadku zbierania danych osobowych z innego źródła niż od osoby, której dane dotyczą, zgodnie z art. 14 ust. 1 i 2 RODO, informacja powinna być poszerzona o:

   a. kategorie odnośnych danych osobowych;

   b. źródle pochodzenia danych osobowych, a jeżeli ma to zastosowanie, o pochodzeniu ich ze źródeł powszechnie dostępnych.

4. Informacje, o której mowa w pkt 2 i 3 każdorazowo należy przekazać indywidualnie osobie, której dane dotyczą przed podjęciem działań z jej danymi, a także dokumentować (najlepiej na piśmie podpisanym przez osobę, której dane dotyczą), że obowiązek informacyjny został wypełniony. Jeśli zamiast formy papierowej do gromadzenia danych wykorzystuje się systemem informatyczny to musi on zapewniać zapisanie w trwałej i wiarygodnej formie, że osoba podająca swoje dane za jego pomocą uzyskała informacje w zakresie określonym w przepisach prawa powszechnie obowiązującego. Klauzula powinna być zrozumiała dla osób, których dane mają być gromadzone i przetwarzane. Poświadczenie wykonania obowiązku informacyjnego może polegać na wypełnieniu odpowiednich formularzy (w tym w formie elektronicznej). Istotne jest, aby pola potwierdzające wyrażenie zgody na zbieranie i przetwarzanie danych w formularzu nie były domyślnie zaznaczane.

5. Treść klauzuli należy skonsultować każdorazowo z Inspektorem Ochrony Danych w celu potwierdzenia zgodności z obowiązującymi przepisami prawa powszechnie obowiązującego.

6. Informowanie powinno się dokonać bez prośby zainteresowanego. Powinno być ono wykonane w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Należy uwzględniać także to, że informowana osoba musi mieć możliwość wniesienia sprzeciwu wobec przetwarzania jej danych i należy stworzyć jej warunki do wyrażenia tego sprzeciwu.

7. Wykonanie obowiązku informacyjnego jest zadaniem osoby przyjmującej dane osobowe, która po otrzymaniu potwierdzenia jego wykonania (w przypadku gdy realizowany jest on w formie papierowej) przekazuje dowód wykonania obowiązku informacyjnego do Inspektora Ochrony Danych.

8. Inspektor Ochrony Danych zobowiązany jest do niezwłocznego i kompleksowego dokonania przeglądu danych zgromadzonych i przetwarzanych w danej Jednostce Organizacyjnej oraz stosowanych klauzul informacyjnych i poinformować o wynikach przeglądu Administratora. W przypadku stwierdzenia, że stosowane dotychczas klauzule informacyjne nie spełniają wymogów określonych w art. 12, 13, 14, 22 i 25 RODO, osoby, których dane zgromadzone i przetwarzane muszą zostać poinformowane o przysługujących im prawach stosownie do wymogów RODO. Obowiązek ten ma zostać wypełniony do dnia 25 maja 2018 r.

9.9 Informowanie o przetwarzanych danych osobowych

1. Każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych osobowych przetwarzanych i przechowywanych w Jednostce Organizacyjnej, a zwłaszcza prawo do uzyskania wyczerpującej informacji o przetwarzanych danych osobowych, które jej dotyczą.

2. Na wniosek osoby, której dane dotyczą, Kierownik Jednostki Organizacyjnej jest zobowiązany do udzielania informacji zgodnie z pkt. 1 Informacja powinna być udzielona formie pisemnej oraz powszechnie zrozumiałej.

3. W razie wniesienia żądania oraz wykazania przez osobę, której dane osobowe dotyczą, że jej dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, administrator danych osobowych, bez zbędnej zwłoki, dokonać uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, chyba że dotyczy to danych osobowych, w odniesieniu do których tryb ich uzupełnienia, uaktualnienia lub sprostowania określają odrębne przepisy.

4. Osoba, której dane dotyczą, ma prawo wniesienia sprzeciwu wobec przetwarzania jej danych w przypadkach przetwarzania niezbędnego do wykonania określonych prawem zadań realizowanych dla dobra publicznego lub niezbędnego dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.

5. W przypadku opisanym w pkt 4 dalsze przetwarzanie kwestionowanych danych jest niedopuszczalne. Kierownik Jednostki Organizacyjnej może jednak pozostawić w zbiorze imię lub imiona i nazwisko osoby oraz numer PESEL lub adres wyłącznie w celu uniknięcia ponownego wykorzystania danych tej osoby w celach objętych sprzeciwem.

