ZARZĄDZENIE NR 48A/2021
BURMISTRZA MIASTA ŻARÓW

z dnia 25 marca 2021 r.

w sprawie zmiany Zarządzenia Nr 119/2018 Burmistrza Miasta Żarów z dnia 9 lipca 2018 r. w sprawie wprowadzenia dokumentacji do użytku służbowego w zakresie ochrony danych osobowych

Na podstawie art. 30 ust. 1 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (Dz. U. z 2022 r. poz. 559 z późn. zm.) i art. 24 ust. 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) (Dziennik Urzędowy Unii Europejskiej, L 119, 4 maja 2016), zarządzam, co następuje:

§ 1. W Zarządzeniu Nr 119/2018 Burmistrza Miasta Żarów z dnia 9 lipca 2018 r. w sprawie wprowadzenia dokumentacji do użytku służbowego w zakresie ochrony danych osobowych zmienia się:

1) Podstawowe zasady ochrony danych osobowych - załącznik nr 1,

3) Politykę bezpieczeństwa danych osobowych - załącznik nr 2,

4) Regulamin monitoringu wizyjnego- załącznik nr 3,

5) Procedury zarządzania dostępem do systemu przetwarzania danych osobowych - załącznik nr 4,

6) Procedury reagowania na naruszenia ochrony danych - załącznik nr 5,

7) Analiza zagrożeń i ryzyka przy przetwarzaniu danych osobowych - załącznik nr 6.

§ 2. Zobowiązuje się wszystkich pracowników Urzędu Miejskiego w Żarowie do zapoznania się z niniejszym zarządzeniem i jego załącznikami oraz do przestrzegania zasad zawartych w tych dokumentach.

§ 3. Wykonanie zarządzenia powierza się Sekretarzowi Gminy Żarów.

§ 4. Załączniki do zarządzenia zawierają informacje prawnie chronione i nie podlegają publikacji.

§ 5. Zarządzenie wchodzi w życie z dniem podjęcia.

Podstawowe zasady ochrony danych osobowych

Urząd Miejski w Żarowie

ul. Zamkowa 2
58-130 Żarów

Dokument do użytku służbowego
Wykonał: mgr inż. Piotr Chałaszczyk
- Inspektor Ochrony Danych
Data aktualizacji: 25.03.2021 r.

Spis treści

Zasady dotyczące dostępu do systemu przetwarzania danych osobowych

1. Dostęp do systemu przetwarzania danych osobowych w Urzędzie Miejskim w Żarowie może uzyskać wyłącznie osoba upoważniona do przetwarzania danych przez Administratora Danych Osobowych. Dotyczy to zarówno dostępu do systemu tradycyjnego (kartotek, ksiąg, skorowidzów, akt osobowych, wykazów itp.), jak i systemu informatycznego. Wzór upoważnienia stanowi Załącznik nr 1 do „Procedur zarządzania dostępem do systemu przetwarzania".
2. Dostęp do systemu informatycznego, w którym przetwarzane są dane osobowe, może uzyskać wyłącznie osoba upoważniona do przetwarzania przez Administratora Danych Osobowych i zarejestrowana jako użytkownik w systemie informatycznym przez Administratora Systemu Informatycznego na podstawie wniosku bezpośredniego przełożonego użytkownika.
3. Każdy upoważniony do przetwarzania pracownik, a także każda upoważniona osoba, zatrudniona w Urzędzie na innej podstawie niż stosunek pracy (np. umowy zlecenia), również stażysta lub praktykant, przed przystąpieniem do systemu przetwarzania jest zobowiązana odbyć szkolenie, zapoznać się z zasadami ochrony danych osobowych opisanymi w niniejszej dokumentacji oraz podpisać oświadczenie o zachowaniu poufności. Oświadczenie zawarte jest w „Upoważnieniu do przetwarzania danych osobowych" (Załącznik nr 1 do „Procedur zarządzania dostępem do systemu przetwarzania").
4. Osoba upoważniona do przetwarzania danych osobowych może je przetwarzać wyłącznie w zakresie ustalonym przez Administratora Danych Osobowych, tylko w celu wykonywania nałożonych na nią obowiązków.
5. Zakres dostępu do zbiorów danych osobowych w systemie informatycznym UM przypisany jest do unikatowego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie.
6. Pracownicy Urzędu nieupoważnieni do przetwarzania danych osobowych, wykonujący prace techniczne, porządkowe i konserwatorskie itp. są zobowiązani do podpisania oświadczenia o zachowaniu poufności (Załącznik nr 3 do „Procedur zarządzania dostępem do systemu przetwarzania").
7. W przypadku konieczności dostępu do obszaru przetwarzania osób nieupoważnionych (niebędących pracownikami UM), które muszą dokonać doraźnych prac o charakterze serwisowym lub innym, podpisują one oświadczenie o zachowaniu poufności (Załącznik nr 3), chyba że czynności odbywają się pod nadzorem osoby upoważnionej do przetwarzania danych.

Zasady postępowania z kluczami do pomieszczeń

1. Kluczami do pomieszczeń należących do obszaru przetwarzania dysponują tylko pracownicy upoważnieni przez Administratora Danych Osobowych.
2. Klucze do pomieszczeń, biurek stanowiskowych, szaf biurowych pozostają pod osobistym nadzorem osób upoważnionych w trakcie wykonywania przez nie obowiązków i osoby te ponoszą za nie pełną odpowiedzialność. Podczas chwilowej nieobecności w pomieszczeniu, pracownicy nie pozostawiają w nim kluczy służących do zabezpieczenia biurek i szaf.
3. Klucze do pomieszczeń szczególnie chronionych pozostają pod osobistym nadzorem osób do tego upoważnionych. Dostęp osób nieupoważnionych do tych pomieszczeń odbywa się pod ścisłym nadzorem osób upoważnionych.

4. Klucze zapasowe wydawane są osobom upoważnionym tylko w uzasadnionych sytuacjach oraz przypadkach awaryjnych. Klucze zapasowe po ich wykorzystaniu zwracane są do depozytu.

Obowiązki osób upoważnionych do przetwarzania danych osobowych

Do obowiązków osób przetwarzających dane osobowe należy:

1. Przetwarzanie danych osobowych na terenie Urzędu tylko w wyznaczonych do tego celu pomieszczeniach lub ich częściach.
2. Zabezpieczenie zbiorów danych osobowych oraz dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych za pomocą środków określonych w dokumentacji ochrony danych osobowych.
3. Nieudzielanie informacji o danych osobowych przetwarzanych w jednostce innym podmiotom, chyba, że obowiązek taki wynika z przepisów prawa.
4. Bezzwłoczne zawiadomienie Inspektora OD lub Administratora Danych Osobowych o wszelkich przypadkach naruszenia bezpieczeństwa danych osobowych, a także o przypadkach utraty lub kradzieży dokumentów lub innych nośników zawierających dane osobowe.
5. Wypełnianie obowiązku informacyjnego przy pozyskiwaniu danych osobowych. Obowiązek informacyjny należy spełnić na piśmie lub w inny sposób, w tym w stosownych przypadkach - elektronicznie. Wzór ogólny klauzuli informacyjnej zawarty jest w Załączniku nr 1 do „Polityki bezpieczeństwa danych osobowych".

Do obowiązków kierującego komórką organizacyjną należy:

1. Wnioskowanie do ADO o nadanie upoważnienia do przetwarzania danych osobowych oraz określanie jego zakresu dla podległych mu pracowników oraz osób wykonujących pracę w ramach umowy cywilno-prawnej (również stażystów, praktykantów i wolontariuszy).
2. Wnioskowanie do ADO o odebranie lub modyfikację upoważnienia w przypadku zmian, które mają wpływ na zakres tego upoważnienia (np. zmiana komórki organizacyjnej, zmiana zakresu zadań, zwolnienie ze świadczenia pracy).
3. Odpowiednie postępowanie w przypadku wystąpienia incydentów naruszeń ochrony danych, zgodnie z „Procedurami reagowania na naruszenia ochrony danych osobowych".
4. Współpraca z Inspektorem OD oraz z Administratorem Systemu Informatycznego w zakresie przestrzegania ochrony danych przez podległych pracowników oraz inne osoby upoważnione do przetwarzania, podlegające kierownikowi komórki organizacyjnej.

Zasady wyrażania zgody na przetwarzanie danych osobowych

5. Aby przetwarzanie danych było zgodne z prawem, powinno się odbywać na podstawie:
   - przepisu prawa,
   - umowy zawartej z podmiotem danych,
   - realizacji celów dla dobra publicznego,

- prawnie usprawiedliwionego celu Administratora Danych Osobowych, jeżeli nie narusza praw i wolności podmiotu danych,
- zgody osoby, której dane dotyczą.

6. Zgoda wyrażana jest na przetwarzanie danych w celu i zakresie podanym w klauzuli informacyjnej udostępnionej osobie, której dane są przetwarzane. Wzór ogólny klauzuli zgody na przetwarzanie danych osobowych zawarty jest w Załączniku nr 2 do „Polityki bezpieczeństwa danych osobowych".
7. Zgoda powinna stanowić odrębne oświadczenie.
8. Zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele.

Metody uwierzytelnienia użytkowników w systemie informatycznym

W Urzędzie Miejskim w Żarowie system informatyczny, w którym przetwarza się dane osobowe, wyposażony jest w mechanizmy uwierzytelniania użytkowników przy pomocy identyfikatora i hasła.

Identyfikator użytkownika

1. Każdy użytkownik systemu informatycznego posiada swój unikatowy identyfikator.
2. Użytkownicy nie mogą używać tych samych identyfikatorów ani wymieniać się nimi.
3. Identyfikator po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielony innej osobie.
4. Kontrolę nad powyższymi czynnościami sprawuje Administrator Systemu Informatycznego.

Hasło użytkownika

1. Hasło dostępu ustala dla siebie użytkownik.
2. Hasło dostępu powinno składać się z unikatowego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry i znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika ani z jego imieniem lub nazwiskiem.
3. W systemie informatycznym zmiana haseł dostępu powinna następować co najmniej co 30 dni.
4. Za zmianę hasła odpowiada użytkownik.
5. Użytkownik niezwłocznie zmienia hasło w przypadku podejrzenia lub stwierdzenia: podglądu, przechwycenia, podsłuchania lub odgadnięcia.
6. Użytkownik zobowiązany jest do utrzymania hasła dostępu w tajemnicy zarówno w czasie zatrudnienia, jak też po jego ustaniu.
7. W sytuacji udostępnienia hasła innej osobie, użytkownik ponosi odpowiedzialność za skutki i następstwa wynikłe z faktu wykorzystania tego hasła przez osoby trzecie.
8. Hasła dostępu wyświetlane są na ekranie monitora w formie niedającej się odczytać osobom postronnym i mogą być znane tylko użytkownikowi.

Zasady korzystania z Internetu, poczty elektronicznej i oprogramowania

Zasady bezpiecznego użytkowania systemu informatycznego

1. Zabrania się użytkownikowi podłączania do systemu informatycznego nieautoryzowanych (prywatnych) nośników informacji. Do komputera można podłączać jedynie służbowe nośniki.
2. Zabrania się użytkownikowi przechowywania na służbowym komputerze jakichkolwiek materiałów niezwiązanych z wykonywanymi obowiązkami służbowymi. Zabrania się w szczególności przechowywania na służbowym komputerze materiałów naruszających prawa autorskie.
3. Zabrania się podłączania prywatnych komputerów oraz innych urządzeń sieciowych do sieci LAN/WAN. Wymaga to akceptacji Administratora Danych Osobowych. Zabrania się również podłączania służbowych komputerów znajdujących się w obszarze funkcjonowania Urzędu nieautoryzowanych sieci LAN/WAN za pomocą urządzeń, które nie są częścią systemu informatycznego jednostki.

Zasady korzystania z oprogramowania

1. Zabrania się instalowania oraz używania oprogramowania innego niż udostępnione przez ADO.
2. Zabrania się kopiowania lub usuwania oprogramowania zainstalowanego w systemie informatycznym Urzędu.
3. Zabrania się przenoszenia programów komputerowych z własnego stanowiska roboczego na inne stanowisko.
4. Zabrania się uruchamiania programów otrzymanych pocztą elektroniczną.
5. Instalowanie jakiegokolwiek oprogramowania związanego z obsługą urządzeń peryferyjnych wchodzących w skład systemu informatycznego może być dokonane wyłącznie przez Administratora Systemu Informatycznego.

Zasady korzystania z Internetu

1. Użytkownik zobowiązany jest do korzystania z Internetu tylko w celach służbowych.
2. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
3. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu rozpoczynającego się frazą „https:”
4. Zabrania się odwiedzania stron o treściach prawnie zabronionych lub powszechnie uznanych za niebezpieczne.
5. Zabrania się pobierania z Internetu plików pochodzących z niewiarygodnych źródeł.

Zasady korzystania z poczty elektronicznej

1. Nadany użytkownikowi adres skrzynki poczty elektronicznej służy wyłącznie do realizacji celów służbowych lub umownych. Wszelka korespondencja elektroniczna niezwiązana z działalnością UM powinna być prowadzona przez prywatną skrzynkę poczty elektronicznej użytkownika.

2. Każdy użytkownik zobowiązany jest do:
   - zwracania szczególnej uwagi na poprawność adresu odbiorcy wiadomości,
   - stosowania metody UDW (ukryte do wiadomości) podczas wysyłania korespondencji do wielu adresatów jednocześnie,
   - nieotwierania wiadomości oraz załączników i linków otrzymanych od nieznanych nadawców (w takiej sytuacji należy skontaktować się z Administratorem Systemu Informatycznego),
   - wykorzystywania mechanizmów kryptograficznych (hasłowanie wysyłanych plików, podpis elektroniczny) w przypadku przesyłania danych osobowych.

Zasady postępowania z elektronicznymi nośnikami informacji zawierającymi dane osobowe

1. Elektroniczne nośniki informacji zawierające dane osobowe na czas ich użyteczności przechowywane są w zamkniętych na klucz szafach/zabezpieczonych meblach biurowych.
2. W przypadku dalszego wykorzystywania w innych celach, nośniki pozbawiane są zapisu danych w sposób uniemożliwiający ich odzyskanie.
3. Elektroniczne nośniki informacji, które zostały przeznaczone do likwidacji, pozbawiane są wcześniej zapisu danych, a w przypadku gdy nie jest to możliwe, uszkadzane w sposób uniemożliwiający ich odczytanie.
4. Zabrania się wynoszenia z Urzędu na jakichkolwiek nośnikach całych zbiorów danych lub jakichkolwiek z nich wypisów, nawet w postaci zaszyfrowanej.

