Załącznik nr 1 do zarządzenia Nr 7/2019 z dnia 30.04.2019 r.
Dyrektora Instytucji Pośredniczącej Aglomeracji Wałbrzyskiej

Polityka Bezpieczeństwa

Spis treści

I. Postanowienia ogólne

A. Definicje

Ilekroć w **niniejszym dokumencie jest mowa o :**

1. **IPAW –** należy przez to rozumieć Instytucje Pośredniczącą Aglomeracji Wałbrzyskiej;
2. **danych osobowych** – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
3. **zbiorze danych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
4. **przetwarzaniu danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, przeglądanie, ujawnianie przez przesłanie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
5. **Administratorze Danych Osobowych (dalej Administratorze Danych)** – należy przez to rozumieć Dyrektora Instytucji Pośredniczącej Aglomeracji Wałbrzyskiej;
6. **Koordynatora Działu IT –** należy przez to rozumieć pracownika IPAW odpowiedzialnego za funkcjonowanie systemu informatycznego IPAW oraz stosowanie technicznych i organizacyjnych środków ochrony;
7. **administratorze systemu –** należy przez to rozumieć pracownika Działu IT, który posiada uprawnienia do administrowania określonymi zasobami informatycznymi IPAW. Czasowo, za zgodą Administratora Danych oraz Koordynatora Działu IT Administratorem Systemu może zostać inny pracownik IPAW lub przedstawiciela firmy współpracującej;
8. **użytkowniku systemu** – należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym IPAW. Użytkownikiem może być pracownik IPAW, osoba wykonująca pracę na podstawie umowy zlecenie lub innej umowy cywilnoprawnej, osoba odbywająca, praktykę, staż w IPAW lub wolontariusz;

9. **sieci lokalnej** - należy przez to rozumieć połączenie systemów informatycznych IPAW wyłącznie dla własnych jej potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnej;
10. **sieci rozległej** - należy przez to rozumieć publiczną sieć telekomunikacyjną w rozumieniu ustawy z dnia z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dziennik Ustaw z 2004 r. Nr 171 poz. 1800 ze zmianami) i nie będącą siecią lokalną;
11. **ustawie –** rozumie się przez to ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U.2018.1000 z dnia 24 maja 2018 r. z późn. zm);
12. **rozporządzeniu –** rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U nr 100, poz. 1024);
13. **umowa użyczenia** - rozumie się przez to umowę użyczenia lokalu pomiędzy IPAW a Gminą Wałbrzych z dnia nr 1/07/2015 z dnia 02.03.2015r.;
14. **porozumienie** – rozumie się przez to „Porozumienie w przedmiocie dostępu do systemu informatycznego" pomiędzy IPAW a Gminą Wałbrzych z dnia 19.06.2015r.;
15. **infrastruktura UMW** - rozumie się przez to udostępniona na potrzeby Instytucji Pośredniczącej Aglomeracji Wałbrzyskiej Infrastrukturę Informatyczną Urzędu Miejskiego w Wałbrzychu, do której dostęp opisuje Porozumienie;
16. **dokumentacja UMW –** rozumie się przez to obowiązującą dokumentację przetwarzania danych osobowych w urzędzie miejskim wprowadzoną zarządzeniem prezydenta Miasta Wałbrzycha w sprawie wprowadzenia dokumentacji przetwarzania danych osobowych w Urzędzie Miejskim w Wałbrzychu;
17. **RODO –** rozumie się przez to Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
18. **DPIA** – oznacza ocenę skutków planowanych operacji przetwarzania dla ochrony danych osobowych, której dokonuje Administrator Danych jeżeli dany rodzaj przetwarzania ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych;
19. **Inspektor Ochrony Danych (IOD)** – należy przez to rozumieć powołaną przez Administratora Danych osobę fizyczna, zobowiązaną do zapewniania przestrzegania przepisów o ochronie

danych osobowych zgodnie z rozdziałem IV pkt. 4 RODO;

20. **odbiorca** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych osobowych przez te organy publiczne musi być zgodne z przepisami o ochronie danych osobowych mającymi zastosowanie stosownie do celów przetwarzania;
21. **powierzenie przetwarzania danych osobowych** - oznacza sytuację zlecenia na podstawie umowy przez Administratora Danych innemu podmiotowi (Procesorowi) dokonywania w jego imieniu określonych operacji na danych osobowych. Procesor nie decyduje samodzielnie o celach i środkach przetwarzania;
22. **rozliczalność** - oznacza odpowiedzialność Administratora Danych za przestrzeganie zasad RODO i możliwość wykazania ich przestrzegania, w szczególności: zgodność z prawem, rzetelność i przejrzystość, ograniczenie celu, minimalizacja danych, prawidłowość danych, ograniczenie przechowywania, integralność i poufność;
23. **szczególne kategorie danych osobowych** – rozumie się przez to dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby, o których mowa w art. 9 ust. 1 RODO.

B. Cel

Wdrożenie Polityki Bezpieczeństwa w IPAW ma na celu zabezpieczenie przetwarzanych przez niego danych osobowych, w tym danych przetwarzanych w systemie informatycznym IPAW i poza nim, poprzez wykonanie obowiązków wynikających z RODO, ustawy i rozporządzenia.

