BURMISTRZ
SOŚNICOWIC

Zarządzenie Nr 63/2019

z dnia 20.05.2019r.

Burmistrza Sośnicowic

w sprawie wprowadzenia Polityki bezpieczeństwa informacji i ochrony danych osobowych w Urzędzie Miejskim w Sośnicowicach

Działając na podstawie art. 24 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.U.UE.L.2016.119.1) zarządzam, co następuje:

§ 1

Wprowadzam:

Politykę bezpieczeństwa informacji iochrony danych osobowych w Urzędzie Miejskim w Sośnicowicach w brzmieniu określonym w Załączniku Nr 1 do niniejszego Zarządzenia.

§2

Zobowiązuje wszystkich pracowników Urzędu Miejskiego w Sośnicowicach do stosowania zasad określonych w Polityce bezpieczeństwa informacji i ochrony danych osobowych.

§3

Traci moc Zarządzenie nr 64/2015 z dnia 26 czerwca 2015r.w sprawie: aktualizacji dokumentacji opisującej sposób przetwarzania danych osobowych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych.

§4

Zarządzenie wchodzi w życie z dniem podjęcia.

BURMISTRZ SOŚNICOWIC

BURMISTRZ
Leszek Kołodziej

Załącznik nr 1
do Zarządzenia Burmistrza Sośnicowic
nr63/2019 z dnia 20.05.2019 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI I OCHRONY DANYCH OSOBOWYCH W URZĘDZIE MIEJSKIM W SOŚNICOWICACH

I. ZASADY I KWESTIE PODSTAWOWE

1. Niniejszy dokument zatytułowany **"Polityka bezpieczeństwa informacji i ochrony danych osobowych"** (dalej jako **Polityka**) stanowi mapę wymogów, zasad i regulacji ochrony danych osobowych w Urzędzie Miejskim w Sośnicowicach z siedzibą w Sośnicowicach przy ul. Rynek 19, reprezentowanym przez Burmistrza Sośnicowic (dalej także jako **"Administrator"** lub **"ADO"**).
2. Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO - rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 lub RODO) (Dz.Urz. UE L 119, s. 1), dalej RODO.
3. Polityka zawiera w szczególności opis zasad ochrony danych osobowych obowiązujących w Urzędzie Miejskim w Sośnicowicach, zwanym dalej "UM".
4. Niniejszy dokument stanowi najwyższej rangi dokument Polityki Bezpieczeństwa Informacji w Urzędzie Miejskim w Sośnicowicach. Jest on wiążący dla wszystkich referatów organizacyjnych, pracowników UM.
5. Z systemów przetwarzania danych osobowych znajdujących się w posiadaniu ADO mogą korzystać inne podmioty, wyłącznie na podstawie odrębnych umów, porozumień lub stosunków prawnych, kształtowanych na podstawie przepisów szczególnych, określających zasady korzystania z tych systemów, w szczególności poprzez wyraźnie zdefiniowanie celu i zakresu takiego korzystania oraz wskazanie odpowiedzialności karnej.
6. Zasady, działania, kompetencje i zakresy odpowiedzialności opisane w niniejszej Polityce bezpieczeństwa informacji i ochrony danych osobowych, obowiązują wszystkich pracowników i współpracowników ADO.
7. Procedury i dokumenty związane z Polityką będą weryfikowane i dostosowywane w celu zapewnienia odpowiedniego poziomu bezpieczeństwa.
8. Polityka określa środki techniczne i organizacyjne zastosowane przez ADO dla zapewnienia ochrony danych w systemie informatycznym oraz w kartotekach papierowych.
9. Polityka została opracowana z uwzględnieniem metod i środków ochrony danych, których skuteczność w czasie ich zastosowania jest powszechnie uznawana. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania właściwej ochrony wraz z zachowaniem ich poufności, integralności i rozliczalności, ze szczególnym uwzględnieniem obowiązujących przepisów prawa dotyczących ochrony danych osobowych.
10. Każdy z pracowników ma obowiązek zapoznania się z treścią niniejszej Polityki. Za bezpieczeństwo danych osobowych przetwarzanych przez ADO odpowiedzialni są wszyscy pracownicy. W szczególności odpowiadają oni za przestrzeganie zasad bezpieczeństwa wynikających z niniejszej Polityki oraz zgłaszanie incydentów i naruszeń, a także wykonywanie zaleceń Inspektora Ochrony Danych.
11. Polityka dotyczy wyposażenia, systemów informatycznych, urządzeń przetwarzających informacje w formie elektronicznej, papierowej lub jakiejkolwiek innej.

12. Nieprzestrzeganie postanowień zawartych w Polityce może skutkować sankcjami w pełnym zakresie dopuszczonym przez stosunek pracy oraz obowiązujące przepisy prawa.
13. Odpowiedzialny za wdrożenie i utrzymanie niniejszej Polityki jest Administrator Danych Osobowych, za nadzór i monitorowanie jej przestrzegania odpowiada Inspektor ochrony danych.

Skróty i definicje:

1. **Polityka** oznacza niniejszą Politykę bezpieczeństwa informacji i ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.
2. **Administrator danych osobowych – (ADO)** Urząd Miejski w Sośnicowicach reprezentowany przez Burmistrza Sośnicowic.
3. **RODO** oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1).
4. **Dane** oznaczają dane osobowe, zgodnie z definicją przyjętą w art. 4 ust. 1 RODO, oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, o ile co innego nie wynika wyraźnie z kontekstu.
5. **Dane wrażliwe** oznaczają dane szczególnych kategorii i dane karne.
6. **Dane szczególnych kategorii** oznaczają dane wymienione w art. 9 ust. 1 RODO, tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej.
7. **Dane karne** oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i czynów zabronionych.
8. **Dane dzieci** oznaczają dane osób poniżej 16. roku życia.
9. **Osoba** oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.
10. **Podmiot przetwarzający** oznacza organizację lub osobę, której ADO powierzył przetwarzanie danych osobowych (np. usługodawca IT, obsługa informatyczna, hosting).
11. **Profilowanie** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.
12. **Eksport danych** oznacza przekazanie danych do państwa trzeciego lub organizacji międzynarodowej.
13. **RCPD** lub Rejestr, oznacza Rejestr Czynności Przetwarzania Danych Osobowych.
14. **Ustawa o ochronie danych osobowych** - Ustawa z dnia 10 maja 2018 r. o ochronie

danych osobowych.

