ZARZĄDZENIE NR OR.120.32.2018
BURMISTRZA WOŁCZYNA

z dnia 24 maja 2018 r.

w sprawie procedurbezpieczeństwa przetwarzania i ochrony danych osobowych

Na podstawie art. 24 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 roku 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), zarządzam co następuje:

§ 1. 1. Wprowadzam procedury bezpieczeństwa przetwarzania i ochrony danych osobowych w Urzędzie Miejskim w Wołczynie, stanowiące załącznik do niniejszego zarządzenia.

2. W skład procedur, o których mowa w ust. 1 wchodzą:

1) Polityka ochrony danych osobowych;

2) Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;

3) Procedura postępowania w przypadku zagrożenia lub naruszenia ochrony danych osobowych;

4) Procedura nadawania, zmiany i cofania upoważnień do przetwarzania danych osobowych;

5) Procedura nadawania, zmiany i cofania uprawnień do przetwarzania danych osobowych w systemach informatycznych;

6) Zasady korzystania z komputerów stacjonarnych i przenośnych urządzeń przetwarzających dane osobowe;

7) Środki organizacyjne i techniczne niezbędne dla zapewnienia poufności, integralności i rozliczalności danych osobowych;

§ 2. Zobowiązuje pracowników Urzędu Miejskiego do zapoznania się z treścią procedur, o których mowa w § 1 oraz do ich przestrzegania.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania z mocą obowiązującą od 25 maja 2018 roku.

BURMISTRZ
mgr Jan Leszek Wiącek

Załącznik do Zarządzenia Nr OR.120.32.2018

Burmistrza Wołczyna z dnia 24 maja 2018 roku

POLITYKA OCHRONY DANYCH OSOBOWYCH W Urzędzie Miejskim w Wołczynie

WSTĘP

Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO – 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)

Ochrona przetwarzanych danych osobowych rozumiana jest natomiast jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Przy czym przez;

- poufność danych należy rozumieć właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
- integralność danych należy rozumieć właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- rozliczalność danych należy rozumieć właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
- dostępność informacji należy rozumieć zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne.

Polityka zawiera:

a) opis zasad ochrony danych obowiązujących w Urzędzie Miejskim w Wołczynie,

b) odwołania do załączników uszczegóławiających (procedury lub instrukcje dotyczące poszczególnych obszarów z zakresu ochrony danych osobowych wymagających doprecyzowania w odrębnych dokumentach).

1. SKRÓTY I DEFINICJE

Polityka oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.

RODO oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

Dane oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu.

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.

Dane karne oznaczają dane wymienione w art. 10 RODO, tj. dane dotyczące wyroków skazujących i naruszeń prawa.

Dane dzieci oznaczają dane osób poniżej 16 roku życia.

Osoba lub **podmiot danych** oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.

Administrator Danych Osobowych (ADO) lub **Administrator** oznacza Urząd Miejski reprezentowany przez Burmistrza Wołczyna.

Podmiot przetwarzający oznacza instytucję lub osobę, której Urząd Miejski powierzył przetwarzanie danych osobowych.

IOD lub **Inspektor** oznacza Inspektora Ochrony Danych Osobowych.

System informatyczny oznacza zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych.

System tradycyjny oznacza zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia i środków trwałych w celu przetwarzania danych osobowych na papierze.

RCPD lub **Rejestr** oznacza Rejestr Czynności Przetwarzania Danych Osobowych.

Organizacja oznacza Urząd Miejski w Wołczynie.

2. CEL POLITYKI OCHRONY DANYCH

2.1. Celem niniejszego dokumentu jest zapewnienie zgodności procesu przetwarzania danych osobowych w Organizacji z obowiązującymi przepisami prawa, w szczególności z RODO, a co za tym idzie zapewnienie przetwarzania tych danych w sposób gwarantujący ich bezpieczeństwo

2.2. Regulacje wewnętrzne zawarte w niniejszym dokumencie określają środki i sposoby ochrony danych osobowych przyjętych przez Administratora danych. Zmiany organizacyjne, zmiany sposobu działania Administratora danych w zakresie mającym wpływ na proces przetwarzania danych osobowych oraz zmiany przepisów prawa będą powodowały konieczność aktualizacji niniejszego dokumentu.

3. ZAKRES STOSOWANIA POLITYKI OCHRONY DANYCH

3.1. Niniejszą Politykę stosuje się w odniesieniu do wszelkich danych osobowych, wobec których Organizacji przysługuje status Administratora Danych Osobowych, przetwarzanych zarówno w systemach informatycznych jak i w systemach tradycyjnych (papierowych) tj. księgach, skorowidzach, wykazach i

innych zbiorach ewidencyjnych, w szczególności danych osobowych przetwarzanych w celach rekrutacyjnych, zatrudnienia i nawiązania współpracy, finansowych i rachunkowych, świadczenia usług, marketingowych oraz windykacyjnych.

3.2. Zakres stosowania Polityki obejmuje ponadto;

a) wszystkich lokalizacje - budynki i pomieszczenia, w których są lub będą przetwarzane informacje podlegające ochronie,

b) wszystkich pracowników w rozumieniu przepisów Kodeksu pracy, współpracowników, praktykantów, stażystów i innych osób mających dostęp do informacji podlegających ochronie.

3.3. Niniejszy dokument podlega przeglądom i aktualizacji, w szczególności w przypadku wystąpienia zmian w przepisach prawa oraz w przypadku wprowadzania zmian w działaniach Administratora danych związanych z przetwarzaniem danych osobowych.

4. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

4.1 **Administrator Danych Osobowych**

Na Administratorze danych spoczywa odpowiedzialność za realizację szeregu zadań wynikających z RODO. Są to w szczególności takie zadania jak;

a)utworzenie nowych klauzul informacyjnych wynikających z obowiązków ADO zawartych w art. 13-14 RODO (art.12),

b) ułatwianie podmiotom danych wykonywania ich praw wynikających z art. 15-22 RODO (art.15-22),

c) wdrożenie i uaktualnianie niniejszej dokumentacji wraz z procedurami ochrony danych (art.24),

d) uwzględnianie ochrony danych w fazie projektowania (art.25),

e) wyznaczanie podmiotów przetwarzających dane osobowe na podstawie umowy lub innego aktu prawnego (art.28),

f) weryfikacja i uaktualnienie upoważnień do przetwarzania danych osobowych (art.28),

g) prowadzenie rejestru czynności przetwarzania danych (art.30),

h) współpraca z organem nadzorczym (art. 31),

i) analiza ryzyk naruszenia praw podmiotów danych (art.32),

j) wdrożenie odpowiednich środków organizacyjnych i technicznych w celu zapewnienia bezpieczeństwa przetwarzania danych odpowiadającego analizowanym ryzykom (art.32),

k) zgłaszanie naruszeń ochrony danych osobowych organowi nadzorczemu (art.33),

l) prowadzenie rejestru naruszeń ochrony danych osobowych (art.33),

m) zawiadamianie podmiotów danych o naruszeniach ochrony ich danych osobowych (art.34),

n) opracowanie dokumentacji określanej jako „ocena skutków dla ochrony danych" w przypadkach wymienionych w art. 35 RODO (art.35),

o) prowadzenie tzw. „uprzednich konsultacji" z organem nadzorczym w przypadku wymienionym w art. 36 RODO (art.36),

p) wyznaczenie inspektora ochrony danych (art.37).

4.2. **Inspektor Ochrony Danych**

Wyznaczenie Inspektora Ochrony Danych jest obligatoryjne w przypadkach wymienionych w art.37 ust.1 RODO. Jest więc także jednym z obowiązków nałożonych na Administratora danych. Inspektor Ochrony Danych wyznaczany jest na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO. Do zadań tych należy;

a) informowanie Administratora danych oraz pracowników odpowiedzialnych za przetwarzanie danych o ich obowiązkach wynikających z RODO,

b) monitorowanie przestrzegania przepisów RODO, Polityki ochrony danych oraz innych przepisów dotyczących ochrony danych osobowych,

c) szkolenia personelu i inne działania zwiększające świadomość wagi przestrzegania przepisów dotyczących ochrony danych osobowych,

d) przeprowadzanie audytów związanych z przetwarzaniem danych osobowych,

e) udzielanie zaleceń co do „oceny skutków dla ochrony danych", wynikającej z art. 35 RODO,

f) współpraca z organem nadzorczym,

g) pełnienie funkcji punktu kontaktowego dla organu nadzorczego oraz podmiotów danych.

4.3. **Administrator Systemów Informatycznych (ASI)**

Wyznaczenie Administratora Systemów Informatycznych nie jest wymagane w żadnych regulacjach prawnych określających sposób zarządzania i zabezpieczania danych osobowych. Niemniej jednak w organizacjach korzystających z narzędzi informatycznych wydaje się być niezbędne. Warunkiem nieodzownym zatrudnienia ASI jest odpowiednia wiedza w zakresie IT. Do jego obowiązków należy w szczególności;

a) współpraca przy przygotowaniu i wdrażaniu dokumentacji ochrony danych osobowych,

b) współpraca przy przeprowadzaniu okresowych audytów związanych z przetwarzaniem danych osobowych,

c) zapewnienie ciągłości działania systemu,

d) zapewnienie awaryjnego źródła zasilania oraz zabezpieczenia przed zakłóceniami w sieci zasilającej,

e) nadzór nad naprawą oraz likwidacją urządzeń komputerowych,

f) kontrola przeglądu i konserwacji systemów informatycznych służących do przetwarzania danych osobowych,

g) zabezpieczenie systemów służących do przetwarzania danych osobowych przed działaniem oprogramowania złośliwego,

h) dostosowanie wszystkich systemów informatycznych służących do przetwarzania danych osobowych do wymogów RODO,

i) zabezpieczenie pomieszczenia serwerowni przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych,

j) ochrona przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem,

k) nadzorowanie stosowania zasady „czystego ekranu".