9.10 Powierzanie przetwarzania danych osobowych

1. Administrator:

   a. przekazuje dane do podmiotów trzecich zgodnie z przepisami prawa powszechnie obowiązującego, w szczególności do: Zakładu Ubezpieczeń Społecznych, Urzędu Skarbowego, Państwowej Inspekcji Pracy, sądów powszechnych, Policji, Agencji Bezpieczeństwa Wewnętrznego, Centralnego Biura Antykorupcyjnego,

   b. powierza przetwarzanie danych osobowych innemu podmiotowi w drodze umowy zawartej w na piśmie, która określa zasady przetwarzania i zabezpieczenia danych osobowych.

2. Umowa powierzenia danych osobowych do przetwarzania musi być zawarta zgodnie ze wzorem obowiązującym w Jednostce będącym ***Załącznikiem nr 1 do Polityki Bezpieczeństwa Informacji Jednostki Organizacyjnej Gminy Lublin***.

3. W przypadku zawarcia umowy powierzenia przetwarzania danych osobowych z podmiotem trzecim, ADO jednocześnie zobowiązuje ten podmiot w formie pisemnej do zachowania poufności powierzanych do przetwarzania danych osobowych oraz sposobów ich zabezpieczeń. Zobowiązanie powinno pozostać w mocy również po zakończeniu przetwarzania.

4. Podmiot, któremu powierzono przetwarzanie danych osobowych, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

5. Podmiot, któremu powierzono przetwarzanie danych osobowych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie ryzyka dla danych objętych ochroną, a w szczególności powinien stosować techniczne i organizacyjne środki bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO .

9.11 Współadministrowanie danymi

1. W przypadku wspólnego przetwarzanie danych w zbiorach przez Jednostkę Organizacyjną z innym podmiotem, na mocy zawartej umowy lub porozumienia, ustalają one wspólnie cele i sposoby przetwarzania danych (są współadministratorami danych). W drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z przepisów prawa powszechnie obowiązującego oraz aktów prawa wewnętrznego obowiązujących w obu podmiotach, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14 RODO,

chyba że przypadające im obowiązki i ich zakres określa prawo powszechnie obowiązujące. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą.

2. Uzgodnienia, o których mowa w pkt 1, należycie odzwierciedlają odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a osobami, których dane dotyczą. Zasadnicza treść uzgodnień jest udostępniana osobom, których dane dotyczą.

3. Niezależnie od uzgodnień, o których mowa w pkt 1, osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wynikające z przepisów prawa powszechnego wobec każdego z Administratorów.

4. Informacja o współadministrowaniu zbiorem danych (wskazanie współadministratorów) odnotowywane jest w Rejestrze Czynności Przetwarzania.

9.12 Przekazanie danych do państwa trzeciego lub organizacji międzynarodowej

1. Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić, gdy Komisja Europejska stwierdzi, że to państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Takie przekazanie nie wymaga specjalnego zezwolenia.

2. W razie braku decyzji, o której mowa w pkt 1 Administrator lub podmiot przetwarzający mogą przekazać dane osobowe do państwa trzeciego lub organizacji międzynarodowej wyłącznie, gdy zapewnią odpowiednie zabezpieczenia, i pod warunkiem, że obowiązują egzekwowalne prawa osób, których dane dotyczą i skuteczne środki ochrony prawnej.

3. W razie braku decyzji stwierdzającej odpowiedni stopień ochrony określonej w pkt 1 oraz braku odpowiednich zabezpieczeń, o których mowa w pkt 2, w tym wiążących reguł korporacyjnych, jednorazowe lub wielokrotne przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej mogą nastąpić wyłącznie pod warunkiem, że:

   a) osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którymi – ze względu na brak decyzji stwierdzającej odpowiedni stopień ochrony oraz na brak odpowiednich zabezpieczeń – może się dla niej wiązać proponowane przekazanie, wyraźnie wyraziła na nie zgodę,

   b) przekazanie jest niezbędne do wykonania umowy między osobą, której dane dotyczą, a administratorem lub do wprowadzenia w życie środków przedumownych podejmowanych na żądanie osoby, której dane dotyczą,

   c) przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, których dane dotyczą, między administratorem a inną osobą fizyczną lub prawną,

   d) przekazanie jest niezbędne ze względu na ważne względy interesu publicznego,

   e) przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń,

f) przekazanie jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą, lub innych osób, jeżeli osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody lub przekazanie następuje z rejestru, który zgodnie z prawem Unii lub prawem państwa członkowskiego ma służyć za źródło informacji dla ogółu obywateli i który jest dostępny dla ogółu obywateli lub dla każdej osoby mogącej wykazać prawnie uzasadniony interes – ale wyłącznie w zakresie, w jakim w danym przypadku spełnione zostały warunki takiego dostępu określone w prawie Unii lub w prawie państwa członkowskiego.