15. **Inspektor Ochrony Danych** (IOD) - osoba odpowiedzialna za zapewnienie przestrzegania przepisów o ochronie danych osobowych oraz za bezpieczeństwo informacji chronionych w Urzędzie Miejskim w Sośnicowicach.
16. **Administrator Systemu** (AS) - wyznaczona przez Administratora osoba odpowiedzialna za sprawne funkcjonowanie systemu informatycznego w Urzędzie Miejskim w Sośnicowicach. Rolę Administratora Systemu pełni informatyk lub osoba go zastępująca.
17. **Anonimizacja** - proces przetwarzania treści poprzez usunięcie informacji pozwalających na identyfikację osób fizycznych.
18. **Audyt bezpieczeństwa** - czynności formalne mające na celu sprawdzenie, czy dane dokumenty lub systemy przetwarzania informacji spełniają założenia Polityki Bezpieczeństwa Informacji.
19. **Autentyczność informacji** - zasada, zgodnie z którą tożsamość osób lub zasobu jest taka, jak deklarowana; autentyczność dotyczy: użytkowników, procesów, systemów i informacji.
20. **Bezpieczeństwo informacji** - zapewnienie odpowiedniego poziomu poufności, integralności i dostępności informacji, ochrona informacji przed nieautoryzowanym dostępem, modyfikacją, zatajeniem, kradzieżą i zniszczeniem.
21. **Bezpowrotne niszczenie informacji** - działania zapewniające, że (przy określonych założeniach pracochłonności) informacja nie może być odzyskana z nośników, na których była zapisana. Obejmuje to również zniszczenie poprzez fizyczne uszkodzenie nośników danych w stopniu uniemożliwiającym ich późniejsze odtworzenie przez osoby niepowołane przy zastosowaniu powszechnie dostępnych metod.
22. **Dokument elektroniczny** - dokument utrwalony na nośnikach magnetycznych, optycznych lub w pamięci układów elektronicznych.
23. **PUODO** - Prezes Urzędu Ochrony Danych Osobowych.
24. **Hasło użytkownika** - specjalny, znany wyłącznie użytkownikowi, ciąg znaków umożliwiający uwierzytelnienie użytkownika w systemie przetwarzania informacji.
25. **Identyfikator użytkownika** - nazwa użytkownika w systemie przetwarzania informacji.
26. **Incydent bezpieczeństwa** - sytuacja kryzysowa związana z nieautoryzowanym dostępem do informacji chronionych, ich zniszczeniem, modyfikacją, utratą lub innym celowym działaniem naruszającym bezpieczeństwo ochrony informacji. Incydentem bezpieczeństwa jest również próba podjęcia wymienionych działań.
27. **Informacje** - treści wszelkiego rodzaju przechowywane na dowolnym nośniku informacji, w postaci tradycyjnej - dokumentacja papierowa jak i elektronicznej - układy elektroniczne oraz inne nośniki, np. magnetyczne lub optyczne. Informacja może być wyrażona za pomocą mowy, pisma, obrazu, rysunku, znaku, kodu, dźwięku lub w jakikolwiek inny sposób.
28. **Informacje chronione** - informacje prawnie chronione przetwarzane przez Administratora, w tym w szczególności dane osobowe. Mają jasno określone reguły dostępu i są chronione przed nieautoryzowanym dostępem, powielaniem,

ujawnieniem, modyfikacją, zatajeniem, jak również zniszczeniem, utratą, nieprawidłowym wykorzystaniem lub kradzieżą.

29. **Informacje jawne** - informacje zabezpieczone przed modyfikacją i utratą (zniszczeniem), nie należące do informacji chronionych.
30. **Integralność informacji** - zasada, zgodnie z którą system realizuje funkcję przetwarzania danych w sposób nienaruszony, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej.
31. **Kopia bezpieczeństwa** - kopia oprogramowania lub danych, pozwalająca na ich dokładne odtworzenie w wypadku utraty oryginału.
32. **Logowanie** - proces uwierzytelniania użytkownika w systemie przetwarzania informacji.
33. **Modyfikacja informacji** - zmiana zapisu informacji w systemie przetwarzania.
34. **Nieautoryzowany dostęp** - wykonanie operacji w systemie przetwarzania danych, do której osoba nie została uprawniona (np. zapis, odczyt, udostępnienie lub usuwanie danych itp.).
35. **Niezawodność informacji** - oznacza spójne, powtarzalne, zamierzone zachowania i skutki.
36. **Nośnik informacji** - pamięć układów elektronicznych, medium magnetyczne, optyczne lub papierowe, na którym zapisuje się i przechowuje informacje.
37. **Poufność informacji** - informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom albo procesom.
38. **Prawa dostępu** - listy określające rodzaj operacji, jakie użytkownik może wykonać na udostępnionej informacji w systemie przetwarzania.
39. **Przetwarzanie danych** - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
40. **Rozliczalność** informacji - właściwość systemu pozwalająca przypisać określone działanie w systemie do osoby fizycznej lub procesu oraz umiejscowić je w czasie.
41. **Serwerownia** - wydzielone pomieszczenie będące środowiskiem pracy komputerów pełniących rolę serwerów, a także aktywnych i pasywnych elementów sieci komputerowych.
42. **System informatyczny** - system przetwarzania informacji składający się z urządzeń komputerowych, oprogramowania oraz zewnętrznych nośników informacji (płyta DVD-R, CD-R, dyski przenośne i inne).
43. **Szyfrowanie** - proces polegający na takim przetworzeniu informacji chronionych, aby nie mogły być one odczytane przez osoby nieupoważnione.
44. **Uwierzytelnianie** - proces pozwalający na jednoznaczną identyfikację użytkownika w systemie przetwarzania informacji.
45. **Użytkownik informacji** - osoba mająca dostęp do informacji chronionych na

określonych prawach. Prawa dostępu są określane poprzez nadanie roli dostępu do informacji.

46. **Użytkownik zewnętrzny** - osoba nie będąca pracownikiem UM lub podmiot, wykorzystujący informacje chronione, których administratorem jest UM.
47. **Zasilanie awaryjne** - zapasowy system zasilania, umożliwiający czasowe dostarczenie zasilania do systemu przetwarzania informacji.