4.4. **Osoby upoważnione do przetwarzania danych osobowych**

4.4.1. Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych w Organizacji zobowiązana jest do ich ochrony w sposób zgodny z przepisami RODO oraz niniejszej Polityki ochrony danych.

4.4.2. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich przetwarzania i zabezpieczenia. Obowiązek ten istnieje także po ustaniu stosunku zatrudnienia oraz świadczenia usług.

4.5. **Osoby i instytucje, którym Organizacja powierza dane osobowe**

Każda osoba lub instytucja, której Organizacja powierza dane osobowe zobowiązana jest do ich ochrony oraz zachowania tajemnicy w sposób zgodny z przepisami RODO oraz zawartej Umowy powierzenia przetwarzania danych.

5. OCHRONA DANYCH OSOBOWYCH W ORGANIZACJI – ZASADY OGÓLNE

5.1. **Filary ochrony danych osobowych w Organizacji**:

a) Legalność – Organizacja dba o ochronę prywatności i przetwarza dane zgodnie z prawem.

b) Bezpieczeństwo – Organizacja zapewnia odpowiedni poziom bezpieczeństwa danych, podejmując stale działania w tym zakresie.

c) Prawa jednostki – Organizacja umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.

d) Rozliczalność –Organizacja dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność z obowiązującymi przepisami.

5.2. **Zasady ochrony danych**

Organizacja przetwarza dane osobowe z poszanowaniem następujących zasad:

a) w oparciu o podstawę prawną i zgodnie z prawem (legalizm);

b) rzetelnie i uczciwie (rzetelność);

c) w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);

d) w konkretnych celach i nie „na zapas" (minimalizacja);

e) nie więcej niż potrzeba (adekwatność);

f) z dbałością o prawidłowość danych (prawidłowość);

g) nie dłużej niż potrzeba (czasowość);

h) zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

6. SYSTEM OCHRONY DANYCH

System ochrony danych osobowych składa się z następujących elementów:

6.1. **Inwentaryzacja danych**

Organizacja dokonuje identyfikacji zasobów danych osobowych, klas danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja), w tym:

a) przypadków przetwarzania danych szczególnych kategorii i danych karnych,

b) przypadków przetwarzania danych osób, których Organizacja nie identyfikuje,

c) przypadków przetwarzania danych dzieci,

d) współadministrowania danymi.

6.2. **Rejestr**

Organizacja opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych Osobowych. Rejestr jest narzędziem rozliczania zgodności z ochroną danych w Organizacji.

6.3. **Podstawy prawne**

Organizacja zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:

a) utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość,

b) inwentaryzuje i uszczegóławia uzasadnienie przypadków przetwarzania danych na podstawie prawnie uzasadnionego interesu.

6.4. **Obsługa praw jednostki**

Organizacja spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:

a) obowiązki informacyjne

Organizacja przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków;

b) możliwość wykonania żądań

Organizacja weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających;

c) obsługa żądań

Organizacja zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany przez RODO oraz dokumentowane;

d) zawiadamianie o naruszeniach

Organizacja stosuje zasady pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.

6.5. **Minimalizacja**

Celem Organizacji jest zoptymalizowanie zasad i metod zarządzania minimalizacją a w tym:

a) zasad zarządzania adekwatnością danych;

b) zasad reglamentacji i zarządzania dostępem do danych;

c) zasad zarządzania okresem przechowywania danych i weryfikacji dalszej przydatności.

6.6. **Bezpieczeństwo**

Organizacja 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.

6.7. **Przetwarzający**

Organizacja stosuje zasady doboru przetwarzających dane na rzecz Organizacji, wymogów co do warunków przetwarzania (umowa powierzenia) oraz zasady weryfikacji wykonywania umów powierzenia.

6.8. **Eksport danych**

Organizacja stosuje zasady weryfikacji dotyczące nie przekazywania danych do państw trzecich (czyli poza UE, Norwegię, Liechtenstein, Islandię) lub do organizacji międzynarodowych oraz zapewnienia zgodnych z prawem warunków takiego przekazywania, jeśli ma ono miejsce.

6.9. **Privacy by design**

Organizacja zarządza zmianami wpływającymi na prywatność. W tym celu w razie potrzeby utworzy procedury uruchamiania nowych projektów uwzględniające konieczność oceny wpływu zmiany na ochronę danych, analizę ryzyka, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

6.10. **Przetwarzanie transgraniczne**

Organizacja stosuje zasady weryfikacji, kiedy zachodzą przypadki przetwarzania transgranicznego oraz zasady ustalania wiodącego organu nadzorczego i głównej jednostki organizacyjnej w rozumieniu RODO.

7. INWENTARYZACJA

7.1. **Dane szczególnych kategorii i dane karne**

Organizacja identyfikuje przypadki, w których przetwarza lub może przetwarzać dane szczególnych kategorii lub dane karne, oraz utrzymuje dedykowane mechanizmy zapewnienia zgodności z prawem przetwarzania takich danych. W przypadku zidentyfikowania przypadków przetwarzania danych szczególnych kategorii lub danych karnych Organizacja postępuje zgodnie z przyjętymi zasadami w tym zakresie.

7.2. **Dane niezidentyfikowane**

Organizacja identyfikuje przypadki, w których przetwarza lub może przetwarzać dane niezidentyfikowane, i utrzymuje mechanizmy ułatwiające realizację praw osób, których dotyczą dane niezidentyfikowane.

7.3. **Współadministrowanie**

Organizacja identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przyjętymi zasadami.

8. REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH

8.1. RCPD 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.

8.2. Organizacja prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe. Rejestr jest jednym z podstawowych narzędzi umożliwiających rozliczanie większości obowiązków ochrony danych.

8.3. W Rejestrze dla każdej czynności przetwarzania danych, którą uznano za odrębną dla potrzeb Rejestru, Organizacja odnotowuje:

a) nazwę czynności,

b) cel przetwarzania,

c) opis kategorii osób,

d) opis kategorii danych,

e) podstawę prawną przetwarzania,

f) sposób zbierania danych,

g) opis kategorii odbiorców danych (w tym przetwarzających),

h) informację o przekazaniu poza EU/EOG,

i) ogólny opis technicznych i organizacyjnych środków ochrony danych.

8.4. Wzór Rejestru stanowi Załącznik do Polityki – „Wzór Rejestru Czynności Przetwarzania Danych". Wzór Rejestru zawiera także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych Organizacja rejestruje informacje w miarę potrzeb i możliwości, z uwzględnieniem tego, że pełniejsza treść Rejestru ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej.

9. PODSTAWY PRZETWARZANIA

9.1. Organizacja dokumentuje w Rejestrze podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.

9.2. Wskazując w dokumentach ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne / władza publiczna, prawnie uzasadniony interes), Organizacja dookreśla podstawę w precyzyjny i czytelny sposób, gdy jest to potrzebne.

9.3. Organizacja wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (e -mail, telefon, SMS itp.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).

10. SPOSÓB OBSŁUGI PRAW JEDNOSTKI I OBOWIĄZKÓW INFORMACYJNYCH

10.1. Organizacja dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane przetwarza.

10.2. Organizacja ułatwia osobom korzystanie z ich praw poprzez różne działania, w tym: zamieszczenie na stronie internetowej informacji lub odwołań (linków) do informacji o prawach osób, sposobie skorzystania z nich w Organizacji, w tym wymaganiach dotyczących identyfikacji oraz metodach kontaktu z Organizacją w tym celu.

10.3. Organizacja dba o dotrzymywanie prawnych terminów realizacji obowiązków względem osób.

10.4. Organizacja wprowadza adekwatne metody identyfikacji i uwierzytelniania osób dla potrzeb realizacji praw jednostki i obowiązków informacyjnych.

10.5. W celu realizacji praw jednostki Organizacja zapewnia mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Organizację, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany,

10.6. Organizacja dokumentuje obsługę obowiązków informacyjnych, zawiadomień i żądań osób.

11. OBOWIĄZKI INFORMACYJNE

11.1. Organizacja określa zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych.

11.2. Organizacja informuje osobę o przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby.

11.3. Organizacja informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby.

11.4. Organizacja informuje osobę o przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej.

11.5. Organizacja określa sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, tam, gdzie to jest możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).

11.6. Organizacja informuje osobę o planowanej zmianie celu przetwarzania danych.

11.7. Organizacja informuje osobę przed uchyleniem ograniczenia przetwarzania.

11.8. Organizacja informuje odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych (chyba że będzie to wymagało niewspółmiernie dużego wysiłku lub będzie niemożliwe).