W związku z tym, że w zbiorach danych IPAW przetwarzane są między innymi szczególne kategorie danych osobowych, a system informatyczny Administratora Danych posiada szerokopasmowe połączenie z internetem, niniejsza Polityka Bezpieczeństwa służy zapewnieniu wysokiego poziomu ochrony danych osobowych. Niniejszy dokument opisuje niezbędny do uzyskania tego bezpieczeństwa zbiór procedur i zasad dotyczących przetwarzania danych osobowych oraz ich zabezpieczenia.

Zawarte w niniejszej Polityce Bezpieczeństwa opisy zasad i procedur przetwarzania danych osobowych i ich zabezpieczenia mają na celu uporządkowanie procesów przetwarzania danych, a także realizację przez ADO zasady rozliczalności.

C. Zakres merytoryczny Polityki Bezpieczeństwa oraz zakres stosowania

1. Niniejszą Politykę Bezpieczeństwa stosuje się do wszelkich czynności stanowiących w myśl RODO przetwarzanie danych osobowych. Bez względu na źródło pochodzenia danych osobowych, ich zakres, cel zebrania, sposób lub czas przetwarzania, stosowane są zasady przetwarzania ujęte w niniejszym dokumencie. Zasadom tym, podlegają również dane powierzone Administratorowi Danych do przetwarzania na podstawie umowy powierzenia przetwarzania..
2. Elementem polityki są prowadzone przez IPAW zgodnie z art. 30 ust. 1 i 2 RODO:
    a) jako Administrator Danych rejestr czynności przetwarzania (dalej: „Rejestr Czynności"),
    b) jako Procesor rejestr kategorii czynności przetwarzania (dalej: „Rejestr Kategorii").
3. Polityka Bezpieczeństwa oraz zawarte w niej Rejestr Czynności i Rejestr Kategorii, zgodnie z art. 30 ust. 3 RODO, są prowadzone w formie elektronicznej lub pisemnej oraz udostępniane przez IPAW na żądanie organu nadzorczego
4. Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych, jak i innych, np. wolontariuszy, praktykantów, stażystów.

II. Administrator Danych - zadania

Administrator Danych realizuje zadania w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych, w tym zwłaszcza:

1. sprawdza zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
2. zapewnia zapoznanie się osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
3. sprawuje nadzór nad wdrożeniem stosownych środków fizycznych, a także organizacyjnych i technicznych – w celu zapewnienia bezpieczeństwa danych,
4. sprawuje nadzór nad funkcjonowaniem systemu zabezpieczeń, w tym także nad prowadzeniem ewidencji z zakresu ochrony danych osobowych,

5. koordynuje i zapewnia wewnętrzne audyty w zakresie bezpieczeństwa informacji oraz przestrzegania przepisów o ochronie danych osobowych nie rzadziej niż raz na rok.
6. nadzoruje udostępnianie danych osobowych odbiorcom danych i innym podmiotom,
7. zatwierdza wzory dokumentów (odpowiednie klauzule w dokumentach) dotyczących ochrony danych osobowych, przygotowywane przez komórki organizacyjne IPAW.
8. nadzoruje prowadzenie ewidencji i innej dokumentacji z zakresu ochrony danych osobowych,
9. prowadzi oraz aktualizuje dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych,
10. podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia systemu informatycznego,
11. zatwierdza materiały szkoleniowe z zakresu ochrony danych osobowych i nadzoruje szkolenia osób upoważnianych do przetwarzania danych osobowych.

Administrator danych przetwarza dane z poszanowaniem następujących zasad:

1. w oparciu o podstawę prawna i zgodnie z prawem (legalizm),
2. rzetelnie i uczciwie (rzetelność),
3. w sposób przejrzysty dla osoby (transparentność),
4. w konkretnych celach i nie „na zapas" (minimalizm),
5. w zakresie nie szerszym niż jest to niezbędne (adekwatność),
6. z dbałością o prawidłowość danych (prawidłowość),
7. przez okres niezbędny (czasowość),
8. zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

III. Inspektor Ochrony Danych

1. IPAW może wyznaczyć Inspektora Ochrony Danych.
2. Osoby, których dane dotyczą, mogą kontaktować się z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.
3. IPAW powierza IOD w szczególności następujące zadania:

a) informowanie Administratora Danych oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów o ochronie danych osobowych i doradzanie im w tej sprawie;
b) monitorowanie przestrzegania RODO, innych przepisów o ochronie danych osobowych oraz polityk i procedur wewnętrznych Administratora Danych w dziedzinie ochrony danych osobowych;
c) podział obowiązków związanych z ochroną danych osobowych w IPAW oraz podejmowanie działań zwiększających świadomość personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym szkolenia i audyty;
d) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych osobowych (DPIA) oraz monitorowanie jej wykonania;
e) współpraca z organem nadzorczym;
f) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

IV. Obszar przetwarzania danych osobowych.

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;

1. Obszarem, w którym przetwarzane są dane osobowe są pomieszczenia w budynku przy ul. Słowackiego 23A, użyczone na podstawie Umowy użyczenia.
2. Obszar, w którym przetwarzane są dane osobowe należy zamykać na czas nieobecności w nim osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do niego osób trzecich.
3. Szczególnym obszarem, w którym przetwarzane są dane o wysokim priorytecie i przebywać w nim mogą jedynie osoby zatrudnione ze specjalnym upoważnieniem są pomieszczenia:
   a) wewnętrzny pokój w pokoju 306 w budynku przy ul. Słowackiego 23A oznaczony jako pomieszczenie infrastruktury informatycznej.