II. OCHRONA DANYCH OSOBOWYCH W URZĘDZIE MIEJSKIM W SOŚNICOWICACH - ZASADY OGÓLNE

1. Legalność – ADO dba o ochronę prywatności i przetwarza dane zgodnie z prawem.
2. Bezpieczeństwo – ADO zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.
3. Prawa Jednostki – ADO umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
4. Rozliczalność – ADO dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

ZASADY OCHRONY DANYCH

ADO przetwarza dane osobowe z poszanowaniem następujących zasad:

1. w oparciu o podstawę prawną i zgodnie z prawem (legalizm);
2. rzetelnie i uczciwie (rzetelność);
3. w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
4. w konkretnych celach i nie "na zapas" (minimalizacja);
5. nie więcej niż potrzeba (adekwatność);
6. z dbałością o prawidłowość danych (prawidłowość);
7. nie dłużej niż potrzeba (czasowość);
8. zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

System ochrony danych

System ochrony danych osobowych w UM składa się z następujących elementów:

1. **Inwentaryzacja danych.** UM dokonuje cyklicznej identyfikacji zasobów danych osobowych w UM, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania ewentualnych danych (inwentaryzacja), w tym:
   a) przypadków ewentualnego przetwarzania danych wrażliwych;
   b) przypadków przetwarzania danych osób, których UM nie identyfikuje (dane niezidentyfikowane);
   c) przypadków przetwarzania danych dzieci;
   d) profilowania;
   e) współadministrowania danymi.
2. **Rejestr.** ADO opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych Osobowych w UM (Rejestr). Rejestr jest narzędziem rozliczania zgodności z ochroną danych w UM, dokumentem opisującym, zgodnie z art. 30 RODO, czynności przetwarzania dokonywane przez Administratora, ma formę pisemną, w tym elektroniczną.
3. **Podstawy prawne.** ADO zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych.
4. **Obsługa praw jednostki.** ADO spełnia obowiązki informacyjne względem osób, których

dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:

a) Obowiązki informacyjne. ADO przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków.

b) Możliwość wykonania żądań. ADO weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających.

c) Obsługa żądań. ADO zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany przez RODO i dokumentowane.

d) Zawiadamianie o naruszeniach. ADO stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

5. **Minimalizacja.** ADO wprowadza zasady i metody zarządzania minimalizacją (*privacy by default*), a w tym:

a) zasady zarządzania adekwatnością danych;

b) zasady reglamentacji i zarządzania dostępem do danych;

c) zasady zarządzania okresem przechowywania danych i weryfikacji dalszej przydatności;

6. **Bezpieczeństwo.** ADO zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:

a) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;

b) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;

c) dostosowuje środki ochrony danych do ustalonego ryzyka;

d) posiada system zarządzania bezpieczeństwem informacji;

e) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych – zarządza incydentami.

7. **Przetwarzający.** ADO posiada zasady doboru podmiotów przetwarzających dane na rzecz UM, wymogów co do warunków przetwarzania (umowa powierzenia), zasad weryfikacji wykonywania umów powierzenia.

8. **Eksport danych.** ADO posiada zasady weryfikacji, czy UM nie przekazuje danych do państw trzecich (czyli poza UE, Norwegię, Lichtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce.

9. ***Privacy by design.*** ADO zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów i inwestycji w UM uwzględniają konieczność oceny wpływu zmiany na ochronę danych, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

10. **Przetwarzanie transgraniczne.** ADO weryfikuje, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego

i głównej jednostki organizacyjnej w rozumieniu RODO.

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH

- RCPD, zgodnie z art. 30 RODO, stanowi formę dokumentowania czynności przetwarzania danych, pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.
- ADO prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe. Wzór Rejestru ADO wprowadza zarządzeniem. Rejestr jest prowadzony w formie papierowej i elektronicznej.
- RCPD jest jednym z podstawowych narzędzi umożliwiających ADO rozliczanie większości obowiązków ochrony danych.
- W Rejestrze, dla każdej czynności przetwarzania danych, którą ADO uznał za odrębną dla potrzeb Rejestru, ADO odnotowuje co najmniej: nazwę czynności, cel przetwarzania, opis kategorii osób, opis kategorii danych, podstawę prawną przetwarzania, sposób zbierania danych, opis kategorii odbiorców danych (w tym przetwarzających), informację o przekazaniu poza EU/EOG; ogólny opis technicznych i organizacyjnych środków ochrony danych.

Podstawy przetwarzania

- ADO dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.
- ADO wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms,) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).

III. OBSŁUGA PRAW JEDNOSTKI I REALIZACJA OBOWIĄZKÓW INFORMACYJNYCH

- ADO dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.
- ADO dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.
- ADO wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.
- W celu realizacji praw jednostki ADO zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez ADO zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany,
- ADO dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

OBOWIĄZKI INFORMACYJNE

- ADO określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.
- ADO informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.
- ADO informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.
- ADO informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.
- ADO informuje osobę o planowanej zmianie celu przetwarzania danych.
- ADO informuje osobę przed uchyleniem ograniczenia przetwarzania.
- ADO informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).
- ADO informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.
- ADO bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

ŻĄDANIA OSÓB

Prawa osób trzecich. Realizując prawa osób, których dane dotyczą, ADO wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste itp.), ADO może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

Nieprzetwarzanie. ADO informuje osobę o tym, że nie przetwarza danych jej dotyczących,

Ograniczenie przetwarzania. ADO dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

1. osoba kwestionuje prawidłowość danych - na okres pozwalający sprawdzić ich prawidłowość,
2. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
3. ADO nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
4. osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją - do czasu stwierdzenia, czy po stronie ADO zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.
5. W trakcie ograniczenia przetwarzania ADO przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego. ADO informuje osobę przed uchyleniem ograniczenia przetwarzania. W przypadku ograniczenia przetwarzania danych ADO informuje osobę o odbiorcach danych, na żądanie tej osoby.

Przenoszenie danych. Na żądanie osoby ADO wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona ADO, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych ADO.

Sprzeciw w szczególnej sytuacji. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez ADO w oparciu o uzasadniony interes ADO lub o powierzone ADO zadanie w interesie publicznym, ADO uwzględni sprzeciw, o ile nie zachodzą po stronie ADO ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

MINIMALIZACJA

ADO dba o minimalizację przetwarzania danych pod kątem: adekwatności danych do celów (ilości danych i zakresu przetwarzania), dostępu do danych, czasu przechowywania danych.

Minimalizacja zakresu

ADO zweryfikował zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO.

Minimalizacja dostępu

ADO stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe).

ADO dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu

i zmianach ról osób, oraz zmianach podmiotów przetwarzających.

ADO dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok.