11.9. Organizacja informuje osobę o prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.

11.10. Organizacja bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

12. ŻĄDANIA OSÓB

12.1. **Prawa osób trzecich.**

Realizując prawa osób, których dane dotyczą, Organizacja 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), Organizacja może się zwrócić do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

12.2. **Nieprzetwarzanie.**

Organizacja informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.

12.3. **Odmowa.**

Organizacja informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.

12.4. **Dostęp do danych**.

Na żądanie osoby dotyczące dostępu do jej danych Organizacja informuje osobę, czy przetwarza jej dane, oraz informuje osobę o szczegółach przetwarzania, zgodnie z art..15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych.

12.5. **Kopie danych.**

Na żądanie Organizacja wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Organizacja może wprowadzić i utrzymywać cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie danych. Cena kopii danych skalkulowana będzie na podstawie oszacowanego jednostkowego kosztu obsługi żądania wydania kopii danych.

12.6. **Sprostowanie danych**.

Organizacja dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Organizacja ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Organizacja informuje osobę o odbiorcach danych, na żądanie tej osoby.

12.7. **Uzupełnienie danych.** Organizacja uzupełnia i aktualizuje dane na żądanie osoby. Organizacja ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Organizacja nie musi przetwarzać danych, które są Organizacji zbędne). Organizacja może polegać na oświadczeniu osoby co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Organizację procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

12.8. **Usunięcie danych**. Na żądanie osoby Organizacja usuwa dane, gdy:

a) dane nie są niezbędne do celów, w których zostały zebrane, ani przetwarzane w innych zgodnych z prawem celach,

b) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,

c) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,

d) dane były przetwarzane niezgodnie z prawem,

e) konieczność usunięcia wynika z obowiązku prawnego,

f) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. profil dziecka na portalu społecznościowym, udział w konkursie na stronie internetowej).

Organizacja określa sposób obsługi prawa do usunięcia danych w taki sposób, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art..17. ust..3 RODO. Jeżeli dane podlegające usunięciu zostały upublicznione przez Organizację, Organizacja podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe o potrzebie usunięcia danych i dostępu do nich. W przypadku usunięcia danych Organizacja informuje osobę o odbiorcach danych, na żądanie tej osoby.

12.9. **Ograniczenie przetwarzania.**

Organizacja dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

a) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,

b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,

c) Organizacja nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,

d) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Organizacji zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

W trakcie ograniczenia przetwarzania Organizacja 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. Organizacja informuje osobę przed uchyleniem ograniczenia przetwarzania. W przypadku ograniczenia przetwarzania danych Organizacja informuje osobę o odbiorcach danych, na żądanie tej osoby.

12.10. **Przenoszenie danych.**

Na żądanie osoby Organizacja 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

Organizacji, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej w systemach informatycznych Organizacji.

12.11. **Sprzeciw w szczególnej sytuacji.**

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

12.12. **Sprzeciw względem marketingu bezpośredniego.**

Jeżeli osoba zgłosi sprzeciw względem przetwarzania jej danych przez Organizację na potrzeby marketingu bezpośredniego Organizacja uwzględni sprzeciw i zaprzestanie takiego przetwarzania.

13. MINIMALIZACJA

Organizacja dba o minimalizację przetwarzania danych pod kątem:

a) adekwatności danych do celów (ilości danych i zakresu przetwarzania),

b) dostępu do danych,

c) czasu przechowywania danych.

13.1. Minimalizacja zakresu

Organizacja zweryfikowała zakres pozyskiwanych danych, zakres ich przetwarzania i ilość przetwarzanych danych pod kątem adekwatności do celów przetwarzania w ramach wdrożenia RODO. Organizacja dokonuje okresowego przeglądu ilości przetwarzanych danych i zakresu ich przetwarzania nie rzadziej niż raz na rok. Organizacja przeprowadza weryfikację zmian co do ilości i zakresu przetwarzania danych w ramach procedur zarządzania zmianą (privacy by design).

13.2. Minimalizacja dostępu

Organizacja stosuje ograniczenia dostępu do danych osobowych: prawne (zobowiązania do poufności, zakresy upoważnień), fizyczne (strefy dostępu, zamykanie pomieszczeń) i logiczne (ograniczenia uprawnień do systemów przetwarzających dane osobowe i zasobów sieciowych, w których rezydują dane osobowe). Organizacja stosuje kontrolę dostępu fizycznego. Organizacja dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób oraz zmianach podmiotów przetwarzających. Organizacja dokonuje okresowego przeglądu ustanowionych użytkowników systemów i aktualizuje ich nie rzadziej niż raz na rok. Szczegółowe zasady kontroli dostępu fizycznego i logicznego

zawarte są w procedurach bezpieczeństwa fizycznego i bezpieczeństwa informacji Organizacji.

13.3. **Minimalizacja czasu**

Organizacja wdraża mechanizmy kontroli cyklu życia danych osobowych w Organizacji, w tym weryfikacji dalszej przydatności danych względem terminów i punktów kontrolnych wskazanych w Rejestrze. Dane, których zakres przydatności ulega ograniczeniu wraz z upływem czasu, są usuwane z systemów informatycznych Organizacji, jak też z akt podręcznych i głównych. Dane takie mogą być archiwizowane oraz znajdować się na kopiach zapasowych systemów i informacji przetwarzanych przez Organizację. Procedury archiwizacji i korzystania z archiwów, tworzenia i wykorzystania kopii zapasowych uwzględniają wymagania kontroli nad cyklem życia danych, a w tym wymogi usuwania danych.

14. BEZPIECZEŃSTWO

Organizacja zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych przez Organizację.

14.1. **Analizy ryzyka i adekwatności środków bezpieczeństwa**

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

14.1.1. Organizacja zapewnia odpowiedni stan wiedzy o bezpieczeństwie informacji, cyberbezpieczeństwie i ciągłości działania – wewnętrznie lub ze wsparciem podmiotów wyspecjalizowanych.

14.1.2. Organizacja kategoryzuje dane oraz czynności przetwarzania pod kątem ryzyka, które przedstawiają.

14.1.3. Organizacja przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii. Organizacja analizuje możliwe sytuacje i scenariusze naruszenia ochrony danych osobowych, uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o rożnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

14.1.4. Organizacja ustala możliwe do zastosowania organizacyjne i techniczne środki bezpieczeństwa i ocenia koszt ich wdrażania. W tym Organizacja ustala przydatność i stosuje 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.

14.2. **Oceny skutków dla ochrony danych**

Organizacja dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie. Organizacja stosuje metodykę oceny skutków przyjętą w Organizacji.

14.3. **Środki bezpieczeństwa**

Organizacja stosuje środki bezpieczeństwa ustalone w ramach analiz ryzyka i adekwatności środków bezpieczeństwa oraz ocen skutków dla ochrony danych. Środki bezpieczeństwa danych osobowych stanowią element środków bezpieczeństwa informacji i zapewnienia cyberbezpieczeństwa w Organizacji i są bliżej opisane w procedurach przyjętych przez Organizację dla tych obszarów.

14.4. **Zgłaszanie naruszeń**

Organizacja stosuje zoptymalizowane zasady pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych w terminie 72 godzin od ustalenia naruszenia.

15. PRZETWARZAJĄCY

Organizacja stosuje zasady doboru i weryfikacji podmiotów przetwarzających dane na rzecz Organizacji opracowane w celu zapewnienia, aby podmioty przetwarzające dawały wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw jednostki i innych obowiązków ochrony danych spoczywających na Organizacji. Organizacja przyjęła minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiące załącznik do Polityki – „Wzór umowy powierzenia przetwarzania danych".

Organizacja rozlicza podmioty przetwarzające z wykorzystania podprzetwarzających, jak też z innych wymagań wynikających z Zasad powierzenia danych osobowych.

16. EKSPORT DANYCH

Organizacja rejestruje w Rejestrze przypadki eksportu danych, czyli przekazywania danych poza Europejski Obszar Gospodarczy (EOG w 2017 r. = Unia Europejska, Islandia, Liechtenstein i Norwegia). Aby uniknąć sytuacji nieautoryzowanego eksportu danych w szczególności w związku z wykorzystaniem publicznie dostępnych usług chmurowych (shadow IT), Organizacja okresowo weryfikuje zachowania użytkowników oraz w miarę możliwości udostępnia zgodne z prawem ochrony danych rozwiązania równoważne.

17. PROJEKTOWANIE PRYWATNOŚCI

Organizacja 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 Organizację 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.

BURMISTRZ

mgr Jan Leszek Wiącek

Załącznik do Zarządzenia Nr OR.120.32.2018

Burmistrza Wołczyna z dnia 24 maja 2018 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

Wstęp

1. Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwaną dalej „Instrukcją" stanowi element Polityki ochrony danych osobowych w Organizacji i zostaje wprowadzona w oparciu o wymogi bezpieczeństwa informacji wynikające z 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 – RODO).
2. Instrukcja zarządzania systemem informatycznym jest dokumentem regulującym zasady oraz procedury zarządzania i administrowania systemem informatycznym Organizacji w zakresie przetwarzania danych osobowych.
3. Zawarte w Instrukcji procedury i wytyczne są przekazywane osobom odpowiedzialnym za ich realizację stosownie do przyznanych uprawnień i zakresu obowiązków.