Zasady postępowania przy przekazywaniu nośników informacji do innej jednostki organizacyjnej

1. Elektroniczne nośniki informacji zawierające dane osobowe przekazywane są do innej jednostki organizacyjnej tylko na pisemny, umotywowany wniosek, gdy jest to bezwzględnie konieczne do realizacji jej zadań regulaminowych.
2. Pliki z informacjami zawarte na nośnikach przekazywanych poza obszar przetwarzania, obowiązkowo zabezpiecza się hasłem dostępu lub szyfrując je.
3. Przed wysłaniem nośnika sporządzana jest kopia przesyłanych danych, a adresat powiadamiany jest o nadanej przesyłce. W przypadku nieotrzymania przez adresata przesyłki, o zaistniałej sytuacji powiadamiany jest Inspektor Ochrony Danych.
4. Elektroniczne nośniki informacji pochodzące od podmiotu zewnętrznego sprawdzane są programem antywirusowym.

Zasady postępowania z komputerami przenośnymi

Użytkownik komputera przenośnego jest zobowiązany do:
- transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia,
- zabezpieczenia komputera przenośnego hasłem, zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym,
- niezezwalania osobom nieupoważnionym i nieuprawnionym do korzystania z komputera przenośnego,

- korzystania z komputera w sposób minimalizujący ryzyko podejrzenia przetwarzanych danych przez osoby postronne, w szczególności zabrania się korzystania z komputera przenośnego w miejscach publicznych i w środkach transportu publicznego.

Zasady postępowania z dokumentami papierowymi

1. Podczas nieobecności w pomieszczeniu lub po zakończeniu pracy, dokumenty oraz wydruki zawierające dane osobowe przechowane są w szafkach i meblach biurowych zamykanych na klucz.
2. Dokumenty i wydruki oraz kserokopie dokumentów nie są pozostawiane na urządzeniach (drukarkach, skanerach, kserokopiarkach) bez nadzoru.
3. Dokumenty i wydruki z danymi osobowymi, niezwłocznie po ustaniu celu ich przetwarzania, niszczone są w niszczarkach.
4. W przypadku konieczności przekazania poza obszar przetwarzania, dokumenty transportowane są i przekazywane z zachowaniem szczególnej ostrożności przez osobę do tego upoważnioną.

Zasady postępowania w przypadku naruszenia ochrony danych osobowych

Osoba, która zauważyła niepokojące zdarzenie lub wyżej wymienione symptomy, które jej zdaniem mogą spowodować zagrożenie bądź przyczynić się do naruszenia zasad ochrony danych osobowych i bezpieczeństwa informacji, zobowiązana jest do natychmiastowego poinformowania o tym Inspektora Ochrony Danych, a w przypadku jego nieobecności Administratora Danych Osobowych. Informacja o pojawieniu się zagrożenia jest przekazywana przez tę osobę osobiście, telefonicznie lub pocztą elektroniczną. Taka informacja powinna zawierać imię i nazwisko osoby zgłaszającej oraz zauważone symptomy zagrożenia.

Do czasu przybycia na miejsce zdarzenia Inspektora Ochrony Danych lub wskazanego przez niego pracownika należy:

- o ile istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego zdarzenia, a następnie uwzględnić w działaniu również ustalenie jego przyczyn lub sprawców,
- rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
- zaniechać (o ile to możliwe) dalszych planowanych przedsięwzięć, które mogą utrudnić udokumentowanie i analizę zaistniałego zdarzenia,
- przygotować opis incydentu,
- nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia Inspektora OD lub osoby przez niego wskazanej.

Polityka bezpieczeństwa danych osobowych

Urząd Miejski w Żarowie

ul. Zamkowa 2
58-130 Żarów

Dokument do użytku służbowego
Wykonał: mgr inż. Piotr Chałaszczyk
- Inspektor Ochrony Danych
Data aktualizacji: 25.03.2021 r.

Spis treści

Wstęp

„Polityka bezpieczeństwa danych osobowych" określa podstawowe zasady dotyczące zapewnienia bezpieczeństwa w zakresie danych osobowych przetwarzanych przez Urząd Miejski w Żarowie, które powinny być przestrzegane i stosowane podczas ich przetwarzania przez kierownictwo Urzędu oraz wszystkich pracowników i współpracowników zarówno w tradycyjnych zbiorach danych, jak i systemach informatycznych.

Przy opracowaniu niniejszego dokumentu uwzględniono regulacje zawarte w następujących aktach prawnych:

- Rozporządzeniu 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.
- Wytycznych GIODO pt. „Wykonywanie obowiązków ABI, przyszłego Inspektora Ochrony Danych Osobowych w świetle ogólnego rozporządzenia o ochronie danych osobowych.
- Wytycznych Grupy Roboczej art. 29 dotyczących Inspektorów Danych Osobowych z dn. 13 grudnia 2016 r.
- Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych.

Zakres stosowania polityki bezpieczeństwa danych osobowych

Zasady określone przez dokumentację ochrony danych osobowych mają zastosowanie do całego systemu przetwarzania danych, zarówno tradycyjnego - papierowego jak i informatycznego, a w szczególności do:

- wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych, zbiorów, wykazów, rejestrów papierowych, w których przetwarzane są lub będą informacje podlegające ochronie,
- informacji będących własnością Urzędu,
- wszystkich nośników papierowych i elektronicznych, na których są lub będą znajdować się informacje podlegające ochronie (również zapis z systemu nadzoru wizyjnego),
- wszystkich lokalizacji, budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie,
- wszystkich pracowników Urzędu, bez względu na funkcję i pełnione zadania, jednakże w szczególności osób, które mają dostęp do danych osobowych w ramach wypełniania obowiązków służbowych lub pełnionych zadań przy ich przetwarzaniu,
- zleceniobiorców, współpracowników, konsultantów, organów kontrolujących Urząd i innych osób mających dostęp do informacji podlegających ochronie.

Zasady dotyczące przetwarzania danych osobowych (legalność przetwarzania)

Dane osobowe muszą być:

1. Przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość"). Jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.
2. Zbierane 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 w myśl art. 89 ust. 1 RODO za niezgodne z pierwotnymi celami („ograniczenie celu").
3. Adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych").
4. Prawidłowe i w razie potrzeby uaktualniane. Należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość").
5. 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. 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 na mocy art. 89 ust. 1 RODO, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania").
6. 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").

Obowiązki informacyjne

Dane osobowe przetwarzane w Urzędzie Miejskim w Żarowie mogą być pozyskiwane bezpośrednio od osób, których dotyczą lub z innych źródeł w granicach dozwolonych przepisami prawa.

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, zgodnie z art. 13 ust. 1 i 2 RODO, nadzorujący przetwarzanie danych (ADO) jest obowiązany poinformować tę osobę w przystępnej dla niej formie o:
   - swojej tożsamości i danych kontaktowych oraz tożsamości i danych kontaktowych swojego przedstawiciela, jeżeli istnieje,
   - danych kontaktowych Inspektora Ochrony Danych,
   - celach przetwarzania, do których mają posłużyć dane osobowe,
   - podstawie prawnej przetwarzania,
   - prawnie uzasadnionym interesie realizowanym przez ADO lub przez stronę trzecią, jeżeli przetwarzanie odbywa się na podstawie prawnie usprawiedliwionego interesu ADO (art. 6 ust. 1 lit. f RODO),
   - odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,
   - transferze danych do państwa trzeciego,
   - okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteriach ustalania tego okresu.

- prawie do żądania od Administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania, wniesienia sprzeciwu wobec przetwarzania, przenoszenia danych,
- prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem (jeżeli przetwarzane są dane zwykłe (art. 6 ust. 1 lit. a) RODO) lub szczególnej kategorii (art. 9 ust. 2 lit. a) RODO),
- prawie wniesienia skargi do organu nadzorczego,
- 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,
- informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu (art. 22 ust. 1 i 4 RODO) oraz istotnych informacjach o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

2. W przypadku zbierania danych osobowych z innego źródła niż od osoby, której dane dotyczą, zgodnie z art. 14 ust. 1 i 2 RODO, nadzorujący przetwarzanie danych (ADO) jest obowiązany poinformować tę osobę w przystępnej dla niej formie o:
   - informacjach z punktów wskazanych powyżej,
   - kategoriach odnośnych danych osobowych,
   - źródle pochodzenia danych osobowych, a jeżeli ma to zastosowanie, o pochodzeniu ich ze źródeł powszechnie dostępnych.

Klauzule informacyjne

Administrator Danych Osobowych powinien przekazać powyższe informacje w formie zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej oraz jasnym i prostym językiem. Obowiązek informacyjny należy spełnić na piśmie lub w inny sposób, w tym w stosownych przypadkach - elektronicznie. Wzór ogólny klauzuli informacyjnej zawarty jest w **Załączniku nr 1** do „Polityki bezpieczeństwa danych osobowych".

Prawa osób, których dane są przetwarzane

1. Prawo do bycia poinformowanym o operacjach przetwarzania.
2. Prawo dostępu do danych osobowych, w tym prawo do uzyskania kopii tych danych.
3. Prawo do żądania sprostowania (poprawiania) danych osobowych - w przypadku, gdy dane są nieprawidłowe lub niekompletne.
4. Prawo do żądania usunięcia danych osobowych (tzw. prawo do bycia zapomnianym) w przypadku, gdy:
   - dane nie są już niezbędne do celów, dla których były zebrane lub w inny sposób przetwarzane,
   - osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania danych osobowych,
   - osoba, której dane dotyczą wycofała zgodę na przetwarzanie danych osobowych, która jest podstawą przetwarzania danych i nie ma innej podstawy prawnej przetwarzania danych,
   - dane osobowe przetwarzane są niezgodnie z prawem,

- dane osobowe muszą być usunięte w celu wywiązania się z obowiązku wynikającego z przepisów prawa.

5. Prawo do żądania ograniczenia przetwarzania danych osobowych w przypadku, gdy:
   - osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych,
   - przetwarzanie danych jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych, żądając w zamian ich ograniczenia,
   - Administrator nie potrzebuje już danych dla swoich celów, ale osoba, której dane dotyczą, potrzebuje ich do ustalenia, obrony lub dochodzenia roszczeń,
   - osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania danych do czasu ustalenia, czy prawnie uzasadnione podstawy po stronie Administratora są nadrzędne wobec podstawy sprzeciwu.
6. Prawo do przenoszenia danych w przypadku, gdy łącznie spełnione są następujące przesłanki:
   - przetwarzanie danych odbywa się na podstawie umowy zawartej z osobą, której dane dotyczą lub na podstawie zgody wyrażonej przez tę osobę,
   - przetwarzanie odbywa się w sposób zautomatyzowany.
7. Prawo sprzeciwu wobec przetwarzania danych w przypadku, gdy łącznie spełnione są następujące przesłanki:
   - zaistnieją przyczyny związane ze szczególną sytuacją osoby, której dane dotyczą, w przypadku przetwarzania danych na podstawie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej przez Administratora,
   - przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą jest dzieckiem.
8. Prawo do tego, by nie podlegać profilowaniu.
9. W przypadku, gdy przetwarzanie danych osobowych odbywa się na podstawie zgody na przetwarzanie danych osobowych (art. 6 ust. 1 lit a RODO), prawo do cofnięcia tej zgody w dowolnym momencie. Cofnięcie to nie ma wpływu na zgodność przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem, z obowiązującym prawem.
10. W przypadku powzięcia informacji o niezgodnym z prawem przetwarzaniu w UM danych osobowych, prawo wniesienia skargi do organu nadzorczego właściwego w sprawach ochrony danych osobowych (Urzędu Ochrony Danych Osobowych).

Zasady wyrażania zgody na przetwarzanie danych osobowych

1. Aby przetwarzanie danych było zgodne z prawem, powinno się odbywać na podstawie:
   - przepisu prawa,
   - umowy zawartej z podmiotem danych,
   - realizacji celów dla dobra publicznego,
   - prawnie usprawiedliwionego celu Administratora Danych Osobowych, jeżeli nie narusza praw i wolności podmiotu danych,
   - zgody osoby, której dane dotyczą.

2. Zgoda wyrażana jest na przetwarzanie danych w celu i zakresie podanym w klauzuli informacyjnej udostępnionej osobie, której dane są przetwarzane i powinna zawierać nazwę i dane kontaktowe Administratora Danych Osobowych. Wzór ogólny klauzuli zgody na przetwarzanie danych osobowych zawarty jest w **Załączniku nr 2** do „Polityki bezpieczeństwa danych osobowych".
3. Zgoda jest wyrażana dla konkretnego administratora danych. W przypadku, gdy administrator udostępnia pozyskane dane innym administratorom (do własnych celów, np. marketingowych), powinien pozyskać odrębną zgodę. Każde udostępnienie danych powinno być odnotowywane przez administratora, aby zachować zasadę rozliczalności.
4. Zgoda powinna stanowić odrębne oświadczenie.
5. Zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebne są zgody na wszystkie te cele.

Udostępnianie danych osobowych

Udostępnienie innemu administratorowi, czyli przekazanie danych osobowych ma miejsce wówczas, gdy jeden administrator udostępnia dane drugiemu i każdy z tych administratorów wykorzystuje je do własnych celów. Urząd Miejski w Żarowie udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa lub za zgodą osoby, której dane dotyczą.

Udostępnienie danych osobowych podmiotowi zewnętrznemu może nastąpić wyłącznie po pozytywnym zweryfikowaniu prawnych przesłanek dopuszczalności takiego udostępnienia. UM może odmówić udostępnienia danych osobowych, jeżeli spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą.

W UM dane osobowe mogą być udostępniane:

1. Osobom i jednostkom organizacyjnym, pod warunkiem wykazania swojego interesu prawnego lub faktycznego do otrzymania takich informacji. W przypadku powołania się na interes prawny wnioskodawca jest zobowiązany wskazać przepis prawa materialnego, na podstawie którego jest uprawniony do żądania udostępnienia danych osobowych innej osoby lub załączyć dokumenty potwierdzające ten interes.
2. Jednostkom organizacyjnym w celach badawczych, statystycznych, badania opinii publicznej, jeżeli po wykorzystaniu dane te zostaną poddane takiej modyfikacji, która nie pozwoli ustalić tożsamości osób, których dane dotyczą.
3. Innym osobom i jednostkom organizacyjnym, jeżeli wykażą interes faktyczny w otrzymaniu danych, pod warunkiem uzyskania zgody osoby, której dane dotyczą. Interes faktyczny, w odróżnieniu od interesu prawnego, to stan, w którym podmiot jest bezpośrednio zainteresowany rozstrzygnięciem sprawy administracyjnej, nie może jednak tego zainteresowania poprzeć przepisami prawa powszechnie obowiązującego, mającymi stanowić podstawę skutecznego żądania stosownych czynności organu administracji.