Minimalizacja czasu

Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu są usuwane z systemów UM. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez ADO.

IV. BEZPIECZEŃSTWO PRZETWARZANIA DANYCH OSOBOWYCH

ADO stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych.

ANALIZY RYZYKA I ADEKWATNOŚCI ŚRODKÓW BEZPIECZEŃSTWA

ADO przeprowadza i dokumentuje analizy adekwatności środków bezpieczeństwa danych osobowych. W tym celu:

1. ADO zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji i ciągłości działania – wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.
2. ADO kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.
3. ADO przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. ADO analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia. Zasady, metodologię przeprowadzenia analizy ryzyka w obszarze ochrony danych osobowych wprowadza ADO zarządzeniem.
4. ADO ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym ADO może ustalić przydatność i stosować takie środki i podejście jak:
   a) pseudonimizacja,
   b) szyfrowanie danych osobowych,
   c) inne środki cyberbezpieczeństwa składające się na zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
   d) środki zapewnienia ciągłości działania i zapobiegania skutkom katastrof, czyli zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

Oceny skutków dla ochrony danych

ADO dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.

Środki bezpieczeństwa - analiza zagrożeń i ryzyk występujących przy przetwarzaniu danych osobowych

Charakterystyka możliwych zagrożeń:

1. Zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), których występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu.
2. Zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki przetwarzających dane, pozostawienie danych lub pomieszczeń bez nadzoru, błędy operatorów systemu, awarie sprzętowe, błędy oprogramowania), przy których może dojść do zniszczenia

danych lub naruszenia ich poufności.

3. Zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, gdzie występuje naruszenia poufności danych. Zagrożenia te możemy podzielić na: nieuprawniony dostęp z zewnątrz (włamanie), nieuprawniony dostęp do danych w wewnątrz (przez osoby nieuprawnione).

W każdym przypadku, w sytuacji stwierdzenia wystąpienia któregokolwiek z zagrożeń należy niezwłocznie powiadomić Administratora danych.

1. **Zagrożenia miejsc przetwarzania danych:**

- Włamania od strony okien – wybite szyby, niedomknięte skrzydła.
- Włamania od strony drzwi – zerwane plomby, uszkodzone klamki, źle działające zamki, niedomknięte drzwi, ślady po narzędziach.
- Oddziaływanie czynników zewnętrznych – pożar, zalanie pomieszczeń, katastrofa budowlana.
- Pozostawienie niezamkniętych drzwi lub okien – jeżeli w pomieszczeniu nie pozostają osoby uprawnione do przetwarzania danych.
- Pozostawienie bez nadzoru osób nieuprawnionych do przebywania w obszarze przetwarzania danych.

2. **Zagrożenia związane z tradycyjnym przetwarzaniem danych:**

- Pozostawienie danych na biurkach, półkach, regałach, itp. po zakończeniu pracy.
- Pozostawienie dokumentów zawierających dane osobowe w kserokopiarce lub skanerze.
- Pozostawienie po zakończeniu pracy otwartych szaf, w których gromadzone są dane osobowe.
- Przechowywanie dokumentów w miejscach do tego nieprzeznaczonych.
- Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.
- Przetwarzanie danych przez osoby nieuprawione.
- Nieuzasadnione sporządzanie kserokopii danych.

3. **Zagrożenia związane z przetwarzaniem danych za pomocą systemów informatycznych:**

- Dopuszczenie zapisywania na nośniki zewnętrzne wynoszone poza obszar przetwarzania lub przesyłanie poprzez Internet danych niezaszyfrowanych.
- Dopuszczanie do nieuzasadnionego kopiowania dokumentów i utraty kontroli nad kopią.
- Sporządzanie kopii danych w sytuacjach nie przewidzianych procedurą.
- Utrata kontroli nad kopią danych osobowych.
- Podmiana lub zniszczenie nośników z danymi osobowymi.
- Pozostawienie zapisanego hasła dostępu do bazy danych.
- Samodzielne instalowanie jakiegokolwiek oprogramowania.
- Obecność nowych programów w komputerze lub inne zmiany w konfiguracji

oprogramowania.

- Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.
- Odczytywanie dyskietek i innych nośników przed sprawdzeniem ich programem antywirusowym.
- Niezabezpieczenie komputera zasilaczem awaryjnym podtrzymującym napięcie na wypadek braku zasilania.
- Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania osób nieuprawnionych.
- Ujawnianie sposobu działania aplikacji oraz jej zabezpieczeń osobom niepowołanym.
- Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej.
- Dopuszczenie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.
- Pojawianie się komunikatów alarmowych.
- Awarie sprzętu i oprogramowania, które mogą wskazywać na działanie osób trzecich.
- Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych.
- Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych.
- Próba nieuzasadnionego przeglądania danych w ramach pomocy technicznej.
- Dopuszczanie, aby osoby inne niż ASI lub osoby przez ASI uprawnione, podłączały jakiekolwiek urządzenia, demontowały elementy sieci lub dokonywały innych manipulacji.
- Ślady manipulacji przy układach sieci komputerowej lub komputerach.
- Obecność nowych urządzeń i kabli o nieznanym przeznaczeniu i pochodzeniu.
- Naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji.

ZGŁASZANIE NARUSZEŃ

ADO stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia. Sposób postępowania w przypadku naruszenia bezpieczeństwa danych opisuje przyjęta w jednostce *„Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych w Urzędzie Miejskim w Sośnicowicach"* wydana Zarządzeniem Burmistrza Sośnicowic. Każdy pracownik, który stwierdzi fakt naruszenia bezpieczeństwa danych ma obowiązek podjąć czynności, zgodnie z przyjętą instrukcją, niezbędne do powstrzymania skutków naruszenia ochrony oraz ustalić przyczynę i sprawcę naruszenia ochrony.

W przypadku stwierdzenia naruszenia ochrony danych osobowych na co może wskazywać: stan urządzeń, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej, należy niezwłocznie powiadomić ADO, IOD, AS.

Na podstawie dokonanych ustaleń ADO, w porozumieniu z AS i IOD, podejmuje odpowiednie decyzje.

PRZETWARZAJĄCY

ADO na podstawie zawartych umów lub innych instrumentów prawnych może zlecić przetwarzanie danych podmiotowi przetwarzającemu (procesorowi). ADO posiada zasady doboru i weryfikacji przetwarzających dane na rzecz UM opracowane w celu zapewnienia, aby przetwarzający dawali wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na ADO. W jednostce prowadzona jest, przez IOD, ewidencja zawartych umów powierzenia - zgodnie z przyjętą w Urzędzie Miejskim w Sośnicowicach procedurą.

