PREZYDENT
MIASTA ŚWIĘTOCHŁOWICE
woj.śląskie

Zarządzenie Nr. 45/2019
Prezydenta Miasta Świętochłowice
z dnia 13.02.2019

w sprawie wprowadzenia Polityki Bezpieczeństwa oraz dobrych praktyk do stosowania w przetwarzaniu danych osobowych w Urzędzie Miejskim w Świętochłowicach

Na podstawie art. 30 ust. 1 i art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2016 r., poz. 446 z zm.4) i art. 24 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/4/WE Prezydent Miasta Świętochłowice zarządza, co następuje:

§ 1

Dla zapewnienia ochrony przetwarzania danych osobowych wprowadza się:

1. Politykę Bezpieczeństwa, która stanowi załącznik numer 1 do niniejszego zarządzenia,
2. Dobre praktyki do stosowania w przetwarzaniu danych osobowych w Urzędzie Miejskim w Świętochłowicach, które stanowią załącznik numer 2 do niniejszego zarządzenia

§ 2

Zobowiązuje się wszystkich pracowników Urzędu Miejskiego w Świętochłowicach do:

1. przestrzegania postanowień zawartych w Polityce Bezpieczeństwa oraz dobrych praktykach do stosowania w przetwarzaniu danych osobowych;
2. zarejestrowania się na platformie https://e-szkolenia.nist.gov.pl/ i odbycia szkolenia: „Zmiany w zakresie danych osobowych w związku z wejściem w życie RODO" oraz dostarczenia do Inspektora Danych Osobowych w terminie 30 dni od wejścia w życie niniejszego zarządzenia certyfikatu/zaświadczenia potwierdzającego odbycie niniejszego szkolenia, a w przypadku nowych pracowników w terminie 10 dni od daty zatrudnienia w Urzędzie Miejskim w Świętochłowicach.

§ 3

Nadzór nad przestrzeganiem postanowień zawartych w Polityce Bezpieczeństwa oraz dobrych praktykach do stosowania w przetwarzaniu danych osobowych powierza się Inspektorowi Ochrony Danych oraz Administratorowi Systemu Informatycznego Urzędu Miejskiego w Świętochłowicach.

§ 4

Jawność załączników do niniejszego zarządzenia podlega ograniczeniu na podst. art. 28 ust. 3 lit. b i art. 38 ust. 5 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych

RADCA PRAWNY
Łukasz Orliński

osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/4/WE.

§ 5

Traci moc Zarządzenie 241/2017 Prezydenta Miasta Świętochłowice z dnia 17 maja 2017 r. w sprawie określenie Polityki Bezpieczeństwa i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

§ 6

Zarządzenie wchodzi w życie z dniem podpisania

PREZYDENT MIASTA
Daniel Begier

08.02.2019
GŁÓWNY SPECJALISTA
ds. kontroli wewnętrznej
Izabela Grzondziel

RADCA PRAWNY
Łukasz Orliński

Załącznik nr 1
do Zarządzenia Nr...../2019
Prezydenta Miasta Świętochłowice
z dnia.....

POLITYKA BEZPIECZEŃSTWA URZĘDU MIEJSKIEGO W ŚWIĘTOCHŁOWICACH

Spis treści

POLITYKA BEZPIECZEŃSTWA URZĘDU MIEJSKIEGO W ŚWIĘTOCHŁOWICACH 1
I. POLITYKA BEZPIECZEŃSTWA 1
1. SŁOWNIK POJĘĆ 6
2. DEFINICJA BEZPIECZEŃSTWA INFORMACJI 6
3. PRAWA OSÓB WYNIKAJĄCE Z RODO 9
Prawo dostępu do Danych 9
Prawo do poprawienia Danych 9
Prawo do ograniczenia przetwarzania danych 10
Prawo do sprzeciwu 10
Prawo do bycia zapomnianym (prawo do usunięcia danych) 10
Prawo do przenoszenia danych 11
4. ZASADY PRZETWARZANIA DANYCH 11
Zasada zgodności z prawem, rzetelności i przejrzystości 12
Zasada ograniczenia celu 12
Zasada minimalizacji danych 12
Zasada prawidłowości 12
Zasada ograniczenia przechowywania 12
Zasada integralności i poufności 13
Zasada rozliczalności 13
5. POZOSTAŁE ZASADY BEZPIECZEŃSTWA STOSOWANE W URZĘDZIE MIEJSKIM W ŚWIĘTOCHŁOWICACH 13
7. PROCESOWE PODEJŚCIE DO BEZPIECZEŃSTWA INFORMACJI 13
6. PRZEGLĄDY SYSTEMU BEZPIECZEŃSTWA 14
7. CELE POLITYKI BEZPIECZEŃSTWA INFORMACJI 15
8. DEKLARACJA KIEROWNICTWA. 15
9. ZAKRES OBOWIĄZYWANIA POLITYKI BEZPIECZEŃSTWA INFORMACJI 15
10. ODPOWIEDZIALNOŚĆ ZA BEZPIECZEŃSTWO INFORMACJI 15
12. STRUKTURA SYSTEMU BEZPIECZEŃSTWA 15
13. MIEJSCE /OBSZARY/ZBIORY/REJESTRY PRZETWARZANIA DANYCH OSOBOWYCH 17
14. PRZETWARZANIE DANYCH OSOBOWYCH 17
15. WYDAWANIE UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH 18
16. SZKOLENIA 18
17. OPIS SYSTEMÓW INFORMATYCZNYCH 19
18. STANDARDY AKCEPTOWALNEGO WYKORZYSTYWANIA SPRZĘTU SŁUŻBOWEGO 19
20. OPIS ZAGROŻEŃ: 19
21. SPOSOBY ZABEZPIECZANIA INFORMACJI 20
21.1. KONTROLA DOSTĘPU DO SYSTEMU INFORMATYCZNEGO 20
21.2. ZASADY DOTYCZĄCE KONT I HASEŁ 20
21.3. POLITYKA CZYSTEGO BIURKA I CZYSTEGO EKRANU 21
..... 22

21.4. ZARZĄDZANIE INCYDENTAMI I NARUSZENIAMI.....22
22. KONSEKWENCJE NARUSZANIA POLITYKI BEZPIECZEŃSTWA INFORMACJI 23
23. POSTANOWIENIA KOŃCOWE.....23

INSTRUKCJA BEZPIECZEŃSTWA SYSTEMU TELEINFORMATYCZNEGO.....26
1. CELE INSTRUKCJI BEZPIECZEŃSTWA SYSTEMU TELEINFORMATYCZNEGO 26
2. ODPOWIEDZIALNOŚĆ ZA BEZPIECZEŃSTWO I ZARZĄDZANIE SYSTEMAMI 26
3. OPIS SYSTEMU.....26
4. SPOSÓB UŻYTKOWANIA SYSTEMU 27
5. BEZPIECZEŃSTWO ZARZĄDZANIA SYSTEMU TELEINFORMATYCZNEGO:.....27
5.1 . KOPIE BEZPIECZEŃSTWA 28
5.2. ZABEZPIECZENIE ANTYWIRUSOWE 28
5.3. KORZYSTANIE Z POCZTY ELEKTRONICZNEJ 28
5.4. KORZYSTANIE Z SIECI INTERNET.....29
Załączniki :.....29
Numer 1 - Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe 30
Numer 2 - Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych 31
Numer 3 - Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi 34
Numer 4 - Sposób przepływu danych pomiędzy poszczególnymi systemami 38
Numer 5 - REJESTR CZYNNOŚCI PRZETWARZANIA 39
CZYNNOŚĆ REKRUTACJA.....42
CZYNNOŚĆ PRZETWARZANIE DANYCH W ZWIĄZKU Z ZATRUDNIENIEM NA UMOWĘ O PRACĘ 44
CZYNNOŚĆ UMOWY CYWILNOPRAWNYCH, NP.: O DZIEŁO, ZLECENIE 46
CZYNNOŚĆ ZARZĄDZANIE KORESPONDENCJĄ URZĘDU 48
CZYNNOŚĆ PROWADZENIE NEWSLETTERÓW, INFORMATORÓW DLA MIESZKAŃCÓW, ETC. 50
CZYNNOŚĆ MONITORING WIZYJNY MIASTA ŚWIĘTOCHŁOWICE 52
CZYNNOŚCI DOTYCZĄCE UMÓW 55
CZYNNOŚCI WYKONYWANIE KONTRAKTÓW.....57
CZYNNOŚĆ KONTAKTY.....59
CZYNNOŚĆ PROWADZENIE EWIDENCJI PRZEDSIĘBIORCÓW, KTÓRZY ZAKOŃCZYLI WYKONYWANIE DZIAŁALNOŚCI GOSPODARCZEJ PRZED DNIEM 1 LIPCA 201 I 61
CZYNNOŚĆ PROWADZENIE EWIDENCJI GRUNTÓW I BUDYNKÓW GMINY ŚWIĘTOCHŁOWICE 63
CZYNNOŚĆ WYMIAR I POBÓR PODATKU OD NIERUCHOMOŚCI 65
CZYNNOŚĆ WYMIAR I POBÓR PODATKU ROLNEGO 67

WYDAWANIE ZEZWOLEŃ NA SPRZEDAŻ NAPOJÓW ALKOHOLOWYCH 69
CZYNNOŚĆ PROWADZENIE EWIDENCJI KIEROWCÓW 71
CZYNNOŚĆ PROWADZENIE EWIDENCJI ZEZWOLEŃ TRANSPORTOWYCH 73
CZYNNOŚĆ PROWADZENIE EWIDENCJI POJAZDÓW 75
CZYNNOŚĆ PROWADZENIE REJESTRU MIESZKAŃCÓW 77
CZYNNOŚĆ PROWADZENIE EWIDENCJI URODZEŃ, MAŁŻEŃSTW I ZGONÓW 79
CZYNNOŚĆ PROWADZENIE REJESTRU WIECZYSTEGO UŻYTKOWNIA I DZIERŻAWY GRUNTÓW 81
CZYNNOŚĆ PROWADZENIE EWIDENCJI ZGŁASZANIA I PRZYJMOWANIA DO ZASOBU PRAC GEODEZYJNYCH I KARTOGRAFICZNYCH NA OBSZARZE GMINY ŚWIĘTOCHŁOWICE 83
CZYNNOŚĆ PROWADZENIE EWIDENCJI UZGADNIANIA USYTUOWANIA PROJEKTOWANYCH SIECI UZBROJENIA TERENU NA OBSZARZE GMINY ŚWIĘTOCHŁOWICE 85
CZYNNOŚĆ PROTOKOŁY USTALEŃ PREZYDENTA MIASTA 87
CZYNNOŚĆ PROWADZENIE REJESTRU WNIOSKÓW 89
CZYNNOŚĆ PROWADZENIE REJESTRU PODAŃ WNOSZONYCH USTNIE DO PREZYDENTA MIASTA 91
CZYNNOŚĆ SYSTEM OBIEGU DOKUMENTÓW 93
CZYNNOŚĆ - PROWADZENIE EWIDENCJI ZGŁOSZONYCH I WYKONANYCH INTERWENCJI ORAZ EWIDENCJA MANDATÓW KARNYCH STRAŻY MIEJSKIEJ W ŚWIĘTOCHŁOWICACH 95
CZYNNOŚĆ OPŁATY ZA ODPADY KOMUNALNE 97
CZYNNOŚĆ UPRAWNIENIA DO BADAŃ TECHNICZNYCH POJAZDÓW 99
CZYNNOŚĆ PROWADZENIE EWIDENCJI INSTRUKTORÓW 101
CZYNNOŚĆ PROWADZENIE EWIDENCJI WYKŁADOWCÓW 103
CZYNNOŚĆ KANDYDCI NA ŁAWNIKÓW 105
CZYNNOŚĆ PROWADZENIE REJSTRU ZAMIESZKANIA CUDZOZIEMCÓW 107
CZYNNOŚĆ PROWADZENIE REJESTRU SPRZĘTU PŁYWAJĄCEGO SŁUŻĄCEGO DO POŁOWU RYB 109
CZYNNOŚĆ PROWADZENIE STAŁEGO REJESTRU WYBORCÓW 111
CZYNNOŚĆ PROWADZENIE DOKUMENTACJI WYBORCZEJ I REFERENDALNEJ 113
CZYNNOŚĆ PROWADZENIE REJESTRACJI I KWALIFIKACJI WOJSKOWEJ 115
CZYNNOŚĆ PROWADZENIEWIDENCJI OBIEKTÓW ŚWIADCZĄCYCH USŁUGI HOTELARSKIE, NIE BĘDĄCE OBIEKTAMI HOTELARSKIMI ORAZ PÓL BIWAKOWYCH 117
CZYNNOŚĆ PROWADZENIE EWIDENCJI STOWARZYSZEŃ ZWYKŁYCH 119
CZYNNOŚĆ PROWADZENIE KONSULTACJI SPOŁECZNYCH GMINY ŚWIĘTOCHŁOWICE 121
Numer 6 - INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH 123
1. Wstęp 124
2. Definicje 124
3. Zabezpieczenia infrastruktury informatycznej i telekomunikacyjnej 124
4. Zabezpieczenia programów i baz przetwarzających dane osobowe 125
5. Procedura dostępu podmiotów zewnętrznych 125

6. Procedura korzystania z Internetu 126
7. Procedura korzystania z poczty elektronicznej 126
8. Procedura nadawania uprawnień do przetwarzania danych osobowych. 127
9. Metody i środki uwierzytelnienia 128
10. Procedura rozpoczęcia, zawieszenia i zakończenia pracy 128
11. Procedura tworzenia kopii zapasowych 129
12. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji i wydruków 129
13. Procedura zabezpieczenia systemu informatycznego, w tym przed wirusami komputerowymi 130
14. Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych 131
15. Procedura wykonywania przeglądów i konserwacji 132

I. POLITYKA BEZPIECZEŃSTWA

Polityka Bezpieczeństwa jest dokumentem nadrzędnym Systemu Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach. Dokument spełnia wymagania Rozporządzenia Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

1. SŁOWNIK POJĘĆ

- **Administrator Danych /AD/** - organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych osobowych).
- Administratorem Danych jest Prezydent Miasta.
- **Inspektor Ochrony Danych** – osoba fizyczna wspierająca administratora danych w realizacji obowiązków dotyczących ochrony danych osobowych;
- **Administrator Systemu Informatycznego /ASI/** - osoba odpowiedzialna za przestrzeganie zasad ochrony danych osobowych w systemach informatycznych – Naczelnik Wydziału Informatyki.
- **Dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Informacje mogą przybierać różne formy. Może być ona zapisywana lub wydrukowana na papierze, przechowywana elektronicznie, przesyłana pocztą lub za pomocą urządzeń elektronicznych.
- **Przetwarzanie danych** - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
- **Naruszenie ochrony danych osobowych** - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
- **Naruszenie Systemu Bezpieczeństwa** - działanie niezgodne z przyjętymi dokumentami Systemu Bezpieczeństwa.
- **Identyfikator** - ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym
- **Hasło** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
- **Incydent** - jedno lub seria niepożądanych lub niespodziewanych zdarzeń, które ze znacznym prawdopodobieństwem mogą zakłócić działania Urzędu oraz zagrozić bezpieczeństwu informacji.

- **Podatność** - słabość zasobu lub grupy zasobów, która może być wykorzystana przez zagrożenie.
- **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
- **Zabezpieczanie danych w systemie informatycznym** - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
- **Przegląd Systemu Bezpieczeństwa** – cykliczna weryfikacja skuteczności przyjętych rozwiązań związanych z bezpieczeństwem informacji
- **Aktywa** - jest to wszystko, co ma wartość dla organizacji (administratora danych lub podmiotu przetwarzającego), np. dane osobowe.
- **Aktywa podstawowe** – są to procesy, działania biznesowe oraz informacje związane z funkcjonowaniem organizacji (w tym dane osobowe).
- **Aktywa wspierające** – są to środki umożliwiające korzystanie z aktywów podstawowych. Przykładem aktywów wspierających jest sprzęt, oprogramowanie, sieć, pracownicy.
- **Anonimizacja** – oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było przypisać konkretnej osobie, której dane dotyczą, za pomocą dodatkowych informacji lub wszelkich innych środków, jakimi dysponuje administrator lub podmiot przetwarzający. Zabieg ten ma charakter trwały i nieodwracalny, powodujący, że po jego przeprowadzeniu nie mamy do czynienia z danymi osobowymi.
- **Grupa Robocza Art. 29** - Grupa Robocza Art. 29 to powołany na mocy Dyrektywy 95/46 zespół roboczy do spraw ochrony osób fizycznych mający charakter doradczy i działający w sposób całkowicie niezależny. Jej misją jest służenie radą Komisji Europejskiej i przyczynianie się do jednolitego stosowania przepisów krajowych przyjętych na mocy dyrektywy. Grupę tworzą przedstawiciele krajowych organów nadzorczych, przedstawiciele organów ustanowionych dla instytucji i organów unijnych (po jednym dla każdej z instytucji i organu) oraz przedstawiciele Komisji Europejskiej. Działania Grupy sprowadzają się głównie do wydawania niemających mocy wiążącej zaleceń, rekomendacji oraz opinii w sprawach unijnych aktów normatywnych z zakresu ochrony prywatności.
- **Identyfikowanie ryzyka** – jest to czynność polegająca na określeniu, co może się zdarzyć (kiedy, gdzie, jak i dlaczego) i spowodować stratę.
- **Kontekst** – są to wszystkie informacje wiążące się z działaniem organizacji, m.in. informacje dotyczące środowiska prawnego, społecznego, politycznego, finansowego czy też technologicznego, np. przepisy dotyczące ochrony danych osobowych.
- **Kryteria akceptacji ryzyka** – są to kryteria, które określają dopuszczalność danego ryzyka.
- **Kryteria oceny ryzyka** - są to kryteria, które określają poziomy odniesienia, względem których określa się ważność ryzyka.

- **Ocena ryzyka** – jest to czynność polegająca na porównaniu wyników uzyskanych podczas analizy ryzyka z kryteriami oceny ryzyka określonymi na etapie ustanawiania kontekstu działania organizacji.
- **Operacja przetwarzania danych osobowych** - każda czynność wykonywana na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
- **Podatność** - jest to słabość, która może być wykorzystana przez zagrożenie, powodując niekorzystne skutki, np. luka w systemie informatycznym.
- **Proces przetwarzania danych osobowych** – zespół operacji (czynności) wykonywanych na danych osobowych lub zestawach danych osobowych w celu osiągnięcia określonego celu przetwarzania.
- **Pseudonimizacja** - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji. Te dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. W przeciwieństwie do anonimizacji, której skutkiem jest nieodwracalne uniemożliwienie identyfikacji osoby, pseudonimizacja jest procesem odwracalnym.
- **RODO** - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), które będzie stosowane od 25 maja 2018 r.; jego celami są skuteczna ochrona podstawowych praw i wolności osób fizycznych, w szczególności prawa do ochrony danych osobowych osób fizycznych oraz uregulowanie zasad i zapewnienie swobodnego przepływu danych osobowych w UE w taki sposób, by ochrona praw jednostki nie stała temu na przeszkodzie.
- **Ryzyko** – wpływ niepewności na cele. W przypadku ryzyka naruszenia praw i wolności osób, których dane dotyczą, celem będzie ochrona tych praw i wolności.
- **Szacowanie ryzyka** – całościowy proces identyfikacji ryzyka, analizy ryzyka oraz oceny ryzyka (definicja przyjęta zgodnie z normą PN-ISO/IEC 27005:2011). W ramach procesu „szacowanie ryzyka" ujęto takie zadania, jak: ustalenie kontekstu, ocena ryzyka, postępowanie z ryzykiem oraz jego monitorowanie i przegląd.
- **Właściciel aktywów** – jest to osoba odpowiedzialna w danym podmiocie za konkretny proces przetwarzania danych i mająca prawo do podejmowania w tym zakresie decyzji, np. dyrektor departamentu, kierownik określonej komórki w organizacji.
- **Zabezpieczenie** - jest to środek, którego celem jest zmniejszenie ryzyka poprzez obniżenie prawdopodobieństwa zrealizowania zagrożenia (czyli wykorzystania istniejącej podatności) lub też minimalizację potencjalnych strat związanych ze

zrealizowanym zagrożeniem, np. program antywirusowy, drzwi antywłamaniowe, stosowanie procedury bezpieczeństwa.

- **Zagrożenie** - jest to źródło potencjalnej szkody, np. zagrożenie naruszenia integralności danych.

2. DEFINICJA BEZPIECZEŃSTWA INFORMACJI

Bezpieczeństwo informacji postrzegane jest przez pryzmat zachowania jego podstawowych cech, definiowanych jako:

- **Poufność** – cecha informacji określająca, że do informacji mają dostęp tylko osoby uprawnione, a wszelkie próby nieuprawnionego dostępu są uniemożliwione dzięki wdrożeniom odpowiednich zabezpieczeń.
- **Integralność** – cecha informacji, dzięki której informacje pozostają kompletne i prawidłowe (pozbawione błędów i przekłamań).
- **Dostępność** – cecha informacji określająca, że informacja jest dostępna dla uprawnionych użytkowników wtedy, gdy mają uzasadnioną potrzebę skorzystania z niej. Celem zarządzania bezpieczeństwem informacji jest zachowanie wszystkich wyżej wymienionych cech. Utrata dowolnej z powyższych cech stanowi naruszenie bezpieczeństwa informacji.

3. PRAWA OSÓB WYNIKAJĄCE Z RODO

Każda osoba powinna mieć kontrolę nad dotyczącymi jej danymi osobowymi, niezależnie od tego kto i w jakim celu te dane przetwarza. Ogólne rozporządzenie o ochronie danych (RODO) przyznaje szereg uprawnień podmiotom danych:

- prawo do bycia poinformowanym o operacjach przetwarzania
- prawo dostępu,
- prawo do sprostowania/uzupełnienia danych,
- prawo do usunięcia danych (prawo do bycia zapomnianym),
- prawo do ograniczenia przetwarzania,
- prawo do przenoszenia danych,
- prawo do sprzeciwu,
- prawo do tego, by nie podlegać profilowaniu.

Prawo dostępu do Danych

Każda osoba, której dane są przetwarzane, ma prawo do wystąpienia do administratora z wnioskiem, o wydanie jej informacji o tym, czy jej dane są przetwarzane, a jeżeli tak, to do uzyskania dostępu do tych danych lub uzyskania ich kopii.