Warunkiem udostępnienia danych jest dołączenie do wniosku stosownych dokumentów:

- dokumentów potwierdzających interes prawny wnioskodawcy (np. wezwania sądowe, wezwania komornicze, dokumenty potwierdzające zobowiązanie wobec wnioskodawcy

osoby, której dane mają być udostępnione np. wyroki sądowe, umowy, wezwania do zapłaty, wezwanie przedsądowe wraz z potwierdzeniem braku odbioru, postanowienia i decyzje innych organów),

- dokumentów potwierdzających interes faktyczny (jeżeli żądanie udostępnienia danych nie wynika wprost z przepisów prawa, wnioskodawca jest zobowiązany przedstawić wiarygodną potrzebę posiadania danych osoby, której dotyczą. Ponadto osoba, której dane dotyczą, musi wyrazić zgodę na udostepnienie jej danych).

W trybie jednostkowym z Rejestru Dowodów Osobistych udostępnia się dane dotyczące jednego dokumentu lub dane dotyczące jednej osoby. Dane jednostkowe udostępnione na podstawie wniosku nie mogą być wykorzystane w innym celu niż wskazany w tym wniosku.

Każde udostępnienie danych osobowych ujęte jest w odpowiednim wykazie.

Powierzenie przetwarzania danych

Powierzenie przetwarzania danych osobowych ma miejsce wówczas, kiedy dane przekazane są innemu podmiotowi w celu wykonania określonych czynności przetwarzania, lecz Administratorem Danych Osobowych pozostaje nadal powierzający dane.

Powierzenie przetwarzania danych osobowych może mieć miejsce wyłącznie na podstawie pisemnej umowy określającej w szczególności:

- przedmiot przetwarzania,
- czas trwania przetwarzania,
- charakter i cel przetwarzania,
- rodzaj danych osobowych,
- kategorie osób, których dane dotyczą,
- obowiązki i prawa Administratora Danych Osobowych.

Umowa musi określać również zakres odpowiedzialności podmiotu, któremu powierzono przetwarzanie danych z tytułu niewykonania lub nienależytego wykonania umowy. Powierzenie przetwarzania danych osobowych musi uwzględniać wymogi wynikające z RODO. W szczególności podmiot zewnętrzny, któremu ma zostać powierzone przetwarzanie danych osobowych, jest zobowiązany przed rozpoczęciem ich przetwarzania do:

- przestrzegania zasad zawartych w niniejszej dokumentacji ochrony danych osobowych,
- wdrożenia odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo i odpowiedni poziom ochrony danych.

Wymagane jest zatem, aby w umowach stanowiących podstawę powierzenia umieszczone zostały prawa Urzędu Miejskiego w Żarowie.

Wzór umowy powierzenia stanowi **Załącznik nr 3,** wykaz podmiotów, z którymi zawarto umowy powierzenia - **Załącznik nr 4** do „Polityki bezpieczeństwa danych osobowych“.

W przypadku, gdy w umowie na świadczenie usług zawartej z podmiotem przetwarzającym uwzględnione są wszystkie wymogi wynikające w RODO, nie ma konieczności sporządzania dodatkowo pisemnej umowy powierzenia.

Współadministrowanie

Współadministrowanie ma miejsce wówczas, gdy więcej niż jeden administrator decyduje o celach i środkach przetwarzania, tzn. decydują o nich wspólnie. Zasady współadministrowania określa art. 26 RODO. Współadministratorami danych może zostać co najmniej dwóch administratorów, którzy zobowiązani są do wspólnego ustalenia:

- celów przetwarzania danych osobowych,
- sposobów (technicznych i organizacyjnych) przetwarzania,
- uzgodnienia relacji zachodzących pomiędzy nimi,
- ustalenia odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO.

Treść tych uzgodnień musi zostać udostępniona osobom, których dane dotyczą. Może ona być udostępniona zarówno w formie papierowej jak i elektronicznej, np. na stronie internetowej.

Osoba, której dane dotyczą, musi zostać poinformowana o wszystkich Administratorach, którzy wspólnie decydują o celach i środkach dla przetwarzania jej danych.

Osoba, której dane dotyczą, może dochodzić swoich praw przysługujących jej w myśl RODO wobec każdego z Administratorów.

Obowiązki Administratora Danych Osobowych

W sferze administracyjnej

1. Zapewnienie odpowiednich pomieszczeń, stosownie zabezpieczonych i wyposażonych do procesu przetwarzania i przechowywania danych osobowych.
2. Zapewnienie ciągłości stosowania odpowiednich środków technicznych i organizacyjnych oraz w razie potrzeby poddawanie ich przeglądom i uaktualnianie.
3. Wdrożenie odpowiednich procedur przetwarzania danych osobowych.
4. Weryfikowanie tożsamości osób wnoszących żądania udzielenia informacji.
5. Ułatwianie osobom, których dane są przetwarzane, wykonywanie ich praw.

W sferze pracowniczej

1. Upoważnianie pracowników do przetwarzania danych osobowych tylko w zakresie niezbędnym do wykonywania obowiązków na danym stanowisku.
2. Zaznajomienie pracowników z prawnymi oraz pracowniczymi konsekwencjami naruszenia bezpieczeństwa danych.
3. Delegowanie pracowników na okresowe szkolenia w zakresie bezpieczeństwa informacji.
4. Podział zadań i obowiązków związanych z organizacją ochrony danych osobowych, w szczególności wyznaczenie Inspektora Ochrony Danych oraz Administratora Systemu Informatycznego.

Obowiązki Inspektora Ochrony Danych

W obszarze administracyjnym

1. Monitorowanie przestrzegania przepisów RODO przez ADO i podmioty przetwarzające w sferze ochrony danych osobowych.
2. Informowanie ADO, podmioty przetwarzające oraz pracowników przetwarzających dane o zmianach przepisów o ochronie danych osobowych.
3. Współpraca z organem nadzorczym (Urząd Ochrony Danych Osobowych).
4. Pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych w Urzędzie.
5. Pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych.
6. Koordynacja procesu analizy i oceny ryzyka związanego z przetwarzaniem danych w Urzędzie.
7. Opiniowanie wszelkich zmian zachodzących przy procesie przetwarzania danych pod kątem ich wpływu na bezpieczeństwo.
8. Współpraca przy zatwierdzaniu wzorów dokumentów dotyczących ochrony danych osobowych przygotowywanych przez komórki organizacyjne Urzędu (odpowiednie klauzule w dokumentach).
9. Koordynacja i aktywny udział w procesie reagowania na incydenty w zakresie naruszenia bezpieczeństwa danych osobowych.

W sferze pracowniczej

Przeprowadzanie szkoleń z bezpieczeństwa informacji dla wszystkich osób upoważnionych do przetwarzania danych osobowych w UM. Szkolenia powinny być ponawiane w przypadku zmian w obowiązujących przepisach prawa, uregulowaniach wewnętrznych lub zmian środków technicznych i organizacyjnych stosowanych przez ADO.

W obszarze dokumentacyjnym

Prowadzenie i aktualizowanie dokumentacji ochrony danych osobowych, w tym:

- Rejestru przetwarzania danych osobowych.
- Wykazu osób, którym nadano upoważnienia do przetwarzania danych osobowych. Ewidencję tych osób stanowi **Załącznik nr 2** do „Procedur zarządzania dostępem do systemu przetwarzania danych osobowych".
- Ewidencji osób, które złożyły oświadczenie o zachowaniu poufności. Wzór oświadczenia wraz z wykazem osób stanowi **Załącznik nr 3** do „Procedur zarządzania dostępem do systemu przetwarzania danych osobowych".
- Wykazu podmiotów, z którymi zawarto umowy powierzenia przetwarzania danych osobowych w rozumieniu RODO oraz sporządzanie umów powierzenia zgodnie z obowiązującymi przepisami. Wykaz podmiotów, z którymi zawarto umowy powierzenia stanowi **Załącznik nr 4**, natomiast wzór umowy powierzenia stanowi **Załącznik nr 3** do „Polityki bezpieczeństwa danych osobowych".

- Raz do roku sporządzanie sprawozdania z przeprowadzenia sprawdzenia wewnętrznego w obszarze ochrony danych. Sprawozdanie stanowi **Załącznik nr 7** do „Polityki bezpieczeństwa danych osobowych".
- Sporządzanie zgłoszeń naruszenia ochrony danych osobowych do organu nadzorczego w przypadku incydentów oraz prowadzenia rejestru tych incydentów. Wzór zgłoszenia stanowi **Załącznik nr 1,** a rejestr incydentów - **Załącznik nr 2** do „Procedur reagowania na naruszenia ochrony danych osobowych".
- Zawiadomienia osoby, której dane dotyczą o naruszeniu ochrony jej danych. Wzór zawiadomienia stanowi **Załącznik nr 3** do „Procedur reagowania na naruszenia ochrony danych osobowych".

Inspektor Ochrony Danych wyznaczany jest przez ADO drogą pisemnego upoważnienia. Wzór upoważnienia Inspektora OD stanowi **Załącznik nr 5** do „Polityki bezpieczeństwa danych osobowych".

Sprawdzenia zgodności przetwarzania danych osobowych z przepisami ODO

Inspektor OD przeprowadza co najmniej raz w roku, w terminie uzgodnionym z ADO, przeglądy przestrzegania przez użytkowników przepisów w zakresie ochrony danych osobowych, z czego sporządza odpowiednie sprawozdanie do ADO. Przegląd taki polega w szczególności na sprawdzeniu:

- dostępu do danych osobowych przez pracowników oraz jego zakresu,
- sposobu i zakresu udostępniania danych osobowych innym podmiotom,
- stosowania środków organizacyjnych i technicznych określonych w dokumentacji ochrony danych osobowych,
- zgodności z obowiązującymi przepisami prawa uregulowań zawartych w dokumentacji ODO oraz dostosowania procedur i instrukcji w niej zawartych do ewentualnych zmian środków technicznych i organizacyjnych w jednostce.

Sprawozdanie sporządzane jest z wyszczególnieniem obszarów, w których występują zagrożenia dla bezpiecznego przetwarzania danych osobowych oraz wskazaniem metod i środków poprawy bezpieczeństwa bądź wyeliminowania tych zagrożeń. Wzór sprawozdania z przeprowadzenia sprawdzenia stanowi **Załącznik nr 7** do „Polityki bezpieczeństwa danych osobowych".

Sprawozdanie takie sporządzane jest również bezpośrednio po wykonaniu czynności sprawdzających w trybie sprawdzenia doraźnego, w przypadku wystąpienia incydentu naruszenia ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia.

Obowiązki Administratora Systemu Informatycznego

W zakresie systemu informatycznego

1. Administrowanie i konserwacja systemu informatycznego.
2. Nadzór nad tworzeniem kopii zapasowych przetwarzanych danych.
3. Monitorowanie poziomu bezpieczeństwa w systemie informatycznym oraz przekazywanie informacji o zagrożeniach Inspektorowi OD, a w przypadku jego nieobecności bezpośrednio ADO.

4. Kontrolowanie przestrzegania zasad bezpiecznego przetwarzania danych w systemie informatycznym przez pracowników Urzędu.
5. Aktywny udział w procesie reagowania na incydenty w zakresie bezpieczeństwa oraz usuwania ich skutków.

W sferze pracowniczej

1. Nadawanie uprawnień dla kont użytkowników systemu informatycznego zgodnie z poleceniem ADO.
2. Zmiana zakresu uprawnień w systemie w przypadku zmiany stanowiska służbowego lub zakresu obowiązków pracowników.
3. Odbieranie uprawnień kontom użytkowników, u których zakończył się okres zatrudnienia.
4. Przeprowadzanie instruktażu prawidłowego postępowania z systemem informatycznym dla osób nowo zatrudnionych.
5. Przeprowadzanie szkoleń z zasad bezpiecznej pracy, pozwalających unikać szkodliwego oprogramowania, a także z zasad postępowania w przypadku wykrycia lub podejrzenia działania złośliwego oprogramowania.

W zakresie prowadzenia dokumentacji związanej z ochroną danych

Prowadzenie i aktualizacja:

- rejestru haseł administracyjnych do zarządzania i administrowania systemem informatycznym,
- rejestru osób, którym nadano uprawnienia w systemie informatycznym.

Administrator Systemu Informatycznego wyznaczany jest przez Administratora Danych Osobowych drogą pisemnego upoważnienia. Wzór upoważnienia ASI stanowi **Załącznik nr 6** do „Polityki bezpieczeństwa danych osobowych“.

Obowiązki osób upoważnionych do przetwarzania danych osobowych

Ochrona danych osobowych przetwarzanych w Urzędzie Miejskim w Żarowie dotyczy wszystkich osób (pracowników i współpracowników), które mają dostęp do informacji zbieranych, przetwarzanych oraz przechowywanych tak w formie tradycyjnej, jak i za pomocą systemu informatycznego bez względu na pełnioną funkcję służbową, zajmowane stanowisko oraz miejsce wykonywania pracy, w tym charakter stosunku pracy. Obowiązek zachowania tajemnicy istnieje również po ustaniu zatrudnienia/współpracy.

Do obowiązków osób przetwarzających dane osobowe należy:

1. Przetwarzanie danych osobowych na terenie Urzędu tylko w wyznaczonych do tego celu pomieszczeniach lub ich częściach.

2. Zabezpieczenie zbiorów danych osobowych oraz dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych za pomocą środków określonych w niniejszej dokumentacji.
3. Nieudzielanie informacji o danych osobowych przetwarzanych w jednostce innym podmiotom, chyba, że obowiązek taki wynika z przepisów prawa.
4. Bezzwłoczne zawiadomienie Inspektora OD lub Administratora Danych Osobowych o wszelkich przypadkach naruszenia bezpieczeństwa danych osobowych, a także o przypadkach utraty lub kradzieży dokumentów lub innych nośników zawierających dane osobowe.
5. Wykorzystywanie komputerów służbowych tylko i wyłącznie do realizacji zadań i obowiązków służbowych.
6. Tworzenie kopii zapasowych dokumentów tworzonych i przechowywanych na lokalnych stacjach roboczych bądź laptopach służbowych przy pomocy udostępnionych przez ASI mechanizmów lub programów.
7. Wykorzystywanie sieci lokalnej, poczty służbowej jak i dostępu do Internetu tylko i wyłącznie w zakresie wymaganym do prawidłowego wykonywania obowiązków służbowych.