ADO rozlicza przetwarzających z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z Zasad powierzenia danych osobowych.

UDOSTĘPNIENIE DANYCH OSOBOWYCH

Administrator udostępnia dane osobowe przetwarzane we własnych zasobach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa. W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe nie mające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.

Dane osobowe mogą być udostępniane:

1. w związku wnioskiem od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów prawa;
2. na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych;
3. na podstawie wniosku osoby, której dane dotyczą;
4. dane osobowe przetwarzane w jednostce udostępnia się na pisemny, umotywowany wniosek, chyba że odrębne przepisy prawa stanowią inaczej;
5. wniosek o udostępnienie danych osobowych powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie;
6. wnioski w sprawie udostępnienia danych osobowych rozpatrywane są przez pracowników merytorycznych jednostki w porozumieniu z IOD.

PROJEKTOWANIE PRYWATNOŚCI

ADO zarządza zmianą mającą wpływ na prywatność w taki sposób, aby umożliwić zapewnienie odpowiedniego bezpieczeństwa danych osobowych oraz minimalizacji ich przetwarzania.
W tym celu zasady prowadzenia projektów i inwestycji przez ADO odwołują się do zasad bezpieczeństwa danych osobowych i minimalizacji, wymagając oceny wpływu na prywatność i ochronę danych, uwzględnienia i zaprojektowana bezpieczeństwa i minimalizacji przetwarzania danych od początku projektu lub inwestycji.

BEZPIECZEŃSTWO PRZETWARZANYCH INFORMACJI W UM

Bezpieczeństwo przetwarzanych w UM informacji rozumiane jest jako zapewnienie

następujących cech tych informacji, tj.:

1) poufności;
2) integralności;
3) rozliczalności;
4) dostępności;
5) autentyczności;
6) niezawodności.

1. Podstawą osiągnięcia spójnej ochrony informacji w UM jest rozpoznanie informacji chronionych, systemów oraz obszarów ich przetwarzania, które podlegają ochronie.
2. Sposoby osiągnięcia spójnej ochrony:
   1) wprowadzenie podziału na informacje jawne i chronione;
   2) określenie informacji, stanowiących tajemnicę UM jako podlegających ochronie ze względu na jego dobro i interes;
   3) określenie informacji chronionych ze względu na wymogi prawne;
   4) możliwość nadawania każdej informacji chronionej odpowiedniej klauzuli tajności;
   5) wprowadzenie podziału informacji chronionych na zbiory danych osobowych oraz pozostałe dane chronione i zarządzanie nimi;
   6) określenie organizacyjnych i technicznych wymogów bezpieczeństwa przetwarzania informacji chronionych;
   7) utworzenie struktur organizacyjnych odpowiedzialnych za zarządzanie bezpieczeństwem i przetwarzaniem informacji;
   8) zarządzanie ciągłością przetwarzania informacji;
   9) standaryzację procedur postępowania oraz opracowanie niezbędnej dokumentacji, tj. zasad zarządzania bezpieczeństwem informacji oraz systemów ich przetwarzania;
   10) wdrożenie rozwiązań technicznych, zapewniających wymagany niniejszym dokumentem poziom bezpieczeństwa przetwarzanych informacji – inwestycje w infrastrukturę sieci i systemów informatycznych oraz fizyczne zabezpieczenie obszarów przetwarzania informacji chronionych;
   11) propagowanie zasad bezpieczeństwa informacji wśród kierownictwa i pracowników instytucji;
   12) szkolenie wszystkich nowozatrudnionych pracowników, którzy będą mieć określone w zakresie obowiązków zadania, z którymi będzie wiązało się przetwarzanie danych osobowych, w zakresie bezpieczeństwa informacji, przeprowadzane w formie instruktażu.
   13) szkolenia okresowe osób posiadających upoważnienie do przetwarzania danych osobowych.
3. Następujące rodzaje informacji zostały zidentyfikowane, jako informacje chronione:
   1) dane osobowe zagregowane w zbiory,
   2) pozostałe dane, takie jak dane kontrahentów stanowiące tajemnicę handlową.
4. Wszelkie informacje przekazywane i przetwarzane w UM, nie oznaczone jako należące

do osób trzecich, będą traktowane jako własność UM.

5. UM chroni zarówno informacje własne jak i powierzone. Informacje stanowiące własność UM nie mogą być zatajane wewnątrz UM, ale mogą być chronione, w tym także przed nieautoryzowanym dostępem.
6. Wszystkie informacje w UM nie są domyślnie chronione, jeżeli nie zostały zidentyfikowane, opisane i oznaczone jako chronione.
7. Bezpieczeństwo informacji jest to również wynik wszystkich ludzkich postaw, akceptowanych wartości i norm postępowania, które tworzą wszyscy pracownicy.
8. Bez względu na zajmowane stanowisko, miejsce wykonywanej pracy oraz charakter stosunku pracy, zasady określone w niniejszej Polityce oraz w dokumentach powiązanych muszą być znane i stosowane przez pracowników oraz w niezbędnym zakresie przez użytkowników zewnętrznych przetwarzających dane, których administratorem jest UM.
9. Zabrania się używania wszelkich systemów przetwarzania informacji w UM do celów prywatnych.
10. Zabrania się używania danych wrażliwych, w formie jakichkolwiek oznaczeń, do kodowania numerów jednolitego rzeczowego wykazu akt lub innych wykazów.
11. Informacje przekazywane, w sytuacjach nieuregulowanych odrębnymi przepisami prawa, podmiotom zewnętrznym do celów statystycznych, badawczych, itp., mogą zostać udostępnione jedynie za wyraźną zgodą Administratora, po uprzednim ich anonimizowaniu.