Administrator Danych jest zobowiązany do udzielenia stosownych informacji wnioskodawcy bez nadmiernych opłat oraz bez zbędnej zwłoki, najpóźniej w terminie 1 miesiąca od otrzymania wniosku.

Prawo do poprawienia Danych

Osoba, której dane są przetwarzane przez administratora ma prawo, w razie stwierdzenia nieścisłości w zgromadzonych danych, w każdej chwili spowodować, żeby jej dane zostały poprawione przez administratora bez zbędnej zwłoki.

Ponadto, jeżeli jest to uzasadnione z uwagi na cel przetwarzania jej danych, osoba, której dane dotyczą, ma prawo żądać od administratora uzupełnienia niekompletnych danych.

Prawo do ograniczenia przetwarzania danych

Każda osoba, której dane są przetwarzane, ma prawo żądać ograniczenia ich przetwarzania w następujących przypadkach:

1. jeżeli kwestionuje prawidłowość danych (ograniczenie następuje na okres sprawdzenia prawidłowości danych przez administratora),
2. wniosła sprzeciw wobec przetwarzania (ograniczenie następuje do czasu stwierdzenia czy podstawy administratora do przetwarzania są nadrzędne wobec podstaw sprzeciwu),
3. przetwarzanie jest niezgodne z prawem, a osoba, której Dane dotyczą, sprzeciwia się ich usunięciu, żądając w zamian ograniczenia ich przetwarzania,
4. dane nie są już potrzebne administratorowi do celów przetwarzania, jednakże osoba, której dane dotyczą potrzebuje ich do ustalenia, dochodzenia lub obrony roszczeń prawnych.

W razie ograniczenia przetwarzania danych na wniosek osoby, której dane dotyczą, administrator będzie uprawniony wyłącznie do przechowywania danych tej osoby. Jakiekolwiek przetwarzanie wybiegające poza ich przechowywanie będzie wymagało odrębnej zgody, chyba że przetwarzanie jest niezbędne z uwagi na ochronę roszczeń lub praw innej osoby lub z uwagi na ważne przesłanki interesu publicznego. W takiej sytuacji, przed uchyleniem ograniczenia przetwarzania, administrator jest zobowiązany poinformować o tym fakcie osobę, która żądała ograniczenia.

Prawo do sprzeciwu

Każda osoba, której dane są przetwarzane może w dowolnym momencie wnieść sprzeciw wobec przetwarzania jej danych.

W razie wniesienia takiego sprzeciwu administrator nie może dalej przetwarzać danych osoby, która wniosła sprzeciw, chyba że wykaże on istnienie ważnych, prawnie uzasadnionych, podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, która wniosła sprzeciw.

W przypadku przetwarzania danych do celów marketingu bezpośredniego, osoba, której dane są przetwarzane ma prawo wnieść sprzeciw wobec przetwarzania jej danych w tym celu. Powyższe dotyczy również sprzeciwu wobec profilowania. Administrator jest zobowiązany poinformować osobę o ww. przysługującym jej uprawnieniu najpóźniej przy okazji pierwszego kontaktu, przy czym wspomniana informacja powinna być przedstawiona w sposób wyraźny i łatwy do zrozumienia - odrębnie od innych informacji.

Prawo do bycia zapomnianym (prawo do usunięcia danych)

Każda osoba, której dane są przetwarzane ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych, a administrator ma obowiązek jej dane usunąć bez zbędnej zwłoki, jeżeli zachodzi przynajmniej jedna z następujących okoliczności:

1. dane nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
2. osoba, której dane dotyczą, cofnęła zgodę na przetwarzanie jej danych i nie ma innej podstawy do ich przetwarzania;
3. osoba, której dane dotyczą wniosła sprzeciw wobec przetwarzania jej danych i nie istnieją nadrzędne prawnie uzasadnione podstawy przetwarzania;
4. dane były przetwarzane niezgodnie z prawem;
5. dane muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;
6. dane zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

Ponadto, jeżeli administrator upublicznił dane, to na wniosek osoby, której dane dotyczą - biorąc pod uwagę dostępną technologię i koszt realizacji - jest zobowiązany do podjęcia rozsądnych działań, w tym środków technicznych, by poinformować administratorów przetwarzających te dane, że osoba, której dane dotyczą, żąda, aby administratorzy ci usunęli wszelkie łącza do tych danych, a także kopię lub replikacje tych danych.

Prawo do bycia zapomnianym może zostać ograniczone w sytuacji, gdy przetwarzanie będzie niezbędne z uwagi na:

1. korzystanie z prawa do wolności wypowiedzi i informacji;
2. wywiązanie się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
3. względy interesu publicznego w dziedzinie zdrowia publicznego;
4. cele archiwalne w interesie publicznym, cele badań naukowych lub historycznych lub cele statystycznych, o ile prawdopodobne jest, że prawo do usunięcia danych uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania;
5. ustalenie, dochodzenie lub obronę roszczeń.

Prawo do przenoszenia danych

Osoba, której dane dotyczą, ma, co do zasady, prawo do uzyskania od administratora kopii przekazanych mu danych, w formacie ustrukturyzowanym, powszechnie używanym i maszynowo czytelnym oraz do żądania przesłania tych danych innemu administratorowi.

4. ZASADY PRZETWARZANIA DANYCH

Główne zasady postępowania przy przetwarzaniu danych osobowych wyznacza art. 5 RODO. Z treści art. 5 RODO wynika, iż Administrator Danych przetwarzający dane powinien dokonywać tego zgodnie z poniższymi zasadami.

Zasada zgodności z prawem, rzetelności i przejrzystości

Zgodnie z nią dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą

1. dla osób fizycznych powinno być przejrzyste, że dotyczące ich dane osobowe są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim stopniu te dane osobowe są lub będą przetwarzane
2. wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych danych osobowych mają być łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem,
3. osoby których dane dotyczą należy informować o tożsamości administratora i celach przetwarzania oraz innych informacji mających zapewnić rzetelność i przejrzystość przetwarzania w stosunku do nich,
4. osobom których dane dotyczą należy zapewnić możliwość uzyskania potwierdzenia i informacji o przetwarzanych danych osobowych ich dotyczących,
5. osobom fizycznym należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem,
6. konkretne cele przetwarzania danych osobowych powinny być wyraźne, uzasadnione i określone w momencie ich zbierania,

Zasada ograniczenia celu

Zgodnie z nią dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami:

1. dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami,
2. dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami,

Zasada minimalizacji danych

Zgodnie z nią dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane,

Zasada prawidłowości

Zgodnie z nią dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane,

Zasada ograniczenia przechowywania

Dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane:

1. dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą,
2. aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu,

Zasada integralności i poufności

Dane osobowe muszą być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i poufność, w tym ochronę przed:

1. niedozwolonym lub niezgodnym z prawem przetwarzaniem- czyli nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu,
2. przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych,

Zasada rozliczalności

Administrator jest odpowiedzialny za przestrzeganie powyższych zasad. Musi on być także w stanie wykazać ich przestrzeganie (to po stronie AD leży ciężar dowodu, że przestrzega zasad rozporządzenia RODO) - wynika stąd, że administrator musi być w stanie udowodnić przestrzeganie, opisanego w art. 25 RODO, obowiązku uwzględniania ochrony danych w fazie projektowania oraz zapewnienia domyślnej ochrony danych.

5. POZOSTAŁE ZASADY BEZPIECZEŃSTWA STOSOWANE W URZĘDZIE MIEJSKIM W ŚWIĘTOCHŁOWICACH

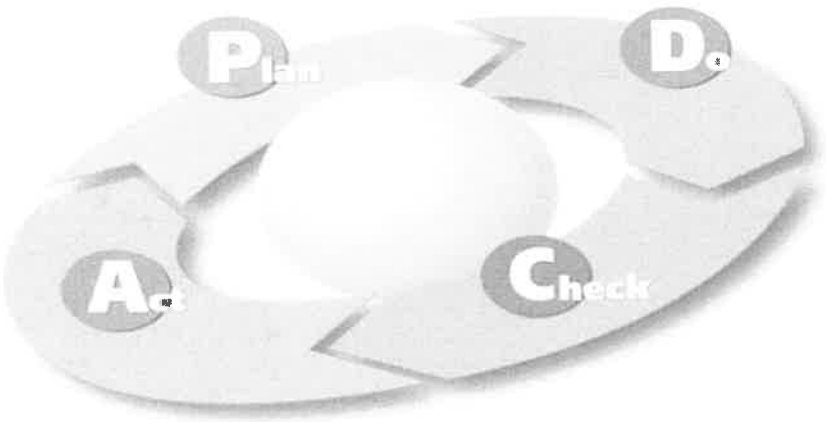
Poniższe zasady stanowią podstawę dla skutecznego zarządzania bezpieczeństwem informacji i są brane pod uwagę przy wprowadzaniu Systemu Bezpieczeństwa:

1. **Zasada uprawnionego dostępu**. Każdy pracownik przeszedł szkolenie z zasad ochrony informacji na platformie https://e-szkolenia.nist.gov.pl/ pt. „Zmiany w zakresie danych osobowych w związku z wejściem w życie RODO", spełnia kryteria dopuszczenia do informacji (posiada upoważnienie do przetwarzania danych osobowych wydane przez Administratora) i podpisał stosowne oświadczenie o zachowaniu poufności.
2. **Zasada przywilejów koniecznych**. Każdy pracownik posiada prawa dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań.

3. **Zasada wiedzy koniecznej**. Każdy pracownik posiada wiedzę o systemie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań.
4. **Zasada świadomości zbiorowej**. Wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych i aktywnie uczestniczą w tym procesie.
5. **Zasada indywidualnej odpowiedzialności**. Za bezpieczeństwo poszczególnych elementów odpowiadają konkretne osoby.
6. **Zasada obecności koniecznej**. Prawo przebywania w określonych miejscach mają tylko osoby upoważnione.
7. **Zasada stałej gotowości**. System jest przygotowany na wszelkie zagrożenia. Niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających.
8. **Zasada adekwatności**. Używane środki techniczne i organizacyjne muszą być adekwatne do sytuacji.
9. **Zasada świadomej konwersacji**. Nie zawsze i wszędzie trzeba mówić, co się wie, ale zawsze i wszędzie trzeba wiedzieć co, gdzie i do kogo się mówi.

7. PROCESOWE PODEJŚCIE DO BEZPIECZEŃSTWA INFORMACJI

Zarządzanie bezpieczeństwem informacji jest stałym procesem, wykonywanym zgodnie z cyklem PDCA, opisanym miedzy innymi w normie ISO/IEC 27001:2013 a pierwotnie opisanym przez dr W. Edwarda Deminga.



Rys: Karn G. Bulsuk (http://karnbulsuk.blogspot.com)

Cykl PDCA zakłada cztery powtarzające się fazy ciągłego doskonalenia procesu:

- Faza P (Plan) – planowanie wdrożenia lub doskonalenia polityki bezpieczeństwa, analiza procesów, planowanie budżetu na bezpieczeństwo itp.
- Faza D (Do) – implementacja, wdrożenie polityki bezpieczeństwa, wdrożenie zmian wynikających z procesów pokontrolnych.
- Faza C (Check) – kontrola stanu faktycznego i porównanie go z planowanym, analiza różnic, identyfikacja źródeł niezgodności.
- Faza A (Act) – działanie, wdrożenie potencjalnych działań naprawczych i doskonalenia.

6. PRZEGLĄDY SYSTEMU BEZPIECZEŃSTWA

Zakłada się, że pełen cykl PDCA dla Systemu Bezpieczeństwa nie powinien przekroczyć jednego roku. Założenie to będzie spełnione przez zrealizowanie przeglądu Systemu Bezpieczeństwa raz na 12 miesięcy. Przegląd Systemu Bezpieczeństwa będzie dokonywany przez Administratora Danych lub upoważnioną do wykonania wskazanej czynności osobę oraz Inspektora Ochrony Danych.

7. CELE POLITYKI BEZPIECZEŃSTWA INFORMACJI

Celem Polityki Bezpieczeństwa Informacji jest wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie wykonać obowiązki w zakresie bezpieczeństwa danych.

8. DEKLARACJA KIEROWNICTWA.

Kierownictwo Urzędu mając na uwadze wartość przetwarzanej w Urzędzie informacji oraz dobro i prawa osób, których dane osobowe przetwarza, pragnie dołożyć szczególnej staranności w ochronę ich interesów. Propaguje aktywne podejście do zarządzania bezpieczeństwem informacji. Kierownictwo deklaruje zaangażowanie w realizację postanowień polityki i propagowanie bezpieczeństwa, w tym bezpieczeństwa informacji wewnątrz organizacji.

9. ZAKRES OBOWIĄZYWANIA POLITYKI BEZPIECZEŃSTWA INFORMACJI

Polityka bezpieczeństwa jest zestawem praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji - danych osobowych. Odnosi się ona do problemów zabezpieczania danych osobowych, zarówno przetwarzanych tradycyjnie, jak i przy wykorzystaniu systemów i technik informatycznych. Polityką Bezpieczeństwa Informacji objęte są wszystkie dane przetwarzane przez organizację, w szczególności dane osobowe zawarte w urządzeniach ewidencyjnych prowadzonych w Urzędzie Miejskim, zarówno w formie papierowej, jak i w systemach informatycznych oraz informacje niejawne. Polityką Bezpieczeństwa Informacji objęte są wszystkie osoby dopuszczone do przetwarzania danych osobowych tj. pracownicy, osoby świadczące pracę na podstawie umowy zlecenia lub o dzieło, praktykanci, stażyści i podmioty zewnętrzne.

10. ODPOWIEDZIALNOŚĆ ZA BEZPIECZEŃSTWO INFORMACJI

Zarządzanie bezpieczeństwem informacji w Urzędzie Miejskim opiera się na następującym podziale odpowiedzialności:

1. **Prezydent Miasta** odpowiedzialny jest za zapewnienie zasobów niezbędnych dla opracowania, wdrożenia, funkcjonowania, utrzymania i doskonalenia Systemu Bezpieczeństwa

Urzędu oraz stosowania poszczególnych zabezpieczeń. Prezydent Miasta wykonuje czynności wynikające z RODO i przypisane Administratorowi Danych, w tym zakresie odpowiada za zarządzanie ryzykiem w zakresie naruszeń oraz czynów zabronionych.

2. **Kierownicy komórek organizacyjnych** odpowiadają za:
   a) Przestrzeganie zasad ochrony informacji przez nich samych, jak i przez podległych im pracowników.
   b) Identyfikowanie i dokumentowanie zagrożeń dla bezpieczeństwa informacji.
   c) Definiowanie oraz realizację działań zapobiegających zagrożeniom.
   d) Zapoznanie pracowników z obowiązkami związanymi z ochroną informacji na stanowiskach pracy.
   e) Przeszkolenie pracowników w zakresie przepisów prawa oraz wewnętrznych zasad przyjętych w pracy, dotyczących ochrony informacji.
   f) Właściwe informowanie stron/właścicieli danych osobowych o przysługujących im prawach z wynikających z przepisów RODO

3. Odpowiedzialność za bezpieczeństwo informacji ponoszą **wszyscy pracownicy** zgodnie z posiadanymi zakresami obowiązków.

4. Każdy pracownik obowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania informacji zgodnie z obowiązującymi w Urzędzie przepisami wewnętrznymi w tym m. in:
   a) Stosować zasady opisane w polityce oraz innych dokumentach wewnętrznych Urzędu.
   b) Chronić informacje podlegające ochronie przed dostępem do nich osób nieuprawnionych.
   c) Chronić dane przed przypadkowym lub umyślnym zniszczeniem, utratą lub modyfikacją.
   d) Chronić sprzęt, wydruki komputerowe i inne nośniki zawierające dane chronione,
   e) Utrzymywać w tajemnicy powierzone hasła, częstotliwości ich zmiany oraz szczegóły technologiczne systemów także po ustaniu zatrudnienia w Urzędzie.
   f) Stosować się do szczegółowych zaleceń w zakresie ochrony antywirusowej, a także do innych zaleceń wynikających z Systemu Bezpieczeństwa Urzędu.
   g) Powiadomić Inspektora Ochrony Danych lub bezpośredniego przełożonego o:
      - Ujawnieniu lub możliwości ujawnienia informacji chronionych osobom nieupoważnionym.
      - Nieautoryzowanej zmianie informacji chronionych lub możliwości wprowadzenia nieautoryzowanych zmian.
      - Zniszczeniu lub możliwości zniszczenia informacji chronionych.
      - Zablokowaniu lub możliwości zablokowania pracy systemu informatycznego przetwarzającego informacje chronione lub uniemożliwienia innego dostępu do informacji chronionych.

12. STRUKTURA SYSTEMU BEZPIECZEŃSTWA

1. **Administrator Danych**

a) wprowadza, zarządza i sprawuje nadzór nad działaniem Systemu Bezpieczeństwa,
b) określa rodzaje zasobów podlegających ochronie,
c) decyduje o celach i środkach przetwarzania danych.

2. **Inspektor Ochrony Danych**

a) sprawuje nadzór nad realizacją zapisów Polityki Bezpieczeństwa Informacji,
b) analizuje raporty z wszelkich zdarzeń związanych z bezpieczeństwem wszystkich zasobów chronionych,
c) monitoruje zachowanie właściwego poziomu bezpieczeństwa informacji,
d) przedstawia okresowy raport o stanie bezpieczeństwa informacji.
e) analizuje ryzyko bezpieczeństwa danych osobowych
f) wykonuje czynności wynikające z zapisów RODO

3. **Administrator Systemu Informatycznego**

a) monitoruje oraz zapewnia ciągłość działania systemu IT,
b) utrzymuje rejestr ważnych aktywów w zakresie systemu informatycznego,
c) utrzymuje konfigurację i wydajność systemu teleinformatycznego,
d) instaluje i konfiguruje sprzęt, systemy i aplikacje,
e) odpowiada za administrację oprogramowaniem systemowym w stopniu umożliwiającym zachowanie bezpieczeństwa systemu i zabezpieczenie danych przed nieupoważnionym dostępem,
f) współpracuje z dostawcami aplikacji,
g) nadzoruje wdrożone aplikacje,
h) zarządza kopiami awaryjnymi danych
i) opracowuje dokumentacje dla systemów teleinformatycznych,
j) opracowuje standardy dotyczące systemów teleinformatycznych,
k) opracowuje procedury określające zarządzanie systemem teleinformatycznym.

13. MIEJSCE /OBSZARY/ZBIORY/REJESTRY PRZETWARZANIA DANYCH OSOBOWYCH

Jako miejsce przetwarzania danych osobowych wyznacza się wszystkie budynki Urzędu Miejskiego w Świętochłowicach, w tym pomieszczenia, w których umożliwiono pracę w systemie informatycznym Urzędu.

1. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe stanowi załącznik nr 1.
2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych stanowi załącznik nr 2.
3. Opis struktury zbiorów danych osobowych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi stanowi załącznik nr 3.

4. Sposób przepływu danych osobowych pomiędzy poszczególnymi systemami stanowi załącznik nr 4.
5. Rejestr czynności przetwarzania stanowi załącznik nr 5.

14. PRZETWARZANIE DANYCH OSOBOWYCH

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych, nadane przez Administratora Danych. Upoważnienie do przetwarzania danych osobowych uzyskuje osoba, której stanowisko pracy wymaga takiego upoważnienia. Upoważnienie określa zakres dostępu do przetwarzania w zakresie poszczególnych celów przetwarzania (dawniej tzw. zbiorów danych osobowych) zarówno w systemie tradycyjnym, jak i elektronicznym
2. Upoważnienie do przetwarzania danych osobowych muszą uzyskać również osoby, pracujące na terenie Urzędu, nie będące etatowymi pracownikami Urzędu Miejskiego: w tym stażyści i praktykanci, pracownicy podmiotów zewnętrznych oraz inne osoby krótkoterminowo upoważnione.
3. Zmiana stanowiska pracy, związana z koniecznością uzyskania dostępu do przetwarzania danych osobowych w innych celach niż dotychczas, wymaga unieważnienia dotychczasowego upoważnienia do przetwarzania danych osobowych oraz nadania nowego upoważnienia do przetwarzania danych osobowych.
4. Każdy pracownik Urzędu, który otrzyma upoważnienie do przetwarzania danych osobowych, zobowiązuje się pisemnie do zachowania w tajemnicy tych danych oraz sposobów ich zabezpieczania.
5. W przypadku współpracy z wykonawcami przetwarzającymi dane osobowe Wydział odpowiedzialny za współpracę zawiera pisemną umowę powierzenia przetwarzania danych.

15. WYDAWANIE UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Upoważnienia do przetwarzania danych osobowych w Urzędzie Miejskim w Świętochłowicach wydaje Administrator Danych.
2. Upoważnienia dla wszystkich pracowników wydawane są za pośrednictwem Wydziału Organizacyjnego.
3. Rejestr upoważnień do przetwarzania danych osobowych prowadzi Wydział Organizacyjny Urzędu Miejskiego w Świętochłowicach.
4. Wydane upoważnienie jest jednocześnie dokumentem upoważniającym Administratora Systemu Informatycznego do założenia profilu użytkownika w ramach danej komórki organizacyjnej w której pracownik będzie wykonywał czynności służbowe.
5. Upoważnienie wygasa z momentem rozwiązania stosunku pracy lub odpowiedniej umowy oraz z upływem czasu na jaki zostało wydane. Z momentem złożenia podpisu na karcie obiegowej Administrator Systemu Informatycznego usuwa przyznane

użytkownikowi uprawnienia do korzystania z systemu, nie usuwając konta i informacji zgromadzonych przez pracownika.

16. SZKOLENIA

Wszyscy pracownicy Urzędu przechodzą szkolenia z zakresu bezpieczeństwa informacji, w tym z ochrony danych osobowych. Inspektor Ochrony Danych lub Administrator Systemu Informatycznego najpóźniej w dniu dopuszczenia do pracy w systemie prowadzi indywidualne szkolenie dla dopuszczanego pracownika. W trakcie szkolenia pracownik zostaje zapoznany z zakresem swoich uprawnień (dotyczy również systemu informatycznego) wynikających z pełnionego stanowiska i potwierdza zrozumienie warunków dostępu do systemu. Ponadto każdy pracownik jest zobowiązany do odbycia szkolenia na platformie https://e-szkolenia.nist.gov.pl/, „Zmiany w zakresie danych osobowych w związku z wejściem w życie RODO"

17. OPIS SYSTEMÓW INFORMATYCZNYCH

W Urzędzie funkcjonuje system informatyczny, przetwarzający informacje, w tym dane osobowe, w formie elektronicznej. Przez obszar systemu objęty niniejszą Polityką rozumie się wszelkie urządzenia techniczne niezbędne do funkcjonowania systemu informatycznego w danej jednostce organizacyjnej, w którym wykonywane są zadania związane z wprowadzaniem, przetwarzaniem oraz archiwizowaniem danych osobowych lub korzystaniem ze zbiorów zawierających dane osobowe oraz pomieszczenia, w których te urządzenia się znajdują.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych stanowi załącznik nr 6.