Do obowiązków kierującego komórką organizacyjną należy:

1. Wnioskowanie do ADO o nadanie upoważnienia do przetwarzania danych osobowych oraz określanie jego zakresu dla podległych mu pracowników oraz osób wykonujących pracę w ramach umowy cywilno-prawnej (również stażystów, praktykantów i wolontariuszy).
2. Wnioskowanie do ADO o odebranie lub modyfikację upoważnienia w przypadku zmian, które mają wpływ na zakres tego upoważnienia (np. zmiana komórki organizacyjnej, zmiana zakresu zadań, zwolnienie ze świadczenia pracy).
3. Odpowiednie postępowanie w przypadku wystąpienia incydentów naruszeń ochrony danych, zgodnie z „Procedurami reagowania na naruszenia ochrony danych osobowych".
4. Współpraca z Inspektorem OD oraz z Administratorem Systemu Informatycznego w zakresie przestrzegania ochrony danych przez podległych pracowników oraz inne osoby upoważnione do przetwarzania, podlegające kierownikowi komórki organizacyjnej.

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Zasady zapewniające bezpieczeństwo danych osobowych realizowane są w Urzędzie Miejskim w Żarowie poprzez zapewnienie danym osobowym cech:

- poufności - właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom,
- integralności - właściwości zapewniającej, że dane osobowe nie zostały zmienione w sposób nieautoryzowany lub nieuprawniony,
- rozliczalności - właściwości zapewniającej, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

W celu zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych wprowadza się następujące środki ochrony fizycznej i organizacyjnej:

1. Wprowadzono politykę bezpieczeństwa przetwarzania danych.
2. Wyznaczono Administratora Systemu Informatycznego.
3. Powołano Inspektora Ochrony Danych.
4. Dostęp do danych osobowych mają tylko osoby upoważnione.
5. Osoby upoważnione zostały zaznajomione z zasadami dotyczącymi ochrony danych osobowych oraz zobowiązane do zachowania ich w tajemnicy.
6. Osoby upoważnione zostały przeszkolone w zakresie ochrony danych osobowych na stanowisku pracy oraz ich bezpiecznego przetwarzania w systemie informatycznym.
7. Inspektor Ochrony Danych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.
8. Budynki Urzędu oraz teren wokół nich objęto działaniem monitoringu wizyjnego. Kamery rozmieszczone zostały na zewnątrz budynków w sposób umożliwiający objęcie swoim zasięgiem jak największego obszaru w miejscach o strategicznym znaczeniu ze względów bezpieczeństwa.
9. Budynki spełniają przepisy dotyczące ochrony przeciwpożarowej. Pomieszczenia wchodzące w skład obszaru przetwarzania zabezpieczone są przed skutkami pożaru za pomocą systemu przeciwpożarowego i wyposażone w sprzęt ppoż. zgodnie z obowiązującymi przepisami.
10. Pomieszczenia, w których przetwarzane są dane osobowe, zabezpieczone są drzwiami zamykanymi na klucz. Klucze do tych pomieszczeń udostępniane są jedynie osobom upoważnionym przez Administratora Danych Osobowych.
11. Osoby nieupoważnione mogą przebywać w obszarze przetwarzania danych wyłączenie w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności.
12. W przypadku, gdy w pomieszczeniu znajduje się część ogólnodostępna oraz część, w której przetwarzane są dane osobowe (np. sekretariat), to część, w której przetwarzane są dane osobowe jest wyraźnie oddzielona od części ogólnodostępnej (np. poprzez odpowiednie ustawienie mebli biurowych uniemożliwiające lub co najmniej ograniczające niekontrolowany dostęp osób niepowołanych do urządzeń lub zbiorów danych osobowych).
13. Dokumenty i nośniki elektroniczne zawierające dane osobowe przechowywane są w segregatorach znajdujących się w szafach na akta zamykanych na klucz oraz zamykanych szafach stalowych.
14. Po ustaniu przydatności dokumentacja papierowa zawierająca dane osobowe jest niszczona mechanicznie przy użyciu niszczarek dokumentów (na wyposażeniu).
15. Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe przeznaczone do likwidacji, pozbawiane są wcześniej zapisu tych danych i niszczone mechanicznie w sposób uniemożliwiający ich użycie oraz odczyt, a w przypadku, gdy nie jest to możliwe, przeznaczane do utylizacji z uzyskaniem potwierdzenia zniszczenia (protokół likwidacji).
16. Monitory komputerów, w których przetwarzane są dane osobowe, zlokalizowane są w sposób uniemożliwiający osobom trzecim podgląd wyświetlanych danych.
17. Podczas chwilowej nieobecności na stanowisku pracy lub krótkiej przerwy w pracy, pracownicy zobowiązani są do uruchomienia wygaszacza ekranu na swojej stacji roboczej.
18. Na każdym stanowisku pracy stosuje się zasadę „czystego biurka“ :
    - na biurku znajdują się dokumenty zawierające dane osobowe osób obsługiwanych w danej chwili, tylko w czasie niezbędnym do wykonania czynności służbowych, a następnie chowane są do zamykanych szaf/mebli biurowych,

- odchodząc od biurka pracownik nie pozostawia dokumentów i nośników zawierających dane osobowe bez nadzoru,
- po zakończeniu pracy dokumenty, nośniki z danymi oraz komputery przenośne zabezpiecza się w zamkniętych szafach/meblach biurowych.

W celu zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych, wprowadza się następujące środki sprzętowe, informatyczne i telekomunikacyjne:

1. Sprzęt komputerowy, drukarki, kserokopiarki oraz niszczarki dokumentów rozlokowane są w pomieszczeniach w sposób minimalizujący dostęp do nich przez osoby postronne.
2. Okablowanie sieciowe zostało rozlokowane w sposób umożliwiający bezpośredni dostęp do niego tylko z pomieszczeń zamykanych na klucz.
3. Zastosowano urządzenia typu UPS chroniące newralgiczne urządzenia systemu informatycznego służące do przetwarzania danych osobowych przed skutkami awarii zasilania.
4. Na serwerze i wszystkich stanowiskach służących do przetwarzania danych osobowych zastosowano oprogramowanie antywirusowe z codzienną aktualizacją bazy sygnatur wirusów.
5. Udostępnienie użytkownikom systemu informatycznego zasobów zawierających dane osobowe następuje na podstawie uprawnień w systemie nadanych przez Administratora Danych Osobowych.
6. Dostęp do zasobów zawierających dane osobowe jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła zabezpieczającego.
7. Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbiorów danych osobowych.
8. Hasła zabezpieczające składają się z minimum 8 znaków, zawierających małe i wielkie litery oraz cyfry lub znaki specjalne.
9. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności użytkownika.
10. Zastosowano cykliczne tworzenie kopii zapasowych w celu ochrony danych osobowych przed utratą.

Postanowienia końcowe

1. Niniejsza „Polityka bezpieczeństwa danych osobowych“ powinna być aktualizowana wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi w Urzędzie, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.
2. Zmiany niniejszej „Polityki bezpieczeństwa danych osobowych“ wymagają przeglądu innych dokumentów dotyczących ochrony danych osobowych obowiązujących w Urzędzie.
3. Osoby upoważnione zobowiązane są do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej dokumentacji ochrony danych osobowych. W wypadku odrębnych od zawartych w dokumentacji uregulowań występujących w innych procedurach lub dokumentach, osoby upoważnione mają obowiązek stosowania zapisów o wyższym poziomie ochrony danych osobowych.

4. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszej dokumentacji ochrony danych osobowych mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, co niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, może być podstawą do wyciągnięcia wniosków dyscyplinarnych wobec osoby, która dopuściła się ich naruszenia.
5. Wobec osoby, która w przypadku naruszenia zasad bezpieczeństwa lub uzasadnionego domniemania takiego naruszenia nie podjęła działań określonych w niniejszej dokumentacji, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.

Załączniki

Załącznik nr 1	- Klauzula informacyjna - wzór ogólny.
Załącznik nr 2	- Klauzula zgody - wzór ogólny.
Załącznik nr 3	- Umowa powierzenia przetwarzania danych.
Załącznik nr 4	- Wykaz podmiotów, z którymi zawarto umowy powierzenia.
Załącznik nr 5	- Upoważnienie Inspektora Ochrony Danych.
Załącznik nr 6	- Upoważnienie Administratora Systemu Informatycznego.
Załącznik nr 7	- Sprawozdanie z przeprowadzenia sprawdzenia wewnętrznego w obszarze ochrony danych.

Regulamin monitoringu wizyjnego

Urząd Miejski w Żarowie

ul. Zamkowa 2
58-130 Żarów

Dokument do użytku służbowego
Wykonał: mgr inż. Piotr Chałaszczyk
- Inspektor Ochrony Danych
Data aktualizacji: 25.03.2021 r.

Spis treści

Wstęp

Regulamin określa zasady funkcjonowania systemu monitoringu wizyjnego na terenie Urzędu Miejskiego w Żarowie, miejsca instalacji kamer, reguły zapisu informacji oraz sposób ich zabezpieczenia, a także możliwość udostępniania zgromadzonych danych o zdarzeniach.

Podstawa prawna

1. Rozporządzenie Parlamentu Europejskiego i Rady 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 rozporządzenia 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), dalej zwane także rozporządzeniem lub RODO.
2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.

Cele monitoringu

1. Ochrona bezpieczeństwa osób i mienia.
2. Ochrona porządku publicznego.
3. Profilaktyka zachowań niepożądanych, destrukcyjnych, zagrażających zdrowiu i bezpieczeństwu.
4. Wyjaśnianie sytuacji konfliktowych.
5. Możliwość ustalania sprawców czynów nagannych (bójki, zniszczenie mienia, kradzieże, itp.)
6. Pozyskiwanie materiału dowodowego.

Zasady funkcjonowania monitoringu wizyjnego

1. Każdy pracownik Urzędu jest poinformowany o funkcjonowaniu monitoringu na jego terenie.
2. Każdy nowo przyjęty pracownik jest informowany o funkcjonowaniu monitoringu podczas procesu zatrudnienia.
3. Miejsca objęte monitoringiem wizyjnym oznakowane są tabliczkami informacyjnymi w sposób widoczny i czytelny.
4. Monitoring nie stanowi środka nadzoru nad jakością wykonywania pracy przez pracowników UM.
5. Monitoring nie obejmuje pomieszczeń socjalnych i sanitarno-higienicznych.
6. Nagrania obrazu zawierające dane osobowe pracowników i innych osób, których w wyniku tych nagrań można zidentyfikować, przetwarzane są wyłącznie do celów, dla których zostały zebrane i przechowywane są przez okres ustalony przez Burmistrza (30 dni).
7. Po upływie okresu ustalonego przez ADO uzyskane w wyniku monitoringu nagrania obrazu podlegają zniszczeniu.

Organizacja systemu monitoringu wizyjnego

1. Monitoring, w skład którego wchodzą kamery oraz rejestrator, umożliwia zapisywanie i odtwarzanie nagrań.
2. Rejestracji i zapisowi na nośniku fizycznym podlega tylko obraz (wizja) z kamer systemu monitoringu, nie rejestruje się dźwięku (fonii).
3. Monitoring funkcjonuje całą dobę.
4. Elementy monitoringu wizyjnego w miarę konieczności i możliwości finansowych są udoskonalane, wymieniane i rozszerzane.
5. Dostęp do danych z monitoringu zapisanych na dysku i możliwość zgrania danych, a także do obserwowania obrazu mają pracownicy Urzędu Miejskiego w Żarowie upoważnieni przez Burmistrza. Rejestr osób upoważnionych do obserwowania i odczytu obrazu stanowi **Załącznik nr 2** do „Regulaminu monitoringu wizyjnego".

Części składowe monitoringu wizyjnego

1. System monitoringu w Urzędzie Miejskim w Żarowie składa się z:
   - kamer rejestrujących zdarzenia obejmujących swoim zasięgiem obszar na zewnątrz budynku

Oznaczenie kamery	Miejsca objęte zasięgiem kamery
Kamera 1	Parking z tyłu budynku Urzędu.
Kamera 2	OK i przejście dla pieszych.
Kamera 3	Od frontu budynku skierowana na ul. Armii Krajowej.
Rejestrator	II piętro, szafa rozdzielcza sieci komputerowej.

   - urządzenia rejestrującego i zapisującego obraz na nośniku fizycznym,
   - kolorowego monitora pozwalającego na podgląd rejestrowanych zdarzeń.
2. Do rejestracji obrazu służą urządzenia wchodzące w skład systemu rejestracji spełniającego wymogi określone Polską Normą PN-EN 50132-7 dla systemów dozorowanych CCTV.

Zasady udostępniania zapisów monitoringu wizyjnego

1. Zapis monitoringu może być udostępniony w formie oglądu za zgodą Burmistrza:
   - pracownikom Urzędu,
   - osobie, której niewłaściwe zachowanie, jak: agresja fizyczna, niszczenie mienia, kradzieże, itp. zarejestrowały kamery, w celu udowodnienia jej takiego zachowania i podjęcia działań interwencyjnych,
   - osobie poszkodowanej w celu oceny zaistniałej sytuacji i uzgodnienia wspólnych działań interwencyjnych, a także udzielenia jej właściwej pomocy.

2. Dane te udostępnia się ponadto uprawnionym instytucjom w zakresie prowadzonych przez nie czynności prawnych, np. policji, sądom, prokuraturze.
3. Dysk przenośny z materiałem może być nagrany i przekazany organom ścigania na ich pisemny wniosek w celu wyjaśnienia prowadzonej sprawy.
4. Osoby, które mają wgląd w obraz zarejestrowany przez monitoring wizyjny, mają świadomość odpowiedzialności za ochronę danych osobowych.

Zasady obowiązujące przy przekazywaniu nośnika elektronicznego z materiałem archiwalnym organom ścigania

1. Przedstawiciel organów ścigania składa pisemnie wniosek o udostępnienie danych z monitoringu wizyjnego na nośniku elektronicznym oraz kwituje jego odbiór.
2. We wniosku określa cel otrzymania nagrania z monitoringu.
3. Przykładowy wniosek o udostępnienie danych z monitoringu wizyjnego stanowi **Załącznik nr 1** do „Regulaminu monitoringu wizyjnego”.
4. Przegrywania materiału z rejestratora dokonywać mogą tylko pracownicy Urzędu upoważnieni przez Burmistrza Miasta Żarów.

Postanowienia końcowe

1. Niniejszy Regulamin stanowi integralną część dokumentacji ochrony danych osobowych w Urzędzie Miejskim w Żarowie.
2. Zapis z systemu monitoringu wizyjnego stanowi zbiór danych osobowych w myśl RODO i podlega ewidencji.
3. W sprawach nieuregulowanych niniejszym Regulaminem ostateczną decyzję podejmuje Burmistrz Miasta Żarów.

Załączniki

Załącznik nr 1	- Wniosek o udostępnienie danych z monitoringu wizyjnego.
Załącznik nr 2	- Rejestr osób upoważnionych do obserwowania i odczytu obrazu monitoringu wizyjnego.