V. Rejestr czynności przetwarzania oraz Rejestr kategorii czynności przetwarzania

1. Artykuł 30 ust. 1 RODO nakłada na IPAW jako Administratora Danych obowiązek prowadzenia rejestru czynności przetwarzania danych osobowych. Dotyczy on czynności przetwarzania, za

które Administrator Danych odpowiada. W Rejestrze Czynności zamieszczone są następujące informacje wymagane przepisami prawa:

a) nazwa oraz dane kontaktowe Administratora Danych oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela Administratora Danych oraz IOD;
b) cele przetwarzania;
c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
e) gdy ma to zastosowanie, informacje o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 RODO, dokumentacja odpowiednich zabezpieczeń;
f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
g) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

Rejestr Czynności stanowi Załącznik nr 1 do Polityki Bezpieczeństwa;

2. Artykuł 30 ust. 2 RODO nakłada na IPAW jako Procesora obowiązek prowadzenia rejestru kategorii czynności przetwarzania danych osobowych. W Rejestrze Kategorii zamieszczone są następujące informacje:

a) dane identyfikujące IPAW jako Procesora (nazwa oraz dane kontaktowe), a także dane przedstawiciela Administratora Danych lub Procesora oraz IOD – jeżeli zostali wyznaczeni;
b) kategorie przetwarzań dokonywanych w imieniu każdego z Administratorów Danych;
c) informacje o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa lub organizacji, a w przypadku przekazań, o których mowa w art. 49 ust. 1 RODO, dokumentację odpowiednich zabezpieczeń, gdy dochodzi do takiego przekazania danych do państwa trzeciego lub organizacji międzynarodowej;
d) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

Rejestr Kategorii stanowi Załącznik nr 2 do Polityki Bezpieczeństwa.

VI. Dokumentacja przetwarzania danych osobowych

Dokumentacja związana z ochroną danych osobowych przechowywana jest przez Administratora Danych.

A. Upoważnienie do przetwarzania danych osobowych

1. W celu zapewnienia, że każda osoba fizyczna mająca dostęp do danych osobowych działa na podstawie upoważnienia do przetwarzania danych osobowych nadanego przez Administratora Danych/Procesora i przetwarza je wyłącznie na ich polecenie, w strukturze wewnętrznej IPAW do przetwarzania danych osobowych dopuszczone są wyłącznie osoby posiadające upoważnienie nadane przez ADO / Procesora.
2. Upoważnienie zawiera w szczególności:
    a) zakres danych objętych upoważnieniem;
    b) zakres operacji przetwarzania;
    c) okres obowiązywania upoważnienia;
    d) oświadczenie o zapoznaniu się z przepisami o ochronie danych osobowych oraz dokumentacją dotyczącą przetwarzania danych osobowych obowiązującą w IPAW;
    e) obowiązek zachowania poufności oraz sposób gromadzenia i zabezpieczania danych osobowych.
3. Upoważnienie do przetwarzania danych osobowych nadawane jest w przypadku:
    a) nowozatrudnionych osób - przed przystąpieniem do wykonywania ich obowiązków;
    b) osób awansowanych bądź w przypadku zmiany zakresu kompetencji – przed przystąpieniem do wykonywania nowych obowiązków.
4. Upoważnienie zostaje nadane na wniosek przełożonego osoby mającej zostać dopuszczoną do przetwarzania danych osobowych, co do zasady w formie pisemnej lub mailowej.
5. Zakres danych osobowych, do których przetwarzania osoba zostaje upoważniona pozostaje w związku z wykonywanymi na rzecz IPAW czynnościami.
6. Wzór upoważnienia do przetwarzania danych osobowych stanowi Załącznik nr 3 do Polityki Bezpieczeństwa.

B. Umowy powierzenia przetwarzania danych osobowych

1. Podstawą przetwarzania danych osobowych w imieniu IPAW przez podmioty trzecie, oraz przetwarzania danych osobowych przez IPAW w imieniu innych administratorów, są umowy powierzenia przetwarzania danych osobowych.

2. Umowy powierzenia zawierane przez IPAW odpowiadają w szczególności wymogom określonym w art. 28 ust. 3 RODO.
3. W przypadku, gdy IPAW zawiera umowę powierzenia przetwarzania danych osobowych, osoba odpowiedzialna za dany proces jest zobowiązana niezwłocznie powiadomić osobę odpowiedzialną za ochronę danych osobowych w IPAW o zawarciu i rozwiązaniu takiej umowy (np. za pośrednictwem wiadomości e-mail).
4. Wzór umowy powierzenia przetwarzania danych osobowych stanowi Załącznik nr 4 do Polityki Bezpieczeństwa.