4. Szczegółowe zasady przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej określone zostały określone w RODO. O wyrażenie zgody na przekazanie danych występuje właściciel zbioru, wskazując cel i zakres przekazywanych danych. Zgodę na ich przekazanie do państwa trzeciego lub organizacji międzynarodowej może wydać Kierownik Jednostki Organizacyjnej po zasięgnięciu opinii Inspektora Ochrony Danych. Administrator zobowiązany jest bezwzględnie przestrzegać postanowień RODO przy przekazywaniu danych do państwa trzeciego lub organizacji międzynarodowej.

10 Kontrola dostępu

Zarządzanie kontrolą dostępu jest realizowane poprzez:

1. nadzór nad dostępem do budynków i pomieszczeń; szczegółowe zasady kontroli dostępu zostały opisane w Dokumentacji,
2. kontrolę dostępu do obszarów przetwarzania danych osobowych; szczegółowe zasady kontroli dostępu zostały opisane Dokumentacji,
3. kontrolę dostępu do sieci i systemów informatycznych; szczegółowe zasady kontroli dostępu zostały opisane w ***Regulaminie Systemu Informatycznego Jednostki Organizacyjnej Gminy Lublin,***
4. zasady nadawania uprawnień dla użytkowników; szczegółowe zasady nadawania uprawnień dla użytkowników zostały opisane w ***Regulaminie Systemu Informatycznego Jednostki Organizacyjnej Gminy Lublin,***
5. zarządzanie hasłami i innymi danymi uwierzytelniającymi, szczegółowe zarządzania hasłami i innymi danymi uwierzytelniającymi zostały opisane w ***Regulaminie Systemu Informatycznego Jednostki Organizacyjnej Gminy Lublin,***
6. politykę czystego biurka; szczegółowe wymagania polityki czystego biurka zostały zapisane w ***Regulaminie Bezpieczeństwa Informacji Jednostki Organizacyjnej Gminy Lublin,***
7. politykę czystego ekranu, szczegółowe wymagania polityki czystego ekranu zostały zapisane w ***Regulaminie Bezpieczeństwa Informacji Jednostki Organizacyjnej Gminy Lublin,***
8. kontrolę systemów i aplikacji; szczegółowe wymagania opisane zostały w ***Regulaminie Systemu Informatycznego Jednostki Organizacyjnej Gminy Lublin,***
9. zabezpieczenia kryptograficzne; szczegółowe wymagania opisane zostały w ***Regulaminie Systemu Informatycznego Jednostki Organizacyjnej Gminy Lublin.***

11 Zarządzanie systemami i sieciami

1. Wszystkie systemy informatyczne przed dopuszczeniem do wykorzystania muszą spełniać minimalne wymagania bezpieczeństwa i standardy wymienione w ***Regulaminie Systemu Informatycznego Jednostki Organizacyjnej Gminy Lublin.***
2. Dla systemów informatycznych stosowane są techniczne i organizacyjne środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.
3. Wdrażanie, eksploatacja oraz utrzymanie systemów informatycznych jest realizowane za pomocą kompetentnych i świadomych zagadnień bezpieczeństwa pracowników oraz firm zewnętrznych.
4. Prowadzona jest kontrola wprowadzanych zmian.
5. Prace testowe i rozwojowe są prowadzone na oddzielnych urządzeniach i środowiskach; prowadzenie prac rozwojowych i testowych może być realizowane przez firmy zewnętrzne na podstawie odpowiednich umów dotyczących rozwoju i utrzymania oprogramowania i aplikacji.
6. Nadzorowanie usług dostarczanych przez strony trzecie, a w szczególności wszelkich wprowadzanych do nich zmian.
7. Stosowana jest ochrona przed wirusami, rootkitami i programami typu malware.
8. Kopie zapasowe są tworzone zgodnie z przyjętymi zasadami oraz stosownie do tych zasad testowane.
9. Stosowane są zasady postępowania z nośnikami danych opisane w ***Regulaminie Systemu Informatycznego Jednostki Organizacyjnej Gminy Lublin.***
10. Monitoruje się systemy informatyczne w celu wykrycia naruszeń bezpieczeństwa informacji oraz ich zapobieganiu.
11. W sytuacji wykrycia incydentu naruszenia bezpieczeństwa stosuje się wdrożone zasady postępowania oraz mechanizmy reagowania na incydenty.
12. Szczegółowe zasady zarządzania systemami i sieciami opisane zostały w dokumencie ***Regulaminie Systemu Informatycznego Jednostki Organizacyjnej Gminy Lublin.***