Procedury zarządzania dostępem do systemu przetwarzania danych osobowych

Urząd Miejski w Żarowie

ul. Zamkowa 2
58-130 Żarów

Dokument do użytku służbowego
Wykonał: mgr inż. Piotr Chałaszczyk
- Inspektor Ochrony Danych
Data aktualizacji: 25.03.2021 r.

Spis treści

Zasady dotyczące dostępu do systemu przetwarzania danych osobowych

1. Dostęp do systemu przetwarzania danych osobowych w Urzędzie Miejskim w Żarowie może uzyskać wyłącznie osoba upoważniona do przetwarzania danych przez Administratora Danych Osobowych. Dotyczy to zarówno dostępu do systemu tradycyjnego (kartotek, ksiąg, skorowidzów, akt osobowych, wykazów itp.), jak i systemu informatycznego. Wzór upoważnienia stanowi **Załącznik nr 1** do „Procedur zarządzania dostępem do systemu przetwarzania". Wszystkie osoby upoważnione do przetwarzania danych osobowych ujęte są w wykazie, który prowadzi i aktualizuje Inspektor Ochrony Danych. Wykaz stanowi **Załącznik nr 2** do „Procedur zarządzania dostępem do systemu przetwarzania".
2. Dostęp do systemu informatycznego, w którym przetwarzane są dane osobowe, może uzyskać wyłącznie osoba upoważniona do przetwarzania przez Administratora Danych Osobowych i zarejestrowana jako użytkownik w systemie informatycznym przez Administratora Systemu Informatycznego na podstawie wniosku bezpośredniego przełożonego użytkownika.
3. Każdy upoważniony do przetwarzania pracownik, a także każda upoważniona osoba, zatrudniona w Urzędzie na innej podstawie niż stosunek pracy (np. umowy zlecenia), również stażysta lub praktykant, przed przystąpieniem do systemu przetwarzania jest zobowiązana odbyć szkolenie, zapoznać się z zasadami ochrony danych osobowych opisanymi w niniejszej dokumentacji oraz podpisać oświadczenie o zachowaniu poufności. Oświadczenie zawarte jest w „Upoważnieniu do przetwarzania danych osobowych" (**Załącznik nr 1** do „Procedur zarządzania dostępem do systemu przetwarzania").
4. Osoba upoważniona do przetwarzania danych osobowych może je przetwarzać wyłącznie w zakresie ustalonym przez Administratora Danych Osobowych, tylko w celu wykonywania nałożonych na nią obowiązków.
5. Zakres dostępu do zbiorów danych osobowych w systemie informatycznym UM przypisany jest do unikatowego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie.
6. Pracownicy Urzędu nieupoważnieni do przetwarzania danych osobowych, wykonujący prace techniczne, porządkowe i konserwatorskie itp. są zobowiązani do podpisania oświadczenia o zachowaniu poufności (**Załącznik nr 3** do „Procedur zarządzania dostępem do systemu przetwarzania").
7. W przypadku konieczności dostępu do obszaru przetwarzania osób nieupoważnionych (niebędących pracownikami UM), które muszą dokonać doraźnych prac o charakterze serwisowym lub innym, podpisują one oświadczenie o zachowaniu poufności (**Załącznik nr 3**), chyba że czynności odbywają się pod nadzorem osoby upoważnionej do przetwarzania danych.
8. Firmy wykonujące na rzecz Urzędu prace zlecone, zobowiązane są do zapewnienia środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzanych danych, a pracownicy tych firm muszą się stosować do zasad ochrony danych osobowych w nich obowiązujących.

Obszar przetwarzania danych osobowych

W Urzędzie Miejskim w Żarowie dane osobowe mogą być przetwarzane wyłącznie w obszarach przetwarzania znajdujących się w siedzibie jednostki organizacyjnej.

Obszarami przetwarzania danych osobowych w UM ustanowiono wszystkie pomieszczenia lub ich wydzielone części, w których dane osobowe zarówno w formie papierowej jak i elektronicznej są tworzone, gromadzone i przechowywane w okresie bieżącego przetwarzania, jak i w postaci archiwów zawartych na nośnikach informatycznych, wydrukach, kartotekach, rejestrach itp.

Obszar przetwarzania danych osobowych w Urzędzie obejmuje pomieszczenia biurowe użytkowane przez kierownictwo Urzędu oraz kierowników i pracowników poszczególnych komórek organizacyjnych:

- Referatu Organizacyjnego **O**,
- Urzędu Stanu Cywilnego **USC**,
- Biura Obsługi Klienta **BOK**,
- Referatu Finansowo-Budżetowego **FB**,
- Referatu Rozwoju **R,**
- Referatu Gospodarki Komunalnej i Inwestycji **GKiL**,
- Referatu Nieruchomości, Gospodarki Przestrzennej i Lokalowej **NGPiL**,
- pracowników na stanowiskach samodzielnych.

Obszar przetwarzania natomiast nie obejmuje ciągów komunikacyjnych, takich jak korytarze, schody i hole oraz pomieszczeń sanitarno-higienicznych, pomieszczeń socjalnych, gospodarczych i szatni.

Gospodarka kluczami

1. Kluczami do pomieszczeń należących do obszaru przetwarzania dysponują tylko pracownicy upoważnieni przez Administratora Danych Osobowych.
2. Klucze do pomieszczeń, biurek stanowiskowych, szaf biurowych pozostają pod osobistym nadzorem osób upoważnionych w trakcie wykonywania przez nich obowiązków i osoby te ponoszą za nie pełną odpowiedzialność. Podczas chwilowej nieobecności w pomieszczeniu, pracownicy nie pozostawiają w nim kluczy służących do zabezpieczenia biurek i szaf.
3. Klucze do pomieszczeń szczególnie chronionych pozostają pod osobistym nadzorem osób do tego upoważnionych. Dostęp osób nieupoważnionych do tych pomieszczeń odbywa się pod ścisłym nadzorem osób upoważnionych.
4. Klucze zapasowe wydawane są osobom upoważnionym tylko w uzasadnionych sytuacjach oraz przypadkach awaryjnych. Klucze zapasowe po ich wykorzystaniu zwracane są do depozytu.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym

Procedura rozpoczęcia pracy w systemie informatycznym

1. Użytkownik systemu rozpoczynający pracę zobowiązany jest do sprawdzenia zabezpieczeń fizycznych pomieszczenia, a także ogólnego stanu sprzętu informatycznego oraz miejsca przechowywania nośników zawierających dane osobowe. W przypadku zauważenia jakichkolwiek nieprawidłowości w działaniu sprzętu informatycznego lub oprogramowania użytkownik zobowiązany jest niezwłocznie zgłosić ten fakt Administratorowi Systemu Informatycznego.

2. Rozpoczęcie pracy na stacji roboczej następuje po wprowadzeniu indywidualnego identyfikatora oraz hasła, mając na uwadze, iż po przekroczeniu określonej liczby prób logowania, dany system informatyczny blokuje dostęp do zbiorów danych na poziomie użytkownika. Użytkownik powinien poinformować o tym zdarzeniu Administratora Systemu Informatycznego.
3. Logowanie się oraz praca na innych stanowiskach niż indywidualne stanowisko komputerowe użytkownika, wymaga zgody Administratora Danych Osobowych i jest dozwolone jedynie w sytuacjach wyjątkowych.
4. Użytkownik w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym ma obowiązek:
   - ustawienia monitorów w pomieszczeniach w sposób uniemożliwiający osobom nieupoważnionym podgląd,
   - zapewnienia, aby w obszarach przetwarzania danych osobowych osoby nieupoważnione nie przebywały bez nadzoru osoby upoważnionej.

Procedura zawieszenia pracy w systemie informatycznym

W przypadku konieczności zawieszenia pracy w systemie informatycznym z powodu tymczasowego opuszczenia stanowiska pracy, użytkownik zobowiązany jest do:

- aktywowania wygaszacza ekranu, zabezpieczonego hasłem,
- wylogowania się z systemu w przypadku, kiedy przerwa w pracy trwa dłużej niż 30 minut,
- niepozostawiania bez nadzoru nośników informacji zawierających dane osobowe - dotyczy to także okresu po zakończeniu pracy (obowiązuje tzw. zasada „czystego biurka” i „czystego ekranu”).

Procedura zakończenia pracy w systemie informatycznym

Przed zakończeniem pracy w systemie informatycznym użytkownik zobowiązany jest:

- zapisać wszelkie zmiany w otwartych aplikacjach,
- wykonać kopie zapasowe, jeżeli jest to przewidziane w dokumentacji systemu,
- zamknąć wszystkie używane programy,
- sprawdzić, czy w urządzeniach nie pozostały wymienne elektroniczne nośniki informacji,
- wyłączyć urządzenia peryferyjne (drukarka, skaner itp.),
- wylogować się i zamknąć system,
- sprawdzić, czy pozostawione stanowisko nie stwarza jakichkolwiek zagrożeń i czy jest prawidłowo zabezpieczone przed uruchomieniem przez osoby postronne.

Metody uwierzytelnienia użytkowników w systemie informatycznym

W Urzędzie Miejskim w Żarowie system informatyczny, w którym przetwarza się dane osobowe, wyposażony jest w mechanizmy uwierzytelniania użytkowników przy pomocy identyfikatora i hasła. Po zalogowaniu się do systemu informatycznego dostęp do poszczególnych programów, baz danych i aplikacji, w których przetwarzane są dane osobowe, jest możliwy po dokonaniu uwierzytelnienia również za pomocą identyfikatora i hasła, i powinien przebiegać zgodnie z instrukcją zawartą w dokumentacji programu/aplikacji.

1. W Urzędzie Miejskim w Żarowie funkcjonuje elektroniczny system obiegu dokumentacji PROSOD pozwalający na zarządzanie, obieg i archiwizację dokumentów Urzędu. Dokumenty zgromadzone są w jednym miejscu na serwerze, a dostęp do nich jest kontrolowany przez system uprawnień użytkowników po dokonaniu uwierzytelnienia za pomocą identyfikatora i hasła.
2. Dostęp do danych geodezyjnych na terenie Gminy Żarów umożliwia pracownikom serwerowa aplikacja internetowa WebEWID.
3. Systemem służącym do zapewnienia bieżącej działalności Urzędu jest zintegrowany system informatyczny MAGISTRAT.
4. Do obsługi gospodarki komunalno-mieszkaniowej wykorzystywany jest system informatyczny THB SEZaM.

Identyfikator użytkownika

1. Każdy użytkownik systemu informatycznego posiada swój unikatowy identyfikator.
2. Użytkownicy nie mogą używać tych samych identyfikatorów ani wymieniać się nimi.
3. Identyfikator po wyrejestrowaniu użytkownika z systemu informatycznego nie może być przydzielony innej osobie.
4. Kontrolę nad powyższymi czynnościami sprawuje Administrator Systemu Informatycznego.

Hasło użytkownika

1. Hasło dostępu ustala dla siebie użytkownik.
2. Hasło dostępu powinno składać się z unikatowego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry i znaki specjalne. Hasło nie może być identyczne z identyfikatorem użytkownika ani z jego imieniem lub nazwiskiem.
3. W systemie informatycznym zmiana haseł dostępu powinna następować co najmniej co 30 dni.
4. Za zmianę hasła odpowiada użytkownik.
5. Użytkownik niezwłocznie zmienia hasło w przypadku podejrzenia lub stwierdzenia: podglądu, przechwycenia, podsłuchania lub odgadnięcia.
6. Użytkownik zobowiązany jest do utrzymania hasła dostępu w tajemnicy zarówno w czasie zatrudnienia, jak też po jego ustaniu.
7. W sytuacji udostępnienia hasła innej osobie, użytkownik ponosi odpowiedzialność za skutki i następstwa wynikłe z faktu wykorzystania tego hasła przez osoby trzecie.
8. W przypadku zastosowania awaryjnego dostępu do systemu informatycznego na poziomie użytkownika (zapomniane hasło, blokada dostępu), Administrator Systemu Informatycznego nadpisuje hasło użytkownika za pomocą nowego hasła początkowego, po dokonaniu uprzedniej weryfikacji tożsamości użytkownika.
9. Hasła dostępu wyświetlane są na ekranie monitora w formie niedającej się odczytać osobom postronnym i mogą być znane tylko użytkownikowi.

Hasło Administratora Systemu Informatycznego

1. Hasła Administratora Systemu Informatycznego przechowywane są w postaci klasycznego zapisu w zabezpieczonej kopercie lub na elektronicznych nośnikach informacji CD-ROM (jednokrotnego

zapisu), w postaci odpowiednio zabezpieczonego pojedynczego pliku w bezpiecznym miejscu wyznaczonym przez Administratora Danych Osobowych.

2. W sytuacjach awaryjnych lub w razie nieobecności Administratora Systemu Informatycznego jego zadania spoczywają na osobach upoważnionych przez ADO. W przypadku wykorzystania haseł podczas nieobecności Administratora Systemu Informatycznego, muszą one być niezwłocznie zmienione po wznowieniu wykonywania obowiązków przez ASI.

Procedury nadawania, rejestrowania i odbierania uprawnień w systemie informatycznym

Nadanie uprawnień w systemie

1. Uprawnienia do przetwarzania danych osobowych w systemach informatycznych nadawane są wyłącznie pracownikom, którzy uzyskali upoważnienie do przetwarzania danych osobowych.
2. Zakres dostępu do danych przetwarzanych w systemie nie może być większy niż w wydanym wcześniej upoważnieniu.
3. Uprawnienia do przetwarzania danych osobowych w systemach informatycznych nadawane są na polecenie Administratora Danych Osobowych przez Administratora Systemu Informatycznego na podstawie wniosku o nadanie, modyfikację lub odebranie uprawnień do przetwarzania danych osobowych przedstawionego przez bezpośredniego przełożonego użytkownika. Wnioski ewidencjonowane są w rejestrze osób uprawnionych do przetwarzania danych w systemach informatycznych przez ASI.
4. Przydzielenie użytkownikowi uprawnień do przetwarzania danych w systemach informatycznych jest jednoznaczne z nadaniem mu loginu oraz hasła tymczasowego.
5. Administrator Systemu Informatycznego przekazuje użytkownikowi jego identyfikator i hasło inicjujące pracę w systemie informatycznym. Użytkownik, po otrzymaniu informacji o założonym koncie z wymaganymi uprawnieniami:
   - loguje się do systemu/aplikacji w celu sprawdzenia poprawności konta i uprawnień,
   - przy pierwszym logowaniu zmienia nadane mu przez Administratora Systemu hasło.