C. Legalność przetwarzania danych osobowych

1. Administrator Danych ewidencjonuje w Rejestrze Czynności podstawy prawne przetwarzania danych osobowych.
2. Wskazując ogólną podstawę prawną przetwarzania, zgodnie z art. 6 ust 1 RODO oraz art. 9 ust. 2 RODO, Administrator Danych dookreśla podstawę w czytelny sposób, gdy jest to potrzebne. W szczególności, w miarę możliwości, Administrator Danych wskazuje przepis prawa , gdy podstawą jest prawo, oraz konkretny interes, gdy powołuje się na prawnie uzasadniony interes administratora lub osoby trzeciej.
3. Kierownik komórki organizacyjnej IPAW ma obowiązek znać podstawy prawne, na jakich komórka przez niego kierowana dokonuje konkretnych czynności przetwarzania danych osobowych.
4. Administrator Danych zarządza zgodami zapewniając rejestrację i weryfikację posiadania zgody osoby na przetwarzanie konkretnych kategorii danych osobowych w konkretnym celu, zgody na komunikację marketingową oraz na komunikację na odległość, odmowy udzielenia zgody, cofnięcia zgody, sprzeciwu oraz żądania ograniczenia przetwarzania jego danych osobowych.

D. Procedura Stosowania DPIA

1. DPIA to proces mający na celu ocenę niezbędności i proporcjonalności przetwarzania danych osobowych oraz pomoc w zarządzaniu ryzykiem naruszenia praw lub wolności osób fizycznych wynikającym z przetwarzania danych osobowych.
2. Administrator Danych każdorazowo w stosunku do poszczególnych kategorii operacji weryfikuje, czy zachodzą podstawy dokonania DPIA. Administrator Danych wdrożył odrębną Procedurę w zakresie postępowania na potrzeby oceny zasadności przeprowadzenia DPIA oraz ew. jej dokonania.

3. Obowiązek przeprowadzenia DPIA spoczywa na podmiocie będącym Administratorem Danych. IPAW w zakresie w jakim występuje jako Procesor może uczestniczyć w przeprowadzaniu DPIA przez administratorów, udzielając im m.in. niezbędnych informacji.
4. W zakresie w jakim IPAW działa jako Procesor i stwierdzi wysokie ryzyko naruszenia praw lub wolności podmiotów danych związane z określonym rodzajem przetwarzania, może przeprowadzić ocenę skutków dla ochrony danych, adekwatnie do wdrożonej procedury DPIA. Przed podjęciem przedmiotowych działań, pracownik IPAW kontaktuje się w tym przedmiocie z administratorem w celu ustalenia wspólnego planu działania.
5. Procedura DPIA stanowi Załącznik nr 5 Polityki Bezpieczeństwa

E. Polityka czystego biurka

1. W celu określenia zasad zapobiegania dostępowi do danych osobowych osób nieuprawnionych, w tym podczas wspólnego korzystania przez większą ilość osób z pomieszczeń i sprzętu współdzielonego, IPAW wdrożył politykę czystego biurka.
2. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do zapewnienia ich bezpieczeństwa oraz uniemożliwienia dostępu do nich osobom nieupoważnionym. W przypadku pracy nad dokumentami zawierającymi dane osobowe nie należy pozostawiać ich bez nadzoru, po zakończonej pracy dokumenty te powinny być bezwzględnie przechowywane w zamkniętych na klucz szafach bądź szufladach. Należy bezwzględnie przestrzegać obowiązku zamykania szafek / szuflad na klucz po zakończeniu pracy i nietrzymania kluczy w zamkach na stałe.
3. Po zakończeniu pracy opuszczane pomieszczenia należy pozostawić zabezpieczone – osoba wychodząca jako ostatnia powinna:
   a) upewnić się, że wszystkie okna w pomieszczeniu zostały zamknięte;
   b) zamknąć drzwi wejściowe do pomieszczenia; oraz
   c) zabezpieczyć w odpowiedni sposób klucze.
4. Żaden pracownik nie powinien przekazywać innym osobom udostępnionych mu haseł i kodów dostępu, trzymać ich na biurku lub utrwalać w łatwo dostępnych miejscach.
5. Monitor komputera powinien być ustawiony w taki sposób, aby osoby nieuprawnione nie miały możliwości wglądu w monitor.
6. W przypadku braku ustawienia włączającego się automatycznie po zdefiniowanym okresie wygaszacza ekranu, każdy pracownik powinien przed oddaleniem się od stanowiska pracy, zablokować komputer lub w przypadku dłuższej nieobecności wylogować się z systemu.

F. Polityka retencji danych

1. Polityka retencji danych opisuje okresy przechowywania określonych, typowych dokumentów, na podstawie obowiązujących przepisów prawa krajowego.
2. Po upływie okresu przechowywania dokumenty zawierające dane osobowe przechowywane w wersji papierowej lub elektronicznej, należy zniszczyć w sposób uniemożliwiający identyfikację osoby, której dane dotyczą.
3. Usunięcie lub zniszczenie dokumentów powinno mieć charakter trwały.
4. Szczegółowe okresy retencji stanowią Załącznik nr 6 do Polityki Bezpieczeństwa.

G. Procedura postępowania z incydentami

1. Procedura ma na celu zapewnienie, aby zdarzenia związane z naruszeniem ochrony danych były zgłaszane w sposób umożliwiający podjęcie szybkich działań korygujących.
2. Naruszeniem ochrony danych osobowych jest każde zjawisko stanowiące naruszenie bezpieczeństwa, którego efektem jest przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych w ramach funkcjonowania IPAW.
3. Każdy kto stwierdził wystąpienie incydentu lub podejrzewa, że mógł on wystąpić zobowiązany jest niezwłocznie poinformować o tym bezpośredniego przełożonego oraz każdorazowo osobę odpowiedzialną za bezpieczeństwo danych osobowych w IPAW.
4. Szczegółowe zasady postępowania w przypadku wystąpienia incydentu określa Instrukcja Postępowania w Sytuacji Naruszenia Bezpieczeństwa Danych Osobowych.