ZARZĄDZANIE UŻYTKOWNIKAMI INFORMACJI CHRONIONYCH

1. IOD prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych
2. Jakakolwiek zmiana w zakresie przyznanych uprawnień podlega niezwłocznie odnotowaniu w ewidencji, o której mowa w ust.1.
3. IOD powiadamiany jest drogą elektroniczną przez pracownika Działu Personalnego o:
   1) zatrudnieniu pracownika,
   2) przeniesieniu pracownika do innej komórki organizacyjnej,
   3) czasowym oddelegowaniu do innej komórki organizacyjnej oraz jego zakończeniu,
   4) ustaniu zatrudnienia pracownika,
   5) zmianie nazwiska pracownika,

NADAWANIE DOSTĘPU DO INFORMACJI PODLEGAJĄCYCH OCHRONIE

Bezpieczeństwo zasobów ludzkich

1. W trakcie procesu zatrudniania należy postępować zgodnie z obowiązującymi przepisami.
2. Kandydat przed przystąpieniem do pracy powinien:

a) przejść stosowne procedury podczas rozpoczęcia zatrudnienia (np. sprawdzić stan zdrowia u lekarza medycyny pracy, przejść szkolenie BHP itp.);

b) zapoznać się z obowiązującymi regulacjami wewnętrznymi, a w szczególności z Polityką oraz Instrukcją zarządzania systemem informatycznym UM. Fakt zapoznania się z dokumentami powinien zostać potwierdzony własnoręcznym podpisem na oświadczeniu

zgodnie z wzorem z załącznika nr 2.

c) przejść szkolenie, z zakresu zasad ochrony danych osobowych stosowanych przez ADO, realizowane przez IOD jednostki.

d) otrzymać upoważnienie do przetwarzania danych.

3. Proces nadawania nowych uprawnień, modyfikacji lub odbierania uprawnień do pracy w systemie informatycznym w trakcie zatrudnienia realizowany jest poprzez odpowiednią procedurę, określoną w Instrukcji zarządzania systemem informatycznym.
4. Pracownicy powinni być regularnie szkoleni i uświadamiani w zakresie ochrony danych osobowych.
5. Szkolenie dla pracowników z zakresu ochrony danych osobowych należy przeprowadzić każdorazowo po:

a) znaczącej zmianie przepisów dotyczących ochrony danych osobowych,

b) wprowadzeniu istotnych zmian w Polityce bezpieczeństwa danych osobowych oraz dokumentach z nią związanych,

c) na wniosek ADO, IOD

Szkolenie może zostać przeprowadzone w dowolnej formie, jednak każde uczestnictwo powinno zostać potwierdzone własnoręcznym podpisem pracownika (na oświadczeniu lub liście uczestników).

Po zakończeniu zatrudnienia pracownika, AS/ Informatyk niezwłocznie blokuje dostęp do uprawnień w systemach informatycznych – blokowane są konta, z których pracownik korzystał. Fakt ustania uprawnień zostaje odnotowany w ewidencji upoważnień.

ŚRODKI ORGANIZACYJNE OCHRONY INFORMACJI

1. Dostęp do danych chronionych posiadają tylko i wyłącznie osoby z odpowiednim pisemnym, imiennym upoważnieniem, udzielonym przez Administratora zgodnie z wzorem z załącznika nr 1.
2. Upoważnienie uprawnia osobę, o której mowa w ust. 1 do przetwarzania danych chronionych wyłącznie w obszarze określonym zakresem czynności pracowniczych lub wynikającym z zadań realizowanych na podstawie umów cywilnoprawnych lub odrębnych regulacji.
3. Każda osoba upoważniona jest zobowiązana zachować szczególną ostrożność przy przetwarzaniu wszelkich danych chronionych.
4. Należy chronić dane przed wszelkim dostępem do nich osób nieupoważnionych.
5. Nośników informacji (w formie papierowej i elektronicznej) z danymi podlegającymi ochronie nie można pozostawiać w miejscach ogólnodostępnych i niezabezpieczonych oraz nie należy udostępniać osobom nieupoważnionym.
6. Pomieszczenia w których są przetwarzane dane chronione muszą być zamykane na klucz lub inny system umożliwiający blokadę wejścia.
7. W przypadku pomieszczeń do których dostęp mają również osoby nieupoważnione, mogą one przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych

i tylko w czasie wymaganym na wykonanie niezbędnych czynności.

8. Miejsca (np. szafy, biurka) przeznaczone do przechowywania danych chronionych muszą być zamykane na klucz.
9. Klucze do tych miejsc posiadają tylko pracownicy upoważnieni.
10. Miejsca z danymi są otwarte tylko na czas potrzebny na dostęp do danych, a następnie zostają zamknięte.
11. Dane chronione w formie papierowej mogą znajdować się w miejscach ogólnodostępnych (np. na biurkach) tylko w trakcie dokonywania czynności służbowych, a następnie muszą być przechowywane w miejscach przeznaczonych do tego celu (np. zamykana szafa).
12. Wydruki robocze zawierające informacje chronione, błędne lub zdezaktualizowane muszą być niezwłocznie bezpowrotnie niszczone przy użyciu niszczarki do papieru lub w inny sposób, zapewniający skuteczne ich usunięcie lub anonimizowanie.
13. Zabrania się przetwarzania danych chronionych poza obszarem przetwarzania, który stanowi siedziba UM.
14. W celu zapobiegania nieautoryzowanemu dostępowi do informacji lub kradzieży informacji i środków jej przetwarzania Administrator stosuje **politykę czystego biurka**. Dokumenty i nośniki danych, zawierające dane osobowe, nie powinny pozostać niezabezpieczone w czasie nawet chwilowej nieobecności w pokoju. Pokój należy zamknąć w sposób uniemożliwiający dostęp dla osób nieuprawnionych. Po zakończeniu pracy dokumenty i komputerowe nośniki z danymi powinny być przechowywane w szafach, a pokoje powinno się zamykać.
15. Szczególną uwagę należy zwrócić na drukarki sieciowe i kserokopiarki dostępne dla większej liczby pracowników. Pracownicy powinni odbierać dokumenty natychmiast po wykonaniu przez urządzenie zleconego zadania. Nie powinny one pozostawać dostępne ani dla obcych osób ani dla pracowników nieposiadających stosownych uprawnień.
16. Polityka czystego ekranu ma na celu zabezpieczenie przed nieautoryzowanym dostępem do systemów teleinformatycznych i zabezpieczenie przez ujawnieniem informacji chronionych oraz przed wglądem do danych wyświetlanych na ekranie monitora przez osoby nieuprawnione. Każdorazowe odejście od stanowiska pracy powinno zostać poprzedzone wylogowaniem się lub zablokowaniem dostępu do systemu tak, aby niemożliwe było uzyskanie nieautoryzowanego dostępu do systemu np. poprzez wywołanie blokowanego hasłem wygaszacza ekranu stosując skrót klawiaturowy (ikonka WINDOWS + L). Po zakończeniu pracy należy zamknąć aktywne aplikacje oraz wyrejestrować się (wylogować się) z systemu lub też zablokować dostęp do systemu.