Odebranie uprawnień w systemie

1. Wyrejestrowania użytkownika z systemu informatycznego dokonuje Administrator Systemu Informatycznego na wniosek bezpośredniego przełożonego i polecenie Administratora Danych Osobowych.
2. Wyrejestrowanie użytkownika następuje poprzez:
   - zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
   - usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).
3. Użytkownika wyrejestrowuje się z systemu w sytuacji ustania jego zatrudnienia lub długotrwałej nieobecności w pracy.
   - Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony

był użytkownik. Rozwiązanie umowy o pracę powoduje utratę dostępu użytkownika do systemu informatycznego oraz do całego systemu przetwarzania danych.

- Podstawą czasowego wyrejestrowania użytkownika z systemu informatycznego może być:
  - nieobecność użytkownika w pracy trwająca dłużej niż 21 dni kalendarzowych,
  - zawieszenie w pełnieniu obowiązków służbowych,
  - wszczęcie postępowania dyscyplinarnego względem osoby upoważnionej do przetwarzania danych.

Zmiana danych identyfikacyjnych użytkownika

W przypadku zmiany danych identyfikacyjnych użytkownika, na wniosek bezpośredniego przełożonego użytkownika, Administrator Systemu Informatycznego dokonuje zmian w systemie informatycznym polegających na wyrejestrowaniu i ponownym zarejestrowaniu użytkownika ze zmienionymi danymi identyfikacyjnymi oraz nadaniu mu nowego identyfikatora i hasła inicjującego pracę w systemie.

Zmiana zakresu dostępu użytkownika

W przypadku zmiany zakresu dostępu użytkownika, na wniosek bezpośredniego przełożonego użytkownika, Administrator Systemu Informatycznego dokonuje zmian w systemie informatycznym polegających na wyrejestrowaniu i ponownym zarejestrowaniu użytkownika ze zmienionym zakresem dostępu oraz nadaniu mu nowego hasła inicjującego pracę w systemie. W przypadku zmiany zakresu dostępu, identyfikator użytkownika nie ulega zmianie.

Sposoby zabezpieczenia systemu informatycznego przed działaniem szkodliwego oprogramowania

1. Obszarami systemu informatycznego narażonymi na ingerencję wirusów oraz innego szkodliwego oprogramowania są m. in.: dysk twardy urządzenia, pamięć RAM, elektroniczne nośniki informacji np. płyty CD /DVD, pamięci USB.
2. Drogą przedostania się wirusów i szkodliwego oprogramowania do systemu mogą być sieci informatyczne, zainfekowane elektroniczne nośniki danych oraz załączniki poczty e-mail, pochodzące od nieznanych nadawców.
3. W celu zabezpieczenia przed atakami z sieci publicznej serwery i stacje robocze znajdujące się w sieciach LAN są chronione przez zaporę ogniową (firewall).
4. Na wszystkich stacjach roboczych i serwerach pracujących pod kontrolą systemu operacyjnego Microsoft Windows zainstalowany jest program antywirusowy.
5. Oprogramowanie antywirusowe sprawuje ciągły nadzór nad uruchamianymi lub wprowadzanymi do systemu programami oraz załącznikami poczty elektronicznej.
6. Za zabezpieczenie systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego odpowiada Administrator Systemu Informatycznego.
7. Użytkownicy systemu poddawani są szkoleniom co do stosowania zasad bezpieczeństwa danych w ramach wewnętrznych szkoleń adaptacyjnych:
   - z zasad bezpiecznej pracy pozwalających unikać szkodliwego oprogramowania,

- z zasad postępowania w przypadku wykrycia lub podejrzenia działania złośliwego oprogramowania (osobą odpowiedzialną za przeprowadzanie szkoleń w powyższym zakresie jest ADO, powierzając do zadanie Administratorowi Systemu Informatycznego).

Zasady korzystania z Internetu, poczty elektronicznej i oprogramowania

Zasady bezpiecznego użytkowania systemu informatycznego

1. Zabrania się użytkownikowi podłączania do systemu informatycznego nieautoryzowanych (prywatnych) nośników informacji. Do komputera można podłączać jedynie służbowe nośniki służące do przenoszenia danych lub tworzenia kopii zapasowych.
2. Zabrania się użytkownikowi przechowywania na służbowym komputerze jakichkolwiek materiałów niezwiązanych z wykonywanymi obowiązkami służbowymi. Zabrania się w szczególności przechowywania na służbowym komputerze materiałów naruszających prawa autorskie. Za wszelkie naruszenia praw autorskich związanych z nieuprawnionymi materiałami przechowywanymi lub pobieranymi na komputer służbowy odpowiada użytkownik.
3. Zabrania się podłączania prywatnych komputerów oraz innych urządzeń sieciowych do sieci LAN/WAN. Wymaga to akceptacji Administratora Danych Osobowych. Zabrania się również podłączania służbowych komputerów znajdujących się w obszarze funkcjonowania Urzędu nieautoryzowanych sieci LAN/WAN za pomocą urządzeń, które nie są częścią systemu informatycznego jednostki.

Zasady korzystania z oprogramowania

1. Zabrania się instalowania oraz używania oprogramowania innego niż udostępnione przez ADO.
2. Zabrania się kopiowania lub usuwania oprogramowania zainstalowanego w systemie informatycznym Urzędu.
3. Zabrania się przenoszenia programów komputerowych z własnego stanowiska roboczego na inne stanowisko.
4. Zabrania się uruchamiania programów otrzymanych pocztą elektroniczną.
5. Instalowanie jakiegokolwiek oprogramowania związanego z obsługą urządzeń peryferyjnych wchodzących w skład systemu informatycznego może być dokonane wyłącznie przez Administratora Systemu Informatycznego.

Zasady korzystania z Internetu

1. Użytkownik zobowiązany jest do korzystania z Internetu tylko w celach służbowych.
2. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
3. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu rozpoczynającego się frazą „https:”
4. Zabrania się odwiedzania stron o treściach prawnie zabronionych lub powszechnie uznanych za niebezpieczne.
5. Zabrania się pobierania z Internetu plików pochodzących z niewiarygodnych źródeł.

Zasady korzystania z poczty elektronicznej

1. W Urzędzie Miejskim w Żarowie przesyłanie wiadomości zawierających dane osobowe odbywa się wyłącznie przez osoby do tego upoważnione.
2. Każdemu użytkownikowi zostaje nadany dedykowany adres skrzynki poczty elektronicznej działający w domenie Administratora OD.
3. Informacja o służbowym adresie skrzynki pocztowej jest jawna i dostępna powszechnie, (np. na stronie internetowej Administratora).
4. Nadany użytkownikowi adres skrzynki poczty elektronicznej służy wyłącznie do realizacji celów służbowych lub umownych. Wszelka korespondencja elektroniczna niezwiązana z działalnością UM powinna być prowadzona przez prywatną skrzynkę poczty elektronicznej użytkownika.
5. Każdy użytkownik zobowiązany jest do:
   - zwracania szczególnej uwagi na poprawność adresu odbiorcy wiadomości,
   - stosowania metody UDW (ukryte do wiadomości) podczas wysyłania korespondencji do wielu adresatów jednocześnie,
   - nieotwierania wiadomości oraz załączników i linków otrzymanych od nieznanych nadawców (w takiej sytuacji należy skontaktować się z Administratorem Systemu Informatycznego),
   - wykorzystywania mechanizmów kryptograficznych (hasłowanie wysyłanych plików, podpis elektroniczny) w przypadku przesyłania danych osobowych.

Zasady postępowania z elektronicznymi nośnikami informacji zawierającymi dane osobowe

1. Elektroniczne nośniki informacji zawierające dane osobowe na czas ich użyteczności przechowywane są w zamkniętych na klucz szafach/zabezpieczonych meblach biurowych.
2. W przypadku dalszego wykorzystywania w innych celach, nośniki pozbawiane są zapisu danych w sposób uniemożliwiający ich odzyskanie.
3. Elektroniczne nośniki informacji, które zostały przeznaczone do likwidacji, pozbawiane są wcześniej zapisu danych, a w przypadku gdy nie jest to możliwe, uszkadzane w sposób uniemożliwiający ich odczytanie.
4. Zabrania się wynoszenia z Urzędu na jakichkolwiek nośnikach całych zbiorów danych lub jakichkolwiek z nich wypisów, nawet w postaci zaszyfrowanej.

Zasady postępowania przy przekazywaniu nośników informacji do innej jednostki organizacyjnej

1. Elektroniczne nośniki informacji zawierające dane osobowe przekazywane są do innej jednostki organizacyjnej tylko na pisemny, umotywowany wniosek, gdy jest to bezwzględnie konieczne do realizacji jej zadań regulaminowych.
2. Pliki z informacjami zawarte na nośnikach przekazywanych poza obszar przetwarzania, obowiązkowo zabezpieczane są przed dostępem osób i podmiotów nieupoważnionych oraz modyfikacją lub zniszczeniem w sposób nieautoryzowany - hasłem dostępu lub szyfrując je.
3. Przed wysłaniem nośnika sporządzana jest kopia przesyłanych danych, a adresat powiadamiany jest o nadanej przesyłce. W przypadku nieotrzymania przez adresata przesyłki, o zaistniałej sytuacji powiadamiany jest Inspektor Ochrony Danych.

4. Elektroniczne nośniki informacji pochodzące od podmiotu zewnętrznego sprawdzane są programem antywirusowym.

Zasady postępowania z komputerami przenośnymi

Użytkownik komputera przenośnego jest zobowiązany do:

- transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia,
- zabezpieczenia komputera przenośnego hasłem, zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym,
- niezezwalania osobom nieupoważnionym i nieuprawnionym do korzystania z komputera przenośnego,
- korzystania z komputera w sposób minimalizujący ryzyko podejrzenia przetwarzanych danych przez osoby postronne, w szczególności zabrania się korzystania z komputera przenośnego w miejscach publicznych i w środkach transportu publicznego.

Procedury zarządzania kopiami zapasowymi

Procedura tworzenia kopii zapasowych

1. Zbiory danych, oprogramowanie oraz konfiguracja systemów operacyjnych serwerów Administratora DO zabezpieczane są w postaci cyklicznie wykonywanych kopii bezpieczeństwa lub kopii archiwalnych.
2. Kopie bezpieczeństwa wykonywane są zawsze przed:
   - dokonaniem zmian w konfiguracji systemów operacyjnych lub oprogramowania,
   - dokonaniem zmian w programach (np. zmiana wersji lub aktualizacja oprogramowania),
   - każdą istotną zmianą danych w bazie danych.
3. Jeśli zaistnieje taka konieczność, tworzone są awaryjne kopie zapasowe, np. przed dokonaniem niezbędnych napraw systemu informatycznego bądź komputera, na którym przetwarzane są dane osobowe.
4. W Urzędzie Miejskim w Żarowie kopie zapasowe tworzone są wg następujących zasad:
   - kopia dzienna - na dwa różne serwery FTP (szyfrowana),
   - kopia tygodniowa - na płytę DVD (deponowana w szafie stalowej),
   - kopia miesięczna - cała zawartość serwera na streamer (szyfrowana).

Procedura przechowywania i niszczenia kopii zapasowych

1. Nośniki informacji zawierające kopie zapasowe zbiorów danych osobowych, programów i narzędzi programowych służących do przetwarzania danych osobowych przechowywane są w sposób uniemożliwiający ich nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie.
2. Dostęp do nośników z kopiami zapasowymi posiada tylko Administrator Danych Osobowych i Administrator Systemu Informatycznego.
3. Serwisowanie lub naprawy nośników zawierających kopie zapasowe przez osoby, które nie są pracownikami Urzędu, odbywa się wyłącznie pod nadzorem Administratora Systemu Informatycznego.

4. W przypadku braku możliwości naprawy uszkodzonych nośników zawierających kopie zapasowe, przeznacza się je do utylizacji z uzyskaniem potwierdzenia zniszczenia. Z wykonanych czynności sporządza się protokół. Protokół likwidacji kopii zapasowych stanowi **Załącznik nr 4** do „Procedur zarządzania dostępem do systemu przetwarzania".

Procedury wykonywania przeglądów i konserwacji systemu informatycznego

1. Przeglądu i konserwacji sprzętu w sieci informatycznej, systemów informatycznych i nośników informacji w Urzędzie Miejskim w Żarowie dokonuje stosownie do potrzeb Administrator Systemu Informatycznego, nie rzadziej niż raz na rok. ASI przynajmniej raz w roku:
   - dokonuje procedury przeglądu zestawów komputerowych będących w użytkowaniu pod kątem występowania usterek sprzętowych,
   - dokonuje przeglądu komputerów czasowo wyłączonych z użytku z powodu usterek, pod kątem możliwości naprawy lub docelowego wycofania z użytku,
   - przeprowadza weryfikację całego oprogramowania użytkowego eksploatowanego na wszystkich komputerach podłączonych do systemu informatycznego pod kątem spełnienia wymogów bezpieczeństwa.
2. W przypadku stwierdzenia nieprawidłowości w działaniu elementów systemu informatycznego, które są niezbędne do zapewnienia realizacji celów wynikających z dokumentacji ochrony danych osobowych, ASI podejmuje niezwłocznie czynności zmierzające do przywrócenia ich prawidłowego działania.

Zasady serwisowania sprzętu komputerowego

1. Użytkownik systemu informatycznego niezwłocznie powiadamia Administratora Systemu o wszelkich nieprawidłowościach i awariach sprzętu informatycznego, mogących prowadzić do próby naruszenia bezpieczeństwa danych osobowych.
2. O powyższych przypadkach ASI zawiadamia niezwłocznie ADO.
3. Wszystkie awarie lub usterki sprzętowe są zgłaszane w dniu wystąpienia i usuwane na bieżąco.
4. Bezwzględnie zabronione jest samodzielne dokonywanie przez użytkowników systemu napraw sprzętu informatycznego, wymiany jego podzespołów oraz wykonywanie innych czynności niezwiązanych bezpośrednio z jego eksploatacją lub niedopuszczonych przez producenta sprzętu w instrukcji obsługi.
5. W przypadku, gdy do przywrócenia prawidłowego działania systemu informatycznego niezbędna jest pomoc podmiotu zewnętrznego, wszelkie czynności na sprzęcie komputerowym zawierającym dane osobowe dokonywane są w obszarze przetwarzania danych osobowych wyłącznie w obecności ASI.
6. Zdiagnozowane usterki elementów zestawów komputerowych są:
   - w przypadku objęcia gwarancją - zgłaszane do autoryzowanych serwisów producenta sprzętu w celu naprawy lub wymiany na elementy wolne od wad,
   - w przypadku braku gwarancji - naprawiane przez osoby do tego upoważnione w jednostce lub przy braku możliwości technicznych oddane do naprawy w serwisach zewnętrznych.

7. W każdym z przypadków, jeżeli w celu dokonania naprawy wymagane jest przekazanie na zewnątrz dysków twardych, ich zawartość jest bezwzględnie archiwizowana i pozbawiana zapisu danych osobowych.