18. STANDARDY AKCEPTOWALNEGO WYKORZYSTYWANIA SPRZĘTU SŁUŻBOWEGO

Każdy pracownik zobowiązany jest do przestrzegania wszelkich regulacji dotyczących obszaru zarządzania bezpieczeństwem informacji. Pracownicy Urzędu muszą być świadomi faktu, że wszystkie systemy informatyczne, w tym telekomunikacyjne, są przeznaczone do użytku służbowego i nie zapewniają prywatności w przypadku wykorzystywania ich do celów pozasłużbowych. Obowiązkiem Administratora Systemu Informatycznego jest okresowe przeglądanie systemów, w tym sposobu wykorzystywania ich przez pracowników i działania pozasłużbowe nie są wyłączone z takich przeglądów. Zakłada się wykorzystanie systemów jedynie dla celów służbowych.

19. PRACOWNICY URZĘDU MIEJSKIEGO NIE MOGĄ WYKORZYSTYWAĆ SPRZĘTU SŁUŻBOWEGO:

- Do działań sprzecznych z przepisami prawa, w tym do przechowywania, przetwarzania lub przesyłania materiałów nielegalnych (w rozumieniu prawa autorskiego, kodeksu karnego innych obowiązujących przepisów prawa).
- Do przesyłania lub wyświetlania materiałów, które mogą narazić inne osoby na otrzymanie lub zobaczenie treści dla nich obraźliwych lub krzywdzących.
- Do podszywania się pod inne osoby lub systemy.
- Do prób uzyskania informacji, do której nie mają dostępu z racji pełnionych funkcji i obowiązków na nich nałożonych (stanowi to naruszenie zasady wiedzy koniecznej).
- Do podłączania nieautoryzowanych urządzeń do sieci Urzędu.
- Do nieautoryzowanego (samodzielnego) odłączania lub przenoszenia urządzeń IT.
- Do samodzielnego instalowania nieautoryzowanego przez organizację oprogramowania.

20. OPIS ZAGROŻEŃ:

Do najważniejszych zagrożeń związanych z bezpieczeństwem informacji należą:

- Kradzież, zniszczenie lub zagubienie dokumentacji, w tym dokumentacji w formie elektronicznej, za pomocą której osoba nieuprawniona może doprowadzić do naruszenia lub czynu zabronionego, zgodnie z wytycznymi RODO
- Kradzież sprzętu elektronicznego: komputera, notebooka, pendrive'a zawierającego dane wrażliwe,
- Obecność wirusa komputerowego,
- Pozostawienie niezabezpieczonych dokumentów,
- Pozostawienie otwartego pomieszczenia podczas nieobecności pracowników,
- Włamanie do pomieszczenia Urzędu,
- Wyciek informacji do osób nieupoważnionych.
- Udostępnienie dokumentów osobie nieuprawnionej.

21. SPOSOBY ZABEZPIECZANIA INFORMACJI

21.1. KONTROLA DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

1. Każda osoba upoważniona do przetwarzania danych w systemie informatycznym, posiada konto użytkownika zakładane przez Administratora
2. Systemu Informatycznego Każde nowe konto użytkownika systemu, jak również wszelkie zmiany w zakresie kont wykonywane są na pisemny wniosek Kierownika komórki organizacyjnej, kierowany do Administratora Systemu Informatycznego na adres mailowy pomoc@swietochlowice.pl. Zgłoszenia ustne lub papierowe będą przyjmowane tylko i wyłącznie w szczególnie uzasadnionych przypadkach.

3. W ramach utworzonego konta, użytkownik otrzymuje identyfikator oraz hasło dostępu.
4. System informatyczny Urzędu wymusza zmianę haseł dostępu nie rzadziej niż co 30 dni.
5. Pracownik jest zobowiązany do zmiany hasła dostępu na kolejny miesiąc w odpowiednim terminie. Konieczność zmiany hasła jest sygnalizowana przez system
6. Hasło należy zachować w tajemnicy i zabezpieczyć przed dostępem osób trzecich.
7. Zabrania się przekazywania haseł dostępu innym pracownikom Urzędu a także – zwłaszcza - osobom niezwiązanym z organizacją pod rygorem zastosowania odpowiedzialności dyscyplinarnej, wynikającej z przepisów określonych w Rozdziale IV Ustawy Kodeks Pracy.
8. Zabrania się zapisywania haseł w miejscach umożliwiających przejęcie przez osoby nieupoważnione oraz umożliwiających identyfikację właściciela, użytkownika systemu.
9. Konieczne jest wykonywanie swoich obowiązków pracy w ramach własnego konta użytkownika. Niedopuszczalne jest korzystanie z jednego konta użytkownika przez wiele osób.
10. Odpowiedzialność za wprowadzenie do systemu informacji błędnych, niezgodnych z prawem lub też zagrażających Urzędu, będzie nakładana na właścicieli kont, niezależnie od faktu, czy zostały one przez niego wprowadzone.
11. Administrator Systemu Informatycznego zobowiązany jest do niezwłocznego informowania Administratora Danych za pośrednictwem Inspektora Ochrony Danych o każdorazowym przypadku nieprzestrzegania powyższych zapisów.

21.2. ZASADY DOTYCZĄCE KONT I HASEŁ

- Minimalna długość hasła: 8 znaków
- Maksymalny czas życia hasła: 30 dni
- Ilość nieudanych prób logowania przed zablokowaniem konta: 5 prób
- Zasady złożoności hasła:
- Nie mogą zawierać nazwy konta użytkownika ani części jego pełnej nazwy dłuższej niż dwa kolejne znaki.
- Muszą zawierać znaki z trzech spośród następujących czterech kategorii:
- Wielkie litery angielskie (od A do Z)
- Małe litery angielskie (od a do z)
- Cyfry systemu dziesiętnego (od 0 do 9)
- Znaki niealfabetyczne (na przykład !, $, #, %)
- Wymagania dotyczące złożoności są wymuszane podczas zmienienia lub tworzenia hasła.

21.3. POLITYKA CZYSTEGO BIURKA I CZYSTEGO EKRANU

Obowiązkiem pracowników Urzędu Miejskiego jest zadbanie, aby informacje wrażliwe, w tym dane osobowe, nie były udostępnione osobom nieuprawnionym. Polityka czystego biurka oznacza, że informacje wrażliwe nie mogą zostać na biurku podczas nieobecności pracownika – musi on wcześniej odpowiednio je zabezpieczyć (np. przez schowanie ich w szafce zamykanej na zamek). Polityka czystego ekranu oznacza obowiązek zablokowania ekranu komputera przed odejściem od niego, poprzez stosowanie, wygaszacza ekranu chronionego hasłem z czasem ustawionym na okres nie dłuższy niż 10 minut.

21.4. ZARZĄDZANIE INCYDENTAMI I NARUSZENIAMI

Wszelkie incydenty noszące znamiona naruszenia polityki bezpieczeństwa (a więc w szczególności noszące znamiona intencjonalnych działań mających na celu narażenie informacji wrażliwych na nieuprawnione ujawnienie, uniemożliwienie dostępu do nich lub spowodowanie naruszenia ich integralności) są zgłaszane przez pracowników Urzędu do Przełożonego lub Inspektora Ochrony Danych. Zgłoszenie incydentu, a także zagrożenia bezpieczeństwa danych osobowych następuje w drodze mailowej na adres pomoc@swietochlowice.pl oraz iod@swietochlowice.pl – wiadomość powinna zawierać tytuł INCYDENT/ZAGROŻENIE DANYCH OSOBOWYCH. Inspektora Ochrony Danych. weryfikuje czy zgłoszenie jest zgłoszeniem incydentu w myśl przyjętego Systemu Bezpieczeństwa Informacji Urzędu.

Do typowych zagrożeń bezpieczeństwa danych osobowych należą:

- niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
- niewłaściwe zabezpieczenie sprzętu IT lub oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
- nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np.: niestosowanie ochrony haseł, niezamykanie pomieszczeń).

Do typowych incydentów bezpieczeństwa danych osobowych należą:

- zdarzenia losowe zewnętrzne (np.: pożar obiektu / pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
- zdarzenia losowe wewnętrzne (np.: awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki użytkowników, utrata / zagubienie danych),
- umyślne incydenty (np.: 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).

Po potwierdzeniu przez Inspektora Ochrony Danych., iż zgłoszone odstępstwo jest incydentem Inspektor Ochrony Danych. podejmuje następujące działania:

- Informuje kierownictwo Urzędu o zaistniałym incydencie.

- Weryfikuje przyczyny wystąpienia incydentu. ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały
- Sprawdza czy podczas incydentu nie doszło do naruszenia danych osobowych wrażliwych opisanych w art. 9 i art. 10 RODO.
- Weryfikuje czy podczas incydentu nie doszło do czynu zabronionego w oparciu o dane osobowe Urzędu.
- zabezpiecza ewentualne dowody, ustala osoby odpowiedzialne za naruszenie
- Wprowadza działania korygujące mające na celu niedopuszczenie do powtórzenia incydentu.
- Informuję osobę zgłaszającą incydent o procedurze skorygowania incydentu.
- O ile to konieczne informuje pracowników Urzędu o zaistniałym incydencie i jego skutkach dla Systemu Bezpieczeństwa Informacji oraz dla Urzędu.
- Dokumentuje prowadzone postępowanie.

UWAGA: naruszenie danych osobowych wrażliwych za pomocą którego dojdzie do czynu zabronionego należy poddać analizie ryzyka oraz jeżeli jest konieczność zgłosić do Urzędu Ochrony Danych Osobowych (dotychczas Generalnego Inspektora Danych Osobowych) do 72 godzin od momentu powzięcia informacji o naruszeniu dodatkowo należy powiadomić osoby, których dane zostały wykorzystane do realizacji naruszenia.

Po potwierdzeniu przez Inspektora Ochrony Danych., iż zgłoszone odstępstwo jest zagrożeniem Inspektor Ochrony Danych. podejmuje następujące działania:

- ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,
- rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości.

22. KONSEKWENCJE NARUSZANIA POLITYKI BEZPIECZEŃSTWA INFORMACJI

Przypadki nieuzasadnionego zaniechania obowiązków wynikających z obowiązującej Polityki Bezpieczeństwa Informacji w Urzędzie mogą być potraktowane jako celowe naruszenie obowiązków pracownika. Wyciągnięte konsekwencje służbowe nie wykluczają możliwości wniesienia sprawy z powództwa cywilnego o naprawienie szkody.

23. POSTANOWIENIA KOŃCOWE

1. Polityka Bezpieczeństwa jest dokumentem wewnętrznym i nie może być udostępniania osobom i instytucjom postronnym w żadnej formie bez zgody ADO.
2. Osoby przetwarzające dane osobowe zobowiązane są do stosowania postanowień zawartych w niniejszej Polityce.
3. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.

4. W sprawach nieuregulowanych w niniejszej Polityce Bezpieczeństwa mają zastosowanie przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/4/WE, ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz 1000) oraz wydane na ich podstawie akty wykonawcze.

PREZYDENT MIASTA
Daniel Beger

INSTRUKCJA BEZPIECZEŃSTWA SYSTEMU TELEINFORMATYCZNEGO

W URZĘDZIE MIEJSKIM W ŚWIĘTOCHŁOWICACH

INSTRUKCJA BEZPIECZEŃSTWA SYSTEMU TELEINFORMATYCZNEGO

Dokument spełnia wymagania Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

1. CELE INSTRUKCJI BEZPIECZEŃSTWA SYSTEMU TELEINFORMATYCZNEGO

Celem Instrukcji jest wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie wykonać obowiązki w zakresie przetwarzania danych osobowych w systemach informatycznych Urzędu.

2. ODPOWIEDZIALNOŚĆ ZA BEZPIECZEŃSTWO I ZARZĄDZANIE SYSTEMAMI

Administrator Danych – odpowiedzialny jest za zabezpieczenia systemu informatycznego oraz dopuszczenie osób do pracy w systemie. Administrator Danych formalnie inicjuje kontrolę systemu informatycznego.

Inspektor Ochrony Danych jest upoważniony do:

a) prowadzenia kontroli prawidłowości przestrzegania Instrukcji Bezpieczeństwa Systemu Teleinformatycznego w całym zakresie jej obowiązywania,
b) wprowadzania zaleceń oraz wydawania poleceń dla wszystkich osób dopuszczonych do systemu – w zakresie niesprzecznym z niniejszą Instrukcją,

Inspektor Ochrony Danych odpowiada również za zabezpieczenie obsługi systemów przez **Administratora Systemu Informatycznego** w przypadku uszkodzenia, awarii lub naruszenia bezpieczeństwa systemu.

Obowiązki **Administratora Systemu Informatycznego**:

a) wykonywanie czynności wynikających z niniejszej Instrukcji w zakresie zabezpieczenia prawidłowego i bezpiecznego funkcjonowania bazy technicznej i oprogramowania, wykonywanie czynności wynikających z niniejszej Instrukcji, związanych z zapewnieniem bezpieczeństwa systemu informatycznego, w tym:
   - wprowadzenia lub usuwanie prawa dostępu do systemu informatycznego dla poszczególnych pracowników na podstawie upoważnienia do przetwarzania danych osobowych,
   - opracowania systemu haseł do poszczególnych obszarów systemu,
   - zapewnienia konfiguracji systemu uniemożliwiającej wprowadzanie lub uzyskiwanie danych z systemu przez niepowołane osoby,
   - przeprowadzanie kontroli systemu informatycznego z polecenia Inspektora Ochrony Danych,
   - monitorowanie bezpieczeństwa dla serwerów oraz urządzeń aktywnych sieci,

- opracowywanie tematyki szkoleń z zakresu systemu oraz urządzeń dla użytkowników systemu – ze szczególną dbałością o wiedzę z zakresu bezpieczeństwa systemów.
- czuwanie zgodnie z wytycznymi niniejszej Instrukcji nad prawidłowością postępowania z nośnikami zawierającymi dane systemu,
- prowadzenie rzetelnej dokumentacji systemu i czuwanie nad prawidłowością sporządzania tej dokumentacji przez inne osoby,
- zapewnienie stałego kontaktu ze sobą lub osobą wskazaną, zaś w przypadku wyjazdów lub niemożności wykonywania swoich obowiązków, powiadomienie o tym fakcie Inspektora Ochrony Danych.

Administrator Systemu Informatycznego posiada następujące kompetencje:

a) przeprowadzanie kontroli systemu informatycznego,
b) podejmowanie kroków zaradczych, w tym wyłączanie systemu lub częściowe ograniczanie dostępu do niego, jeżeli w jego ocenie istnieje zagrożenie dla prawidłowego funkcjonowania systemu lub bezpieczeństwa danych w nim się znajdujących.

Użytkownik Systemu

Użytkownikiem systemu jest osoba, która w ramach swoich obowiązków służbowych korzysta z systemu informatycznego w Urzędzie. Dopuszczenia użytkownika do systemu dokonuje Administrator Systemu Informatycznego.

3. OPIS SYSTEMU

Przez obszar systemu objęty niniejszą Instrukcją rozumie się wszelkie urządzenia techniczne, systemy oraz aplikacje niezbędne do funkcjonowania systemu informatycznego w Urzędzie, w którym wykonywane są zadania związane z wprowadzaniem, przetwarzaniem oraz archiwizowaniem danych osobowych lub korzystaniem ze zbiorów zawierających dane osobowe oraz pomieszczenia, w których te urządzenia się znajdują.

4. SPOSÓB UŻYTKOWANIA SYSTEMU

1. System informatyczny eksploatowany jest na komputerach wolnostojących i przenośnych podłączonych do sieci lokalnej Urzędu.
2. Dołączanie do systemu innych urządzeń teletransmisyjnych, nie należących do struktury sieci musi zostać zgłoszone do Administratora Systemu Informatycznego.
3. Podłączenie prywatnego komputera lub komputera przenośnego wymaga uzyskania zezwolenia Administratora Danych.
4. Dostęp do poszczególnych obszarów systemu jest zabezpieczony za pomocą haseł według hierarchii dostępu opracowanej przez Administratora Systemu Informatycznego, sprawdzonej pod względem formalnym przez Inspektora Ochrony Danych .
5. W szczególności zabezpieczeniom za pomocą haseł podlega:
   a) dostęp do serwerów sieciowych,

b) dostęp do urządzeń aktywnych sieci,
c) dostęp do konfiguracji serwerów,
d) dostęp do konfiguracji stacji roboczych,
e) dostęp do systemu dla poszczególnych użytkowników systemu,

6. Konfiguracja serwerów oraz aplikacji zapewniają odporność systemu na zanik zasilania energetycznego lub inne przypadkowe uszkodzenia poszczególnych stacji roboczych. W szczególności:
   a) Serwery są zasilane wyłącznie przez urządzenia zasilające UPS.
   b) Za prawidłowość podłączenia, monitorowanie stanu baterii odpowiada Administrator Systemu Informatycznego.
   c) Konfiguracja serwerów zapewnia automatyczne bezpieczne wyłączanie serwera w wypadku zaniku zasilania energetycznego, dłuższego niż czas podtrzymania dobranego UPS.
   d) Administrator Systemu Informatycznego odpowiedzialny jest za wykonanie przynajmniej jednego próbnego zamknięcia awaryjnego systemów w kwartale.
7. Konfiguracja w systemie musi zapewnić odnotowanie w systemie faktu rozpoczęcia pracy przez każdego z użytkowników, Wykaz logów podlega zabezpieczeniu łącznie z danymi systemu.
8. Konfiguracja systemów powinna zapewniać możliwość pozyskania informacji o realizacji praw osób fizycznych, w tym prawa do: dostępu do danych, modyfikacji danych, kopiowania danych, przenoszenia danych, usunięcia danych.

UWAGA – każdy system i aplikacja powinny posiadać informację o zgodności rozwiązań technicznych z wytycznymi RODO.

5. BEZPIECZEŃSTWO ZARZĄDZANIA SYSTEMU TELEINFORMATYCZNEGO:

5.1 . KOPIE BEZPIECZEŃSTWA

1. Użytkownicy są świadomi, że archiwizacji podlegają dane zapisane na dyskach sieciowych udostępnianych na potrzeby poszczególnych komórek organizacyjnych oraz dysków prywatnych użytkowników zlokalizowanych na dysku sieciowym. Z dysków tych wykonywana jest codzienna pełna kopia.
2. Administrator Systemu Informatycznego konfiguruje kopie w ten sposób, że po zakończeniu pracy Urzędu dane z serwera plików i serwerów bazodanowych są przenoszone na serwer kopii zapasowych.
3. Z serwera kopii zapasowych prowadzony jest pełen zapisanych na dysk zewnętrzny.
4. Wszystkie kopie bezpieczeństwa i backupy powinny być zlokalizowane w innej strefie pożarowej budynku Urzędu.

5.2. ZABEZPIECZENIE ANTYWIRUSOWE

1. Za politykę antywirusową odpowiedzialny jest Administrator Systemu Informatycznego.

2. Program antywirusowy i konfiguracja systemu zapewniają kontrolę całego systemu informatycznego:
   a) na bieżąco,
   b) przynajmniej raz dziennie, jeżeli z przyczyn technicznych nie możliwe jest jej zapewnienie na bieżąco,
   c) każdorazowo przy korzystaniu z nośników wymienialnych,

5.3. KORZYSTANIE Z POCZTY ELEKTRONICZNEJ

1. Poczta elektroniczna może być wykorzystywana tylko do celów służbowych.
2. Zabrania się rozsyłania m.in.:
   a) ogłoszeń komercyjnych,
   b) tzw. łańcuszków szczęścia (listów, które wykorzystując elementy socjotechniki generują niepożądany ruch na serwerach poczty elektronicznej),
   c) treści wulgarnych,
   d) materiałów erotycznych,
   e) treści niezgodnych z obowiązującymi przepisami prawa,
   f) treści prawem chronionych bez odpowiedniego zabezpieczenia np. szyfrowanie.
3. Korespondencja, którą przechowuje i dostarcza system pocztowy jest własnością Pracodawcy. Pracodawca w celach dowodowych oraz bezpieczeństwa systemów ma prawo do kontroli skrzynek pocztowych użytkowników. O wynikach kontroli powinien być poinformowany użytkownik. 4. Korespondencja elektroniczna, jak i pliki mogą zostać udostępnione innemu pracownikowi. Czynności tej dokonać można na pisemny wniosek przełożonego pracownika, którego dane mają zostać udostępnione. We wniosku wskazuje się powód udostępnienia oraz osobę, której udostępnia się opisywane zasoby.
4. Pracodawca rezerwuje sobie prawo natychmiastowej blokady skrzynki pocztowej w uzasadnionych przypadkach. Nadzór i opiekę techniczną nad systemem poczty elektronicznej sprawuje ASI.

5.4. KORZYSTANIE Z SIECI INTERNET

1. Użytkownicy mogą korzystać z dostępu do Internetu tylko w celach służbowych a praca w sieci Internet nie może zagrażać bezpieczeństwu systemów informatycznych.
2. Pracodawca może wprowadzić kategoryzację stron internetowych oraz zablokować dostęp do wybranych kategorii.
3. Zabrania się:
   a) wykorzystywania sieci Internet w sposób, który mógłby narazić organizację na utratę dobrego imienia,
   b) pobierania oprogramowania (w tym w wersjach darmowych), nie związanego z wykonywanymi obowiązkami służbowymi,
   c) instalowania urządzeń udostępniających Internet na sprzęcie Pracodawcy bez zgody Administratora Systemu Informatycznego.