12 Pozyskiwanie, rozwój i utrzymanie systemów informatycznych

1. Każdy obecny i nowy system informatyczny spełnia wymagania bezpieczeństwa zapisane w Dokumentacji. W szczególności stosuje się zasady:
   a. stosowanie minimalnych wymagań bezpieczeństwa informacji podczas zakupu lub budowy nowych systemów informatycznych,
   b. testowanie bezpieczeństwa nowych systemów przed dopuszczeniem ich do eksploatacji,
   c. nadzorowanie dostępu do kodów źródłowych oprogramowania,
   d. dbałość o aktualizacje oprogramowania,
   e. minimalizowanie ryzyka utraty informacji w wyniku awarii,
   f. ochronę przed błędami, utratą, nieuprawnioną modyfikacją,

g. stosowanie mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,

h. zapewnienie bezpieczeństwa plików systemowych,

i. redukcję ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów informatycznych,

j. niezwłoczne podejmowanie działań po dostrzeżeniu nieujawnionych podatności systemów informatycznych na możliwość naruszenia bezpieczeństwa,

k. kontrolę zgodności systemów informatycznych z odpowiednimi normami i politykami bezpieczeństwa.

2. W stosownym przypadku przeprowadza się ocenę skutków zgodnie z art. 35 RODO w sytuacji, gdy przetwarzanie w nowym systemie może wiązać się z dużym prawdopodobieństwem powodowania wysokiego ryzyka utraty praw lub wolności osób fizycznych.

3. Dla systemów służących do przetwarzania danych osobowych stosuje się zasadę domyślnej ochrony danych oraz ochrony na etapie projektowania.

4. Za zapewnienie właściwego przebiegu procesu pozyskiwania, rozwoju i utrzymania systemów informatycznych odpowiedzialny jest Kierownik Jednostki Organizacyjnej.

13 Minimalne środki bezpieczeństwa fizycznego i środowiskowego informacji chronionych

1. Przetwarzanie informacji chronionych musi być prowadzone wyłącznie w pomieszczeniach odpowiednio zabezpieczonych przed nieuprawnionym dostępem, uszkodzeniem bądź zniszczeniem sprzętu i danych.

2. Zabezpieczenia pomieszczeń z elementami Systemu Jednostki są opisane w ***Regulaminie Systemu Informatycznego Jednostki Organizacyjnej Gminy Lublin oraz Regulaminie Bezpieczeństwa informacji***

3. Zabezpieczenia w pomieszczeniach pracowniczych powinny spełniać minimalne wymagania wymienione poniżej:

   a. drzwi do pomieszczenia zwykłe – nie przeciwpożarowe, nie antywłamaniowe,

   b. zamki w drzwiach do pomieszczenia zwykłe – nie antywłamaniowy,

   c. pomieszczenia zabezpieczone są przed skutkami pożaru za pomocą wolnostojącej gaśnicy zgodnie z obowiązującymi przepisami p.poż.,

   d. szafki, w których przechowuje się dokumenty nie zawierające danych osobowych - niemetalowe, zamykane na zamki zwykłe,

   e. szafki, w których przechowuje się dokumenty zawierające dane osobowe lub inne informacje chronione - solidnej konstrukcji zamykane na klucz lub szafy metalowe bądź w sejfy, w przypadku, gdy wskazuje na to wynik szacowania ryzyka.

4. Zabezpieczenia danych osobowych w pomieszczeniu archiwum powinny spełniać minimalne wymagania wymienione poniżej:

   a. drzwi antywłamaniowe i przeciwpożarowe,

   b. czujnik temperatury,

   c. czujnik wilgotności,

d. czujnik dymu wraz z możliwością alarmowania,

e. gaśnica w pomieszczeniu,

f. ograniczenie dostępu do pomieszczenia tylko dla osób upoważnionych przez Kierownika Jednostki Organizacyjnej,

g. żaluzje przeciwsłoneczne w oknach,

h. regały metalowe lub drewniane przeznaczone na przechowywanie dokumentacji z pierwszą półką na wysokości min. 15 cm.

5. Osoby pracujące w pomieszczeniach są odpowiedzialne za właściwe ich zabezpieczenie w trakcie pracy, jak i po jej zakończeniu. Szczegółowe zasady opisane są w ***Regulaminie Bezpieczeństwa Informacji Jednostki Organizacyjnej Gminy Lublin***.