Zasady wycofywania z użytkowania stacji roboczych

1. W każdym przypadku, kiedy uszkodzeniu ulegnie jednostka centralna zestawu komputerowego, monitor lub drukarka, a zestaw komputerowy jako całość lub jego poszczególne elementy nie posiadają ważnej gwarancji, następuje oszacowanie możliwości jak i kosztów naprawy. Jeżeli koszty naprawy przekraczają wartość zakupu nowego elementu składowego lub naprawa jest niemożliwa, przeprowadza się procedurę wycofania takiego elementu z dalszej eksploatacji:
   - sporządza się krótką notatkę o braku możliwości naprawy lub nieopłacalności jej realizacji,
   - zgłasza fakt wycofania sprzętu z użytku osobie odpowiedzialnej za prowadzenie ewidencji ilościowo - wartościowej sprzętu komputerowego,
   - dokonuje wykreślenia ze stanu ewidencyjnego,
   - w przypadku jednostki centralnej, zabezpiecza dysk twardy poprzez jego wymontowanie i pozostawienie w jednostce lub poddanie procedurze pozbawienia zapisu danych w uprawnionych do tego podmiotach,
   - dokonuje złomowania poprzez przekazanie firmom wyspecjalizowanym w utylizacji nośników.
2. Za powyższe czynności odpowiedzialny jest Administrator Systemu Informatycznego.

Zasady postępowania z dokumentami papierowymi

1. Podczas nieobecności w pomieszczeniu lub po zakończeniu pracy, dokumenty oraz wydruki zawierające dane osobowe przechowane są w szafkach i meblach biurowych zamykanych na klucz.
2. Dokumenty i wydruki oraz kserokopie dokumentów nie są pozostawiane na urządzeniach (drukarkach, skanerach, kserokopiarkach) bez nadzoru.
3. Dokumenty i wydruki z danymi osobowymi, niezwłocznie po ustaniu celu ich przetwarzania, niszczone są w niszczarkach.
4. W przypadku konieczności przekazania poza obszar przetwarzania, dokumenty transportowane są i przekazywane z zachowaniem szczególnej ostrożności przez osobę do tego upoważnioną.

Załączniki

Załącznik nr 1	- Upoważnienie do przetwarzania danych osobowych.
Załącznik nr 2	- Wykaz osób upoważnionych do przetwarzania danych osobowych.
Załącznik nr 3	- Oświadczenie o zachowaniu poufności.
Załącznik nr 4	- Protokół likwidacji kopii zapasowych.

Procedury reagowania na naruszenia ochrony danych osobowych

Urząd Miejski w Żarowie

ul. Zamkowa 2
58-130 Żarów

Dokument do użytku służbowego
Wykonał: mgr inż. Piotr Chałaszczyk
- Inspektor Ochrony Danych
Data aktualizacji: 25.03.2021 r.

Spis treści

Naruszenie - informacje ogólne

Zgodnie z art. 4 pkt. 12 RODO naruszeniem praw i wolności osób fizycznych zgodnie z RODO jest m.in. powstanie uszczerbku fizycznego, szkód majątkowych lub niemajątkowych osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi bądź ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne.

Rodzaje zagrożeń

1. Zagrożenia losowe zewnętrzne:
   - klęski żywiołowe,
   - przerwy w zasilaniu (ich wystąpienie może prowadzić do utraty integralności danych lub ich zniszczenia,
   - uszkodzenia infrastruktury technicznej systemu (ich wystąpienie może prowadzić do naruszenia ciągłości pracy systemu, natomiast nie dochodzi do naruszenia poufności danych).
2. Zagrożenia losowe wewnętrzne:
   - niezamierzone pomyłki operatorów,
   - awarie sprzętowe,
   - błędy oprogramowania (w wyniku ich wystąpienia może dojść do zniszczenia danych, może nastąpić zakłócenie ciągłości pracy systemu i naruszenia poufności danych).
3. Zagrożenia zamierzone (świadome i celowe naruszenia poufności danych):
   - nieuprawniony dostęp do systemu z zewnątrz,
   - nieuprawniony dostęp do systemu z wewnątrz,
   - nieuprawnione przekazanie danych,
   - kradzież, zniszczenie elementów systemu.

Symptomy świadczące o możliwości naruszenia ochrony danych osobowych

O naruszeniu ochrony danych osobowych mogą świadczyć:

- ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie i przechowywanie danych (wybite szyby w oknach, wyłamane drzwi wejściowe lub zamki, wyłamane kraty zabezpieczające, aktywność systemów alarmowych),
- ślady włamania lub prób włamania do pomieszczeń, w których znajdują się poszczególne elementy systemu, np.: serwery, stacje robocze lub urządzenia sieciowe,
- ślady włamania lub prób włamania do biurek/szafek, w których przechowywane są w postaci elektronicznej lub papierowej nośniki lub dokumenty zawierające dane osobowe,
- kradzież komputera, w którym przechowywane są dane osobowe,
- stan stacji roboczej (problemy z uruchomieniem, rozkręcona obudowa, uruchomiony komputer pomimo jego prawidłowego wyłączenia po zakończeniu pracy itp.),
- brak dostępu do funkcji programów,

- brak możliwości uruchomienia aplikacji pozwalającej na dostęp do danych osobowych, brak możliwości zalogowania się do tej aplikacji,
- ograniczone w stosunku do normalnej sytuacji uprawnienia użytkownika w strukturze aplikacji (np. brak możliwości wykonania pewnych operacji normalnie dostępnych, nieprawidłowości w wykonywanych operacjach),
- poszerzone uprawnienia w obrębie aplikacji w stosunku do dotychczas przyznanych (np. wgląd do szerszego niż zwykle zakresu danych),
- inny zakres lub różnice w zawartości zbioru danych osobowych dostępnych dla użytkownika (np. ich całkowity lub częściowy brak lub nadmiar),
- pogorszenie jakości danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub niepożądaną modyfikację w systemie,
- znaczne spowolnienie działania systemu informatycznego,
- pojawienie się komunikatów alarmowych od części systemu, która zapewnia ochronę zasobów, pojawienie się komunikatów informujących o niespójności i błędach w danych.
- zagubienie bądź kradzież nośnika z zawartością danych osobowych,
- niewłaściwe niszczenie nośników zawierających dane osobowe, pozwalające na ich odczyt,
- brak aktualnych kopii bezpieczeństwa danych osobowych,
- wykonywanie nieuprawnionych kopii zapasowych.

O naruszeniu może świadczyć również nieuprawnione przetwarzanie danych osobowych, np. gdy dostęp do danych osobowych mają osoby, które najprawdopodobniej tego dostępu nie potrzebują, a także przypadki ujawnienia danych osobowych lub nienależytego zabezpieczenia ich przed osobami nieupoważnionymi.

Źródła informacji o incydentach

- Zgłoszenia od pracowników Urzędu.
- Zgłoszenia od osób upoważnionych do systemu przetwarzania, niebędących pracownikami Urzędu.
- Zgłoszenia od pracowników reprezentujących podmiot zewnętrzny, którzy mają dostęp do systemów przetwarzania i zobowiązali się do przestrzegania zasad ochrony danych osobowych w Urzędzie.
- Zgłoszenia z automatycznych systemów monitorowania (np. system alarmowy, system informatyczny).
- Analizy incydentów naruszenia bezpieczeństwa mających miejsce w przeszłości.
- Wyniki kontroli i audytów (wewnętrznych i zewnętrznych).

Zasady postępowania w przypadku naruszenia ochrony danych osobowych

Osoba, która zauważyła niepokojące zdarzenie lub wyżej wymienione symptomy, które jej zdaniem mogą spowodować zagrożenie bądź przyczynić się do naruszenia zasad ochrony danych osobowych i bezpieczeństwa informacji, zobowiązana jest do natychmiastowego poinformowania o tym Inspektora Ochrony Danych, a w przypadku jego nieobecności Administratora Danych Osobowych. Informacja o pojawieniu się zagrożenia jest przekazywana przez tę osobę osobiście, telefonicznie

lub pocztą elektroniczną. Taka informacja powinna zawierać imię i nazwisko osoby zgłaszającej oraz zauważone symptomy zagrożenia.

Do czasu przybycia na miejsce zdarzenia Inspektora Ochrony Danych lub wskazanego przez niego pracownika należy:

- o ile istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego zdarzenia, a następnie uwzględnić w działaniu również ustalenie jego przyczyn lub sprawców,
- rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
- zaniechać (o ile to możliwe) dalszych planowanych przedsięwzięć, które mogą utrudnić udokumentowanie i analizę zaistniałego zdarzenia,
- przygotować opis incydentu,
- nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia Inspektora OD lub osoby przez niego wskazanej.

Po otrzymaniu zgłoszenia o wystąpieniu symptomów wskazujących na możliwość zaistnienia naruszenia bezpieczeństwa danych osobowych, Inspektor Ochrony Danych jest zobowiązany do stwierdzenia, czy rzeczywiście doszło do naruszenia ochrony danych osobowych oraz do:

- niezwłocznego podjęcia odpowiednich kroków w celu powstrzymania lub ograniczenia dostępu do danych osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów jej ingerencji,
- przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej,
- zapisania wszelkich informacji związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu bezpieczeństwa danych lub czasu samodzielnego wykrycia tego faktu,
- wygenerowania i wydrukowania (jeżeli zasoby systemu na to pozwalają) wszystkich możliwych dokumentów i raportów, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrzenia ich datą i podpisem.

Po wyeliminowaniu bezpośredniego zagrożenia Administrator Systemu Informatycznego wspólnie z Inspektorem OD mają obowiązek przeprowadzić analizę stanu systemu informatycznego, a w szczególności sprawdzić:

- stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
- zawartość zbiorów danych osobowych, których dotyczy naruszenie,
- sposób działania programów, których dotyczy naruszenie,
- jakość komunikacji w sieci telekomunikacyjnej,
- obecność wirusów komputerowych.

Zgłoszenie naruszenia ochrony danych osobowych do UODO

W przypadku stwierdzenia naruszenia Administrator Danych Osobowych bez zbędnej zwłoki, w terminie 72 godzin jest zobowiązany zgłosić je organowi nadzorczemu (Urząd Ochrony Danych Osobowych), chyba, że jest mało prawdopodobne, by takie naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. W przypadku niezgłoszenia naruszenia w wyżej

wymienionym terminie, ADO będzie musiał dołączyć do zgłoszenia wyjaśnienia dotyczące przyczyn opóźnienia.

W Urzędzie Miejskim w Żarowie zgłoszenie do Urzędu Ochrony Danych Osobowych sporządzane jest w imieniu i na wniosek ADO przez Inspektora OD i powinno zawierać następujące informacje:

- dane Administratora Danych Osobowych,
- datę i godzinę naruszenia,
- nazwę organu nadzorczego,
- imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych,
- kategorie i przybliżoną liczbę osób, których dane dotyczą,
- kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
- środki zastosowane lub proponowane przez Administratora Danych Osobowych w celu zaradzenia naruszeniu, w tym w stosownych przypadkach, środki w celu zminimalizowania jego ewentualnych negatywnych skutków,
- okoliczności i charakter naruszenia,
- możliwe konsekwencje naruszenia.

Wzór zgłoszenia naruszenia do organu nadzorczego stanowi **Załącznik nr 1** do „Procedur reagowania na naruszenia ochrony danych osobowych". Inspektor OD przechowuje kopie wszystkich zgłoszeń o naruszeniu ochrony danych osobowych oraz prowadzi ewidencję interwencji związanych z zaistniałymi incydentami. Rejestr incydentów naruszenia ochrony danych stanowi **Załącznik nr 2** do „Procedur reagowania na naruszenia ochrony danych osobowych".

Zawiadomienie o naruszeniu ochrony danych osobowych osoby, której dane dotyczą

W przypadku, gdy incydent naruszenia ochrony danych będzie powodował wysokie ryzyko naruszenia praw lub wolności osoby, której dane dotyczą, ADO ma obowiązek poinformowania tej osoby o naruszeniu jej danych. W Urzędzie Miejskim w Żarowie w imieniu i na polecenie ADO zawiadomienia takiego dokonuje Inspektor Ochrony Danych bez zbędnej zwłoki, opisując jasnym i prostym językiem charakter naruszenia.

Zawiadomienie powinno zawierać następujące informacje:

- nazwę i dane kontaktowe Administratora Danych Osobowych,
- imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych,
- możliwe konsekwencje naruszenia ochrony danych osobowych,
- środki zastosowane lub proponowane przez Administratora Danych Osobowych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach, środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Wzór zawiadomienia o naruszeniu ochrony danych osobowych osoby, której dane dotyczą stanowi **Załącznik nr 3** do „Procedur reagowania na naruszenia ochrony danych osobowych".

Zawiadomienie nie jest wymagane, jeśli:

- Administrator Danych Osobowych wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie,

w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu,
- Administrator Danych Osobowych zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
- wymagałoby ono niewspółmiernie dużego wysiłku (w takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób).

W przypadku, gdy ADO nie zawiadomił jeszcze osoby, której dane dotyczą o naruszeniu ochrony danych osobowych, a naruszenie to spowoduje wysokie ryzyko, Urząd Ochrony Danych Osobowych może od niego tego zażądać lub może stwierdzić, że spełniony został jeden z warunków wymienionych wyżej.

Usunięcie skutków naruszenia

1. Inspektor OD we współpracy z ASI zobowiązany jest do usunięcia skutków incydentu i przywrócenia stanu pierwotnego (tj. stanu sprzed incydentu) dokumentów i danych oraz systemu informatycznego polegające na:
   - sprawdzeniu kompletności kartotek/dokumentów,
   - przeprowadzeniu analizy spójności przetwarzanych danych osobowych,
   - ewentualnym odtworzeniu kopii zapasowych danych i plików konfiguracyjnych,
   - przeprowadzeniu analizy poprawności funkcjonowania systemu informatycznego,
   - powtórnym zabezpieczeniu danych przetwarzanych w systemie informatycznym, w szczególności danych konfiguracyjnych tego systemu.
2. W dalszej kolejności należy usunąć skutki fizycznych zniszczeń pomieszczeń oraz miejsc przetwarzania danych w celu przywrócenia akceptowalnego poziomu zabezpieczeń danych.
3. Inspektor OD określa na podstawie zebranych informacji przyczyny zaistnienia incydentu. Jeżeli incydent był spowodowany celowym działaniem, może poinformować organy uprawnione do ścigania przestępstw o fakcie celowego naruszenia bezpieczeństwa danych osobowych przetwarzanych w jednostce organizacyjnej.
4. Inspektor Ochrony Danych odpowiedzialny jest za przeprowadzenie przynajmniej raz w roku analizy zaistniałych incydentów w celu:
   - określenia skuteczności podejmowanych działań wyjaśniających i naprawczych,
   - określenia wymaganych działań zwiększających bezpieczeństwo i minimalizujących ryzyko zaistnienia incydentów,
   - określenia potrzeb w zakresie dodatkowych szkoleń osób przetwarzających dane i administratorów systemu informatycznego służącego do przetwarzania danych osobowych.