I. Procedura nadawania, zmiany i cofania uprawnień do przetwarzania danych osobowych w systemach informatycznych

1. Do przetwarzania danych osobowych w systemach informatycznych na terenie Organizacji dopuszczone są jedynie te osoby, które posiadają ważne upoważnienia do przetwarzania danych w poszczególnych zbiorach danych nadane przez Administratora Danych Osobowych (ADO). Dodatkowym wymogiem jest posiadanie uprawnień do przetwarzania takich danych przy użyciu systemów informatycznych. Osobą upoważnioną do nadawania uprawnień w systemach informatycznych jest Administrator Systemów Informatycznych (ASI).
2. Przełożony osoby jest odpowiedzialny za dopuszczanie podwładnych do przetwarzania danych osobowych, dlatego jest zobowiązany do złożenia wniosku do ASI o nadanie odpowiednich uprawnień do przetwarzania danych osobowych w określonych we wniosku systemach informatycznych. Podstawą złożenia takiego wniosku jest ważne upoważnienie do nadania takich uprawnień. Uprawnień nie można nadawać na okres dłuższy niż obowiązuje odpowiednie upoważnienie.
3. W przypadku konieczności cofnięcia uprawnień, bezpośredni przełożony występuje z odpowiednim wnioskiem do ASI.

4. W przypadku konieczności zmiany uprawnień bezpośredni przełożony przedstawia jeden wniosek o cofnięcie uprawnień oraz drugi wniosek o nadanie uprawnień do innych zbiorów lub systemów informatycznych.

5. Wnioski, o których mowa wyżej składa się do ASI gdzie prowadzony jest rejestr uprawnień.

6. Bezpośredni przełożony jest zobowiązany do natychmiastowego przedstawiania wniosków dotyczących nadania lub cofnięcia uprawnień w przypadku przyjmowania obowiązków lub zdawania obowiązków przez podwładnego.

7. ASI jest odpowiedzialny za nadawanie i cofanie uprawnień niezwłocznie po otrzymaniu odpowiedniego wniosku co odnotowuje na wniosku oraz w rejestrze uprawnień.

8. Wzór uprawnienia, rejestr uprawnień oraz wnioski o nadanie i cofnięcie uprawnień są załącznikami do niniejszej procedury.

II. Stosowane metody i środki uwierzytelnienia oraz procedura związana z ich zarządzaniem i użytkowaniem

1. System informatyczny przetwarzający dane osobowe posiada mechanizm uwierzytelniający użytkownika, wykorzystujący identyfikator i hasło. System ten posiada zaimplementowane mechanizmy pozwalające na:

   a) ustawienie hasła tymczasowego,

   b) wymuszanie okresowej zmiany hasła.

   c) kontrole jakości hasła.

   d) sprawdzanie, czy wprowadzone hasło różni się od pięciu ostatnio stosowanych.

2. Dostęp do systemu informatycznego jest możliwy wyłącznie po podaniu identyfikatora i właściwego hasła. Po rozwiązaniu umowy o pracę lub odwołaniu z pełnionej funkcji identyfikator może być przydzielony tej samej osobie w przypadku jej ponownego zatrudnienia, nie można natomiast przydzielać wolnego identyfikatora innej osobie o takim samym imieniu i nazwisku.

3. Hasło używane do dostępu do systemu informatycznego przetwarzającego dane osobowe powinno spełniać warunki ustalone przez Administratora danych, czyli takie warunki jak;

   a) Powinno składać się z unikalnego zestawu co najmniej ośmiu znaków.

   b) Powinno zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.

   c) Hasło nie może być identyczne z identyfikatorem użytkownika.

4. Zabrania się użytkownikom systemu udostępniania swojego identyfikatora i hasła innym osobom oraz korzystania przez osoby upoważnione do przetwarzania danych osobowych z identyfikatora lub hasła innego użytkownika.

5. Użytkownik jest zobowiązany do:

   a) Nie ujawniania hasła innym osobom (w przypadku podejrzenia, że hasło mogło zostać ujawnione użytkownik jest zobowiązany niezwłocznie zmienić hasło)

   b) Zachowania hasła w tajemnicy również po wygaśnięciu jego ważności.

   c) Nie przechowywaniu wcześniej zapisanego hasła w miejscu łatwo dostępnym

6. Dla identyfikatorów krytycznych dla działania danego systemu, hasło jest składowane w zaklejonej kopercie w metalowej szafie zamykanej na zamek. Tak składowane hasło może być wykorzystywane w sytuacjach kryzysowych wyłącznie przez Administratora danych lub osobę przez niego wyznaczoną.

7. Niedopuszczalne jest podglądanie haseł wprowadzanych do systemu przez innych użytkowników.

8. Hasło użytkownika jest składowane w systemie przetwarzania w bezpieczny sposób, nie jest pokazywane na ekranie lub wydrukach w postaci otwartego tekstu oraz nie może być przesyłane przez sieć otwartym tekstem.

III. Tryb pracy na poszczególnych stacjach roboczych

1. Pracownicy w ramach zakresów obowiązków mają określone miejsce i czas pracy.

2. W pomieszczeniach, w którym przetwarzane są dane osobowe osoby nieuprawnione nie powinny przebywać bez nadzoru osoby posiadające odpowiednie upoważnienia.

3. W pomieszczeniach tych ekrany monitorów komputerowych powinny być ustawione w sposób uniemożliwiający osobom nieuprawnionym odczyt danych. Przed osobami nieuprawnionymi należy chronić również wydruki leżące na biurkach i w otwartych szafkach.

4. Rozpoczęcie pracy w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła.

5. System informatyczny przetwarzający dane osobowe posiada mechanizmy pozwalające na określenie uprawnień użytkownika do korzystania z przetwarzanych informacji. Uprawnienia, o którym mowa mogą w szczególności obejmować:

   a) prawo do odczytu danych,

   b) prawo do modyfikacji istniejących danych,

   c) prawo do usuwania danych.

6. Zakres uprawnienia pracownika może być uzależniony od specyfiki systemu informatycznego lub aplikacji, w którym przetwarzane są dane osobowe.

7. Każdy dostęp użytkownika do zasobów informacyjnych przetwarzanych w systemie informatycznym jest poprzedzony weryfikacją uprawnień użytkownika. System informatyczny posiada mechanizm pozwalający na odebranie użytkownikowi wszystkich uprawnień do przetwarzanych zasobów informacyjnych

8. Przed opuszczeniem pokoju należy zniszczyć w sposób uniemożliwiający ich odczytanie lub schować do zamykanych na klucz szaf wszelkie wykonane wydruki zawierające dane osobowe oraz zamknąć okna.

9. Opuszczając pokój, należy zamknąć drzwi na klucz. W przypadku pokoi w których pracuje dwie lub więcej osób, czynności, o których mowa wykonuje pracownik opuszczający w danym dniu pokój jako ostatni.

10. Zabrania się użytkownikom pracującym w systemie informatycznym przetwarzającym dane osobowe:

    a) udostępniania stacji roboczej osobom nieupoważnionym,

    b) udostępniana stacji roboczej do konserwacji lub naprawy bez porozumienia z Administratorem Systemów Informatycznych bądź bezpośrednim przełożonym,

    c) używania nielicencjonowanego oprogramowania komputerowego.

IV. Tryb pracy na komputerach przenośnych, na których przetwarzane są dane osobowe

1. Przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują procedury określone w Polityce ochrony danych oraz Instrukcji, dotyczące pracy na stacjach roboczych.

2. Praca na komputerze przenośnym możliwa jest po wprowadzeniu hasła i indywidualnego identyfikatora użytkownika. Jeżeli system operacyjny nie wymusza okresowej zmiany hasła użytkownicy są zobowiązani zmieniać hasła w komputerach przenośnych zgodnie z wytycznymi Administratora Systemów Informatycznych .

3. Pliki zawierające dane osobowe przechowywane na komputerach przenośnych powinny być zaszyfrowane lub zabezpieczone hasłem przed otwarciem

4. Pracownicy przetwarzający dane osobowe na powierzonych komputerach przenośnych obowiązani są do przechowywania tych danych nie dłużej niż jest to wymagane, a następnie do trwałego usuwania ich z pamięci komputerów przenośnych.

5. Obowiązuje zakaz samodzielnej modernizacji oprogramowania i sprzętu w powierzonych komputerach przenośnych. Wszelkie zmiany mogą być dokonywane tylko pod nadzorem Administratora Systemów Informatycznych, stosownie do wymagań

niniejszej Instrukcji. W razie wystąpienia usterek w pracy komputerów przenośnych lub w razie wystąpienia konieczności aktualizacji ich oprogramowania należy zgłosić to Administratorowi Systemów Informatycznych.

6. Komputery powinny być wyposażone w odpowiednie programy ochrony antywirusowej, których aktualizację sugeruje automatycznie system.