H. Współadministrowanie

1. Jeśli IPAW w stosunku do niektórych operacji na danych osobowych może ustalać cele i sposoby przetwarzania wspólnie z innymi podmiotami, w celu prawidłowego wywiązywania się z obowiązków określonych w art. 26 RODO, IPAW każdorazowo przed rozpoczęciem takich operacji na zasadzie wspólnej administracji danymi zawiera umowę.
2. Treść zawieranej umowy spełnienia warunki dotyczące uzgodnień, o których stanowi art. 26 RODO, w szczególności w przejrzysty sposób określa odpowiednie zakresy odpowiedzialności IPAW i pozostałych współadministratorów dotyczącej wypełniania obowiązków wynikających z RODO, w tym:
    a) w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw;

b) poziomu bezpieczeństwa danych osobowych; oraz

c) obowiązków w odniesieniu do spełniania obowiązku podawania informacji, o których mowa w art. 13 i 14 RODO.

3. IPAW dochowuje staranności, aby zawierane umowy każdorazowo należycie odzwierciedlały odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą.
4. Zasadnicza treść umowy jest udostępniana podmiotom, których dane dotyczą.

I. Obowiązek informacyjny

1. Administrator Danych wykonuje obowiązki informacyjne określone w art. 13 i 14 RODO w sposób zgody z prawem oraz efektywny, stosując aktualne wzory klauzul informacyjnych.
2. Aktualne wzory klauzul informacyjnych udostępniane są na zasobach sieciowych IPAW oraz na stronach internetowych IPAW.
3. Administrator Danych informuje osoby:
   a) o przetwarzaniu danych osobowych, przy pozyskiwaniu danych od osoby, w zakresie zgodnym z art. 13 RODO,
   b) o przetwarzaniu danych, przy pozyskiwaniu danych niebezpośrednio od osoy, w zakresie zgodnym z art. 14 RODO, chyba że zachodzą przesłanki wyłączające taki obowiązek,
   c) o przetwarzaniu danych niezidentyfikowanych, tam gdzie jest to możliwe (np. tabliczka o objęciu obszaru monitoringiem wizyjnym).

J. Realizacja praw osób, których dane dotyczą

1. Administrator Danych dokłada wszelkich starań, aby przekazywane informacje oraz sposób komunikacji z osobami, których dane dotyczą były czytelne i zrozumiałe dla odbiorców.
2. Administrator Danych ułatwia osobom, których dane dotyczą, wykonywanie przysługujących im praw związanych z przetwarzaniem ich danych osobowych.
3. Prawa jednostki wykonywane są przez Administratora Danych w terminie jednego miesiąca. Wykonywanie żądań wymagających większego nakładu pracy i czasu może zostać przedłużone o dwa miesiące, za powiadomieniem osoby.
4. Administrator Danych weryfikuje tożsamość osób, chcących zrealizować swoje prawa związane z przetwarzaniem danych osobowych.
5. W przypadku realizacji przez podmiot danych jego praw w stosunku do danych osobowych

przetwarzanych przez IPAW jako procesora, IPAW pomaga administratorowi wywiązać się z obowiązku odpowiadania na żądania podmiotów danych.

Prawo dostępu do danych i prawo do kopii danych

6. Podmiot danych, w zakresie przetwarzania jego danych osobowych posiada prawo dostępu do swoich danych osobowych oraz prawo do otrzymania ich kopii.

Prawo do sprostowania danych

7. Na żądanie podmiotu danych, Administrator Danych dokonuje stosownego sprostowania nieprawidłowych danych. Administrator Danych ma prawo odmówić sprostowania danych osobowych, gdy poweźmie uzasadnione wątpliwości co do prawidłowości danych, których zamieszczenia domaga się wnioskodawca. Odmawiając, Administrator Danych umożliwi wnioskodawcy wykazanie prawidłowości danych osobowych zgłoszonych w sprostowaniu.
8. Na wniosek osoby Administrator uzupełnia i aktualizuje dane osobowe, weryfikując je w tym samym trybie jak przy ich pierwotnym pozyskaniu.

Prawo do usunięcia danych osobowych

9. Administrator Danych usuwa dane na żądanie podmiotu danych, gdy podstawy ich dalszego przetwarzania lub prawo nakazuje ich usunięcie.
10. Realizacja prawa następuje w taki sposób, aby zapewnić osiągnięcie celu tego prawa, w tym przede wszystkim zaprzestanie dalszego przetwarzania, jednak przy poszanowaniu wszystkich zasad ochrony danych osobowych, w tym bezpieczeństwa pozostałych danych osobowych przetwarzanych przez Administratora Danych.
11. Przed uwzględnieniem wniosku o usunięcie danych osobowych weryfikowane są wszystkie podstawy przetwarzania danych osobowych, w tym w szczególności:
    a) czy usunięcie danych nie spowoduje zagrożenia bezpieczeństwa pozostałych danych osobowych przetwarzanych przez Administratora Danych,
    b) czy nie zachodzi potrzeba przechowywania danych osobowych dla celów dowodowych,
    c) czy nie zachodzą inne wyjątki, o których mowa w art. 17 ust. 3 RODO.