Zabrania się:

1. wynoszenia dokumentacji będącej własnością UM oraz nośników zawierających dane w celach nie związanych z działalnością jednostki;
2. wyrzucania dokumentów zawierających dane osobowe bez uprzedniego ich trwałego zniszczenia, najlepiej w przeznaczonych do tego niszczarkach dokumentów o odpowiednim poziomie bezpieczeństwa;
3. pozostawiania dokumentów, kopii dokumentów zawierających dane osobowe w drukarkach, kserokopiarkach;

4. pozostawiania kluczy w drzwiach, szafach, biurkach, zostawiania otwartych pomieszczeń, w których przetwarza się dane osobowe – w czasie nieobecności upoważnionego pracownika;
5. pozostawiania, bez nadzoru, osób trzecich przebywających w pomieszczeniach UM, w których przetwarzane są dane osobowe;
6. pozostawiania, bez nadzoru, dokumentów na biurku, w szczególności po zakończeniu pracy, pozostawiania otwartych dokumentów na ekranie monitora;
7. ignorowania nieznanych osób z zewnątrz poruszających się w obszarze przetwarzania danych osobowych;
8. przekazywania, udostępniania informacji będących danymi osobowymi osobom nieupoważnionym.

KOMPETENCJE I ODPOWIEDZIALNOŚĆ W ZARZĄDZANIU BEZPIECZEŃSTWEM DANYCH OSOBOWYCH

Administrator Danych Osobowych (ADO):

1. Formułuje i wdraża warunki techniczne i organizacyjne służące ochronie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Decyduje o zakresie, celach oraz metodach przetwarzania i ochrony danych osobowych.
3. Odpowiada za zgodne z prawem przetwarzanie danych osobowych.
4. Wyznacza na stanowisko Inspektora Ochrony Danych.
5. Powołuje na stanowisko Administratora Systemu.
6. Wydaje upoważnienia do przetwarzania danych osobowych określając w nich zakres i termin ważności.
7. Odpowiada za prowadzenie Rejestru czynności przetwarzania zgodnie z art. 30 RODO.

Inspektor Ochrony Danych IOD

1. Inspektor ochrony danych (IOD) ma za zadanie zapewnianie przestrzegania przepisów o ochronie danych osobowych w UM oraz wykonywanie zadań wynikających z art. 39 RODO. Inspektor wykonuje ponadto obowiązki powierzone przez Administratora z zakresu realizacji polityki bezpieczeństwa informacji i ochrony danych osobowych.
2. Inspektor (IOD) w szczególności:

a) nadzoruje przestrzeganie zasad ochrony, o których mowa w przepisie art. 39 RODO,

b) jest umocowany do przetwarzania danych chronionych na podstawie pisemnego upoważnienia wydanego przez Administratora,

c) sporządza projekty aktualizacji Polityki Bezpieczeństwa Informacji oraz wspomaga AS w aktualizacji Instrukcji Zarządzania Systemem Informatycznym;

d) opiniuje projekty dokumentów mających wpływ na bezpieczeństwo informacji chronionych w UM;

e) nadzoruje pod względem bezpieczeństwa danych osobowych pracę pracowników UM.

f) analizuje zgłoszenia zdarzeń związanych z bezpieczeństwem informacji chronionych, otrzymywane od pracowników UM;

g) przeprowadza szkolenia, o których mowa w art. 39 ust. 1 lit. a RODO,

h) prowadzi ewidencję osób uprawnionych do przetwarzania danych osobowych zgodnie z wzorem z załącznika nr 3;

Administratora systemu (AS) / Informatyk

1. Administrator Systemu (AS) / Informatyk
   1) Uprawnienia i obowiązki:
      a) AS ma za zadanie dbać o poprawne, efektywne i bezpieczne działanie administrowanego systemu informatycznego,
      b) zapewnia ciągłość działania systemu,
      c) inicjuje, koordynuje i nadzoruje działania mające na celu poprawę wydajność i bezpieczeństwa systemu, w tym opiniuje i wdraża wymagane procedury,
      d) instaluje i konfiguruje sprzęt i oprogramowanie,
      e) zakłada, likwiduje oraz blokuje/ odblokowuje konta użytkowników,
      f) dokonuje aktualizacji Instrukcji Zarządzania Systemem Informatycznym,
      g) przyznaje/ odbiera prawa dostępu do aplikacji służących do przetwarzania danych chronionych w systemie informatycznym.

Pracownik Przetwarzający Dane:

1. Chroni prawo do prywatności osób fizycznych powierzających swoje dane osobowe poprzez przetwarzanie ich zgodnie z przepisami prawa oraz zasadami określonymi w polityce bezpieczeństwa i instrukcji zarządzania systemem informatycznym.
2. Zapoznaje się z zasadami określonymi w polityce i instrukcji zarządzania systemem informatycznym oraz składa oświadczenie o znajomości zawartych w nich zapisów.

WYKAZ BUDYNKÓW I POMIESZCZEŃ TWORZĄCYCH OBSZAR PRZETWARZANIA DANYCH OSOBOWYCH.

Obszar, w którym przetwarzane są dane osobowe tworzą budynki oraz wydzielone kondygnacje budynków Urzędu Miejskiego w Sośnicowicach.
Stały dostęp do pomieszczeń, w których przetwarzane są dane osobowe mają tylko osoby upoważnione. Przebywanie osób upoważnionych po godzinach pracy w pomieszczeniach, w których przetwarzane są dane osobowe jest dopuszczalne jedynie za zgodą Administratora Danych Osobowych.
ADO może zezwolić na przebywanie w obszarze przetwarzania danych osobowych, osobom sprzątającym te pomieszczenia poza godzinami pracy UM bez konieczności obecności osoby dopuszczonej do przetwarzania danych. Osoby zatrudnione na stanowiskach obsługi podpisują klauzulę poufności, która zobowiązuje ich do zachowania w tajemnicy wszelkich informacji dotyczących przetwarzanych danych osobowych i stosowanych zabezpieczeń.
Wykaz budynków oraz pomieszczeń Urzędu Miejskiego w Sośnicowicach, w których wyłącznie możliwe jest przetwarzanie danych osobowych zawiera załącznik nr 4

1. W budynkach użytkowanych przez UM wyznacza się następujące strefy bezpieczeństwa:
   1) strefa publiczna,
   2) strefa ograniczonego dostępu,
   3) strefa ścisłej kontroli dostępu.
2. Strefę publiczna:
   1) strefę publiczną stanowią pomieszczenia ogólnodostępne oraz ciągi komunikacyjne;
   2) dostęp do strefy publicznej nie jest ograniczony.
3. Strefa ograniczonego dostępu:
   1) strefę ograniczonego dostępu stanowią pomieszczenia, w których są przetwarzane dane chronione,
   2) dostęp do strefy ograniczonego dostępu posiadają osoby upoważnione przez ADO,
   3) osoby postronne mogą przebywać w strefie ograniczonego dostępu wyłącznie w obecności osób upoważnionych przez ADO,
4. Strefa ścisłej kontroli dostępu:
   1) Strefę ścisłej kontroli dostępu stanowią pomieszczenia serwerowni;
   2) Zasady dostępu do strefy ścisłej kontroli dostępu zostaną określone w odrębnych aktach wewnętrznych wydanych przez ADO.