V. Procedury tworzenia kopii zapasowych zbiorów danych osobowych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Dane osobowe przetwarzane w systemie informatycznym podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Całe zbiory mogą być kopiowane tylko przez Administratora Systemów Informatycznych, osoby przez niego wyznaczonej lub automatycznie przez system, z zachowaniem procedur ochrony danych osobowych. W systemie informatycznym wykorzystującym technologie klient — serwer kopie zapasowe wykonuje się po stronie serwera. Obowiązuje zakaz przesyłania i wynoszenia poza obszar Organizacji, na jakichkolwiek nośnikach danych, całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej, za wyjątkiem wykonywania kopii bezpieczeństwa oraz prac konserwacyjnych/wdrożeniowych związanych z migracją danych pomiędzy systemami informatycznymi przy udziale podmiotu trzeciego na warunkach określonych w umowie powierzenia przetwarzania danych osobowych.

2. Za proces tworzenia kopii zapasowych odpowiada Administrator Systemów Informatycznych, który w szczególności określa;

   a) techniczny sposób tworzenia kopii zapasowych, w szczególności sprzęt, oprogramowanie i nośniki, których wykorzystanie uzasadnione jest możliwością współpracy z istniejącą w Organizacji infrastrukturą informatyczną oraz wielkością danych osobowych, które podlegają zabezpieczeniu poprzez utworzenie kopii zapasowych,

   b) rodzaj kopii zapasowych (pełne, przyrostowe, różnicowe)

3. Oprócz Administratora Systemów Informatycznych dostęp do kopii zapasowych zapisanych na nośnikach magnetycznych ma Administrator Danych Osobowych oraz osoby przez niego uprawnione.

4. Administrator Systemów Informatycznych jest odpowiedzialny za wykonywanie ustaleń w zakresie:

   a) grafiku tworzenia kopii zapasowych,

   b) procesu tworzenia kopii zapasowych,

   c) procesu weryfikacji poprawności utworzenia kopii zapasowych,

d) okresowego — z częstotliwością uzależnioną od czasu przechowywania kopii zapasowych — testowania możliwości odtworzenia danych z kopii zapasowych,

e) zabezpieczenia dostaw nośników wykorzystywanych do tworzenia kopii zapasowych,

f) koordynacji procesu odtwarzania danych w razie wystąpienia awarii.

5. Grafik tworzenia kopii zapasowych uwzględnia nazwę zbioru, częstotliwości tworzenia kopii zapasowych, informację o nośniku, na którym kopia ma być wykonana oraz imię, nazwisko i stanowisko pracownika, który jest odpowiedzialny za sporządzenie kopii zapasowej. Grafik zatwierdza Administrator danych. Administrator Systemów Informatycznych jest odpowiedzialny za jego realizację.

6. Pomieszczenie, w którym przechowywane są kopie zapasowe, jest zabezpieczone przed;

a) dostępem osób nieupoważnionych,

b) niewłaściwymi warunkami klimatycznymi (temperatura, wilgotność),

c) promieniowaniem elektromagnetycznym.

7. Administrator Systemów Informatycznych jest odpowiedzialny za tworzenie dokumentacji dotyczącej zarządzania kopiami zapasowymi, która powinna obejmować:

a) rodzaj kopii zapasowej,

b) zakres danych kopii zapasowej,

c) rodzaj i numer nośnika kopii zapasowej,

d) miejsce składowania kopii zapasowej,

e) datę wykonania kopii zapasowej,

f) imię i nazwisko osoby potwierdzającej wykonanie kopii zapasowej,

g) datę testu możliwości odtworzenia danych z wykorzystaniem kopii zapasowej,

h) imię i nazwisko osoby wykonującej test możliwości odtworzenia danych z kopii zapasowej,

i) datę odtwarzania danych po wystąpieniu naruszenia systemu ochrony danych osobowych,

j) imię i nazwisko osoby wykonującej odtwarzanie danych z kopii zapasowej po wystąpieniu naruszenia systemu ochrony danych osobowych,

k) datę likwidacji nośnika kopii zapasowej,

l) imię i nazwisko osoby potwierdzającej likwidację kopii zapasowej.

8. Administrator Systemów Informatycznych jest odpowiedzialny za prowadzenie dziennika wykonanych kopii zapasowych. Zapisy w dzienniku uwzględniają numery

ewidencyjne nośników. Są one zapisywane w postaci D/T - gdzie: D oznacza dzień utworzenia kopii zapasowej, T— typ kopii zapasowej (pełny, przyrostowy, różnicowy),

9. Administrator Systemów Informatycznych jest odpowiedzialny za przeprowadzanie testów możliwości odtworzenia danych z kopii zapasowych. Testy odtworzeniowe wybranych systemów informatycznych przeprowadzane są nie rzadziej niż raz na dwanaście miesięcy i obejmują sprawdzanie możliwości odtworzenia przechowywanych danych osobowych. Fakt przeprowadzenia testów ASI odnotowuje w dzienniku wykonywanych kopii zapasowych.

10. Negatywne wyniki testu lub zaistnienie problemów w trakcie odtwarzania danych może stanowić podstawę do zmiany sposobu tworzenia kopii zapasowych w Organizacji lub zmiany technologii wykorzystywanej do tworzenia kopii zapasowych (urządzenia, nośniki)

VI. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii programów i narzędzi programowych służących do ich przetwarzania

1. Zbiory danych przechowywane są na dyskach serwerów Organizacji oraz nośnikach danych. Jeżeli zachodzi taka potrzeba to dane przetwarzane w pamięci poszczególnych stacji roboczych lub komputerów przenośnych są umieszczane przez użytkowników w odpowiednich miejscach na serwerze, przydzielonych wybranemu użytkownikowi przez Administratora Systemów Informatycznych.

2. ASI prowadzi w systemie elektronicznym ewidencję nośników przenośnych używanych do zapisu danych osobowych z uwzględnieniem:

   a) numeru ewidencyjnego nośnika,

   b) rodzaju informacji zapisanych na nośniku oraz celu, w jakim dane te zostały zapisane,

   c) imię i nazwisko osoby, na wniosek której zapisano dane na nośniku,

   d) daty pierwotnego zapisania danych na nośniku,

   e) miejsca przechowywania nośnika,

   f) adnotacji o numerze ewidencyjnym umowy powierzenia przetwarzania danych osobowych w przypadku przekazania nośnika poza teren Organizacji,

   g) daty likwidacji nośnika lub usunięcia zapisanych na nim danych,

   h) imię i nazwisko osoby, która dokonała likwidacji nośnika lub usunięcia danych z nośnika,

3. Nośniki przenośne (takie jak dyski zewnętrzne, płyty CD/DVD itp.), na których przechowywane są dane osobowe podlegają ścisłej ewidencji i kontroli. Każdy nośnik posiada numer ewidencyjny, w postaci: DO – XXX – YYY / ZZZZ, gdzie XXX – oznacza nazwę komórki organizacyjnej, w której zapisano dane na nośniku, YYY — oznacza kolejny numer nośnika, ZZZZ — rok.

4. Nośnik przenośny może być wykorzystany do przenoszenia danych osobowych pod warunkiem zabezpieczenia go przed kradzieżą lub utratą. Nośnik może być przekazywany tylko pomiędzy osobami upoważnionymi do przetwarzania danych osobowych

5. Wydruki z danymi osobowymi oznaczane są numerami ewidencyjnymi w postaci:

   DO – W – XXX – YYY / ZZZZ, gdzie: XXX — oznacza nazwę komórki organizacyjnej, w której stworzono wydruk, YYY — kolejny numer wydruku, wykonany w danej komórce organizacyjnej, YYYY – rok.

6. Administrator Systemów Informatycznych prowadzi w systemie elektronicznym ewidencję wydruków danych osobowych (chodzi o wydruki z danymi osobowymi całych baz danych) ze szczególnym uwzględnieniem faktu przekazania wydruku poza teren Organizacji. Ewidencja, o której mowa, powinna obejmować:

   a) numer ewidencyjny wydruku,

   b) rodzaj informacji na wydruku,

   c) imię i nazwisko lub identyfikator osoby, która sporządziła wydruk,

   d) datę sporządzenia wydruku,

   e) cel, w jakim wydruk został sporządzony,

   f) miejsce przechowywania wydruku,

   g) adnotację o przekazaniu wydruku poza teren Organizacji lub zniszczenia wydruku.

7. Nośniki danych osobowych oraz wydruki powinny być przechowywane w zamkniętych szafkach wewnątrz obszaru przeznaczonego do przetwarzania danych osobowych i nie powinny być bez uzasadnionej potrzeby wynoszone poza ten obszar. Przekazywanie nośników danych osobowych i wydruków poza teren Organizacji może odbywać się zgodnie z postanowieniami niniejszej Instrukcji, Polityki ochrony danych oraz powszechnie obowiązującymi przepisami prawa.

8. Kopie zapasowe przechowywane są na terenie Organizacji w szafie zamykanej na klucz zlokalizowanej w pomieszczeniu ASI lub innym , określonym przez Administratora danych (stanowiącym obszar przetwarzania danych osobowych, określony w Polityce ochrony danych).

9. Dane osobowe na nośnikach lub wydrukach, należy przechowywać nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania, a następnie usunąć. Dane znajdujące się na nośnikach wielokrotnego zapisu należy usunąć zgodnie z zapisem w rozdz. IX pkt. 8

niniejszej Instrukcji. Nośniki jednokrotnego zapisu z danymi osobowymi należy niszczyć zgodnie z obowiązującymi w Organizacji przepisami dotyczącymi gospodarki środkami trwałymi oraz wartościami niematerialnymi i prawnymi. Trwałe zniszczenie danych zapisanych na nośnikach lub wydrukach może także odbywać się na polecenie osoby, na której wniosek dane zapisano lub na polecenie Administratora danych oraz osób przez niego wyznaczonych.