14 Domyślna ochrona i ochrona w fazie projektowania

1. Podczas tworzenia produktów, usług i aplikacji, które opierają się na przetwarzaniu danych osobowych albo przetwarzają dane osobowe w celu realizacji swojego zadania, Administrator oraz podmioty przetwarzające podczas opracowywania i projektowania biorą pod uwagę prawo do ochrony danych osobowych.
2. Wytwórcy produktów, usług i aplikacji z uwzględnieniem stanu wiedzy technicznej zapewniają Administratorowi i podmiotom przetwarzającym możliwość wywiązania się obowiązków ochrony danych osobowych.
3. Stosowanie zasad domyślnej ochrony oraz ochrony w fazie projektowania sprowadza się do stosowania zabezpieczeń organizacyjnych i technicznych adekwatnych do oszacowanego ryzyka dla projektowanych lub planowanych operacji przetwarzania, a w szczególności do stosowania:
    a. pseudonimizacji,
    b. szyfrowania,
    c. minimalizacji danych,
    d. ograniczenia do niezbędnej ilości zbieranych danych osobowych,
    e. ograniczenia do niezbędnego zakresu przetwarzania danych,
    f. ograniczenia do niezbędnego okresu przechowywania danych,
    g. technik zapewniających odpowiedni poziom dostępności,
    h. zasady nie udostępniania danych osobowych bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.
4. Zasadę uwzględniania ochrony danych w fazie projektowania i zasadę domyślnej ochrony danych należy też brać pod uwagę w zamówieniach publicznych na produkty, usługi i aplikacje, które służą do przetwarzania danych osobowych.

15 Zarządzanie incydentami

1. Każde naruszenie bezpieczeństwa danych osobowych wymaga odpowiedniej reakcji, w tym w szczególności poinformowania o wystąpieniu naruszenia Inspektora Ochrony Danych i , który ma obowiązek poinformowania

o niniejszym niezwłocznie Kierownika Jednostki Organizacyjnej. Obowiązek w tym zakresie spoczywa na wszystkich pracownikach i osobach trzecich, które uzyskały dostęp na mocy zawartej umowy do gromadzonych danych.

2. Podstawą do podjęcia decyzji o sposobie reagowania na incydent jest ocena skutków incydentu, której dokonuje Inspektor Ochrony Danych wraz z administratorem zbioru, którego incydent dotyczy.

3. W przypadku naruszenia ochrony danych osobowych, Kierownik Jednostki bez zbędnej zwłoki – nie później niż w terminie 72 godzin od stwierdzeniu naruszenia – zgłasza je, stosownie do postanowień art. 55 RODO, organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

4. W przypadku zgłoszenia wystąpienia naruszenia po upływie 72 godzin do zgłoszenia dołącza się wyjaśnienie przyczyn opóźnienia.

Rejestr incydentów prowadzony jest przez Inspektora Ochrony Danych w formie elektronicznej lub papierowej, zgodnie ze wzorem zawartym w ***Załączniku nr 9 do PBI.***

16 Załączniki

Integralną częścią Polityki są następujące załączniki:

1. Załącznik nr 1 – Wzór umowy powierzenia danych osobowych
2. Załącznik nr 2 do Polityki Bezpieczeństwa Informacji – Wzór wykazu budynków, pomieszczeń i części pomieszczeń, w których przetwarzane są dane osobowe
3. Załącznik nr 3 do Polityki Bezpieczeństwa Informacji – Procedura sprawdzeń
4. Załącznik nr 4 do Polityki Bezpieczeństwa Informacji – Wzór Rejestru umów powierzenia
5. Załącznik nr 5 do Polityki Bezpieczeństwa Informacji – Wzór Ewidencji osób upoważnionych do przetwarzania danych osobowych
6. Załącznik nr 6 do Polityki Bezpieczeństwa Informacji – Wzór upoważnienia do przetwarzania danych osobowych
7. Załącznik nr 7 do Polityki Bezpieczeństwa Informacji – Procedura szacowania ryzyka
8. Załącznik nr 8 do Polityki Bezpieczeństwa – Wzór Rejestru czynności przetwarzania
9. Załącznik nr 9 do Polityki Bezpieczeństwa – Wzór Rejestru incydentów
10. Załącznik nr 10 do Polityki Bezpieczeństwa – Wzór Rejestru kategorii przetwarzania

b-

17 Dokumenty związane

1. Regulamin Systemu Informatycznego Jednostki Organizacyjnej Gminy Lublin.
2. Regułamin Bezpieczeństwa Informacji Jednostki Organizacyjnej Gminy Lublin.