PREZYDENT MIASTA
Daniel Begier

Załącznik nr 2
do Polityki Bezpieczeństwa

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

L.p.	Nazwa zbioru	Nazwa programu
1	Ewidencja przedsiębiorców, którzy zakończyli wykonywanie działalności gospodarczej przed dniem 1 lipca 2011	SEDziG
2	Ewidencja gruntów i budynków Gminy Świętochłowice	EwOpis
3	Wymiar i pobór podatku od nieruchomości	PON, Firma, Posesja
4	Wymiar i pobór podatku rolnego	PON-ROL
5	Wymiar i pobór podatku od środków transportowych	POD-PRZY, POD-0560, Pojazd
6	Rejestr skarg	*forma papierowa*
7	Zezwolenia na sprzedaż napojów alkoholowych	Koncesja
8	Ewidencja kierowców	Kierowca
9	Ewidencja zezwoleń transportowych	*forma papierowa*
10	Ewidencja pojazdów	Rejestr
11	Rejestr mieszkańców	PB_EWID2
12	Rejestracja urodzeń, małżeństw i zgonów	PB_USC
13	Wieczyste użytkowanie i dzierżawa gruntów	Umowy, UW
14	Ewidencja zgłaszania i przyjmowania do zasobu prac geodezyjnych i kartograficznych na obszarze Gminy Świętochłowice	Ośrodek

15	Ewidencja uzgadniania usytuowania projektowanych sieci uzbrojenia terenu na obszarze Gminy Świętochłowice	Ośrodek
16	Protokoły ustaleń Prezydenta Miasta	*forma papierowa*
17	Rejestr wniosków	*forma papierowa*
18	Rejestr podań wnoszonych ustnie do Prezydenta Miasta	*forma papierowa*
19	System obiegu dokumentów	e-SOD
20	Akta osobowe oraz inne dokumenty pracownicze	QUORUM
21	Ewidencja zgłoszonych i wykonanych interwencji oraz wwidencja mandatów karnych Straży Miejskiej w Świętochłowicach	eMandat
22	Odpady komunalne	EkoKosz, EkoKosz2, Odpady
23	Uprawnienia do badań technicznych pojazdów	*forma papierowa*
24	Ewidencja instruktorów	*forma papierowa*
25	Ewidencja wykładowców	*forma papierowa*
26	Kandydaci na ławników	*forma papierowa*
27	Rejestr zamieszkania cudzoziemców	PB_EWID2
28	Rejestr sprzętu pływającego służącego do połowu ryb	*forma papierowa*
29	Stały rejestr wyborców	PB_EWID2
30	Dokumentacja wyborcza i referendalna	*forma papierowa*
31	Rejestracja i kwalifikacja wojskowa	*forma papierowa*
32	Świadczenia na rzecz obrony	*forma papierowa*

33	Ewidencja obiektów świadczących usługi hotelarskie, nie będące obiektami hotelarskimi oraz pól biwakowych	*forma papierowa*
34	Ewidencja stowarzyszeń zwykłych	*forma papierowa*
35	Konsultacje społeczne Gminy Świętochłowice	*forma papierowa*

PREZYDENT MIASTA
Daniel Beger

Załącznik nr 3
do Polityki Bezpieczeństwa

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

Opis struktury przetwarzanych danych osobowych oraz relacji pomiędzy danymi, procesy przetwarzania oraz struktura danych zostały zawarte w dokumentacji technicznej systemów informatycznych dostępnej u dostawców oprogramowania.

L.p.	Nazwa zbioru	Struktura danych
1	Ewidencja przedsiębiorców, którzy zakończyli wykonywanie działalności gospodarczej przed dniem 1 lipca 2011	Nazwiska i imiona, adres zamieszkania lub pobytu, miejsce pracy, PESEL
2	Ewidencja gruntów i budynków Gminy Świętochłowice	Nazwiska i imiona, imiona rodziców, adres zamieszkania lub pobytu, numer ewidencyjny PESEL
3	Wymiar i pobór podatku od nieruchomości	Nazwiska i imiona, adres zamieszkania lub pobytu
4	Wymiar i pobór podatku rolnego	Nazwiska i imiona, adres zamieszkania lub pobytu
5	Wymiar i pobór podatku od środków transportowych	Nazwiska i imiona, adres zamieszkania lub pobytu
6	Rejestr skarg	Nazwiska i imiona, adres zamieszkania lub pobytu
7	Zezwolenia na sprzedaż napojów alkoholowych	Nazwiska i imiona, adres zamieszkania lub pobytu, miejsce pracy
8	Ewidencja kierowców	Nazwiska i imiona, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL
9	Ewidencja zezwoleń transportowych	Nazwiska i imiona, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL

10	Ewidencja pojazdów	Nazwiska i imiona, adres zamieszkania lub pobytu, numer ewidencyjny PESEL
11	Rejestr mieszkańców	Nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, miejsce pracy, zawód, wykształcenie, seria i numer dowodu osobistego, obywatelstwo, stan cywilny, stosunek do powszechnego obowiązku obrony kraju
12	Rejestracja urodzeń, małżeństw i zgonów	Nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, wykształcenie, seria i numer dowodu osobistego
13	Wieczyste użytkowanie i dzierżawa gruntów	Nazwiska i imiona, adres zamieszkania lub pobytu
14	Ewidencja zgłaszania i przyjmowania do zasobu prac geodezyjnych i kartograficznych na obszarze Gminy Świętochłowice	Nazwiska i imiona, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, Numer Identyfikacji Podatkowej, miejsce pracy, numer uprawnień zawodowych
15	Ewidencja uzgadniania usytuowania projektowanych sieci uzbrojenia terenu na obszarze Gminy Świętochłowice	Nazwiska i imiona, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, Numer Identyfikacji Podatkowej, miejsce pracy
16	Protokoły ustaleń Prezydenta Miasta	Nazwiska i imiona, adres zamieszkania lub pobytu, numer telefonu
17	Rejestr wniosków	Nazwiska i imiona, adres zamieszkania lub pobytu, numer telefonu
18	Rejestr podań wnoszonych ustnie do Prezydenta Miasta	Nazwiska i imiona, adres zamieszkania lub pobytu, numer telefonu
19	System obiegu dokumentów	Nazwiska i imiona, adres zamieszkania lub pobytu, adres poczty elektronicznej
20	Akta osobowe oraz inne dokumenty pracownicze	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, Numer Identyfikacji

		Podatkowej, miejsce pracy, zawód, wykształcenie, seria i numer dowodu osobistego, numer telefonu
21	Ewidencja zgłoszonych i wykonanych interwencji oraz ewidencja mandatów karnych Straży Miejskiej w Świętochłowicach	Nazwiska i imiona, imiona rodziców, data urodzenia, miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, miejsce pracy, zawód, wykształcenie, seria i numer dowodu osobistego, numer telefonu, skazania, mandaty karne, orzeczenia o ukaraniu, inne orzeczenia wydane w postępowaniu sądowym lub administracyjnym
22	Odpady komunalne	Nazwiska i imiona, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, numer telefonu, adres poczty elektronicznej, inne orzeczenia wydane w postępowaniu sądowym lub administracyjnym
23	Uprawnienia do badań technicznych pojazdów	Nazwiska i imiona, data i miejsce urodzenia, numer telefonu, adres email, numer ewidencyjny diagnosty
24	Ewidencja instruktorów	Nazwiska i imiona, adres zamieszkania lub pobytu, numer ewidencyjny PESEL
25	Ewidencja wykładowców	Nazwiska i imiona, adres zamieszkania lub pobytu, numer ewidencyjny PESEL
26	Kandydaci na ławników	Nazwiska i imiona, imiona rodziców, data i miejsce urodzenia, obywatelstwo, adres zamieszkania lub pobytu, wykształcenie, dane zatrudnienia, dane kontaktowe (telefon, adres email), numer ewidencyjny PESEL, wizerunek twarzy
27	Rejestr zamieszkania cudzoziemców	Nazwiska i imiona, data i miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL

28	Rejestr sprzętu pływającego służącego do połowu ryb	Nazwiska i imiona, adres zamieszkania lub pobytu
29	Stały rejestr wyborców	Nazwiska i imiona, imię ojca, data urodzenia, numer ewidencyjny PESEL, adres zamieszkania lub pobytu, obywatelstwo
30	Dokumentacja wyborcza i referendalna	Nazwiska i imiona, imię ojca, data urodzenia, numer ewidencyjny PESEL, adres zamieszkania lub pobytu, obywatelstwo,
31	Rejestracja i kwalifikacja wojskowa	Nazwiska i imiona, numer ewidencyjny PESEL, miejsce urodzenia, seria i numer DO, adres zamieszkania lub pobytu
32	Świadczenia na rzecz obrony	Nazwiska i imiona
33	Ewidencja obiektów świadczących usługi hotelarskie, nie będące obiektami hotelarskimi oraz pól biwakowych	Nazwiska i imiona, adres zamieszkania lub pobytu
34	Ewidencja stowarzyszeń zwykłych	Nazwiska i imiona, data i miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL
35	Konsultacje społeczne Gminy Świętochłowice	Nazwiska i imiona, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, adres email, numer telefonu

PREZYDENT MIASTA
Daniel Beger

Załącznik nr 4
do Polityki Bezpieczeństwa

Sposób przepływu danych pomiędzy poszczególnymi systemami

L.p.	Nazwy systemów	Przepływ danych
1.	EwOpis - EwMapa	automatyczny przepływ danych pomiędzy modułami systemu Strateg (poprzez interfejs programowy)
2.	Firmy – Kasa – Odpady – Pojazdy – Posesja – Rejestr Opłat – Wyciągi	automatyczny przepływ danych pomiędzy modułami systemu Ratusz ze wspólną bazą danych
3.	PB_EWID - Źródło	automatyczne pobieranie danych z Systemu Rejestrów Państwowych do Rejestru Mieszkańców poprzez moduł SRP
4.	PB_USC - Źródło	półautomatyczne przenoszenie danych, dane eksportowane są z systemu PB_USC do pliku XML, następnie importowane są do systemu Źródło
5.	Quorum (Płace) – bankowość elektroniczna	półautomatyczne przenoszenie danych, dane eksportowane są z programu Płace do pliku, który importowany jest do systemu bankowości elektronicznej

PREZYDENT MIASTA
Daniel Jęger

08.02.2019
GŁÓWNY SPECJALISTA
ds. kontroli wewnętrznej
Izabela Grzondziel

Załącznik nr 5

do Polityki Bezpieczeństwa

REJESTR CZYNNOŚCI PRZETWARZANIA

W URZĘDZIE MIEJSKIM W ŚWIĘTOCHŁOWICACH

Spis treści:

CZYNNOŚĆ REKRUTACJA 42
CZYNNOŚĆ PRZETWARZANIE DANYCH W ZWIĄZKU Z ZATRUDNIENIEM NA UMOWĘ O PRACĘ 44
CZYNNOŚĆ UMOWY CYWILNOPRAWNYCH, NP.: O DZIEŁO, ZLECENIE 46
CZYNNOŚĆ ZARZĄDZANIE KORESPONDENCJĄ URZĘDU 48
CZYNNOŚĆ PROWADZENIE NEWSLETTERÓW, INFORMATORÓW DLA MIESZKAŃCÓW, ETC 50
CZYNNOŚĆ MONITORING WIZYJNY MIASTA ŚWIĘTOCHŁOWICE 52
CZYNNOŚCI DOTYCZĄCE UMÓW 55
CZYNNOŚCI WYKONYWANIE KONTRAKTÓW 57
CZYNNOŚĆ KONTAKTY 59
CZYNNOŚĆ PROWADZENIE EWIDENCJI PRZEDSIĘBIORCÓW, KTÓRZY ZAKOŃCZYLI WYKONYWANIE DZIAŁALNOŚCI GOSPODARCZEJ PRZED DNIEM 1 LIPCA 2011 61
CZYNNOŚĆ PROWADZENIE EWIDENCJI GRUNTÓW I BUDYNKÓW GMINY ŚWIĘTOCHŁOWICE 63
CZYNNOŚĆ WYMIAR I POBÓR PODATKU OD NIERUCHOMOŚCI 65
CZYNNOŚĆ WYMIAR I POBÓR PODATKU ROLNEGO 67
WYDAWANIE ZEZWOLEŃ NA SPRZEDAŻ NAPOJÓW ALKOHOLOWYCH 69
CZYNNOŚĆ PROWADZENIE EWIDENCJI KIEROWCÓW 71
CZYNNOŚĆ PROWADZENIE EWIDENCJI ZEZWOLEŃ TRANSPORTOWYCH 73
CZYNNOŚĆ PROWADZENIE EWIDENCJI POJAZDÓW 75
CZYNNOŚĆ PROWADZENIE REJESTRU MIESZKAŃCÓW 77
CZYNNOŚĆ PROWADZENIE EWIDENCJI URODZEŃ, MAŁŻEŃSTW I ZGONÓW 79
CZYNNOŚĆ PROWADZENIE REJESTRU WIECZYSTEGO UŻYTKOWNIA I DZIERŻAWY GRUNTÓW 81
CZYNNOŚĆ PROWADZENIE EWIDENCJI ZGŁASZANIA I PRZYJMOWANIA DO ZASOBU PRAC GEODEZYJNYCH I KARTOGRAFICZNYCH NA OBSZARZE GMINY ŚWIĘTOCHŁOWICE 83
CZYNNOŚĆ PROWADZENIE EWIDENCJI UZGADNIANIA USYTUOWANIA PROJEKTOWANYCH SIECI UZBROJENIA TERENU NA OBSZARZE GMINY ŚWIĘTOCHŁOWICE 85
CZYNNOŚĆ PROTOKOŁY USTALEŃ PREZYDENTA MIASTA 87
CZYNNOŚĆ PROWADZENIE REJESTRU WNIOSKÓW 89
CZYNNOŚĆ PROWADZENIE REJESTRU PODAŃ WNOSZONYCH USTNIE DO PREZYDENTA MIASTA 91
CZYNNOŚĆ SYSTEM OBIEGU DOKUMENTÓW 93
CZYNNOŚĆ - PROWADZENIE EWIDENCJI ZGŁOSZONYCH I WYKONANYCH INTERWENCJI ORAZ EWIDENCJA MANDATÓW KARNYCH STRAŻY MIEJSKIEJ W ŚWIĘTOCHŁOWICACH 95
CZYNNOŚĆ OPŁATY ZA ODPADY KOMUNALNE 97

CZYNNOŚĆ UPRAWNIENIA DO BADAŃ TECHNICZNYCH POJAZDÓW 99
CZYNNOŚĆ PROWADZENIE EWIDENCJI INSTRUKTORÓW 101
CZYNNOŚĆ PROWADZENIE EWIDENCJI WYKŁADOWCÓW 103
CZYNNOŚĆ KANDYDCI NA ŁAWNIKÓW 105
CZYNNOŚĆ PROWADZENIE REJSTRU ZAMIESZKANIA CUDZOZIEMCÓW 107
CZYNNOŚĆ PROWADZENIE REJESTRU SPRZĘTU PŁYWAJĄCEGO SŁUŻĄCEGO DO POŁOWU RYB 109
CZYNNOŚĆ PROWADZENIE STAŁEGO REJESTRU WYBORCÓW 111
CZYNNOŚĆ PROWADZENIE DOKUMENTACJI WYBORCZEJ I REFERENDALNEJ 113
CZYNNOŚĆ PROWADZENIE REJESTRACJI I KWALIFIKACJI WOJSKOWEJ 115
CZYNNOŚĆ PROWADZENIEWIDENCJI OBIEKTÓW ŚWIADCZĄCYCH USŁUGI HOTELARSKIE, NIE BĘDĄCE OBIEKTAMI HOTELARSKIMI ORAZ PÓL BIWAKOWYCH 117
CZYNNOŚĆ PROWADZENIE EWIDENCJI STOWARZYSZEŃ ZWYKŁYCH 119
CZYNNOŚĆ PROWADZENIE KONSULTACJI SPOŁECZNYCH GMINY ŚWIĘTOCHŁOWICE 121

CZYNNOŚĆ REKRUTACJA

Przetwarzanie danych zawartych w CV

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane w siedzibie Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Cele związane z rekrutacją na stanowisko, dane zbierane w oparciu o art. 6 ust 1 litera a oraz art. 9 ust 2 litera h Rozporządzenia parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych

Podstawa prawna

Ustawa Kodeks Pracy i zgoda na przetwarzanie danych wynikające z art. 6 ust 1 litera a oraz art. 9 ust 2 litera h Rozporządzenia parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych

osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

Okres przetwarzania

Do zakończenia realizacji celu, czyli do zatrudnienia lub w przypadku klauzuli otwartej do czasu cofnięcia zgody na przetwarzanie

Opis kategorii osób, których dane dotyczą

Kandydaci do pracy

Kategorie danych osobowych

Dane identyfikacyjne, dane adresowe, dane o wykształceniu, dane o doświadczeniu zawodowym, dane o stażu pracy (oraz inne wymagające zgody na przetwarzanie)

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy i Komornicy

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO"

CZYNNOŚĆ PRZETWARZANIE DANYCH W ZWIĄZKU Z ZATRUDNIENIEM NA UMOWĘ O PRACĘ

(prowadzenie rejestru pracowników, aktów osobowych pracowników i byłych pracowników i ewidencja czasu pracy zgodnie z Ustawą Kodeks Pracy)

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane w siedzibie Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania (zbiór):

Prowadzenie rejestru pracowników związane z zatrudnieniem zgodnie z Ustawą Kodeks Pracy oraz dane zbierane w oparciu o art. 6 ust 1 litera a oraz art. 9 ust 2 litera h Rozporządzenia parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych

Podstawa prawna

Ustawa Kodeks Pracy

Okres przetwarzania

Przez okres 50 lat od zakończenia zatrudnienia dla podstawowych danych kadrowych oraz do 24 miesięcy od zakończenia przetwarzania dla innych celów związanych z pozyskiwaniem danych od pracowników zatrudnionych w Urzędzie. Podstawa prawna Ustawa o narodowym zasobie archiwalnym i archiwach

Opis kategorii osób, których dane dotyczą

Pracownicy etatowi Urzędu oraz rodziny, w tym małoletni.

Kategorie danych osobowych

Dane identyfikacyjne, dane adresowe, dane o wykształceniu, dane o doświadczeniu zawodowym, dane o stażu pracy, dane o stanowisku i zakresie obowiązków, dane o stopniu niepełnosprawności,

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji tj. Sądy, Komornicy, Zakład Ubezpieczeń Społecznych, firmy ubezpieczeniowe (dotyczy osób posiadających polisy ubezpieczeniowe i pakiety medyczne dla siebie i członków swoich rodzin) np. PZU, firmy sportowe (dla osób posiadających wykupione pakiety sportowe dla siebie i członków rodzin) , Państwowy Fundusz Rehabilitacji i Osób Niepełnosprawnych (dla osób niepełnosprawnych – na podstawie art 26 ust 1 punkt 2 Ustawa z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych oraz inne podmioty, którym powierza się lub udostępnia dane.

Kategorie danych osobowych

Dane identyfikacyjne dane adresowe, dane o wykształceniu i przebiegu pracy, absencji (urlopy, zwolnienia lekarskie, rehabilitacyjne i inne) dane o zakresie obowiązków, kary i nagrody, inne dane wymagane zgodnie z Kodeksem Pracy

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO"

CZYNNOŚĆ UMOWY CYWILNOPRAWNYCH, NP.: O DZIEŁO, ZLECENIE

(osoby realizujące czynności w oparciu o umowy cywilnoprawne, w tym zlecenie i umowy o działo)

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane w siedzibie Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania (zbiór):

Realizacja obowiązków wybijanych z umowy cywilnoprawnej w oparciu o art. 6 ust 1 litera a oraz art. 9 ust 2 litera h Rozporządzenia parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, Kodeks Cywilny oraz inne w tym przepisy podatkowe oraz dotyczące rachunkowości Urzędu.

Podstawa prawna

Kodeks Cywilny, Ustawa Ordynacja podatkowa, Ustawa o podatkach od osób fizycznych

Okres przetwarzania

Przez okres 50 lat na podstawie przepisów Ustawy o emeryturach i rentach z funduszu ubezpieczeń społecznych.

Opis kategorii osób, których dane dotyczą

Pracownicy zatrudnieni w oparciu o umowy cywilnoprawne oraz rodziny, w tym małoletni.

Kategorie danych osobowych

Dane identyfikacyjne dane adresowe, dane o wykształceniu i przebiegu pracy, absencji (urlopy, zwolnienia lekarskie, rehabilitacyjne i inne) dane o zakresie obowiązków, kary i nagrody, inne dane wymagane zgodnie z Kodeksem Pracy

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji tj. Sądy, Komornicy, Zakład Ubezpieczeń Społecznych oraz firmy ubezpieczeniowe (dotyczy osób posiadających polisy ubezpieczeniowe i pakiety medyczne dla siebie i członków swoich rodzin) np. PZU, pakiety sportowe (dla osób posiadających wykupione pakiety sportowe dla siebie i członków rodzin, Państwowy Fundusz Rehabilitacji i Osób Niepełnosprawnych (dla osób niepełnosprawnych – na podstawie art 26 ust 1 punkt 2 Ustawa z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych oraz inne podmioty, którym powierza się lub udostępnia dane.

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ ZARZĄDZANIE KORESPONDENCJĄ URZĘDU

(zarządzanie korespondencją Urzędu, w tym pisma wchodzące i wychodzące w formie tradycyjnej i elektronicznej wraz z załącznikami zawierającymi dane osobowe, w tym wynikające z art. 9 i art. 10 RODO)

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Cele związane z przyjmowaniem i wysyłaniem korespondencji do Interesariuszy Urzędu, zarówno w formie elektronicznej, jak i tradycyjnej. Osoba przysyłająca pismo nie jest zobowiązana do wyrażenia zgody na przetwarzanie danych osobowych, O ile współpraca z interesariuszem wymaga jednak takiej zgody, dane powinny być zbierane w oparciu o:

a) art. 6 ust 1 litera a RODO (od osób, których dane dotyczą)
b) art. 6 ust 1 litera b RODO (od osób które działają w imieniu innej osoby)
c) art. 6 ust 1 litera f RODO (w zakresie prawnie usprawiedliwionego celu Administratora danych)
d) art. 9 ust 2 litera h RODO (w zakresie art. 6 ust 1 litera a) gdy przekazywane są dane z art. 9 RODO

Podstawa prawna

Art. 6 Ust 1 litera f Rozporządzenia parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych

Okres przetwarzania

Do zakończenia okresu wynikającego z kontekstu prawnego dokumentu (w zależności od tego czego merytorycznie dotyczy pismo) przez okres odpowiedni do kategorii przetwarzanych danych.

Kategorie danych osobowych

Wszelkie dane osobowe włącznie z art. 9 i 10 przesyłane za pomocą poczty tradycyjnej lub elektronicznej

Opis kategorii osób, których dane dotyczą

Nadawcy i odbiorcy korespondencji

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ PROWADZENIE NEWSLETTERÓW, INFORMATORÓW DLA MIESZKAŃCÓW, ETC.