VII. Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu

1. System informatyczny Organizacji chroniony jest przed działaniem wirusów komputerowych oprogramowaniem antywirusowym aktualizowanym na bieżąco. Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się przy wykorzystaniu oprogramowania zainstalowanego na serwerach, stacjach roboczych oraz komputerach przenośnych. Oprogramowanie to sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.

2. W celu zapewnienia ochrony antywirusowej Administrator Systemów Informatycznych jest odpowiedzialny za zarządzanie systemem wykrywającym i usuwającym wirusy oraz inne niebezpieczne kody. System antywirusowy powinien być skonfigurowany w następujący sposób:

a) skanowanie dysków twardych stacji roboczych zawierających potencjalnie niebezpieczne kody — nie rzadziej niż raz na miesiąc,

b) skanowanie informacji przesyłanych do systemu informatycznego pod kątem pojawienia się niebezpiecznych kodów — na bieżąco.

3. Administrator Systemów Informatycznych jest odpowiedzialny za.

a) instalację i konfigurację systemu antywirusowego na wszystkich elementach systemu informatycznego przetwarzającego dane osobowe,

b) nadzór nad uaktualnianiem bazy wirusów systemu antywirusowego,

c) reagowanie na fakt wykrycia wirusa poprzez: określenie źródła infekcji; usunięcie wirusa, o ile nie zostało automatycznie wykonane przez system antywirusowy; podjęcie kroków minimalizujących ryzyko rozprzestrzeniania się wirusa; podjęcie działań zmierzających do zapobieżenia tego rodzaju wypadkom w przyszłości,

d) zarządzanie systemem antywirusowym, w tym określenie warunków działania systemu, aby zapewnić jego maksymalną efektywność przy jednoczesnej możliwie największej minimalizacji negatywnego wpływu działania systemu antywirusowego na korzystanie przez użytkowników z systemu informatycznego Organizacji.

4. Systemy antywirusowe zainstalowane na stacjach roboczych powinny być skonfigurowane w następujący sposób:

   a) zablokowane możliwości ingerencji użytkownika w ustawienia oprogramowania antywirusowego,

   b) możliwość centralnego uaktualniania bazy wirusów,

   c) możliwość centralnego zbierania informacji o wynikach pracy oprogramowania,

   d) możliwość centralnej konfiguracji oprogramowania.

5. W przypadku wystąpienia infekcji i braku możliwości automatycznego usuwania wirusów przez system antywirusowy, ASI powinien podjąć działania zmierzające do usunięcia zagrożenia. Działania te w szczególności powinny obejmować:

   a) usunięcie zainfekowanych plików, o ile jest to akceptowane ze względu na prawidłowe funkcjonowanie systemu informatycznego,

   b) odtworzenie plików z kopii zapasowych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane,

   c) odłączenie stacji roboczej od sieci komputerowej Organizacji do czasu usunięcia zagrożenia.

6. Pracownikom Organizacji zabrania się otwierania załączników do wiadomości przesłanych pocztą elektroniczną niewiadomego pochodzenia (zwłaszcza napisanych w obcym języku), gdyż mogą one stanowić źródło infekcji wirusem komputerowym.

VIII. Sposób realizacji wymogów dotyczących funkcjonalności oprogramowania zgodnych z RODO

1. Wymogi te związane są głównie z realizacją praw osób, których dane dotyczą oraz obowiązków Administratora danych. Systemy informatyczne, w których przetwarzane są dane osobowe muszą umożliwiać m.in.;

   a) ograniczenie okresu przetwarzania danych do zgodnego z celem ich przetwarzania (ograniczenie przechowywania) (art. 5 ust. 1 lit. e)

   b) wycofanie zgody, na podstawie której przetwarzane są dane (art. 7 ust. 3)

   c) realizację prawa dostępu osobie, której dane dotyczą (art. 15 Ust. 3)

   d) realizację prawa do sprostowania danych (art. 16)

   e) realizację prawa do bycia zapomnianym (art. 17)

   f) realizację prawa do ograniczenia przetwarzania (art. 18)

   g) realizację prawa do przenoszenia danych (art. 20)

h) realizację prawa do sprzeciwu (art. 21)

i) realizację prawa do niepodlegania zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu (art. 22)

j) realizację decyzji organu nadzorczego o czasowym lub całkowitym ograniczeniu przetwarzania, w tym zakazu przetwarzania (art. 58 ust. 2 lit. f)

2. Aktualne funkcjonalności systemów informatycznych stosowanych w Organizacji nie obejmują odnotowywań powyższych wymogów. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym aktualne systemy zapewniają odnotowanie:

   a) daty pierwszego wprowadzenia danych do systemu,

   b) identyfikatora pracownika wprowadzającego dane osobowe do systemu,

   c) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą,

   d) informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia,

   e) sprzeciwu,

3. System informatyczny Administratora danych umożliwia również automatycznie sporządzenie i wydrukowanie dla każdej osoby, której dane są przetwarzane w systemie, raportu zawierającego informacje, o których mowa w punkcie 2.

IX. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

1. Zabronione jest samodzielne naprawianie sprzętu komputerowego przez użytkowników jak również samowolne instalowanie oprogramowania przez użytkowników.

2. Wszelkie prace związane z przeglądami, naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego wysokiego poziomu bezpieczeństwa tych danych.

3. Nadzór nad przeglądem i konserwacją systemu sprawuje Administrator Systemów Informatycznych.

4. Prace serwisowe mogą być wykonywane przez ASI. Prace serwisowe mogą być również wykonywane przez firmy, z którymi została podpisana stosowna umowa normująca w szczególności zasady ochrony danych osobowych.

5. Osobą upoważnioną do zgłaszania firmie serwisowej usterki systemu i konieczności jego naprawy oraz nadzoru nad wykonywanymi pracami jest ASI lub też inni pracownicy Organizacji wyznaczeni przez Administratora danych.

6. W sytuacji gdy naprawa dotyczy komponentu, na którym nie są przechowywane dane osobowe i który nie jest podłączony do systemu informatycznego wówczas nie jest wymagany nadzór nad przebiegiem prac serwisowych.

7. W przypadku konieczności przeprowadzania prac serwisowych poza siedzibą Organizacji dane z naprawianego urządzenia muszą zostać usunięte. Od powyższego możliwe jest odstępstwo, jeżeli urządzenie, podczas przechowywania poza siedzibą Organizacji, będzie pod stałym nadzorem ASI lub też wyznaczonego przez Administratora danych innego pracownika Organizacji.

8. Nośniki wielokrotnego zapisu zawierające dane osobowe przeznaczone do likwidacji uszkadza się w sposób mechaniczny uniemożliwiający odczytanie zapisanych na nich danych. Nośniki wielokrotnego zapisu zawierające dane osobowe przeznaczone do powtórnego wykorzystania pozbawia się wcześniej zapisu tych danych poprzez usunięcie wszystkich danych znajdujących się na nośniku poprzez proces formatowania nośnika lub usunięcia danych i co najmniej dwukrotnego nadpisania całej pamięci nośnika innymi danymi wykorzystując do tego celu odpowiednie oprogramowanie. Nośniki jednokrotnego zapisu oraz wydruki z danymi osobowymi przeznaczone do likwidacji należy zniszczyć przy pomocy specjalnego urządzenia (niszczarki dokumentów) w sposób uniemożliwiający ich odczytanie. Nośniki jednokrotnego lub wielokrotnego zapisu, zawierające dane osobowe, likwiduje się pod nadzorem ASI lub innej osoby wyznaczonej przez Administratora danych.

9. Zużyty sprzęt służący do przetwarzania danych osobowych może być zbywany dopiero po trwałym usunięciu danych, a urządzenia uszkodzone mogą być przekazywane w celu utylizacji właściwym podmiotom, jeśli trwałe usunięcie danych wymagałoby nadmiernych nakładów ze strony Administratora danych.

10. Przegląd programów i narzędzi programowych na stacjach roboczych przeprowadzany jest na bieżąco przez Administratora Systemów Informatycznych.

X. Przetwarzanie danych osobowych w zbiorach doraźnych

1. Dostęp do danych osobowych powinien odbywać się poprzez dedykowane aplikacje, działające w architekturze klient-serwer, lub przynajmniej, przechowujące dane na serwerach plików, nie zaś na indywidualnych stanowiskach komputerowych pracowników. Gdy zachodzi potrzeba przetwarzania danych na stacji lokalnej lub w innym formacie, np. dane do raportu w postaci pliku arkusza kalkulacyjnego, można tego dokonać w doraźnym zbiorze danych osobowych pod warunkiem, że zapisane dane będą należycie chronione, tj.

   a) uniemożliwi się dostęp do danych osobom nieuprawnionym.

   b) uniemożliwi się zmiany danych, a tym samym zafałszowanie informacji pochodzących z systemu.

c) zabezpieczy się bezpośredni dostęp do danych hasłem.