Załączniki

Załącznik nr 1	- Zgłoszenie naruszenia ochrony danych osobowych.
Załącznik nr 2	- Rejestr incydentów naruszenia ochrony danych.

Załącznik nr 3	- Zawiadomienie o naruszeniu ochrony danych osobowych osoby, której dane dotyczą.

Analiza zagrożeń i ryzyka przy przetwarzaniu danych osobowych

Urząd Miejski w Żarowie

ul. Zamkowa 2
58-130 Żarów

Dokument do użytku służbowego
Wykonał: mgr inż. Piotr Chałaszczyk
- Inspektor Ochrony Danych
Data aktualizacji: 25.03.2021 r.

Spis treści

Wstęp

Analiza ryzyka jest procesem kluczowym z uwagi na całość systemu bezpieczeństwa danych osobowych. Ma ona na celu ustalenie, jakie są potencjalne zagrożenia związane z przetwarzaniem danych osobowych oraz dobranie zabezpieczeń, które będą najodpowiedniejsze dla Urzędu Miejskiego w Żarowie.

Administrator Danych Osobowych ze względu na ciążące na nim obowiązki wynikające z przepisów prawa zobowiązany jest do zastosowania środków technicznych i organizacyjnych, które mają zapewnić ochronę przetwarzanych danych osobowych w świetle adekwatnych zagrożeń. Skuteczność zastosowanych środków podlega cyklicznym badaniom. Przy stosowaniu zabezpieczeń uwzględniane są zmieniające się warunki oraz postęp techniczny (informatyczny), co może powodować konieczność zmiany lub modernizowania wprowadzonych wcześniej przez Administratora Danych Osobowych systemów ochrony.

Przy opracowaniu niniejszego dokumentu uwzględniono regulacje zawarte w następujących aktach prawnych:

- Rozporządzeniu 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,
- Wytycznych GIODO pt. „Wykonywanie obowiązków ABI, przyszłego inspektora ochrony danych w świetle ogólnego rozporządzenia o ochronie danych osobowych”,
- Wytycznych Grupy Roboczej art. 29 dotyczących inspektorów ochrony danych z dn. 13 grudnia 2016 r.
- Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych.

Wymogi dotyczące bezpieczeństwa danych osobowych

Bezpieczeństwo przetwarzanych informacji zawierających dane osobowe wymaga:

- zapewnienia ochrony fizycznej stanowisk komputerowych przed nieuprawnionym dostępem,
- ochrony nośników technicznych i wydruków dokumentów, w tym określenia zasad ochrony ich przed nieuprawnionym dostępem,
- zapewnienia dostępności do danych osobowych znajdujących się na technicznych nośnikach informacji oraz w pamięci systemu informatycznego dla upoważnionych użytkowników,
- zapewnienia możliwości kontroli nośników, na których przetwarzane są dane osobowe,
- zabezpieczenia przed nieupoważnionym dostępem do danych osobowych znajdujących się w zasobach systemu informatycznego,
- zapewnienia możliwości kontroli dostępu do zasobów systemu informatycznego oraz wykonywanych na nim czynności.

W celu maksymalnego wyeliminowania zagrożenia dla całego systemu ochrony danych osobowych w Urzędzie Miejskim w Żarowie zostały wdrożone procedury kontrolne, na które składają się:

- prowadzenie odpowiedniej dokumentacji,
- fizyczna ochrona danych osobowych,
- bezpieczne środowisko komputerowe,

- „kodeks dobrych praktyk” wdrożony przez Inspektora OD.

Zagrożenia dla systemu ochrony danych osobowych

System ochrony danych osobowych w Urzędzie Miejskim w Żarowie narażony jest na zagrożenia wystąpienia incydentu powodującego utratę poufności, rozliczalności i integralności informacji.

Poufność

Poufność, to zapewnienie danym osobowym niemożności ich udostępniania nieupoważnionym osobom czy podmiotom.

Zagrożenia, jakie można wyróżnić ze względu na utratę poufności w systemie:

- klęska żywiołowa, w wyniku której utracono poufność danych osobowych,
- nieuprawniony dostęp do pomieszczenia, w którym przetwarzane są dane osobowe,
- pokonanie zabezpieczeń fizycznych lub programowych,
- ujawnienie haseł dostępu do stanowiska komputerowego, na którym przetwarzane są dane osobowe,
- udostępnianie danych osobowych osobom nieupoważnionym,
- niedyskrecja osób upoważnionych do przetwarzania danych osobowych,
- podsłuch lub podgląd danych osobowych,
- niekontrolowana obecność osób nieupoważnionych w obszarze przetwarzania danych osobowych,
- nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik,
- utrata nośnika zawierającego dane osobowe,
- nieuprawnione wyniesienie danych osobowych zawartych na nośniku,
- naprawy i konserwacje systemów lub sieci teleinformatycznej służących do przetwarzania danych osobowych przez osoby nieupoważnione do przetwarzania danych osobowych,
- elektromagnetyczna emisja ujawniająca,
- stosowanie korupcji oraz szantażu w celu wydobycia określonych informacji od wybranych pracowników placówki.

Skala identyfikacji skutków utraty zasobów dla atrybutu poufności danych osobowych.	
Wartość	Skutki
< 0 >	Brak skutków utraty poufności
< 1 – 3 >	Niski skutek utraty poufności
< 4 – 7 >	Średni skutek utraty poufności
< 8 – 9 >	Wysoki skutek utraty poufności
< 9 – 10 >	Całkowita utrata poufności

Integralność

Integralność, to cecha zapewniająca, że dane nie zostały zmodyfikowane lub zniszczone w sposób nieautoryzowany.

Zagrożenia, jakie można wyróżnić ze względu na utratę integralności przez system:

- nielegalny dostęp do danych osobowych, w tym do stanowiska komputerowego,
- błędy, pomyłki,
- brak mechanizmów uniemożliwiających skasowanie lub zmianę logów przez Administratora lub użytkownika,
- wadliwe działanie systemu operacyjnego,
- brak w wykorzystywanych aplikacjach mechanizmów zapewniających integralność danych,
- celowe lub przypadkowe uszkodzenie systemu operacyjnego lub urządzeń sieciowych,
- celowe lub przypadkowe uszkodzenie, zniszczenie lub nieuprawniona modyfikacja danych,
- działanie złośliwego oprogramowania (wirusy),
- pożar, zalanie, ekstremalna temperatura, itp.,
- zagrożenia zewnętrzne (np. klęski żywiołowe, atak terrorystyczny).

Skala identyfikacji skutków utraty zasobów dla atrybutu integralności danych osobowych.	
Wartość	Skutki
< 0 >	Utrata integralności nie występuje
< 1 – 3 >	Niski skutek utraty integralności
< 4 – 7 >	Średni skutek utraty integralności
< 8 – 9 >	Wysoki skutek utraty integralności
< 10 >	Bezwzględny skutek utraty integralności

Rozliczalność

Rozliczalność to cecha zapewniająca działanie podmiotu przetwarzającego dane osobowe, która może być przypisana w sposób jednoznaczny tylko temu jednemu podmiotowi.

Zagrożenia, jakie można wyróżnić ze względu na utratę rozliczalności systemu:

- brak kontroli nad dokumentami wykonywanymi na stanowisku komputerowym w zakresie ich kopiowania i drukowania,
- wprowadzenie zmian w treści dokumentu zawierającego dane osobowe,
- błędy oprogramowania lub sprzętu,
- nieprzydzielenie użytkownikom indywidualnych identyfikatorów,
- niewłaściwa administracja systemem informatycznym,
- niewłaściwa konfiguracja systemu informatycznego,
- zniszczenie lub sfałszowanie logów systemowych,
- brak rejestracji udostępnienia danych osobowych,
- podszywanie się pod innego użytkownika,

- niespełnienie przez system wymagań ustanowionych w dokumentacji wewnętrznej ochrony danych osobowych.

Skala identyfikacji skutków utraty zasobów dla atrybutu rozliczalności danych osobowych.	
Wartość	Skutki
< 0 >	Utrata rozliczalności nie występuje
< 1 – 3 >	Niski skutek utraty rozliczalności
< 4 – 6 >	Średni skutek utraty rozliczalności
< 7 – 8 >	Wysoki skutek utraty rozliczalności
< 9 >	Ekstremalny skutek utraty rozliczalności

Podatność systemu ochrony danych osobowych na zagrożenia

Podatność systemu to słabość zasobu lub zabezpieczenia systemu teleinformatycznego, która może zostać wykorzystana przez zagrożenie.

Przebieg kontroli podatności systemu ochrony danych osobowych		
Lp.	Zakres kontroli	Podejmowane czynności
1	Dokumentacja ODO	Sprawdzenie, czy dokumentacja ODO jest aktualna względem obowiązującego stanu prawnego oraz faktycznego.
		Sprawdzenie, czy osoby, które mają dostęp do danych osobowych, mają upoważnienia do przetwarzania danych osobowych - upoważnienie powinno odzwierciedlać zakres obowiązków.
		Sprawdzenie, czy osoby, które mogą mieć dostęp do danych osobowych, ale nie są upoważnione, podpisały oświadczenie o zachowaniu poufności.
		Sprawdzenie, czy prowadzona jest aktualna ewidencja osób przetwarzających dane osobowe.
2	Fizyczna ochrona danych osobowych	Kontrolowanie osób przetwarzających dane osobowe - czy stosują się do „zasady czystego biurka”.
		Sprawdzenie, czy w pomieszczeniu znajdują się szafy zamykane na klucz, w których przechowuje się dokumentację zawierającą dane osobowe podlegające ochronie.

		Sprawdzenie, czy w pomieszczeniu znajduje się niszczarka dokumentów (jeśli nie to w jaki sposób niszczy się zbędną dokumentację, która nie podlega archiwizacji).
3	Ochrona środowiska komputerowego	Kontrola sposobu uwierzytelnienia użytkowników systemu (systemów) informatycznego.
		Kontrolowanie aktywności systemu antywirusowego.
		Kontrolowanie, czy pracownik korzysta z wygaszacza ekranu.
		Sprawdzenie, czy monitor komputera został usytuowany w sposób uniemożliwiający wgląd do danych - osobom postronnym.
4	Kontrola praktyki	Przeprowadzenie sprawdzenia pod kątem : • próby nieuprawnionego dostępu do danych osobowych, • działanie zewnętrznych aplikacji, wirusów czy złośliwego oprogramowania, • nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym, • próba nieuprawnionej interwencji przy sprzęcie komputerowym, • wynoszenie niezabezpieczonych pamięci z miejsca pracy, • udzielanie informacji osobom postronnym, pomijając formalny tryb administracyjny.

Skala identyfikacji podatności systemu na określone zagrożenia.	
Wartość	Skutki
< 0 >	Brak podatności
< 1 – 4 >	Niski poziom
< 5 – 7 >	Średni poziom
< 8 – 9 >	Wysoki poziom
< 10 >	Ekstremalny poziom

Analiza zagrożeń i szacowanie ryzyka

Aby poprawnie przeprowadzić analizę ryzyka, Administrator Danych Osobowych określa:

1. Zasoby, które będzie chronić:
   - sprzęt komputerowy przechowujący dane (dysk twardy),
   - dane osobowe przetwarzane w formie papierowej i elektronicznej,
   - aplikacje, w których przetwarzane są dane osobowe,
   - pomieszczenia, w których pracują osoby przetwarzające dane osobowe.
2. Zagrożenia - czynnik, który może powodować wystąpienie incydentu naruszenia.

3. Podatność - słabość zasobów, która może być wykorzystana przez potencjalne zagrożenie.
4. Skutki - jaki wpływ będzie miał zaistniały incydent na utratę danych osobowych.
5. Ryzyko - iloczyn wartości skutków i prawdopodobieństwa wystąpienia zagrożenia.

Określenie poziomu ryzyka utraty bezpieczeństwa danych osobowych:

- niski - niskie szkody w przypadku realizacji zagrożenia i niska możliwość jego wystąpienia,
- średni - wysokie szkody w przypadku realizacji zagrożenia i niska możliwość jego realizacji bądź niskie szkody w przypadku realizacji zagrożenia i wysoka możliwość jego realizacji,
- wysoki - wysokie szkody w przypadku realizacji zagrożenia i wysoka możliwość jego wystąpienia,
- maksymalny - wysokie szkody w przypadku realizacji zagrożenia oraz wysoka możliwość jego wystąpienia, skutkująca nie tylko na organizację, ale na podmioty trzecie.

Skala identyfikacji poziomu ryzyka	
Wartość	Poziom ryzyka
<1-20>	Niski poziom ryzyka utraty bezpieczeństwa danych osobowych
<21-60>	Średni poziom ryzyka utraty bezpieczeństwa danych osobowych
<61-80>	Wysoki poziom ryzyka utraty bezpieczeństwa danych osobowych
<81-100>	Maksymalny poziom ryzyka utraty bezpieczeństwa danych osobowych

Administrator Danych Osobowych wyznacza poziom ryzyka akceptowalnego, powyżej którego będą określone działania zapobiegawcze i/lub korygujące. W przypadku, kiedy wartość oszacowanego ryzyka przekracza próg ryzyka akceptowalnego, ADO podejmuje działania wdrażające stosowne zabezpieczenia. Tabelę szacowania ryzyka oraz wnioski i działania naprawcze ADO stanowi **Załącznik nr 1**.

Administrator Danych Osobowych po oszacowaniu ryzyka przystępuje do etapu postępowania z ryzykiem, w ramach którego może podjąć cztery różne działania:

- unikanie ryzyka - odejście od działań, które wiążą się z ryzykiem, jeżeli ryzyko jest duże, a system, w którym ono występuje, nie przynosi odpowiednich korzyści,
- ograniczenie ryzyka (redukcja) - podjęcie działań ograniczających ryzyko lub zmniejszających podatność,
- przekazanie ryzyka - przeniesienie ryzyka na podmiot zewnętrzny, odpowiedzialność zostaje przekazana w odpowiednich zapisach umowy,
- akceptacja ryzyka - gdy koszty działań w celu niwelowania ryzyka przekraczają oczekiwane lub występują określone trudności w przeciwdziałaniu ryzyka.

Załączniki

Załącznik nr 1	- Tabela szacowania ryzyka oraz wnioski i działania naprawcze ADO.