(wysyłanie newsletterów i informacji)

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Cele związane z realizacją procesu obsługi mieszkańców Świętochłowic, w tym informowanie o zagrożeniach, eventach, etc.

Podstawa prawna

Zgoda z art. 6 ust 1 litera a Rozporządzenia parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i
w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych

Okres przetwarzania

Do zakończenia okresu w jakim określono cel przetwarzania lub do cofnięcia zgody na przetwarzanie

Kategorie danych osobowych

Dane kontaktowe osób korzystających z newslettera i powiadomień Urzędu Miejskiego

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu korzystający z newslettera i systemu powiadamiania.

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ MONITORING WIZYJNY MIASTA ŚWIĘTOCHŁOWICE

(system wideo)

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:,

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania:

Cele związane z przetwarzaniem wizerunku na podstawie art. 6 ust 1 litera a, art. 6 ust 1 litera ci f Rozporządzenia parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych ora uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

Podstawa prawna

Na podstawie art. 111 Ustawy o ochronie danych osobowych oraz art. 94 pkt 2 Ustawy Kodeks Pracy, art. 120 Ustawy Kodeks Pracy i art. 100 Ustawy Kodeks Pracy.

Okres przetwarzania

Przez okres 90 dni od momentu utrwalenia.

Kategorie danych osobowych

Wizerunek osób objętych obszarem monitorowania

Opis kategorii osób, których dane dotyczą

Osoby znajdujące się w siedzibie lub na posesji Administratora Danych lub zarejestrowane na potrzeby bezpieczeństwa lokalnego w punktach miasta objętych monitoringiem.

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji.

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".
UWAGA: cel przetwarzania może być związany z przetwarzaniem danych sensytywnych zgodnych z art. 9 (np. stan zdrowia) i art. 10 (np. informacje o mandatach)

UWAGI DODATKOWE

Jeśli monitoring miejski zostanie przekazany w posiadanie Policji, ale jednocześnie Urząd Miejski będzie posiadał podgląd wymagane będzie podpisanie umów powierzania zgodnych z art. 28 RODO.
Osoby przetwarzające dane podpisują upoważnienia do przetwarzania danych wraz z oświadczeniami.

Należy rozważyć przygotowanie informacji dla pracowników jednostki oraz przygotować tablice informacyjne dotyczące monitorowania siedziby Urzędu.

Wzór zapisu w regulaminie pracy o monitoringu

1. W celu

.....

(podać cel, np. zapewnienie bezpieczeństwa i higieny pracy)

zgodnie z art. 5 i art. 6 ust. 1 pkt c i f rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku

z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz.UE.L.2016.119.1), wprowadza się monitoring

.....

(określić rodzaj, np. wizyjny, i podać obszar działania, np. pomieszczenia pracy)

.....

polegający na

.....

(podać zakres działania, np. nagrania wideo)

2. Materiały pozyskane z monitoringu będą wykorzystane wyłącznie w celu określonym w pkt 1.

3. Dostęp do materiałów pozyskanych z monitoringu mają jedynie osoby, które są upoważnione do przetwarzania zawartych tam danych.

4. Materiały pozyskane z monitoringu będą przechowywane przez okres ....., (podać okres, np. 90 dni) po upływie którego będą niszczone w sposób uniemożliwiający ich odtworzenie.

5. Pracownik, którego dane znajdują się w materiałach pozyskanych z monitoringu, ma prawo dostępu do tych danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, a także przysługuje mu prawo do przenoszenia danych i prawo wniesienia sprzeciwu.

CZYNNOŚCI DOTYCZĄCE UMÓW

(informacje o osobach reprezentujących interesariuszy oraz wynikające z realizacji umów)

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja umów

Podstawa prawna

Umowa realizowana przez Administratora danych

Kategorie danych osobowych

– imię nazwiska, nazwa firmy i stanowisko, numer NIP, nr konta bankowego, adres podmiotu, adres mail, nr telefonu, nr faksu

Okres przetwarzania

Do zakończenia okresu w jakim określono cel przetwarzania oraz zakończenia umowy lub do momentu zakończenia wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze jednostki, osoby reprezentujące z ramienia Administratora Danych oraz Interesariuszy,

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚCI WYKONYWANIE KONTRAKTÓW

(informacje o osobach reprezentujących interesariuszy oraz związanych z realizacją umów lub kontraktów na rzecz Urzędu Miejskiego lub z upoważnienia Urzędu Miejskiego)

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja kontraktów i umów

Podstawa prawna

Kontrakt realizowany przez Administratora Danych lub na rzecz Administratora Danych

Kategorie danych osobowych

– imię nazwiska, nazwa firmy i stanowisko, numer NIP, nr konta bankowego, adres podmiotu, adres mail, nr telefonu, nr faksu, uprawnienia do realizacji kontraktu, wymagane przez Interesariusza oświadczenia o stanie zdrowia, dopuszczeniu do realizacji prac, inne

Okres przetwarzania

Do zakończenia okresu w jakim określono cel przetwarzania oraz zakończenia kontraktów, serwisów i gwarancji wynikających z celu przetwarzania lub do momentu zakończenia wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu, osoby reprezentujące, osoby realizujące umowę lub kontrakt z ramienia Administratora Danych oraz Interesariuszy, pracownicy i podwykonawcy Administratora Danych i Interesariuszy

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ KONTAKTY

(książki adresowe, listy kontaktów w poczcie elektronicznej)

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Kontakt z interesariuszami i pracownikami

Podstawa prawna

W oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

Interesariusze, z którymi kontakt utrzymuje Administrator Danych – imię nazwiska, nazwa firmy i stanowisko, numer NIP, adres podmiotu, adres mail, nr telefonu, nr faksu

Okres przetwarzania

Do momentu ustania przydatności

Opis kategorii osób, których dane dotyczą

Osoby będące interesariuszami i pracownicy

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ PROWADZENIE EWIDENCJI PRZEDSIĘBIORCÓW, KTÓRZY ZAKOŃCZYLI WYKONYWANIE DZIAŁALNOŚCI GOSPODARCZEJ PRZED DNIEM 1 LIPCA 2011

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

– imię nazwiska, adres zamieszkania lub pobytu, miejsce pracy, dane adresowe miejsca pracy, dane kontaktowe

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Przedsiębiorcy

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ PROWADZENIE EWIDENCJI GRUNTÓW I BUDYNKÓW GMINY ŚWIĘTOCHŁOWICE

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

– imię nazwiska, imiona rodziców, adres zamieszkania lub pobytu, PESEL, numer ewidencyjny

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ WYMIAR I POBÓR PODATKU OD NIERUCHOMOŚCI

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

– imię, nazwisko, imiona rodziców, adres zamieszkania lub pobytu

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ WYMIAR I POBÓR PODATKU ROLNEGO

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

– imię, nazwisko, imiona rodziców, adres zamieszkania lub pobytu

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

WYDAWANIE ZEZWOLEŃ NA SPRZEDAŻ NAPOJÓW ALKOHOLOWYCH

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

– imię, nazwisko, imiona rodziców, adres zamieszkania lub pobytu, miejsce pracy

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ PROWADZENIE EWIDENCJI KIEROWCÓW

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

– imię, nazwisko, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ PROWADZENIE EWIDENCJI ZEZWOLEŃ TRANSPORTOWYCH

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

– imię, nazwisko, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ PROWADZENIE EWIDENCJI POJAZDÓW

Administrator Danych

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ PROWADZENIE REJESTRU MIESZKAŃCÓW

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

– imię nazwiska, imiona rodziców, data urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, miejsce pracy, zawód, wykształcenie, seria i numer dowodu osobistego, obywatelstwo, stan cywilny, stosunek do powszechnego obowiązku obrony kraju,

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ PROWADZENIE EWIDENCJI URODZEŃ, MAŁŻEŃSTW I ZGONÓW

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

– imię nazwiska, imiona rodziców, data urodzenia, data zawarcia małżeństwa, data zgonu, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, wykształcenie, seria i numer dowodu osobistego

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ PROWADZENIE REJESTRU WIECZYSTEGO UŻYTKOWNIA I DZIERŻAWY GRUNTÓW

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

– imię, nazwisko, adres zamieszkania lub pobytu

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ PROWADZENIE EWIDENCJI ZGŁASZANIA I PRZYJMOWANIA DO ZASOBU PRAC GEODEZYJNYCH I KARTOGRAFICZNYCH NA OBSZARZE GMINY ŚWIĘTOCHŁOWICE

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

– imię, nazwisko, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, numer NIP, miejsce pracy, numer uprawnień zawodowych

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ PROWADZENIE EWIDENCJI UZGADNIANIA USYTUOWANIA PROJEKTOWANYCH SIECI UZBROJENIA TERENU NA OBSZARZE GMINY ŚWIĘTOCHŁOWICE

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

– imię nazwiska, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, numer NIP, miejsce pracy,

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ PROTOKOŁY USTALEŃ PREZYDENTA MIASTA

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

– imię nazwiska, adres zamieszkania lub pobytu, numer telefonu i adres mail,

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ PROWADZENIE REJESTRU WNIOSKÓW

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

– imię nazwiska, adres zamieszkania lub pobytu, numer telefonu, adres mail,

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ PROWADZENIE REJESTRU PODAŃ WNOSZONYCH USTNIE DO PREZYDENTA MIASTA

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

– imię nazwiska, adres zamieszkania lub pobytu, numer telefonu, adres mail,

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ SYSTEM OBIEGU DOKUMENTÓW

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

– imię nazwiska, adres zamieszkania lub pobytu, adres mail,

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ - PROWADZENIE EWIDENCJI ZGŁOSZONYCH I WYKONANYCH INTERWENCJI ORAZ EWIDENCJA MANDATÓW KARNYCH STRAŻY MIEJSKIEJ W ŚWIĘTOCHŁOWICACH

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

- imiona, nazwiska, imiona rodziców, data urodzenia, miejsce zamieszkania lub pobytu, numer ewidencyjny PESEL, miejsce pracy, zawód, wykształcenie, seria i numer dowodu osobistego, seria i numer prawa jazdy, seria i numer paszportu, numer telefonu, adres mail, skazania, mandaty karne, orzeczenia o ukaraniu, inne orzeczenia wydane w postepowaniu sądowym lub administracyjnym, orzeczenia o ukaraniu, stan zdrowia, nałogi

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ OPŁATY ZA ODPADY KOMUNALNE

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

- imiona nazwiska, imiona rodziców, data urodzenia, miejsce zamieszkania lub pobytu, numer ewidencyjny PESEL, numer telefonu, adres mail, skazania, inne orzeczenia wydane w postepowaniu sądowym lub administracyjnym

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ UPRAWNIENIA DO BADAŃ TECHNICZNYCH POJAZDÓW

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

imiona, nazwiska, data i miejsce urodzenia, numer telefonu, adres mail, numer ewidencyjny diagnosty

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne.

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ PROWADZENIE EWIDENCJI INSTRUKTORÓW

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

imiona, nazwiska, adres zamieszkania lub pobytu, numer ewidencyjny PESEL

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne.

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ PROWADZENIE EWIDENCJI WYKŁADOWCÓW

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

imiona nazwiska, adres zamieszkania lub pobytu, numer ewidencyjny PESEL

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ KANDYDCI NA ŁAWNIKÓW

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

- imiona nazwiska, imiona rodziców, data i miejsce urodzenia, obywatelstwo, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, dane kontaktowe, wizerunek twarzy

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz Dobrych praktykach RODO".

CZYNNOŚĆ PROWADZENIE REJSTRU ZAMIESZKANIA CUDZOZIEMCÓW

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

- imiona nazwiska, data i miejsce urodzenia, obywatelstwo, adres zamieszkania lub pobytu, numer ewidencyjny PESEL,

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz Dobrych praktykach RODO".

CZYNNOŚĆ PROWADZENIE REJESTRU SPRZĘTU PŁYWAJĄCEGO SŁUŻĄCEGO DO POŁOWU RYB

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

- imiona nazwiska, adres zamieszkania lub pobytu

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ PROWADZENIE STAŁEGO REJESTRU WYBORCÓW

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

- imiona nazwiska, imię ojca, data urodzenia, numer ewidencyjny PESEL, adres zamieszkania lub pobytu, obywatelstwo

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ PROWADZENIE DOKUMENTACJI WYBORCZEJ I REFERENDALNEJ

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

- imiona nazwiska, imię ojca, data urodzenia, numer ewidencyjny PESEL, adres zamieszkania lub miejsce pobytu

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ PROWADZENIE REJESTRACJI I KWALIFIKACJI WOJSKOWEJ

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

- imiona nazwiska, numer ewidencyjny PESEL, miejsce urodzenia, seria i numer dowodu osobistego, seria i numer książeczki wojskowej, adres zamieszkania i pobytu

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ PROWADZENIEWIDENCJI OBIEKTÓW ŚWIADCZĄCYCH USŁUGI HOTELARSKIE, NIE BĘDĄCE OBIEKTAMI HOTELARSKIMI ORAZ PÓL BIWAKOWYCH

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

- imiona, nazwiska, adres zamieszkania lub pobytu

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ PROWADZENIE EWIDENCJI STOWARZYSZEŃ ZWYKŁYCH

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

- imiona nazwiska, data i miejsce urodzenia, adres zamieszkania lub pobytu, numer ewidencyjny PESEL

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

CZYNNOŚĆ PROWADZENIE KONSULTACJI SPOŁECZNYCH GMINY ŚWIĘTOCHŁOWICE

Administrator Danych

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Inspektor Ochrony Danych

Izabela Grzondziel

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800
fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

Miejsca przetwarzania:

Pomieszczenia biurowe Administratora Danych zlokalizowane we wszystkich siedzibach Urzędu Miejskiego w Świętochłowicach.

Cele przetwarzania

Realizacja zadań w imieniu Administratora Danych lub z upoważnienia Administratora Danych dla pracowników oraz interesariuszy w oparciu o art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Podstawa prawna

Zgodna z art. 6 ust 1 litera f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Kategorie danych osobowych

- imiona nazwiska, adres zamieszkania lub pobytu, numer ewidencyjny PESEL, adres mail i numer telefonu

Okres przetwarzania

Do zakończenia okresu realizacji celu oraz na czas wzajemnych roszczeń

Opis kategorii osób, których dane dotyczą

Interesariusze Urzędu Miejskiego w Świętochłowicach

Kategorie odbiorców:

Podmioty mające podstawę prawną uzyskania informacji, w tym Sądy, Komornicy, Firmy windykacyjne,

Zabezpieczenia techniczne i organizacyjne

Zabezpieczania opisano w „Polityce Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach" oraz „Dobrych praktykach RODO".

PREZYDENT MIASTA
Daniel Bager

08.02.2019
GŁÓWNY SPECJALISTA
ds. kontroli wewnętrznej
Izabela Grzondziel

Załącznik nr 6
do Polityki Bezpieczeństwa

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

W URZĘDZIE MIEJSKIM W ŚWIETOCHŁOWICACH

1. Wstęp

Instrukcja stanowi zestaw procedur opisujących zasady zabezpieczania danych osobowych przetwarzanych w zbiorach papierowych i w systemach informatycznych Urzędu Miejskiego w Świętochłowicach.

2. Definicje

- Administrator Danych Osobowych (ADO) – Prezydent Miasta, decydujący o celach i środkach przetwarzania danych osobowych.
- Inspektor Ochrony danych Osobowych (IOD) – osoba powołana przez ADO, odpowiedzialna za organizację ochrony danych osobowych.
- Administrator Systemu Informatycznego (ASI) – osoba lub podmiot sprawujący zadania związane z administracją systemami, bazami lub aplikacjami ADO.

3. Zabezpieczenia infrastruktury informatycznej i telekomunikacyjnej

1. Zastosowano zasilanie awaryjne (UPS) do serwerów oraz do elementów aktywnych sieci komputerowej.
2. Dostęp do komputerów przenośnych wynoszonych poza obszar przetwarzania, zawierających dane osobowe odbywa się poprzez podanie loginu i hasła.
3. Dane osobowe na komputerach przenośnych wynoszonych poza obszar organizacji muszą być przechowywane na zaszyfrowanych partycjach.
4. W przypadku dostępu do danych osobowych przez Internet, stosuje się szyfrowanie połączenia (SSL lub VPN).
5. W przypadku dostępu do danych osobowych przez Internet, wymagane jest uwierzytelnianie (podanie loginu i hasła) .
6. Zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
7. Lokalizacja urządzeń komputerowych uniemożliwia osobom niepowołanym dostęp do nich.
8. Dostęp do stacji roboczych lub systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła lub karty procesorowej i kodu PIN.
9. Użyto system IDS/IPS do ochrony dostępu do sieci komputerowej.

4. Zabezpieczenia programów i baz przetwarzających dane osobowe

1. Dostęp do danych osobowych w programie lub w bazie wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła lub karty procesorowej i kodu PIN.
2. Zastosowano mechanizm umożliwiający automatyczną rejestrację identyfikatora użytkownika i datę pierwszego wprowadzenia danych osobowych.
3. Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych elementach zbioru danych osobowych.
4. Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.
5. Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
6. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
7. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

5. Procedura dostępu podmiotów zewnętrznych

1. Inspektor Danych Osobowych prowadzi rejestr podmiotów zewnętrznych, którym Administrator Danych Osobowych udostępnia dane osobowe oraz podmiotów, którym powierzono przetwarzanie danych osobowych w formie usługi zewnętrznej.
2. Administrator Danych Osobowych powierza do przetwarzania dane osobowe będące w jego obszarze fizycznym podmiotom zewnętrznym w oparciu o umowę poufności. Podmiot zewnętrzny zobowiązany jest do zachowania poufności powierzonych danych i przetwarzania ich zgodnie z celem umowy.
3. Administrator Danych Osobowych powierza dane osobowe do przetwarzania w formie usługi zewnętrznej podmiotom zewnętrznym w oparciu o umowę powierzenia przetwarzania danych. Podmiot zewnętrzny zobowiązany jest do przetwarzania danych zgodnie z zakresem i celem określonym w umowie powierzenia przetwarzania danych osobowych. Podmiot zewnętrzny zobowiązany jest do stosowania zabezpieczeń określonych w rozporządzeniu 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. z 2004 r., nr 100, poz. 1024) i należy uwzględnić to w stosownej umowie dotyczącej powierzenia danych.

6. Procedura korzystania z Internetu

1. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek nielegalnych plików i programów.
2. Pliki pobierane z nieznanego lub niezaufanego źródła mogą być ściągane tylko w uzasadnionych przypadkach, pod nadzorem Administratora Systemu Informatycznego.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie samodzielnie instalowane lub uruchamiane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na stronach tego typu często zainstalowane jest szkodliwe oprogramowanie, które może zainfekować system operacyjny komputera).
5. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą „https:", w razie wątpliwości należy skonsultować się z Administratorem Systemu Informatycznego.
6. Przy korzystaniu z Internetu, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
7. W zakresie dozwolonym przepisami prawa, Pracodawca zastrzega sobie prawo do kontrolowania sposobu korzystania przez Użytkownika z Internetu pod kątem wyżej opisanych zasad.
8. W uzasadnionym zakresie, Pracodawca zastrzega sobie prawo kontroli czasu spędzanego przez Użytkownika w Internecie.
9. Pracodawca może również blokować dostęp do niektórych treści dostępnych przez Internet.

7. Procedura korzystania z poczty elektronicznej

1. Przesyłanie danych osobowych z użyciem maila może odbywać się tylko przez osoby do tego uprawnione.
2. W przypadku przesyłania danych osobowych należy wykorzystywać mechanizmy kryptograficzne.
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków, duże i małe litery oraz cyfry lub znaki specjalne, a hasło należy przekazać inną metodą, np. mailem, telefonicznie lub SMS-em.
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
6. Nie należy otwierać załączników (plików) w mailach nadesłanych przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę bez wcześniejszego przeskanowania ich programem antywirusowym.

7. Nie należy otwierać stron internetowych wskazanych łączami w mailach od nieznanych nadawców, gdyż mogą to być łącza do stron zainfekowanych lub niebezpiecznych.
8. Podczas wysyłania maili do wielu adresatów jednocześnie, należy chronić adresy odbiorców i w razie konieczności użyć opcji „Ukryte do wiadomości – UDW".
9. Przy korzystaniu z maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
10. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.

8. Procedura nadawania uprawnień do przetwarzania danych osobowych.

1. Procedura opisuje zasady przyznawania, modyfikacji i usuwania uprawnień użytkownika do przetwarzania zbiorów danych osobowych w systemach informatycznych oraz w wersji papierowej. Celem procedury jest minimalizacja ryzyka utraty poufności danych w wyniku nieuprawnionego dostępu do danych osobowych przez osoby nieupoważnione.
2. Zarządzanie uprawnieniami użytkowników
   a) Przyznanie, zmiana lub anulowanie upoważnienia do przetwarzania danych osobowych w systemie informatycznym lub w zbiorze papierowym realizowane jest na pisemny wniosek bezpośredniego przełożonego przekazywany ASI na adres email: pomoc@swietochlowice.pl .
   b) Przed nadaniem upoważnienia, ASI zobowiązany jest do sprawdzenia, czy osoba upoważniona:
      - odbyła szkolenie z zakresu przestrzegania zasad bezpieczeństwa danych osobowych oraz została zapoznana z Polityką Bezpieczeństwa Urzędu Miejskiego w Świętochłowicach;
      - podpisała oświadczenie o zachowaniu poufności danych i sposobów ich zabezpieczeń,
      - będzie przetwarzać dane osobowe w zakresie i celu określonym upoważnieniu.
   c) Wydział Organizacyjny Urzędu Miejskiego w Świętochłowicach jest zobowiązany do bieżącej aktualizacji upoważnień i ich zakresu oraz prowadzenie rejestru osób upoważnionych do przetwarzania danych osobowych.
3. Każdy użytkownik musi posiadać swój własny indywidualny identyfikator. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielany innej osobie.
4. Zarządzanie uprawnieniami administratorów
   a) Administratorów Systemów Informatycznych wyznacza pisemnie Administrator Danych Osobowych lub ASI wyznaczony jest poprzez zakres umowy zawartej z podmiotem zewnętrznym.
   b) Jeżeli jest to możliwe, każdy Administrator Systemu Informatycznego zobowiązany jest do bieżącej pracy na koncie roboczym. Użycie konta administracyjnego powinno mieć miejsce wyłącznie gdy jest to niezbędne.

c) Jeżeli jest to możliwe, każdy Administrator Systemu Informatycznego powinien pracować na koncie administratora przypisanym mu osobiście.