2. W przypadku podejrzenia lub stwierdzenia naruszenia systemu ochrony danych osobowych w zbiorze doraźnym należy natychmiast zawiadomić bezpośredniego przełożonego lub też Administratora Systemów Informatycznych.

3. W sprawach nieuregulowanych w niniejszym rozdziale zastosowanie mają przepisy RODO.

XI. Postanowienia końcowe

1. Uprawnienia do przetwarzania danych osobowych w systemach informatycznych wydane na podstawie dotychczas obowiązującego Zarządzenia, powinny zostać poddane weryfikacji i w razie potrzeby zostać zmienione.

2. W sprawach nieokreślonych niniejszą Instrukcją należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.

3. Niezastosowanie się do procedur określonych w Instrukcji może skutkować pociągnięciem pracownika do odpowiedzialności.

BURMISTRZ

mgr Jan Leszek Wiącek

Załącznik do Zarządzenia Nr OR.120.32.2018

Burmistrza Wołczyna z dnia 24 maja 2018 r.

PROCEDURA POSTĘPOWANIA W PRZYPADKU ZAGROŻENIA LUB NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Instrukcja definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Celem Instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:

a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,

b) niewłaściwe zabezpieczenie sprzętu i oprogramowania przed wyciekiem, kradzieżą, nieuprawnionym zaszyfrowaniem bądź utratą danych osobowych,

c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników.

2. Do typowych incydentów bezpieczeństwa danych osobowych należą:

a) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),

b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/ zagubienie danych),

c) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

3. Każdy pracownik Organizacji w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować Administratora Danych Osobowych.

4. Do czasu przybycia na miejsce zagrożenia bądź naruszenia ochrony danych osobowych Administratora Danych Osobowych lub upoważnionej przez niego osoby, osoba powiadamiająca powinna:

a) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków, a następnie ustalić przyczyny, lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe,

b) zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,

c) udokumentować wstępnie zaistniałe naruszenie,

d) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia.

5. W przypadku stwierdzenia wystąpienia zagrożenia, Administrator danych prowadzi postępowanie wyjaśniające w toku, którego:

a) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,

b) inicjuje ewentualne działania dyscyplinarne,

c) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości,

d) dokumentuje prowadzone postępowania

e) w przypadkach tego wymagających powiadamia Inspektora Ochrony Danych

6. W przypadku stwierdzenia incydentu (naruszenia), Administrator danych prowadzi postępowanie wyjaśniające w toku, którego:

a) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,

b) zabezpiecza ewentualne dowody oraz w uzasadnionych przypadkach zawiadamia organy ścigania,

c) ustala osoby odpowiedzialne za naruszenie,

d) podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),

e) inicjuje działania dyscyplinarne,

f) wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,

g) dokumentuje prowadzone postępowania,

h) w przypadkach tego wymagających powiadamia Inspektora Ochrony Danych

BURMISTRZ

mgr Jan Leszek Wiącek

Załącznik do Zarządzenia Nr OR.120.32.2018

Burmistrza Wołczyna z dnia 24 maja 2018 r.

Procedura nadawania, zmiany i cofania upoważnień do przetwarzania danych osobowych

1. Do przetwarzania danych osobowych na terenie jednostki dopuszczone są jedynie te osoby, które posiadają ważne upoważnienia do przetwarzania danych w poszczególnych zbiorach danych nadane przez Administratora Danych Osobowych (ADO).
2. Przełożony osoby, jest odpowiedzialny za dopuszczanie podwładnych do przetwarzania danych osobowych, dlatego jest zobowiązany do złożenia wniosku do ADO o nadanie odpowiednich upoważnień do przetwarzania danych osobowych w określonych we wniosku zbiorach.
3. Wniosek o nadanie upoważnień jest załącznikiem do niniejszej procedury.
4. W przypadku konieczności cofnięcia upoważnień, bezpośredni przełożony, występuje z odpowiednim wnioskiem do ADO. Wniosek jest załącznikiem do niniejszej procedury.
5. W przypadku konieczności zmiany upoważnień bezpośredni przełożony przedstawia jeden wniosek o cofnięcie upoważnień oraz drugi wniosek o nadanie upoważnień do innych zbiorów.
6. Wnioski, o których mowa wyżej składa się do Wydziału Organizacyjnego Urzędu Miejskiego w Wołczynie.
7. O akceptacji lub odmowie akceptacji wniosku decyduje ADO podpisując wniosek lub odmawiając jego podpisania przedstawiając uzasadnienie odmowy.
8. Zaakceptowany wniosek jest podstawą do przygotowania odpowiedniego upoważnienia, będącego załącznikiem do niniejszej procedury. Podpisane upoważnienie wprowadzane jest do rejestru upoważnień z adnotacją numeru z rejestru na zatwierdzonym upoważnieniu. Jeden egzemplarz upoważnienia otrzymuje osoba, której upoważnienie dotyczy, a drugi przechowywany jest wraz z rejestrem upoważnień.
9. Rejestr upoważnień wraz z upoważnieniami prowadzony jest przez Wydział Organizacyjny Urzędu Miejskiego w Wołczynie.
10. Bezpośredni przełożony jest zobowiązany do natychmiastowego przedstawiania wniosków dotyczących nadania lub cofnięcia upoważnień w przypadku przyjmowania obowiązków lub zdawania obowiązków przez podwładnego.

BURMISTRZ

mgr Jan Leszek Wiącek

....., dn. ..... r.

Administrator Danych Osobowych

w .....

Wniosek o nadanie upoważnienia do przetwarzania danych osobowych

W związku z 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 – wnoszę o nadanie upoważnień Pani/Panu:

.....
(imię i nazwisko)

.....
(stanowisko)

do przetwarzania danych osobowych w ramach pełnionych obowiązków służbowych na zajmowanym stanowisku w następujących zbiorach danych oraz w zakresie czynności przetwarzania;

Lp.	Nazwa zbioru danych osobowych	Zakres upoważnienia wgląd, wprowadzanie, modyfikowanie, udostępnianie, usuwanie
1.		
2.		
...		

Osoba uzyskująca zgodę do przetwarzania danych osobowych, będzie przetwarzała dane zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, Ustawy z dnia ..... o ochronie danych osobowych, Kodeksu pracy, a także Polityką ochrony danych osobowych Pracodawcy.

Okres ważności od: ..... do.....

Osoba wnioskująca:
.....

Zatwierdzam:

.....
Data i podpis Administratora Danych Osobowych

....., dn. ..... r.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

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)

.....

(stanowisko)

do przetwarzania danych osobowych w ramach pełnionych obowiązków służbowych na zajmowanym stanowisku w poniższych zbiorach danych oraz w zakresie czynności przetwarzania danych;

Lp.	Nazwa zbioru danych osobowych	Zakres czynności przetwarzania danych wgląd, wprowadzanie, modyfikowanie, udostępnianie, usuwanie, niszczenie
1.		
2.		
...		

Upoważniam Panią/Pana do tworzenia/posiadania dla potrzeb wykonywanej pracy zestawień, ewidencji oraz rejestrów z danymi osobowymi, z zachowaniem pełnej ich ochrony przy zastosowaniu środków technicznych i organizacyjnych wdrożonych w Urzędzie Miejskim w Wołczynie.

Jednocześnie zobowiązuję Panią/Pana do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, ustawy z dnia ..... o ochronie danych osobowych, Kodeksu pracy, a także polityką ochrony danych osobowych Pracodawcy.

Okres ważności od: ..... do: .....

.....

podpis osoby uprawnionej do nadania upoważnienia

Data wygaśnięcia* .....

Odwołano, dnia .....

.....

(podpis osoby uprawnionej do odwołania upoważnienia)

* Data rozwiązania stosunku pracy/umowy cywilnoprawnej.

Numer w rejestrze upoważnień: .....

Załącznik do Zarządzenia Nr OR.120.32.2018

Burmistrza Wołczyna z dnia 24 maja 2018 r.

Procedura nadawania, zmiany i cofania uprawnień do przetwarzania danych osobowych w systemach informatycznych

1. Do przetwarzania danych osobowych w systemach informatycznych na terenie jednostki dopuszczone są jedynie te osoby, które posiadają ważne upoważnienia do przetwarzania danych w poszczególnych zbiorach danych nadane przez Administratora Danych Osobowych (ADO). Dodatkowym wymogiem jest posiadanie uprawnień do przetwarzania takich danych przy użyciu systemów informatycznych. Osobą upoważnioną do nadawanie uprawnień w systemach informatycznych jest Administrator Systemów Informatycznych (ASI).
2. Przełożony osoby, jest odpowiedzialny za dopuszczanie podwładnych do przetwarzania danych osobowych, dlatego też jest zobowiązany do złożenia wniosku do ASI o nadanie odpowiednich uprawnień do przetwarzania danych osobowych w określonych we wniosku systemach informatycznych. Podstawą złożenia takiego wniosku jest ważne upoważnienie do nadania takich uprawnień. Uprawnień nie można nadawać na okres dłuższy niż obowiązuje odpowiednie upoważnienie.
3. Wniosek o nadanie uprawnień jest załącznikiem do niniejszej procedury.
4. W przypadku konieczności cofnięcia uprawnień, bezpośredni przełożony, występuje z odpowiednim wnioskiem do ASI. Wniosek jest załącznikiem do niniejszej procedury.
5. W przypadku konieczności zmiany uprawnień bezpośredni przełożony przedstawia jeden wniosek o cofnięcie uprawnień oraz drugi wniosek o nadanie uprawnień do innych zbiorów.
6. Wnioski, o których mowa wyżej składa się do ASI gdzie prowadzony jest rejestr uprawnień.
7. Bezpośredni przełożony jest zobowiązany do natychmiastowego przedstawiania wniosków dotyczących nadania lub cofnięcia uprawnień w przypadku przyjmowania obowiązków lub zdawania obowiązków przez podwładnego.
8. ASI jest odpowiedzialny za nadawanie i cofanie uprawnień niezwłocznie po otrzymaniu odpowiedniego wniosku, co odnotowuje na wniosku oraz w rejestrze uprawnień.