Prawo do ograniczenia przetwarzania

12. Na żądanie osoby Administrator Danych dokonuje ograniczenia przetwarzania danych osobowych, gdy:
    a) osoba kwestionuje prawidłowość danych osobowych – na okres pozwalający dokonać sprawdzenia ich prawidłowości,

b) przetwarzanie jest niezgodne z prawem, a osoba sprzeciwia się usunięciu danych, żądając w zamian ograniczenia ich przetwarzania,

c) Administrator Danych nie potrzebuje już danych osobowych, ale są one potrzebne osobie do ustalenia, dochodzenia lub obrony roszczeń,

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

13. W trakcie ograniczenia przetwarzania Administrator Danych przechowuje dane, natomiast ich nie przetwarza w sposób czynny, bez zgody osoby, 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.

Prawo do sprzeciwu

14. Prawo do sprzeciwu znajduje zastosowanie wyłącznie w sytuacji, gdy podstawą przetwarzania danych osobowych jest:

    a) niezbędność przetwarzania do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi Danych; bądź

    b) niezbędność przetwarzania do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora Danych lub przez stronę trzecią.

15. Osoba, której dane dotyczą może wnieść sprzeciw w dowolnym momencie, po rozpoczęciu przetwarzania danych osobowych, z przyczyn związanych ze szczególną sytuacją danej osoby.

16. Administrator Danych każdorazowo po ustaleniu, że żądanie dotyczy operacji opartych na podstawie prawnej wymienionej powyżej, weryfikuje, czy przetwarzanie objęte sprzeciwem:

    a) ma miejsce na potrzeby marketingu bezpośredniego;

    b) następuje do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO;

    i następnie:

    c) jeśli sprzeciw wniesiono wobec przetwarzania dla celów marketingu bezpośredniego (w tym np. związanego z nim profilowania) – Administrator Danych zaprzestaje dalszego przetwarzania;

    d) jeśli sprzeciw wniesiono wobec przetwarzania do celów badań naukowych lub historycznych lub do celów statystycznych – Administrator Danych weryfikuje możliwość powołania się na okoliczność, iż przetwarzanie danych osobowych jest niezbędne do

wykonania zadania realizowanego w interesie publicznym, i w zależności od przypadku, zaprzestaje lub kontynuuje przetwarzanie danych osobowych;

e) jeśli sprzeciw wniesiono wobec przetwarzania w pozostałych przypadkach – Administrator Danych zestawia podstawy do przetwarzania, na które się powołuje przy przetwarzaniu danych osobowych objętych sprzeciwem z interesami, prawami i wolnościami osoby, której dane dotyczą. Administrator Danych w szczególności weryfikuje możliwość odmowy uczynienia zadość żądaniu z powołaniem się na: istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania danych osobowych, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą lub istnienie podstaw do ustalenia, dochodzenia lub obrony roszczeń. W takich przypadkach, pomimo wniesienia sprzeciwu przez osobę, której dane dotyczą, Administrator Danych odmawia spełnienia żądania zaprzestania przetwarzania.

VII. Środki Techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

A. Środki ochrony fizycznej

1. Pomieszczenia w budynku przy pl. Słowackiego 23A, w których zlokalizowany jest obszar przetwarzania danych osobowych są zamykane po zakończeniu pracy. Budynek jest dozorowany w godzinach pracy, oraz wyposażony w system alarmowy.
2. Urządzania służące do przetwarzania danych osobowych znajdują się w pomieszczeniach zabezpieczonych.
3. Serwery oraz komputery służące do przechowywania danych są udostępnione w ramach Infrastruktury UMW, środki ochrony fizycznej wydzielonej infrastruktury opisuje dokumentacja UMW.
4. Przebywanie osób nieuprawnionych w pomieszczeniach tworzących obszar przetwarzania danych osobowych dopuszczalne jest tylko w obecności osoby zatrudnionej przy przetwarzaniu danych lub w obecności Administratora Danych lub innej osoby upoważnionej.
5. Pomieszczenia, o których mowa powyżej powinny być zamykane na czas nieobecności w nich osób zatrudnionych przy przetwarzaniu danych, w sposób uniemożliwiający dostęp do nich osób trzecich.
6. W przypadku przebywania osób postronnych w pomieszczeniach, o których mowa wyżej, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób

aby uniemożliwiać im wgląd w dane.

7. Do przebywania w pomieszczeniu infrastruktury informatycznej uprawnieni są Administrator Danych oraz pracownicy Działu IT.
8. Przebywanie w pomieszczeniu infrastruktury informatycznej osób nieuprawnionych (konserwator, osoba sprzątająca) dopuszczalne jest tylko w obecności jednej z osób upoważnionych, o których mowa w pkt. 7, a w przypadku ich nieobecności – w obecności osoby pisemnie upoważnionej przez Administratora Danych. Rejestr wejść jest prowadzony w Dziale IT.