9. Metody i środki uwierzytelnienia

1. Procedura ma zapewniać, że do systemów informatycznych przetwarzających dane osobowe mają dostęp jedynie osoby do tego upoważnione.
2. Ogólne zasady postępowania z hasłami
   a) ASI informuje użytkownika o nadaniu pierwszego hasła do systemu.
   b) Użytkownik systemu zobowiązany jest do niezwłocznej zmiany tego hasła.
   c) Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.
   d) Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
   e) Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.
3. Hasła użytkowników – na przynajmniej jednym poziomie zabezpieczeń (system, zasoby sieciowe, aplikacje) muszą spełniać następujące wymagania:
   a) Hasło składa się co najmniej z 8-miu znaków.
   b) Hasło składa się z dużych i małych liter oraz z cyfr i znaków specjalnych.
   c) Zmiana hasła odbywa się nie rzadziej niż raz na 30 dni.
   d) O ile jest to możliwe, zmiana hasła jest wymuszana przez system, w przeciwnym przypadku użytkownicy są zobowiązani do samodzielnej zmiany hasła.
4. Hasła administratorów
   a) Hasło administratora składa się co najmniej z 8-miu znaków.
   b) Hasło składa się z dużych i małych liter oraz z cyfr i znaków specjalnych.
   c) W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.
   d) W przypadkach awaryjnych hasło może być udostępnione osobie zastępującej administratora za wiedzą Inspektora Ochrony Danych Osobowych.
   e) Po ustaniu sytuacji awaryjnej administrator jest zobowiązany do zmiany hasła.

10. Procedura rozpoczęcia, zawieszenia i zakończenia pracy

Procedura ma na celu zabezpieczenie danych osobowych przed nieuprawnionym dostępem i utratą poufności w sytuacji, gdy użytkownik rozpoczyna, przerywa lub kończy pracę w systemie informatycznym przetwarzającym dane osobowe.

a) Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem identyfikatora i hasła. Każdy użytkownik musi posiadać indywidualny identyfikator. Zabrania się pracy wielu użytkowników na wspólnym koncie.
b) Użytkownik jest zobowiązany do powiadomienia ASI o podejrzeniu lub stwierdzeniu próby logowania się do systemu osoby nieupoważnionej.

c) W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym ASI, który odpowiada za odblokowanie systemu użytkownikowi.
d) Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym wglądu do danych wyświetlanych na monitorach komputerowych.
e) Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu.
f) Po zakończeniu pracy, użytkownik zobowiązany jest wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy oraz zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki, na których znajdują się dane osobowe.

11. Procedura tworzenia kopii zapasowych

1. Tworzeniu kopii podlegają zasoby znajdujące się na serwerach plików, aplikacji oraz baz danych.
2. Wykonywane kopie umieszcza się na przeznaczonej do tego sieciowej macierzy dyskowej.
3. Dopuszczalne jest wykonywanie kopii pośrednich, umieszczanych na innych serwerach.
4. Kopie wykonuje się jako kopie całościowe.
5. Kopie wykonywane są w cyklu tygodniowym.
6. Opracowuje się szczegółowy harmonogram wykonywania kopii bezpieczeństwa, który podlega zatwierdzeniu przez Inspektora Ochrony Danych Osobowych.
7. Do wykonywania i kontrolowania wykonanych kopii bezpieczeństwa upoważnieni są Administratorzy Systemu Informatycznego.

12. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji i wydruków

1. Procedura określa sposób postępowania z nośnikami (dyskami twardymi, płytami CD/DVD, przenośnymi pamięciami USB) na których znajdują się dane osobowe, celem zabezpieczenia ich przed niszczeniem, kradzieżą oraz dostępem osób nieupoważnionych.
2. Zabezpieczenie elektronicznych nośników informacji
   a) Nośniki danych są przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych).
   b) Zabrania się wynoszenia poza obszar przetwarzania wymiennych nośników informacji, bez zgody ADO, IOD lub AIS.
   c) Dane osobowe znajdujące się na nośnikach elektronicznych, wynoszone poza obszar przetwarzania, muszą być zaszyfrowane.
   d) W sytuacji przekazywania nośników z danymi osobowymi poza obszar przetwarzania należy stosować następujące zasady bezpieczeństwa:
      - adresat powinien zostać powiadomiony o przesyłce,

- dane przed wysłaniem powinny zostać zaszyfrowane, a hasło podane adresatowi inną drogą.

e) Osoby wykorzystujące nośniki zobowiązane są do niezwłocznego i trwałego usuwania (kasowania) danych osobowych po ustaniu celu ich przechowywania (chyba, że z powodu odrębnych przepisów należy dane zachowywać).

f) Podlegające likwidacji uszkodzone lub przestarzałe nośniki, a szczególności twarde dyski z danymi osobowymi, są komisyjnie niszczone w sposób fizyczny.

g) Nośniki informacji zamontowane w sprzęcie IT, a w szczególności twarde dyski z danymi osobowymi powinny być wymontowane lub wyczyszczone specjalistycznym oprogramowaniem, zanim zostaną przekazane poza obszar przetwarzania.

h) Osoby wykorzystujące elektroniczne nośniki z danymi osobowymi są zobowiązane do zabezpieczeniach ich przed dostępem osób nieupoważnionych, szczególnie poza godzinami pracy.

3. Zabezpieczenie kopii zapasowych zostało opisane w procedurze tworzenia kopii zapasowych.

4. Zabezpieczenie dokumentów i wydruków

a) Dokumenty i wydruki trwałe z danymi osobowymi przechowuje się w archiwum lub w zabezpieczonych fizycznie pomieszczeniach, biurkach i szafach zamykanych na klucz.

b) Pracownicy są zobowiązani do zabezpieczania dokumentów przed dostępem osób nieupoważnionych podczas swojej nieobecności w pomieszczeniach lub po zakończeniu pracy.

c) Zabrania się pozostawiania wydruków oraz kserokopii na drukarkach, skanerach i kserokopiarkach bez nadzoru.

d) Niszczenie dokumentów zawierających dane osobowe, w tym wydruków tymczasowych powinno odbywać się z użyciem niszczarek.

e) Za zapewnienie bezpieczeństwa dokumentów i wydruków odpowiedzialni są kierownicy właściwych komórek organizacyjnych oraz podległe im osoby przetwarzające dane osobowe.

13. Procedura zabezpieczenia systemu informatycznego, w tym przed wirusami komputerowymi

1. Ochrona antywirusowa. Procedura określa sposób zabezpieczenia systemów informatycznych przed szkodliwym oprogramowaniem oraz nieautoryzowanym dostępem do systemów przetwarzających dane osobowe.

a) Za zaplanowanie i zapewnienie ochrony antywirusowej odpowiada ASI, w tym za zapewnienie odpowiedniej ilości licencji dla użytkowników.

b) System antywirusowy zainstalowano na serwerach oraz stacjach roboczych.

c) System antywirusowy zapewnia ochronę systemu operacyjnego, przechowywanych plików oraz poczty elektronicznej.

d) Użytkownicy zobowiązani są do skanowania programem antywirusowym plików wprowadzonych z nośników zewnętrznych.
e) Administratorzy Systemów Informatycznych zapewniają stałą aktywność programu antywirusowego, program antywirusowy musi być aktywny podczas pracy systemu informatycznego przetwarzającego dane osobowe.
f) Aktualizacja definicji wirusów powinna odbywać się automatycznie.
g) W przypadku stwierdzenia pojawienia się wirusa, każdy użytkownik winien powiadomić ASI.

2. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej. Stosowane zabezpieczenia mają na celu zabezpieczenie systemów informatycznych przed nieautoryzowanym dostępem do sieci lokalnej.
   a) Za planowanie, konfigurowanie i aktywowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku sieci lokalnej i sieci rozległej odpowiada ASI.
   b) Stosowany jest Firewall sprzętowy.
   c) Zastosowano mechanizmy kontroli dostępu do sieci w postaci IDS/IPS do wykrywania i blokowania ataków do sieci komputerowej oraz technikę NAT.
   d) Sieć bezprzewodową zabezpieczono technologią WPA lub WPA2.
   e) Zastosowano mechanizmy monitorujące przeglądanie Internetu przez użytkowników. Uwzględniają one blokowanie określonych stron internetowych oraz analizę przesyłanych informacji pod kątem niebezpiecznego oprogramowania.

14. Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych

1. Odbiorcą danych jest każdy, komu udostępnia się dane osobowe, z wyłączeniem:
   a) osoby, której dane dotyczą,
   b) osoby, upoważnionej do przetwarzania danych,
   c) administratora mającego siedzibę w państwie trzecim,
   d) podmiotu, któremu powierzono przetwarzanie danych,
   e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
2. System przetwarzający dane osobowe udostępniane odbiorcom musi umożliwiać rejestrację:
   a) nazwy jednostki organizacyjnej lub imienia i nazwiska osoby, której udostępniono dane,
   b) zakresu udostępnianych danych,
   c) daty udostępnienia.
3. Dane osobowe udostępnia się odbiorcy danych na wniosek ze wskazaniem przez odbiorcę podstawy prawnej legalizującej przetwarzanie danych osobowych.
4. Odnotowanie informacji o udostępnieniu danych powinno nastąpić niezwłocznie po udostępnieniu danych:
   a) w systemie informatycznym, jeśli przetwarza udostępnione dane osobowe,
   b) w ewidencji udostępnionych danych osobowych, dla danych przetwarzanych w formie papierowej.

5. Naczelnicy Wydziałów odpowiadają za udostępnienie danych osobowych w sposób zgodny z ich przeznaczeniem.
6. Na żądanie osoby, której dane zostały udostępnione, informacje o udostępnieniu danych są zamieszczane w raporcie z systemu informatycznego lub wyciągu z rejestru papierowego, a raport przekazywany jest tej osobie.

15. Procedura wykonywania przeglądów i konserwacji

1. Procedura ma na celu zapewnienie ciągłości działania systemów informatycznych przetwarzających dane osobowe oraz zabezpieczenie danych osobowych przed ich nieuprawnionym udostępnieniem.
2. Przeglądy i konserwacje systemu informatycznego i aplikacji
   a) ASI odpowiada za bezawaryjną pracę systemu IT, w tym: stacji roboczych, aplikacji serwerowych, baz danych oraz poczty elektronicznej.
   b) Przegląd i konserwacja systemu informatycznego powinny być wykonywane w terminach określonych przez producentów systemu lub zgodnie z harmonogramem ASI, jednak nie rzadziej, niż raz w roku.
   c) Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI.
   d) ASI odpowiada za optymalizację zasobów serwerowych, wielkości pamięci i dysków.
   e) ASI odpowiada za sprawdzanie poprawności działania systemu IT, w tym: stacji roboczych, serwerów, drukarek, baz danych, poczty elektronicznej.
   f) ASI odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia.
   g) Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego, wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.
   h) Czynności konserwacyjne i naprawcze wykonywane doraźnie przez osoby nie posiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych), muszą być wykonywane pod nadzorem osób upoważnionych, a w razie konieczności należy udzielić takim osobom stosownych upoważnień.
   i) Przed przekazaniem uszkodzonego sprzętu komputerowego z danymi osobowymi do naprawy poza Urząd, należy:
      - wymontować nośniki z danymi osobowymi,
      - trwale usunąć dane osobowe z użyciem specjalistycznego oprogramowania,
      - nadzorować proces naprawy przez osobę upoważnioną przez Administratora Systemu Informatycznego, gdy nie ma możliwości usunięcia danych z nośnika.
3. Aktualizacje oprogramowania

a) ASI odpowiada za aktualizację oprogramowania zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service pack-i, łatki).
b) ASI odpowiada za zapewnienie licencjonowanego oprogramowania do przetwarzania danych osobowych.

PREZYDENT MIASTA
Daniel Beger

Załącznik nr 2
do Zarządzenia Nr...../2019
Prezydenta Miasta Świętochłowice
z dnia.....

DOBRE PRAKTYKI RODO

URZĄD MIEJSKI W ŚWIĘTOCHŁOWICACH

DOBRA PRAKTYKA: 4
UWAGA KONSULTANTA: 4
WZÓR KLAUZULI ZAWIERANY W CV – PROPOZYCJA KONSULTANTA 4
ALTERNATYWNA REKOMENDOWANA KLAUZULZA 4
CEL PRZETWARZANIA – ROZMOWA KWALIFIKACYJNA 5
DOBRA PRAKTYKA: 5
WZÓR ZGODY WRAZ Z KLAUZULĄ INFORMACYJNĄ 5
DOBRA PRAKTYKA 7
UWAGA KONSULTANTA: 7
WZÓR ZGODY WRAZ Z KLAUZULĄ INFORMACYJNĄ 7
WZÓR DLA PRACOWNIKA ZE STWIERDZONĄ NIEPEŁNOSPRAWNOŚCIĄ 8
DOBRA PRAKTYKA 10
UWAGA KONSULTANTA: 10
WZÓR ZGODY WRAZ Z KLAUZULĄ INFORMACYJNĄ 10
CEL PRZETWARZANIA – PODPISYWANIE UMÓW POWIERZANIA Z INTERESARIUSZAMI URZĘDU 12
WYMAGANIE RODO 12
UWAGA KONSULTANTA: 12
WZÓR UMOWY POWIERZENIA 12
CEL PRZETWARZANIA – ZAWARCIE UBEZPIECZENIA PRZEZ PRACOWNIKA (W SWOIM IMIENIU I RODZINY, W TYM NIELETNICH) 16
DOBRA PRAKTYKA: 16
UWAGA KONSULTANTA: 16
WZÓR ZGODY WRAZ Z KLAUZULĄ INFORMACYJNĄ 16
WZÓR UMOWY POWIERZENIA Z UBEZPIECZYCIELEM 17
CEL PRZETWARZANIA - MARKETING BEZPOŚREDNI 22
UWAGI KONSULTANTA 22
DZIAŁANIE ZGODNE Z RODO 23
PRAWO DO SPRZECIWU NA MARKETING BEZPOŚREDNI 23
DOBRA PRAKTYKA W MARKETINGU 23
WZÓR MAILA DO KLIENTA W BAZIE MARKETINGOWEJ I HANDLOWEJ. 23
WZÓR MAILA DO KLIENTA Z ZAPROSZENIEM NA EVENT / SZKOLENIE ORGANIZOWANY PRZEZ ADMINISTRATORA DANYCH. 25
CEL PRZETWARZANIE DANYCH NIEZBĘDNYCH DO OTRZYMYWANIA NEWSLETTERA (formularze internetowe) 26

UWAGA KONSULTANTA: 26
TREŚĆ NIEZBĘDNA DO WYSYŁKI NEWSLETTERA 26
UPOWAŻNIENIE I OŚWIADCZENIE PRACOWNIKA URZĘDU 26
DOBRE PRAKTYKI BEZPIECZEŃSTWA TELEINFORMATYCZNEGO 28
Bezpieczeństwo urządzeń mobilnych 28
Bezpieczeństwo nośników zewnętrznych 28
Bezpieczeństwo komputerów mobilnych (laptopów) 28
Oprogramowanie antywirusowe 28
Zapora sieciowa (firewall) 29
Aktualizacje systemów i aplikacji 29
Utwardzenie konfiguracji systemów 29
Najmniejsze możliwe uprawnienia 29
Rozliczalność użytkowników i logowanie do systemu 29
Nadawanie i odbieranie uprawnień 29
Regularne skany podatnościowe 30
Bezpieczna komunikacja 30
Wykrywanie incydentów bezpieczeństwa 30
Kontrola dostępu do Internetu 30
Bezpieczna utylizacja sprzętu 30
Kontrola dostępu do sieci wewnętrznej 30
Archiwizacja danych 31
Blokada ekranu 31
Hasła 31
Wysoka dostępność systemów i usług 31

CEL PRZETWARZANIA – OBIEG CV (PRZETWARZANIE CV)

DOBRA PRAKTYKA:

1. W Urzędzie powinien być ograniczony dostęp do CV.
2. Urząd powinien określić osobę, do której przesyłane (przekazywane) są CV przesłane (przekazane) do innych pracowników.
3. Po otrzymaniu pisma (maila) zawierającego CV, każda inna osoba poza określoną w punkcie 2 przekazuje je osobie określonej w punkcie 2 i usuwa otrzymane CV w sposób trwały.
4. CV zbierane są do konkretnej rekrutacji, której celem jest znalezienie pracownika na konkretne stanowisko
5. CV przesłane w odpowiedzi na prowadzoną rekrutację, które nie będą już potrzebne (wybrano osobę – inne CV nie będą już potrzebne do zrealizowania celu) należy trwale usunąć. Alternatywą jest uzyskanie zgody na przetwarzanie danych do celów rekrutacji obecnych i przyszłych.

UWAGA KONSULTANTA:

1. Należy usunąć dotychczas zebrane do konkretnych rekrutacji cv lub alternatywnie wezwać osobę składającą dane do uzupełnienia zgody.

WZÓR KLAUZULI ZAWIERANY W CV – PROPOZYCJA KONSULTANTA

Na podstawie art. 6 ust 1 litera a Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) **wyrażam zgodę na przetwarzanie moich danych osobowych w celu** prowadzonej przez Urząd Miejski w Świętochłowicach XXXXX **rekrutacji na stanowisko** XXXXX

ALTERNATYWNA REKOMENDOWANA KLAUZULZA

Na podstawie art. 6 ust 1 litera a Rozporządzenia parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) **wyrażam zgodę na przetwarzanie moich danych osobowych w celu** prowadzonej przez Urząd Miejski w Świętochłowicach XXXXX **rekrutacji na stanowisko** XXXXX oraz na potrzeby wszystkich prowadzonych w przyszłości rekrutacji.

UWAGA: CV, które nie zawierają zgody usuwamy natychmiast bądź wzywamy do uzupełnienia klauzuli

CEL PRZETWARZANIA – ROZMOWA KWALIFIKACYJNA

DOBRA PRAKTYKA:

1. Po zaproszeniu na rozmowę kwalifikacyjną przekazujemy rekrutowanemu następujące pismo do podpisu

WZÓR ZGODY WRAZ Z KLAUZULĄ INFORMACYJNĄ

Ja niżej podpisany:

..... oświadczam, że:

na podstawie **art 6 ust 1 litera a** oraz **art. 6 ust 1 litera b** Rozporządzenia Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) **wyrażam zgodę na przetwarzanie moich danych osobowych w celach związanych z realizowanym procesem rekrutacyjnym** prowadzonym przez Urząd Miejski e Świętochłowicach

Zostałem poinformowany, że:

1. Administratorem Danych zgromadzonych w zakresie realizacji wskazanego celu jest:
   Prezydent Miasta

   Urząd Miejski w Świętochłowicach

   Ul. Katowicka 54
   41 – 600 Świętochłowice
   tel.: (32) 3491-800 fax: (32) 3491-812
   e-mail: um@swietochlowice.pl
2. Administrator Danych powołał Inspektora Ochrony Danych
   Inspektor Ochrony Danych

   Urząd Miejski w Świętochłowicach

   Ul. Katowicka 54
   41 – 600 Świętochłowice
   tel.: (32) 3491-800 fax: (32) 3491-812
   e-mail: iod@swietochlowice.pl

3. Zgromadzone przez Administratora Danych dane nie będą udostępniane innym podmiotom.
4. Dane osobowe nie będą przekazywane do państwa trzeciego
5. Moje dane osobowe będą przetwarzane na czas prowadzonej rekrutacji oraz ewentualnych roszczeń a następnie zostaną trwale usunięte przez Administratora Danych.
6. Podanie przeze mnie danych jest dobrowolne. Niepodanie danych będzie skutkowało niemożnością uczestniczenia w procesie rekrutacyjnym Administratora Danych.
7. W oparciu o zgromadzone dane nie będzie wykonywane profilowanie.

Oświadczam, że zostałam/ -em poinformowany o przysługujących mi prawach:

1. Dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do kopiowania i przenoszenia danych oraz prawo wniesienia sprzeciwu,
2. Wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uznam, iż przetwarzanie danych osobowych dotyczących mnie narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.

Data i czytelny podpis

CEL PRZETWARZANIA – ZATRUDNIENIE NA UMOWĘ O PRACĘ

DOBRA PRAKTYKA

1. Od pracowników odbieramy klauzule informacyjne, które pozwalają na przetwarzanie danych osobowych przez kadry, jednocześnie pozwalając na realizację innych celów związanych z codziennymi obowiązkami pracownika i obowiązkami Administratora Danych.

UWAGA KONSULTANTA:

1. Rekomenduje się podpisanie klauzul z wszystkimi etatowymi pracownikami Urzędu

WZÓR ZGODY WRAZ Z KLAUZULĄ INFORMACYJNĄ

Ja niżej podpisany:

..... *oświadczam, że:*

na podstawie art 6* ust 1 litera a oraz art. 6 ust 1 litera b** Rozporządzenia Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) ***wyrażam zgodę na przetwarzanie moich danych osobowych w celach związanych z zatrudnieniem *w zakresie danych zgodnych z art.* 221 Ustawy z 26 czerwca 1974 r. - Kodeks pracy (tekst jedn.: Dz.U. z 2018 r., poz. 108) oraz innych celach wynikających z zawieranych przez Administratora Danych umów oraz kontraktów i innych zobowiązań wynikających z przepisów prawa.

Do celów takich należą przede wszystkim: przekazywanie moich danych w celu realizacji umowy lub kontraktu realizowanego dla innego Administratora Danych, gdzie niezbędne jest podanie moich danych personalnych, w tym dokumentów potwierdzających kwalifikacje i uprawnienia, informacje o stanie zdrowia czy możliwości pracy w szczególnych warunkach (np. SEP, prace na wysokości, prawo jazy, paszport) dane kontaktowe, dane niezbędne do wyrobienia wizy (w oparciu o wytyczne państwa trzeciego), dane niezbędne do zakwaterowania na potrzeby wyjazdów służbowych, dane niezbędne do roszczeń innych podmiotów, w tym dane przekazywane na wniosek Sądu lub Komornika, oraz dla realizacji wszystkich celów wynikających z przepisów prawa.