BURMISTRZ

mgr Jan Leszek Wiącek

....., dn. ..... r.

Administrator Systemów Informatycznych

w .....

Wniosek o nadanie uprawnienia do przetwarzania danych osobowych

W związku z 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 – wnoszę o nadanie uprawnień Pani/Panu:

.....

(imię i nazwisko)

.....

(stanowisko)

do przetwarzania danych osobowych w ramach pełnionych obowiązków służbowych na zajmowanym stanowisku przy użyciu poniższych systemów informatycznych, zgodnie z wcześniej nadanymi upoważnieniami:

.....

.....

Osoba uzyskująca zgodę do przetwarzania danych osobowych, będzie przetwarzała dane zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, ustawy z dnia ..... o ochronie danych osobowych, Kodeksu pracy, a także polityką ochrony danych osobowych Pracodawcy.

Okres ważności uprawnienia od: ..... do: .....

Numer w rejestrze upoważnień: .....

Numer w rejestrze uprawnień: .....

Osoba wnioskująca: .....

Zatwierdzam;

.....

Data i podpis Administratora Systemów Informatycznych

....., dn. ..... r.

UPRAWNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

W związku z 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 uprawnienie Pani/Panu:

.....
(imię i nazwisko)

.....
(stanowisko)

do przetwarzania danych osobowych w ramach pełnionych obowiązków służbowych na zajmowanym stanowisku przy użyciu poniższych systemów informatycznych, zgodnie z wcześniej nadanymi upoważnieniami:

.....

.....

Jednocześnie zobowiązuję Panią/Pana do przetwarzania danych osobowych, zgodnie z udzielonym uprawnieniem oraz z przepisami RODO, Ustawy z dnia ..... o ochronie danych osobowych, Kodeksu pracy, a także Polityką ochrony danych osobowych Pracodawcy.

Okres ważności od: ..... do: .....

.....
podpis osoby uprawnionej do nadania upoważnienia

Data wygaśnięcia* .....

Odwołano, dnia .....

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

* Data rozwiązania stosunku pracy/umowy cywilnoprawnej.

Numer w rejestrze uprawnień: .....

Załącznik do Zarządzenia Nr OR.120.32.2018
Burmistrza Wołczyna z dnia 24 maja 2018 r.

Zasady korzystania z komputerów stacjonarnych i przenośnych urządzeń przetwarzających dane osobowe

1. Przetwarzanie danych osobowych przy użyciu komputerów przenośnych odbywać się może wyłącznie na podstawie upoważnień Administratora Danych Osobowych (ADO).
2. Zabrania się przetwarzania jakichkolwiek danych osobowych, dla których administratorem, współadministratorem lub przetwarzającym jest ADO, na jakimkolwiek innym sprzęcie niż sprzęcie udostępnionym przez ADO.
3. Zasady dotyczące korzystania z komputerów, komputerów przenośnych dotyczą również tabletów i telefonów komórkowych (smartfonów).
4. Osoba użytkująca komputer, w którym przetwarzane są dane osobowe, zobowiązana jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieuprawnionych oraz przed zniszczeniem. Osoba użytkująca komputer przenośny zobowiązana jest dodatkowo do zabezpieczenia sprzętu przed kradzieżą oraz zwrócenia szczególnej uwagi na ewentualne jego zagubienie.
5. Użytkownik komputera nie może podłączać się do sieci, do której nie uzyskał zgody na podłączenie od Administratora Systemów Informatycznych (ASI).
6. Użytkownik komputera nie może instalować bez zgody ASI jakichkolwiek programów, aplikacji oraz ściągania jakichkolwiek danych z nieznanych lub nie udostępnionych przez ASI źródeł.
7. Komputer, na którym przetwarzane są dane osobowe nie może być wykorzystywany do celów prywatnych.
8. Użytkownik nie może wykorzystywać innych niż służbowe zewnętrznych nośników danych i podłączać je do sprzętu służbowego pracodawcy. Służbowe nośniki danych nie mogą być podłączane do innych niż będący w użytkowaniu pracodawcy sprzęt.
9. Przechowywanie danych osobowych na zewnętrznych nośnikach danych w innych niż archiwizowanie celach jest niedozwolone.
10. Użytkownik musi mieć zawsze włączony zainstalowany przez ASI program antywirusowy.
11. Użytkownik musi mieć zawsze zainstalowane hasło do uruchamiania systemu oraz wygaszacz ekranu wraz z zainstalowanym hasłem.
12. Użytkownik komputera przenośnego zobowiązany jest dodatkowo do:

1) pamiętania o tym, by zawsze było ustawione hasło do zalogowania się w systemie komputerowym, Użytkownik zobowiązany jest do zachowania w tajemnicy identyfikatora i hasła do komputera;
2) pamiętania o ustawieniu wygaszaczy wraz z krótkim czasem nieaktywności użytkownika;
3) transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia.
4) korzystania z komputera w sposób minimalizujący ryzyko podejrzenia przetwarzania danych osobowych przez osoby nieuprawnione, w szczególności zabrania się na korzystanie z komputera w miejscach publicznych i środkach transportu publicznego.
5) zakazu udostępniania komputera przenośnego osobom nieuprawnionym.
6) umożliwienia, poprzez podłączenie komputera przenośnego do sieci informatycznej pracodawcy, aktualizacji wzorców wirusów w oprogramowaniu antywirusowym.
7) w przypadku wykonywania obowiązków zawodowych wiążących się z pracą poza obiektami pracodawcy, bezpośredni przełożeni występują dla swoich pracowników o zgodę ADO na użytkowanie komputera przenośnego poza terenem obiektów pracodawcy.

13. Administrator Systemów Informatycznych jest odpowiedzialny za prowadzenie ewidencji komputerów przenośnych wykorzystywanych do przetwarzania danych osobowych .Ewidencja ta powinna obejmować w szczególności:

a Typ i numer seryjny komputera.

b Adres IP komputera.

c Imię i nazwisko osoby będącej użytkownikiem komputera.

d System operacyjny zainstalowany na komputerze.

e Numer upoważnienia z rejestru upoważnień do przetwarzania danych osobowych prowadzonego przez Wydział Organizacyjny Urzędu Miejskiego w Wołczynie.

14. W razie zagubienia, kradzieży lub zniszczenia komputera przenośnego użytkownik zobowiązany jest do natychmiastowego powiadomienia bezpośredniego przełożonego, który informację tę przekazuje ASI.

BURMISTRZ

mgr Jan Leszek Wiącek

Załącznik do Zarządzenia Nr OR.120.32.2018

Burmistrza Wołczyna z dnia 24 maja 2018 r.

ŚRODKI ORGANIZACYJNE I TECHNICZNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI DANYCH OSOBOWYCH

ŚRODKI ORGANIZACYJNE

1. Sporządzono i wdrożono Politykę Bezpieczeństwa.
2. Sporządzono i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
3. Wyznaczono Inspektora Ochrony Danych.
4. Do przetwarzania danych osobowych dopuszczono wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.
5. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.
6. Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.
7. Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.
8. Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy.
9. Stworzono procedurę postępowania w przypadku zagrożenia lub naruszenia ochrony danych osobowych.
10. Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych.
11. Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym.
12. Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych.
13. Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.
14. Dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonując takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści, aby po dokonaniu usunięcia danych niemożliwa była identyfikacja osób.

ŚRODKI TECHNICZNE

1. Zbiory danych osobowych przechowywane są w pomieszczeniach zabezpieczonych drzwiami zwykłymi z zamkiem bębenkowym.
2. Zbiory danych osobowych przechowywane są w pomieszczeniach, w których okna zabezpieczone są za pomocą rolet.
3. Pomieszczenia, w którym przetwarzane są zbiory danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy.
4. Pomieszczenia, w których przetwarzane są zbiory danych osobowych zabezpieczone są przed skutkami pożaru za pomocą wolnostojącej gaśnicy.
5. Zbiory danych osobowych w formie papierowej przechowywane są w zamkniętych niemetalowych szafach.
6. Zbiory danych osobowych w formie papierowej przechowywane są w zamkniętych metalowych szafach.
7. Kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są w zamkniętych niemetalowych szafach.
8. Kopie zapasowe/archiwalne zbiorów danych osobowych przechowywane są w zamkniętych metalowych szafach.
9. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.
10. Dostęp do systemu operacyjnego komputerów, w których przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.
11. Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.
12. Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
13. Użyto system Firewall do ochrony dostępu do sieci komputerowej.

BURMISTRZ

mgr Jan Leszek Wiącek