V. POSTANOWIENIA KOŃCOWE

1. Polityka jest dokumentem wewnętrznym i nie może być udostępniania osobom nieupoważnionym w żadnej formie.
2. Każda osoba przetwarzająca dane osobowe zobowiązana jest do zapoznania się z treścią Polityki Bezpieczeństwa oraz Instrukcją Zarządzania Systemem Informatycznym.
3. Użytkownik zobowiązany jest złożyć oświadczenie, o tym, iż znane są mu przepisy Rozporządzenia RODO, Ustawy o ochronie danych osobowych, oraz zapisy obowiązującej Polityką bezpieczeństwa i Instrukcji zarządzania systemem informatycznym.
4. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy RODO oraz Ustawy o ochronie danych osobowych.
5. Pracownicy zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.

VI. SPIS ZAŁĄCZNIKÓW

1. Załącznik nr 1- Upoważnienie do przetwarzania danych
2. Załącznik nr 2- Oświadczenie pracownika
3. Załącznik nr 3- Ewidencja osób upoważnionych
4. Załącznik nr 4- Wykaz pomieszczeń stanowiących obszar przetwarzania danych osobowych Urzędu Miejskiego w Sośnicowicach

BURMISTRZ
Leszek Kołodziej

UPOWAŻNIENIE

DO PRZETWARZANIA DANYCH OSOBOWYCH NR.....

Z dniem .....2018r, na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1) – dalej RODO – nadaję upoważnienie Pani/Panu:

.....

.....

(imię i nazwisko)

do przetwarzania danych osobowych, do których ma Pani/Pan dostęp w związku z wykonywaniem powierzonych obowiązków służbowych na stanowisku ..... w Urzędzie Miejskim w Sośnicowicach, zgodnie z przydzielonym zakresem czynności, udzielonymi pełnomocnictwami, oraz poleceniami Administratora danych.

Upoważnienie traci swą moc najpóźniej w dniu jego odwołania lub ustania stosunku pracy. Niniejszy dokument uchyla wcześniej wydane upoważnienia.

.....
(data i podpis pracownika)

.....
(podpis osoby uprawnionej do nadania upoważnienia)

Data wygaśnięcia[1)].....

Odwołano, dnia .....

.....
(podpis osoby uprawnionej do odwołania upoważnienia)

[1)] data rozwiązania stosunku pracy/umowy cywilnoprawnej

OŚWIADCZENIE

Oświadczam, iż zapoznałam/em się z przepisami dotyczącymi ochrony danych osobowych, w szczególności z przepisami Rozporządzenia Parlamentu Europejskiego nr 2016/679 tzw. Rodo, Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych oraz wprowadzonymi i wdrożonymi do stosowania przez Administratora Danych procedurami określonymi w Polityce bezpieczeństwa informacji, oraz Instrukcji zarządzania systemem informatycznym.

Zobowiązuję się do:

- przetwarzania danych osobowych na polecenia Administratora danych, w zakresie i celu zgodnym z nadanym upoważnieniem,
- zachowania w tajemnicy danych osobowych, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań służbowych lub obowiązków pracowniczych, również po ustaniu zatrudnienia,
- niewykorzystywania danych osobowych w celach pozasłużbowych,
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych, również po ustaniu zatrudnienia,
- korzystania ze sprzętu IT oraz oprogramowania wyłącznie w związku z wykonywaniem obowiązków pracowniczych,
- wykorzystywania jedynie legalnego oprogramowania pochodzącego od Pracodawcy,
- należytej dbałości o sprzęt i oprogramowanie zgodnie z dokumentacją ochrony danych osobowych,
- natychmiastowego zgłaszania do Administratora zaobserwowania próby lub faktu naruszenia danych osobowych, zabezpieczenia fizycznego pomieszczenia, bezpieczeństwa zbioru/zbiorów lub systemów informatycznych.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane przez Pracodawcę za naruszenie obowiązków pracowniczych w rozumieniu Kodeksu Pracy, za naruszenie ustawy o ochronie danych osobowych.

.....

(data i podpis pracownika)

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Lp.	Nazwisko i imię pracownika	Stanowisko/komórka organizacyjna	Data nadania upoważnienia	Nr upoważnienia	Identyfikator/ Login w systemie informatycznym
1	2	3	4	5	6

		17	Referat Gospodarki Gminnej
		18	Referat Gospodarki Gminnej
2	Urząd Miejski w Sośnicowicach Rynek 17 Budynek Rady Gminy	PARTER	
		19	Referat Organizacyjny i Spraw Obywatelskich , KW
		19A	Referat Gospodarki Gminnej
		STARE ARCHIWUM	Referat Organizacyjny i Spraw Obywatelskich
		NOWE ARCHIWUM	Referat Organizacyjny i Spraw Obywatelskich
		I PIĘTRO	
		20	Referat Organizacyjny i Spraw Obywatelskich
		21	Referat Organizacyjny i Spraw Obywatelskich
		22	Sala narad
		23A	Referat Gospodarki Gminnej, Referat Organizacyjny i Spraw Obywatelskich
		23B	Referat Organizacyjny i Spraw Obywatelskich, Informacje Niejawne
3	Urząd Miejski w Sośnicowicach ul. Kościuszki 22 Budynek Urzędu Stanu Cywilnego	I PIĘTRO	
		SALA ŚLUBÓW	USC
		BIURO USC	USC
		EWIDENCJA LUDNOŚCI, DOWODY OSOBISTE	Referat Organizacyjny i Spraw Obywatelskich