B. Środki sprzętowe, informatyczne i telekomunikacyjne

1. System informatyczny oraz systemy przetwarzające dane zabezpieczone są przed nieupoważnionym dostępem osób trzecich systemem uwierzytelniania i autoryzacji użytkowników.
2. Urządzenia wchodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego, systemy składowania danych zabezpieczone na wypadek zaniku napięcia albo awarii w sieci zasilającej urządzeniami podtrzymującymi napięcie (UPS).
3. Siec lokalna podłączona do Internetu za pomocą zestawu „Zapór Ogniowych" (Firewall) tworzących strefę zdemilitaryzowaną (*ang. demilitarized zone – DMZ*).
4. Na wszystkich serwerach oraz wszystkich stacjach roboczych zainstalowano oprogramowanie antywirusowe. Poczta elektroniczna wpływająca do IPAW skanowana jest programem antywirusowym zarówno przed wysłaniem jak i podczas odbierania wiadomości.
5. W ramach Infrastruktury UMW wdrożono system kopii zapasowych z wykorzystaniem nośników zewnętrznych.
6. W ramach Infrastruktury UMW nośniki zawierające kopie zapasowe przechowywane są w szafie pancernej, w innym pomieszczeniu niż serwerownia – miejsce składowania danych.
7. W ramach Infrastruktury UMW i IPAW kluczowe składniki systemu informatycznego tj. serwery, brzegowe urządzenia sieciowe, stacje robocze, nośniki danych oraz strategiczne urządzenie wspomagające (urządzenia UPS, streamery, NAS itp.) posiadają określony cykl życia (*ang. live time*). Po upłynięciu tego okresu winny być wymienione na nowe. Zestawienie sprzętu wraz z określonym cyklem życia stanowi załącznik nr 7 do Polityki Bezpieczeństwa.

C. Środki ochrony w ramach oprogramowania systemu

1. Dostęp fizyczny do baz danych osobowych zastrzeżony jest wyłącznie Administratora Systemu.
2. Konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych jedynie za pośrednictwem aplikacji.
3. System informatyczny pozwala zdefiniować odpowiednie prawa dostępu do zasobów informatycznych systemu.
4. W sieciowym systemie operacyjnym zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do systemu.

D. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych

1. Aplikacje służące do przetwarzania danych osobowych muszą posiadać mechanizmy jednoznacznego uwierzytelniania użytkownika i autoryzacji poziomu uprawnień za pomocą 1 z 2 metod:
    1. Autentykacja i autoryzacja za pomocą domeny MS Active Directory protokołem Kerberos, ADSI, LDAP ;
    2. Dodatkowego loginu i hasła dostępu na poziomie aplikacji przetwarzającej dane.
2. Dla każdego użytkownika systemu informatycznego jest ustalony odrębny identyfikator.
3. Zdefiniowano użytkowników i ich prawa dostępu do danych osobowych na poziomie systemu informatycznego (unikalny identyfikator i hasło w domenie MS Active Driectory).
4. Systemy informatyczne, które udostępniają dane osobowe muszą spełniać warunki opisane z art. 32 i 33 ustawy i § 7 rozporządzenia. Wymagane w przywołanych przepisach obowiązki sprowadzają się m.in. do zapewnienia i udostępniania – na żądanie osoby, której dane są przetwarzane – informacji o:
    1) dacie, od kiedy przetwarza się w zbiorze jej dane osobowe, oraz treści tych danych,
    2) źródle, z którego pochodzą dane jej dotyczące, chyba że administrator jest obowiązany do zachowania w tym zakresie tajemnicy państwowej, służbowej lub zawodowej,
    3) sposobie i zakresie udostępniania jej danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane,
    4) sposobie, w jaki zebrano dane.

E. Środki ochrony w ramach systemu informatycznego

1. Wszystkie komputery IPAW są skonfigurowane w sposób uniemożliwiający logowanie

lokalne. Jedynym możliwym uruchomieniem systemu jest logowanie do domeny Active Directrory o nazwie um.local za pomocą ważnego identyfikatora i hasła dostępu.

2. Zastosowano automatyczny i zabezpieczony hasłem wygaszacz ekranu w przypadku dłuższej nieaktywności użytkownika.
3. Każdy użytkownik systemu może i powinien na czas przerwy w pracy w systemie informatycznym zablokować komputer za pomocą klawiatury, kombinacją klawiszy [windows] + L

F. Środki organizacyjne

1. Administrator danych przyznaje uprawnienia dostępu do przetwarzania danych osobowych w formie upoważnienia.
2. Osoby upoważnione do przetwarzania danych osobowych są przed dopuszczeniem ich do pracy z tymi danymi zapoznawane z przepisami o ochronie danych osobowych, procedurami przetwarzania danych oraz podstawowymi zagrożeniami związanymi z przetwarzaniem danych w systemie informatycznym.
3. Dział Kadr i Płac prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, oraz oświadczeń o zapoznaniu się z przepisami:
   - ochronie danych osobowych,
   - obwiązującej Polityce Bezpieczeństwa IPAW,
   - obowiązującej Instrukcji zarządzania systemami informatycznym IPAW,

   Wzór oświadczenia stanowi załącznik 8 do Polityki Bezpieczeństwa.
4. Osobę, która utraciła uprawnienia dostępu do danych osobowych, należy niezwłocznie wyrejestrować i unieważnić jej hasło oraz podjąć inne niezbędne czynności uniemożliwiające jej dalszy dostęp do danych.
5. Czynności wymienione w pkt. 19 wykonuje Administrator Systemu na polecenie Administratora Danych lub osoby upoważnionej.
6. Nie wolno wykorzystywać identyfikatora osoby, która utraciła uprawnienia do dostępu do danych. Identyfikator osoby winien być unikalny.
7. Wprowadzono Instrukcje Zarządzania Systemem Informatycznym.
8. Wprowadzono zasadę czystego biurka i czystego ekranu.
9. Zdefiniowano procedury postępowania w sytuacji naruszenia ochrony danych osobowych.
10. Wprowadzono obowiązek rejestracji wszystkich przypadków awarii systemu, działań konserwacyjnych w systemie oraz naprawy systemu.

11. Określono sposób postępowania z nośnikami informacji.
12. Podczas wymiany informacji z osobą której tożsamości nie można zweryfikować (np. rozmowa telefoniczna, nie podpisany podpisem elektronicznym e-mail) urzędnik może przekazać informacje dot. pracy IPAW nie zakazane prawem, a będące w jego posiadaniu lub objęte zakresem jego kompetencji lub uprawnień.

    Szczególnie powinny to być informacje zależne od potrzeb i oczekiwań klientów a dotyczące:

    - organizacji pracy IPAW,
    - obowiązującego prawa zewnętrznego i miejscowego w tym treści tego prawa oraz o zmianach tego prawa,
    - naborze kandydatów do służby urzędniczej,
    - obowiązujących procedur,
    - prowadzonych rejestrach, ewidencjach i archiwach oraz o sposobach i zasadach udostępniania danych w nich zawartych,
    - rodzajów usług publicznych,
    - treści aktów administracyjnych i ich rozstrzygnięć nie rozstrzygnięć dotyczących spraw indywidualnych bo nie wiemy z kim rozmawiamy ,
    - stanowiska w prawach publicznych zajęte przez organy władzy stanowiącej i wykonawczej,
    - kompetencji kierownictwa IPAW i urzędników,
    - inne informacje, będące powszechnie znanymi, które mogą przyczynić się do nawiązania kontaktu z klientem i są potrzebne lub oczekiwane przez klienta.
13. Podczas wymiany informacji z osobą której tożsamości nie można zweryfikować (np. rozmowa telefoniczna, nie podpisany podpisem elektronicznym e-mail) urzędnik nie może przekazać informacji dotyczących:

    - danych osobowych stron postępowania administracyjnego,
    - przebiegu indywidualnego postępowania administracyjnego,
    - tajemnicy handlowej i skarbowej,
    - informacji niejawnych,
14. Każdy dokument papierowy przeznaczony do wyrzucenia powinien być uprzednio zniszczony w sposób uniemożliwiający jego odczytanie (np. przy pomocy niszczarki do dokumentów).
15. W umowach zawieranych z kontrahentami zewnętrznymi należy umieszczać klauzulę o zachowaniu poufności. W uzasadnionych przypadkach w powyższych umowach należy określić sankcję za złamanie takiej klauzuli.

16. W ramach porozumienia, Gmina Wałbrzych dokonuje badania skuteczności zabezpieczeń Zintegrowanego Systemu Zarządzania Jakością i Bezpieczeństwa Informacji, opisanego w załączniku nr 1.2 do Polityki Bezpieczeństwa Dokumentacji UMW.

G. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych

Niezastosowanie się do prowadzonej przez Administratora Danych Polityki Bezpieczeństwa przetwarzania danych osobowych, której założenia określa niniejszy dokument, i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych będzie potraktowane jako ciężkie naruszenie obowiązków pracowniczych.

Niezależnie od powyższego, osoby popełniające przestępstwo mogą być pociągnięte do odpowiedzialności karnej zwłaszcza na podstawie art. 51-52 ustawy oraz art. 266 Kodeksu karnego.

VIII. Postanowienia końcowe.

1. Osoba upoważniona przez Administratora Danych dokonuje corocznie przeglądów i w razie konieczności aktualizacji Polityki Bezpieczeństwa. Weryfikacja zapisów jest prowadzona pod kątem zgodności stanu deklarowanego ze stanem faktycznym.
2. Polityka Bezpieczeństwa, a w szczególności Rejestr Czynności i Rejestr Kategorii podlegają aktualizacji każdorazowo w przypadku zmiany zbioru danych, a także w przypadku zmiany przepisów prawa dotyczącego ochrony danych osobowych. Aktualizacja jest przeprowadzana przez osobę upoważnioną przez ADO.
3. W celu zapewnienia kontroli nad procesem przetwarzania danych osobowych oraz w celu zapewnienia aktualności dokumentu Polityki Bezpieczeństwa, wszystkie działania dotyczące sfery ochrony danych osobowych są raportowane oraz konsultowane z osobą upoważnioną przez Administratora Danych.
4. Każda osoba upoważniona do przetwarzania danych osobowych przez IPAW ma obowiązek zapoznania się z Polityką Bezpieczeństwa i stosowania zasad w niej opisanych. IPAW udostępnia do zapoznania się osobom upoważnionym treść dokumentu lub wyciąg z dokumentu w wersji elektronicznej lub papierowej, na etapie rozpoczynania współpracy, co dana osoba potwierdza poprzez podpisanie się na otrzymanym upoważnieniu.

DYREKTOR
INSTYTUCJI POŚREDNICZĄCEJ
AGLOMERACJI WAŁBRZYSKIEJ
Bożena Dróżdż