Zostałem poinformowany, że:

1. *Administratorem Danych zgromadzonych w zakresie realizacji wskazanego celu jest:*
   Prezydent Miasta

   Urząd Miejski w Świętochłowicach

   Ul. Katowicka 54
   41 – 600 Świętochłowice
   tel.: (32) 3491-800 fax: (32) 3491-812
   e-mail: um@swietochlowice.pl
2. *Administrator Danych powołał Inspektora Ochrony Danych*
   Inspektor Ochrony Danych

   Urząd Miejski w Świętochłowicach

   Ul. Katowicka 54
   41 – 600 Świętochłowice
   tel.: (32) 3491-800 fax: (32) 3491-812

e-mail: iod@swietochlowice.pl

3. Zgromadzone przez Administratora Danych dane, mogą zostać udostępniane *odbiorcom tylko i wyłącznie na podstawie przepisów prawa lub w związku z wykonywaniem pracy na rzecz Administratora Danych lub jego interesariuszy w w/w celach.*
4. *Odbiorcami danych mogą być instytucje do tego uprawnione, tj. Sądy, Komornicy Sądowi, Ubezpieczyciele,*
5. *Dane osobowe nie będą przekazywane do państwa trzeciego*
6. *Dane osobowe będą przetwarzane przez okres 50 lat dla celów związanych z Ustawą Kodeks Pracy lub w okresach przewidzianych innymi przepisami prawa lub zawartymi umowami i kontraktami.*
7. *Podanie przeze mnie danych jest wymogiem ustawowym wynikającym z* Kodeksu pracy (tekst jedn.: Dz.U. z 2018 r., poz. 108)
8. *W oparciu o zgromadzone dane nie będzie wykonywane profilowanie.*

Oświadczam, że zostałam/ -em poinformowany o przysługujących mi prawach:

1. Dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do kopiowania i przenoszenia danych oraz prawo wniesienia sprzeciwu,
3. Wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uznam, iż przetwarzanie danych osobowych dotyczących mnie narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.

Data i czytelny podpis

WZÓR DLA PRACOWNIKA ZE STWIERDZONĄ NIEPEŁNOSPRAWNOŚCIĄ

Ja niżej podpisany:

…… *oświadczam, że:*

na podstawie art 6* ust 1 litera a oraz art. 6 ust 1 litera b** oraz zgodnie z **art. 9 ust 2 litera h** Rozporządzenia Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) ***wyrażam zgodę na przetwarzanie moich danych osobowych w celach związanych z zatrudnieniem *w zakresie danych zgodnych z art. 221* Ustawy z 26 czerwca 1974 r. - Kodeks pracy (tekst jedn.: Dz.U. z 2018 r., poz. 108) oraz innych celach wynikających z zawieranych przez Administratora Danych umów oraz kontraktów i innych zobowiązań wynikających z przepisów prawa.

Do celów takich należą przede wszystkim: przekazywanie moich danych w celu realizacji umowy lub kontraktu realizowanego dla innego Administratora Danych, gdzie niezbędne jest podanie moich danych personalnych, w tym dokumentów potwierdzających kwalifikacje i uprawnienia, informacje o stanie zdrowia czy możliwości pracy w szczególnych warunkach (np. SEP, prace na wysokości, prawo jazy, paszport) dane kontaktowe, dane niezbędne do wyrobienia wizy (w oparciu o wytyczne państwa trzeciego), dane niezbędne do zakwaterowania na potrzeby wyjazdów służbowych, dane niezbędne do roszczeń innych podmiotów, w tym dane przekazywane na wniosek Sądu lub Komornika, oraz dla realizacji wszystkich celów wynikających z przepisów prawa.

Zostałem poinformowany, że:

1. *Administratorem Danych zgromadzonych w zakresie realizacji wskazanego celu jest:*
   Prezydent Miasta

   Urząd Miejski w Świętochłowicach

   Ul. Katowicka 54
   41 – 600 Świętochłowice
   tel.: (32) 3491-800 fax: (32) 3491-812
   e-mail: um@swietochlowice.pl
2. *Administrator Danych powołał Inspektora Ochrony Danych*
   Inspektor Ochrony Danych

   Urząd Miejski w Świętochłowicach

   Ul. Katowicka 54
   41 – 600 Świętochłowice
   tel.: (32) 3491-800 fax: (32) 3491-812
   e-mail: iod@swietochlowice.pl
3. Zgromadzone przez Administratora Danych dane, mogą zostać udostępniane *odbiorcom tylko i wyłącznie na podstawie przepisów prawa lub w związku z wykonywaniem pracy na rzecz Administratora Danych lub jego interesariuszy w w/w celach.*
4. *Odbiorcami danych mogą być instytucje do tego uprawnione, tj. Sądy, Komornicy Sądowi, Ubezpieczyciele,*
5. *Dane osobowe nie będą przekazywane do państwa trzeciego*
6. *Dane osobowe będą przetwarzane przez okres 50 lat dla celów związanych z Ustawą Kodeks Pracy lub w okresach przewidzianych innymi przepisami prawa lub zawartymi umowami i kontraktami.*
7. *Podanie przeze mnie danych jest wymogiem ustawowym wynikającym z* Kodeksu pracy (tekst jedn.: Dz.U. z 2018 r., poz. 108)
8. *W oparciu o zgromadzone dane nie będzie wykonywane profilowanie.*

Oświadczam, że zostałam/ -em poinformowany o przysługujących mi prawach:

1. Dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do kopiowania i przenoszenia danych oraz prawo wniesienia sprzeciwu,
2. Wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uznam, iż przetwarzanie danych osobowych dotyczących mnie narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.

Data i czytelny podpis

CEL PRZETWARZANIA – ZATRUDNIENIE NA UMOWĘ ZLECENIE I O DZIEŁO

DOBRA PRAKTYKA

1. Od pracowników zatrudnionych na umowy cywilnoprawne odbieramy klauzule informacyjne, które pozwalają na przetwarzanie danych osobowych przez kadry, jednocześnie pozwalając na realizację innych celów związanych z codziennymi obowiązkami pracownika i obowiązkami Administratora Danych.

UWAGA KONSULTANTA:

1. Rekomenduje się podpisanie klauzul z wszystkimi pracownikami zatrudnionymi w oparciu o umowy cywilnoprawne.

WZÓR ZGODY WRAZ Z KLAUZULĄ INFORMACYJNĄ

Ja niżej podpisany:

..... *oświadczam, że:*

na podstawie art 6* ust 1 litera a oraz art. 6 ust 1 litera b** Rozporządzenia Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) ***wyrażam zgodę na przetwarzanie moich danych osobowych w celach związanych z realizacją umowy cywilnoprawnej *w zakresie danych zgodnych* z zapisami Ustawy z 26 czerwca 1974 r. - Kodeks pracy (tekst jedn.: Dz.U. z 2018 r., poz. 108) oraz innych celach wynikających z zawieranych przez Administratora Danych umów oraz kontraktów i innych zobowiązań wynikających z przepisów prawa.

Do celów takich należą przede wszystkim: przekazywanie moich danych w celu realizacji umowy lub kontraktu realizowanego dla innego Administratora Danych, gdzie niezbędne jest podanie moich danych personalnych, w tym dokumentów potwierdzających kwalifikacje i uprawnienia, informacje o stanie zdrowia czy możliwości pracy w szczególnych warunkach (np. SEP, prace na wysokości, prawo jazy, paszport) dane kontaktowe, dane niezbędne do wyrobienia wizy (w oparciu o wytyczne państwa trzeciego), dane niezbędne do zakwaterowania na potrzeby wyjazdów służbowych, dane niezbędne do roszczeń innych podmiotów, w tym dane przekazywane na wniosek Sądu lub Komornika, oraz dla realizacji wszystkich celów wynikających z przepisów prawa.

Zostałem poinformowany, że:

1. *Administratorem Danych zgromadzonych w zakresie realizacji wskazanego celu jest:*
   Prezydent Miasta

   Urząd Miejski w Świętochłowicach

   Ul. Katowicka 54
   41 – 600 Świętochłowice
   tel.: (32) 3491-800 fax: (32) 3491-812
   e-mail: um@swietochlowice.pl
2. *Administrator Danych powołał Inspektora Ochrony Danych*
   Inspektor Ochrony Danych

   Urząd Miejski w Świętochłowicach

   Ul. Katowicka 54
   41 – 600 Świętochłowice

tel.: (32) 3491-800 fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

3. Zgromadzone przez Administratora Danych dane, mogą zostać udostępniane *odbiorcom tylko i wyłącznie na podstawie przepisów prawa lub w związku z wykonywaniem pracy na rzecz Administratora Danych lub jego interesariuszy w w/w celach.*
4. *Odbiorcami danych mogą być instytucje do tego uprawnione, tj. Sądy, Komornicy Sądowi, Ubezpieczyciele,*
5. *Dane osobowe nie będą przekazywane do państwa trzeciego*
6. *Dane osobowe będą przetwarzane przez okres 50 lat dla celów związanych z Ustawą Kodeks Pracy lub w okresach przewidzianych innymi przepisami prawa lub zawartymi umowami i kontraktami.*
7. *Podanie przeze mnie danych jest wymogiem ustawowym wynikającym z* Kodeksu pracy (tekst jedn.: Dz.U. z 2018 r., poz. 108)
8. *W oparciu o zgromadzone dane nie będzie wykonywane profilowanie.*

Oświadczam, że zostałam/ -em poinformowany o przysługujących mi prawach:

1. Dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do kopiowania i przenoszenia danych oraz prawo wniesienia sprzeciwu,
2. Wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uznam, iż przetwarzanie danych osobowych dotyczących mnie narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.

Data i czytelny podpis

CEL PRZETWARZANIA – PODPISYWANIE UMÓW POWIERZANIA Z INTERESARIUSZAMI URZĘDU

WYMAGANIE RODO

1. Administrator Danych ma prawo powierzyć przetwarzanie danych innym Administratorom Danych. W celu realizacji takiego prawa należy każdorazowo podpisać „Umowę powierzania przetwarzania danych" zgodną z wytycznymi art. 28 RODO. Dotyczy to sytuacji, w której Administrator Danych zleca usługi na zewnątrz, np. obsługa w zakresie kadr i płac, obsługa księgowa, obsługa prawna, obsługa BHP, obsługa informatyczna i w każdym innym przypadku, gdy przekazywane są dane pracowników do innego Administratora Danych.

UWAGA KONSULTANTA:

1. Należy upewnić się, iż usługi powierzane na zewnątrz nie są pod powierzane bez zgody Administratora Danych.
2. Należy podpisać umowy powierzania z „pracownikami" kontraktowymi, pracującymi w systemie B2B.

WZÓR UMOWY POWIERZENIA

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w dniu _____ 2018 roku w Świętochłowicach [zwana dalej '**Umową**'], pomiędzy:

Gminą Świętochłowice z siedzibą w **Urzędzie Miejskim w Świętochłowicach** (41-600), przy ul. **Katowickiej 54**, NIP 627-10-08-169, reprezentowaną przez:

1. _____ -

_____

2. _____ -

_____ zwanym w dalszej części Umowy '**Administratorem danych**' lub '**Administratorem**', a (wskazać nazwę jednostki) z siedzibą w _____ (00-000), przy ul. _____, wpisaną do Rejestru Przedsiębiorców prowadzonego przez Sąd _____ Wydział ____ Gospodarczy KRS pod numerem _____, NIP _____, REGON _____, kapitał zakładowy w wysokości _____ wpłacony w całości, e - mail: _____, reprezentowaną przez:

1. _____ -

_____

2. _____ -

_____ zwaną w dalszej części Umowy „**Podmiotem przetwarzającym**";

zwanymi są łącznie w dalszej części Umowy „**Stronami**", a każdy z nich z osobna „**Stroną**".

§ 1 Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 ogólnego Rozporządzenia Parlamentu Europejskiego 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) (zwanego w dalszej części 'Rozporządzeniem') dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie, a Podmiot przetwarzający dane te przyjmuje.

2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

§ 2 Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał dane powierzone mu na podstawie niniejszej Umowy w związku z realizacją i wyłącznie w celu prawidłowej realizacji: zawartej przez Strony umowy:

Nr: _____ z dnia _____ r.

dotyczące (należy wpisać np. danych kadrowych, płacowych, księgowych, prawnych, informatycznych etc.) pracowników oraz członków rodziny Administratora Danych.

2. Powierzone dane dotyczą:
   a. pracowników Administratora (wpisać zakres danych przekazywanych)
   b. członków rodzin pracowników Administratora (wpisać zakres danych przekazywanych)

§ 3 Obowiązki Podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim pracownikom oraz współpracownikom, którzy będą przetwarzali powierzone dane w celu realizacji niniejszej Umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, o której mowa w art. 28 ust 3 pkt b Rozporządzenia, przetwarzanych danych przez swoich pracowników oraz współpracowników, których upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej Umowy- zarówno w trakcie okresu trwania ich zatrudnienia w Podmiocie przetwarzającym lub trwania umowy współpracy, jak i po wygaśnięciu umów łączących tych pracowników i współpracowników z Podmiotem przetwarzającym.
5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usunie wszelkie dane osobowe oraz wszelkie ich istniejące kopie, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający, będzie nakazywało w tym czasie przechowywanie takich danych osobowych.
6. W granicach swoich możliwości Podmiot przetwarzający pomoże Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36

Rozporządzenia. Administrator udzieli Podmiotowi przetwarzającemu minimum 14 dniowego terminu na wywiązanie się z powyższego obowiązku.

7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi w ciągu 24 godzin.

§ 4 Prawo kontroli

1. Administrator danych, zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia, ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia Umowy oraz odpowiednich przepisów prawa.
2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego, z minimum 7- dniowym jego uprzedzeniem dokonanym na piśmie.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w uzasadnionym do tego celu terminie, w miarę możliwości nie dłuższym jednak niż 7 dni.
4. Podmiot przetwarzający udostępni Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§ 5 Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą Umową do dalszego przetwarzania swoim podwykonawcom wyłącznie w celu wykonania Umowy i po uprzednim pisemnym poinformowaniu Administratora danych o tym fakcie, wskazując dane identyfikujące tego podwykonawcę.
2. Przekazanie powierzonych danych osobowych poza granice kraju może nastąpić jedynie na pisemne polecenie Administratora danych, chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający poinformuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie. W zakresie tym Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.
4. Podwykonawcy, którym Podmiot przetwarzający powierza przetwarzanie danych osobowych w ramach prowadzonej działalności znani w dniu podpisania umowy, którym powierzenie przetwarzania nie wymaga odrębnego informowania wg pkt 1:

(należy wskazać nazwę Podmiotu)

§ 6 Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w niniejszej Umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są mu wiadome, lub

realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez właściwy dla Polski organ nadzorujący. Niniejszy zapis § 6 ust. 2 dotyczy jednak wyłącznie danych osobowych powierzonych przez Administratora danych.

§ 7 Czas trwania Umowy

1. Niniejsza Umowa obowiązuje od dnia jej zawarcia przez czas nieokreślony, z zastrzeżeniem §8 poniżej.
2. Niniejsza Umowa obejmuje kolejne następujące po sobie umowy lub zamówienia na przedłużenie usług wskazanych w §2 pkt 1.

§ 8 Rozwiązanie Umowy

1. Każda ze Stron może wypowiedzieć niniejszą Umowę z zachowaniem 1-miesięcznego okresu wypowiedzenia. Uprawnienie to nie może być jednak realizowane w okresie trwania umowy wskazanej w §2 pkt 1.
2. Administrator danych może rozwiązać niniejszą Umowę ze skutkiem natychmiastowym w przypadku, gdy Podmiot przetwarzający:
   a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
   b) przetwarza dane osobowe w sposób niezgodny z Umową;
   c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez poinformowania Administratora danych.
3. Z dniem wygaśnięcia umowy wskazanej w §2 pkt 1 automatycznemu rozwiązaniu ulega niniejsza Umowa, chyba, że Strony postanowią inaczej.
4. Z dniem wygaśnięcia umowy wskazanej w §2 pkt 1 podmiot przetwarzający zobowiązuje się do niezwłocznego usunięcia danych osobowych.

§ 9 Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych w związku z realizacją niniejszej Umowy [dalej jako '**Dane poufne**'].
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem go do zachowania w tajemnicy Danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa, decyzji sądu lub właściwego organu lub Umowy.

§ 10 Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
2. Wszelkie zmiany lub uzupełnienia niniejszej Umowy wymagają dla swej ważności formy pisemnego aneksu.
3. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
4. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej Umowy będzie sąd właściwy Administratora danych.

PODPISY:

W imieniu

W imieniu **Administratora danych**

CEL PRZETWARZANIA – ZAWARCIE UBEZPIECZENIA PRZEZ PRACOWNIKA (W SWOIM IMIENIU I RODZINY, W TYM NIELETNICH)

DOBRA PRAKTYKA:

1. Od pracowników odbieramy klauzule informacyjne, które pozwalają na przetwarzanie danych osobowych pracownika oraz członków rodziny (innych uposażonych) w tym małoletnich, dla których pracownik jest rodzicem lub opiekunem prawnym

UWAGA KONSULTANTA:

1. Należy zweryfikować czy w umowach z ubezpieczycielem nie zawarto informacji o tym, że to ubezpieczyciel jest Administratorem Danych. Wtedy to na nim ciąży obowiązek informacyjny dla pracowników Urzędu. Niezależnie od tego kto jest Administratorem Danych, jeśli to pracownik Urzędu przetwarza dane zbierając kwestionariusze (w tym skany np. aktów urodzenia, aktów zgonów, etc), przesyła je do ubezpieczyciela, posiadając kopię to należy Urząd traktować jako Administratora Danych przetwarzających dane pracowników do celów ubezpieczeniowych. Jeśli pracownik Urzędu przetwarza dane pracowników do celów ubezpieczeniowych ale ubezpieczyciel jest Administrator Danych należy zweryfikować umowę w związku z potrzebą podpisania Umowy powierzania przetwarzania danych pomiędzy Urzędem a ubezpieczycielem.
2. Rekomenduje się podpisanie klauzul z wszystkimi etatowymi pracownikami Urzędu którzy zawarli(będą zawierali) umowy ubezpieczeniowe
3. Rekomenduje się podpisanie umów powierzenia przetwarzania danych osobowych z ubezpieczycielem.

WZÓR ZGODY WRAZ Z KLAUZULĄ INFORMACYJNĄ

Ja niżej podpisany:

..... oświadczam, że:

na podstawie art 6* ust 1 litera a oraz art. 6 ust 1 litera f** Rozporządzenia Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) ***wyrażam zgodę na przetwarzanie moich danych osobowych w celach związanych z ubezpieczeniem moim oraz członków mojej rodziny.

Zostałem poinformowany, że:

1. *Administratorem Danych zgromadzonych w zakresie realizacji wskazanego celu jest:*
   Prezydent Miasta

   Urząd Miejski w Świętochłowicach

   Ul. Katowicka 54
   41 – 600 Świętochłowice
   tel.: (32) 3491-800 fax: (32) 3491-812
   e-mail: um@swietochlowice.pl
2. *Administrator Danych powołał Inspektora Ochrony Danych*
   Inspektor Ochrony Danych

   Urząd Miejski w Świętochłowicach

   Ul. Katowicka 54

41 – 600 Świętochłowice
tel.: (32) 3491-800 fax: (32) 3491-812
e-mail: iod@swietochlowice.pl

3. Zgromadzone przez Administratora Danych dane, mogą zostać udostępniane *odbiorcom tylko i wyłącznie na podstawie przepisów prawa do celów związanych z ubezpieczeniem.*
4. *Odbiorcami danych mogą być instytucje do tego uprawnione, tj. Sądy, Komornicy Sądowi, Ubezpieczyciele,*
5. *Dane osobowe nie będą przekazywane do państwa trzeciego*
6. *Dane osobowe będą przetwarzane przez okres trwania umowy ubezpieczenia lub* do momentu sprzeciwu. Okres ten może zostać przedłużony do czasu, upływu okresu przedawnienia ewentualnych roszczeń, jeśli przetwarzanie danych osobowych będzie niezbędne do dochodzenia lub obrony przed takimi roszczeniami.
7. *W oparciu o zgromadzone dane nie będzie wykonywane profilowanie.*

Oświadczam, że zostałam/ -em poinformowany o przysługujących mi prawach:

1. Dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do kopiowania i przenoszenia danych oraz prawo wniesienia sprzeciwu,
2. Wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uznam, iż przetwarzanie danych osobowych dotyczących mnie narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.

Data i czytelny podpis

WZÓR UMOWY POWIERZENIA Z UBEZPIECZYCIELEM

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w dniu _____ 2018 roku w XXXXXXXXXX [zwana dalej '**Umową**'], pomiędzy:

_____ z siedzibą w _____ (00-000), przy ul. _____, wpisaną do Rejestru Przedsiębiorców prowadzonego przez Sąd _____Wydział ____ Gospodarczy KRS pod numerem _____, NIP _____, REGON _____, kapitał zakładowy w wysokości _____ wpłacony w całości, e - mail: _____, reprezentowaną przez:

3._____ -

_____

4._____ -

_____ zwanym w dalszej części Umowy **'Administratorem danych'** lub **'Administratorem'**, a

(wskazać nazwę ubezpieczyciela) z siedzibą w _____ (00-000), przy ul. _____, wpisaną do Rejestru Przedsiębiorców prowadzonego przez Sąd _____Wydział ____ Gospodarczy KRS pod numerem _____, NIP _____, REGON _____, kapitał

zakładowy w wysokości _____ wpłacony w całości, e - mail: _____, reprezentowaną przez:

3. _____ -

_____

4. _____ -

_____ zwaną w dalszej części Umowy „**Podmiotem przetwarzającym**";

zwanymi są łącznie w dalszej części Umowy **„Stronami"**, a każdy z nich z osobna **„Stroną"**.

§ 11 Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 ogólnego Rozporządzenia Parlamentu Europejskiego 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) (zwanego w dalszej części 'Rozporządzeniem') dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie, a Podmiot przetwarzający dane te przyjmuje.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

§ 12 Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał dane powierzone mu na podstawie niniejszej Umowy w związku z realizacją i wyłącznie w celu prawidłowej realizacji: zawartej przez Strony umowy:

   Nr: _____ z dnia _____r.

   dotyczące ubezpieczenia pracowników oraz członków rodziny Administratora Danych.

2. Powierzone dane dotyczą:
   a. pracowników Administratora (wpisać zakres danych przekazywanych ubezpieczycielowi)
   b. członków rodzin pracowników Administratora (wpisać zakres danych przekazywanych ubezpieczycielowi)

§ 13 Obowiązki Podmiotu przetwarzającego

3. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
4. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.

5. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim pracownikom oraz współpracownikom, którzy będą przetwarzali powierzone dane w celu realizacji niniejszej Umowy.
6. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, o której mowa w art. 28 ust 3 pkt b Rozporządzenia, przetwarzanych danych przez swoich pracowników oraz współpracowników, których upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej Umowy- zarówno w trakcie okresu trwania ich zatrudnienia w Podmiocie przetwarzającym lub trwania umowy współpracy, jak i po wygaśnięciu umów łączących tych pracowników i współpracowników z Podmiotem przetwarzającym.
7. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usunie wszelkie dane osobowe oraz wszelkie ich istniejące kopie, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający, będzie nakazywało w tym czasie przechowywanie takich danych osobowych.
8. W granicach swoich możliwości Podmiot przetwarzający pomoże Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia. Administrator udzieli Podmiotowi przetwarzającemu minimum 14 dniowego terminu na wywiązanie się z powyższego obowiązku.
9. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi w ciągu 24 godzin.

§ 14 Prawo kontroli

1. Administrator danych, zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia, ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia Umowy oraz odpowiednich przepisów prawa.
2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego, z minimum 7- dniowym jego uprzedzeniem dokonanym na piśmie.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w uzasadnionym do tego celu terminie, w miarę możliwości nie dłuższym jednak niż 7 dni.
4. Podmiot przetwarzający udostępni Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§ 15 Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą Umową do dalszego przetwarzania swoim podwykonawcom wyłącznie w celu wykonania Umowy
2. i po uprzednim pisemnym poinformowaniu Administratora danych o tym fakcie, wskazując dane identyfikujące tego podwykonawcę.
3. Przekazanie powierzonych danych osobowych poza granice kraju może nastąpić jedynie na pisemne polecenie Administratora danych, chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający poinformuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
4. Podwykonawca winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie. W zakresie tym Podmiot przetwarzający

ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

5. Podwykonawcy, którym Podmiot przetwarzający powierza przetwarzanie danych osobowych w ramach prowadzonej działalności znani w dniu podpisania umowy, którym powierzenie przetwarzania nie wymaga odrębnego informowania wg pkt 1:

§ 16 Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w niniejszej Umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są mu wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez właściwy dla Polski organ nadzorujący. Niniejszy zapis § 6 ust. 2 dotyczy jednak wyłącznie danych osobowych powierzonych przez Administratora danych.

§ 17 Czas trwania Umowy

1. Niniejsza Umowa obowiązuje od dnia jej zawarcia przez czas nieokreślony, z zastrzeżeniem §8 poniżej.
2. Niniejsza Umowa obejmuje kolejne następujące po sobie umowy lub zamówienia na przedłużenie usług wskazanych w §2 pkt 1.

§ 18 Rozwiązanie Umowy

1. Każda ze Stron może wypowiedzieć niniejszą Umowę z zachowaniem 1-miesięcznego okresu wypowiedzenia. Uprawnienie to nie może być jednak realizowane w okresie trwania umowy wskazanej w §2 pkt 1.
2. Administrator danych może rozwiązać niniejszą Umowę ze skutkiem natychmiastowym w przypadku, gdy Podmiot przetwarzający:
   d) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
   e) przetwarza dane osobowe w sposób niezgodny z Umową;
   f) powierzył przetwarzanie danych osobowych innemu podmiotowi bez poinformowania Administratora danych.

3. Z dniem wygaśnięcia umowy wskazanej w §2 pkt 1 automatycznemu rozwiązaniu ulega niniejsza Umowa, chyba, że Strony postanowią inaczej.

4. Z dniem wygaśnięcia umowy wskazanej w §2 pkt 1 podmiot przetwarzający zobowiązuje się do niezwłocznego usunięcia danych osobowych.

§ 19 Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych w związku z realizacją niniejszej Umowy [dalej jako '**Dane poufne**'].

2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem go do zachowania w tajemnicy Danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa, decyzji sądu lub właściwego organu lub Umowy.

§ 20 Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
2. Wszelkie zmiany lub uzupełnienia niniejszej Umowy wymagają dla swej ważności formy pisemnego aneksu.
3. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
4. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej Umowy będzie sąd właściwy Administratora danych.

PODPISY:

W imieniu **Ubezpieczyciela** W imieniu **Administratora danych**

CEL PRZETWARZANIA - MARKETING BEZPOŚREDNI

UWAGI KONSULTANTA

Należy pamiętać, iż zgodnie z RODO tworzenie bazy marketingowej w oparciu o otrzymane wizytówki jest nielegalne. Atrybut nielegalności będzie możliwy do usunięciu poprzez działania Administrator Danych opisane w dalszej części opisu.

Należy pamiętać, iż motyw 32 RODO określa zasady wyrażania zgody, która *powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwolenie osoby, których dane dotyczą, na przetwarzanie dotyczących jej danych osobowych.*

Na pozyskującym zgodę ciąży obowiązek udowodnienia, że faktycznie i skutecznie ją pozyskał. Zgodnie z motywem 32 RODO zgoda może mieć formę pisemnego (w tym elektronicznego) lub ustnego oświadczenia. Jednakże ustne oświadczenie bywa trudne do udowodnienia (potrzebne jest nagranie lub obiektywni świadkowie).

Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą. Zgodnie z ust. 4 usprawiedliwionym celem jest marketing bezpośredni własnych produktów lub usług. Jednakże warto zwrócić uwagę, że art. 172 ustawy Prawo Telekomunikacyjne, ogranicza zasady legalnie świadczonego marketingu produktów własnych bez pozyskania zgody odbiorcy. Zgodnie z nim, na działania marketingowe świadczone elektronicznie musi zostać pozyskana zgoda. *Zakazane jest używanie telekomunikacyjnych urządzeń końcowych (TUK) i automatycznych systemów wywołujących (ASW) dla celów marketingu bezpośredniego, chyba że abonent lub użytkownik końcowy uprzednio wyraził na to zgodę*. Za złamanie zakazu, o którym mowa w Prawie Telekomunikacyjnym grozi kara do 3% przychodu.

Bezpośrednio w RODO w Preambule w punkcie 47 zapisano:

„Podstawą prawną przetwarzania mogą być prawnie uzasadnione interesy administratora, w tym administratora, któremu mogą zostać ujawnione dane osobowe, lub strony trzeciej, o ile w świetle rozsądnych oczekiwań osób, których dane dotyczą, opartych na ich powiązaniach z administratorem nadrzędne nie są interesy lub podstawowe prawa i wolności osoby, której dane dotyczą. Taki prawnie uzasadniony interes może istnieć na przykład w przypadkach, gdy zachodzi istotny i odpowiedni rodzaj powiązania między osobą, której dane dotyczą, a administratorem, na przykład, gdy osoba, której dane dotyczą, jest klientem administratora lub działa na jego rzecz. Aby stwierdzić istnienie prawnie uzasadnionego interesu, należałoby w każdym przypadku przeprowadzić dokładną ocenę, w tym ocenę tego, czy w czasie i w kontekście, w którym zbierane są dane osobowe, osoba, której dane dotyczą, ma rozsądne przesłanki by spodziewać się, że może nastąpić przetwarzanie danych w tym celu. Interesy i prawa podstawowe osoby, której dane dotyczą, mogą być nadrzędne wobec interesu administratora danych w szczególności w przypadkach, gdy dane osobowe są przetwarzane w sytuacji, w której osoby, których dane dotyczą, nie mają rozsądnych przesłanek, by spodziewać się dalszego przetwarzania. Ponieważ dla organów publicznych podstawę prawną przetwarzania danych osobowych powinien określić ustawodawca, prawnie uzasadniony interes administratora nie powinien mieć zastosowania jako podstawa prawna do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań. **Prawnie uzasadnionym interesem administratora, którego sprawa dotyczy, jest również przetwarzanie danych osobowych bezwzględnie niezbędne do zapobiegania oszustwom. Za działanie wykonywane w prawnie uzasadnionym interesie można uznać przetwarzanie danych osobowych do celów marketingu bezpośredniego".**

DZIAŁANIE ZGODNE Z RODO

W ocenie Konsultanta przekazanie na targach lub podczas bezpośredniego spotkania wizytówki, przekazanie informacji telefonicznej z prośbą o przesłanie informacji, czy oferty spełnia przesłanki 47 punktu Preambuły do RODO „[interesariusz] ma rozsądne przesłanki by spodziewać się, że może nastąpić przetwarzanie danych w tym celu"

PRAWO DO SPRZECIWU NA MARKETING BEZPOŚREDNI

Należy jednak pamiętać, że punkt 70 Preambuły RODO mówi:

„Jeżeli dane osobowe są przetwarzane do celów marketingu bezpośredniego, osoba, której dane dotyczą, powinna mieć prawo wnieść w dowolnym momencie, bezpłatnie sprzeciw wobec tego przetwarzania, pierwotnego lub dalszego – w tym profilowania, o ile jest ono powiązane z marketingiem bezpośrednim. Prawo to powinno zostać wyraźnie podane do wiadomości osobie, której dane dotyczą, oraz powinno być przedstawione jasno i oddzielnie od wszelkich innych informacji".

Artykuł 21 RODO określa w punkcie 1, że „osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f), w tym profilowania na podstawie tych przepisów. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń. 2.Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim. 3.Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów".

DOBRA PRAKTYKA W MARKETINGU

1. Należy w pierwszym możliwym momencie przekazać do Interesariusza maila z następującą informacją:

WZÓR MAILA DO KLIENTA W BAZIE MARKETINGOWEJ I HANDLOWEJ.

„Szanowna Pani/ Szanowny Panie

Pani/Pana dane osobowe (imię nazwisko, adres korespondencyjny, adres poczty elektronicznej, stanowisko, nr telefonu/ są w naszej bazie danych osób do których wysyłamy informację handlowe, marketingowe oraz oferty. Dołożyliśmy wszelkich starań, aby zadbać o ich bezpieczeństwo.

Jeśli nie chce Pani/ Pan otrzymywać od nas informacji marketingowych, w tym o promocjach oraz informacji handlowych, prosimy o taką informację na adres e-mail: ..... lub na numer telefonu ..... lub pocztą tradycyjną na adres: .....z dopiskiem dane osobowe.

W każdym momencie może Pani/ Pan zgłosić sprzeciw do wobec przetwarzania pani/ Pana danych. Wystarczy wysłać e-mail na adres .....

Administratorem Danych jest .....z siedzibą w .....

Inspektor Ochrony Danych, z którym można się skontaktować pod adresem e-mail ..... w każdej sprawie dotyczącej danych.

Pani/ Pana dane mogą być przekazywane naszym podwykonawcom – dostawcom usług informatycznych – wyłącznie w celu realizacji naszych celów. Od 25 maja 2018r podstawą prawną przetwarzania danych osobowych znajdujących się w bazie osób korzystających z informacji marketingowych i handlowych jest art. 6 ust 1 litera f Rozporządzenia PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), tj prawnie uzasadniony interes realizowany przez Administratora Danych.

Oznacza to, że Pani/ Pana dane będą przetwarzane przede wszystkim w celu przesyłania informacji i ofert, a także w celach analitycznych, statystycznych oraz ewentualnego ustalenia i dochodzenia roszczeń, oraz ochrony przez roszczeniami. Dane osobowe będą przetwarzane do momentu sprzeciwu. Okres ten może zostać przedłużony do czasu, upływu okresu przedawnienia ewentualnych roszczeń, jeśli przetwarzanie danych osobowych będzie niezbędne do dochodzenia lub obrony przed takimi roszczeniami.

Przysługuje Pani/ Panu prawo dostępu do tych danych, sprostowania i usunięcia lub ograniczenia przetwarzania, a także prawo do przenoszenia tych danych do innego Administratora Danych.

W każdym czasie może Pani/ Pan wnieść skargę do organu nadzorującego przestrzeganie przepisów o ochronie danych osobowych, jeśli uzna Pani/Pan że przetwarzanie Pani/ Pana danych narusza Rozporządzenia PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Powyższe informacje dotyczą przetwarzania Pani/ Pana danych osobowych do celów wskazanych powyżej i znajdujących się w bazie osób korzystających z informacji marketingowych i handlowych.

WZÓR MAILA DO KLIENTA Z ZAPROSZENIEM NA EVENT / SZKOLENIE ORGANIZOWANY PRZEZ ADMINISTRATORA DANYCH.

Szanowna Pani/ Szanowny Panie
Pani/Pana dane osobowe (imię nazwisko, adres korespondencyjny / adres poczty elektronicznej, stanowisko, nr telefonu/ są w naszej bazie danych osób zapraszanych na organizowane przez nasz Urząd wydarzenia i szkolenia. Dołożyliśmy wszelkich starań, aby zadbać o ich bezpieczeństwo.
Jeśli nie chce Pani/ Pan otrzymywać od nas informacji i zaproszeń, prosimy o taką informację na adres e-mail: ..... lub na numer telefonu ..... lub pocztą tradycyjną na adres: .....z dopiskiem dane osobowe.
W każdym momencie może Pani/ Pan zgłosić sprzeciw do wobec przetwarzania pani/ Pana danych. Wystarczy wysłać e-mail na adres .....
Administratorem Danych jest .....z siedzibą w .....
Inspektor Ochrony Danych, z którym można się skontaktować pod adresem e-mail ..... w każdej sprawie dotyczącej danych.
Pani/ Pana dane mogą być przekazywane naszym podwykonawcom – dostawcom usług informatycznych – wyłącznie w celu realizacji naszych celów. Od 25 maja 2018r podstawą prawną przetwarzania danych osobowych znajdujących się w bazie osób zapraszanych na wydarzenia jest art. 6 ust 1 litera f Rozporządzenia PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), tj prawnie uzasadniony interes realizowany przez Administratora Danych. Oznacza to, że Pani/ Pana dane będą przetwarzane przede wszystkim w celu przesyłania informacji i zaproszeń, a także w celach analitycznych, statystycznych oraz ewentualnego ustalenia i dochodzenia roszczeń, oraz ochrony przez roszczeniami. Dane osobowe będą przetwarzane do momentu sprzeciwu. Okres ten może zostać przedłużony do czasu, upływu okresu przedawnienia ewentualnych roszczeń, jeśli przetwarzanie danych osobowych będzie niezbędne do dochodzenia lub obrony przed takimi roszczeniami.
Przysługuje Pani/ Panu prawo dostępu do tych danych, sprostowania i usunięcia lub ograniczenia przetwarzania, a także prawo do przenoszenia tych danych do innego Administratora Danych.
W każdym czasie może Pani/ Pan wnieść skargę do organu nadzorującego przestrzeganie przepisów o ochronie danych osobowych, jeśli uzna Pani/Pan że przetwarzanie Pani/ Pana danych narusza Rozporządzenia PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
Powyższe informacje dotyczą przetwarzania Pani/ Pana danych osobowych do celów wskazanych powyżej i znajdujących się w bazie osób zapraszanych na organizowane przez nas wydarzenia i szkolenia.

CEL PRZETWARZANIE DANYCH NIEZBĘDNYCH DO OTRZYMYWANIA NEWSLETTERA (formularze internetowe)

UWAGA KONSULTANTA:
Jeśli Urząd ofertuje możliwość wysyłki newslettera elektronicznego należy uzyskać od Klienta zgodę na przetwarzanie jego danych osobowych.

TREŚĆ NIEZBĘDNA DO WYSYŁKI NEWSLETTERA

1. **Treść obecnej klauzuli należy zastąpić treścią:**

   .....
   „Wyrażam zgodę na przetwarzanie danych osobowych dla potrzeb niezbędnych do przesyłania newslettera Urzędu Miejskiego w Świętochłowicach".
   UWAGA: Brak zaznaczenia pola uniemożliwia wysłanie wniosku.

2. **Dodanie klauzul informacyjnych:**

Administratorem podanych danych osobowych jest

Prezydent Miasta

Urząd Miejski w Świętochłowicach

Ul. Katowicka 54
41 – 600 Świętochłowice
tel.: (32) 3491-800 fax: (32) 3491-812
e-mail: um@swietochlowice.pl

Podanie danych jest dobrowolne, ale niezbędne w celu cyklicznej wysyłki newslettera firmowego.
Podane dane będą przetwarzane na podstawie art. 6 ust. 1 lit. a zgodnie z treścią Ogólnego Rozporządzenia o Ochronie Danych Osobowych z dnia 27 kwietnia 2016 r.
Administrator Danych powołał Inspektora Ochrony Danych, z którym można skontaktować się za pośrednictwem poczty elektronicznej: iod@swietochlowice.pl
Dane osobowe będą przechowywane przez okres 24 miesięcy (Termin do ustalenia można regulować według własnego uznania) od wygaśnięcia ostatniego kontraktu.
Osobie, której dane dotyczą przysługuje prawo do:

1) dostępu do treści swoich danych, ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania;
2) wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna, iż przetwarzanie danych osobowych narusza przepisy Ogólnego Rozporządzenia o Ochronie Danych Osobowych z dnia 27 kwietnia 2016 r.

3. Dodanie pola chceck box:

   Oświadczam, że zapoznałem się z powyższymi informacjami i wyrażam zgodę na przetwarzanie danych osobowych.

UWAGA: Brak zaznaczenia pola uniemożliwia wysłanie wniosku o przesyłanie newslettera

UPOWAŻNIENIE I OŚWIADCZENIE PRACOWNIKA URZĘDU

Ostrów Wielkopolski, dnia .....

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Działając na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) **upoważniam Panią/Pana**:

Imię Nazwisko pracownika .....

zatrudnioną/-ego na stanowisku .....

do przetwarzania danych osobowych związanych z celami przetwarzania Administratora Danych, do których mam dostęp w związku z wykonywaniem czynności służbowych.

OŚWIADCZAM

Ja niżej podpisany: .....

- **Stwierdzam, iż jest mi znana definicja danych osobowych** Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
- **Stwierdzam, iż są mi znane prawa osób fizycznych do ochrony danych osobowych wynikające z** Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy
  95/46/WE (ogólne rozporządzenie o ochronie danych)
- **Stwierdzam, że przetwarzając dane osobowe, do których mam dostęp w związku z realizacją prac, będę działał/-a zgodnie z zasadami** opisanymi w Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
- **Zobowiązuję się do zachowania w tajemnicy danych osobowych**, do których mam lub będę miał/a dostęp w związku z wykonywaniem czynności służbowych, a w szczególności nie będę w celach niezgodnych z celem przetwarzania danych, wykorzystywał/a danych osobowych, z którymi zapoznałem/am się, o ile nie są one powszechnie znane.
- **Zobowiązuję się do zachować w tajemnicy** sposoby zabezpieczenia danych osobowych stosowne u Administratora Danych o ile nie są one powszechnie znane lub nie wynikają w sposób oczywisty z innych powszechnie znanych informacji.
- Ponadto **przyjmuję do wiadomości**, iż sposoby zabezpieczenia danych stosowane u Administratora Danych są tajemnicą przedsiębiorstwa w rozumieniu art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 roku o zwalczaniu nieuczciwej konkurencji (tekst jednolity Dz. U. 2003, Nr 153, poz. 1503 z późn. zm.)
- **Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane przez Administratora Danych** za naruszenie przepisów karnych.
- Po zapoznaniu się z treścią art. 266 § 1 Kodeksu karnego, który stanowi: „kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze

ograniczenia wolności albo pozbawiania wolności do lat 2, **zobowiązuję się nie ujawniać nikomu i w żaden sposób oraz nie wykorzystywać informacji, z którymi zapoznam się u Administratora Danych, w innym celu, niż to określono w umowie.**

DATA I CZYTELNY PODPIS

DOBRE PRAKTYKI BEZPIECZEŃSTWA TELEINFORMATYCZNEGO

Bezpieczeństwo urządzeń mobilnych

Dostęp do danych organizacji z wykorzystaniem urządzeń mobilnych (smartfony, tablety) możliwy jest wyłącznie z urządzeń służbowych, przekazanych przez pracodawcę do wykonywania wymaganych zadań. Wszystkie urządzenia mobilne w organizacji, na których znajdują się lub są przetwarzane dane osobowe, powinny być chronione przed nieuprawnionym dostępem do danych w przypadku kradzieży lub zgubienia urządzenia. Każde urządzenie mobilne powinno być zaszyfrowane (z karta pamięci włącznie), a dostęp do urządzenia chroniony pinem (min. 6 cyfrowym), hasłem (min. 8 znakowym), odciskiem palca lub skanem twarzy. Urządzenia powinny być tak skonfigurowane, aby po 10 nieudanych próbach zalogowania do urządzenia następowało automatyczne wyzerowanie urządzenia z danych na nim przechowywanych. Administratorzy powinni mieć możliwość zdalnego zarządzania urządzeniem, wymuszając polityki haseł i konfiguracji oraz mieć możliwość zdalnego wyczyszczenia (resetu) urządzenia. Wymaga to wdrożenia systemu MDM (Mobile Device Management) przez organizację.

Bezpieczeństwo nośników zewnętrznych

Organizacja powinna kontrolować użycie nośników zewnętrznych (pendrive'y, dyski przenośne), a ich wykorzystanie przez pracowników winno być dozwolone wyłącznie w uzasadnionych przypadkach za zgodą przełożonego. Nie dopuszcza się używania urządzeń prywatnych, każdy nośnik zewnętrzny winien być przekazany przez pracodawcę w ramach sprzętu służbowego. Stacje robocze powinny być ściśle kontrolowane pod kątem podłączanych urządzeń. Dopuszcza się możliwość podłączenia wyłącznie urządzeń zidentyfikowanych i zatwierdzonych przez administratorów. Każde urządzenie przenośne powinno być w pełni zaszyfrowane, uniemożliwiając odczytanie jego zawartości bez podania hasła, pinu lub klucza. Zaleca się także wdrożenie kompleksowej technologii DLP (Data Leakage Protection).

Bezpieczeństwo komputerów mobilnych (laptopów)

Dopuszcza się korzystanie z komputerów mobilnych będących własnością organizacji w ramach powierzonego sprzętu służbowego. Konfiguracja każdego laptopa powinna być maksymalnie utwardzona przez wykorzystanie centralnych zasad zgodnie z najlepszymi praktykami. Dysk każdego laptopa powinien być w pełni zaszyfrowany, uniemożliwiając dostęp do znajdujących się na dysku danych osobom nieupoważnionym (zgubienie, kradzież).

Oprogramowanie antywirusowe

Każdy komputer/system wykorzystywany w organizacji powinien być wyposażony w oprogramowanie antywirusowe. System antywirusowy powinien działać w oparciu o centralną konsolę, dając możliwość administratorom centralne zarządzanie ustawieniami agentów oraz generowanie raportów. Definicje baz oprogramowania antywirusowego powinny być na bieżąco aktualizowane. Nie dopuszcza się starszej wersji bazy niż 48h. Dotyczy to również urządzeń mobilnych, których producent dopuszcza instalację oprogramowania antywirusowego (np. Android).

Zapora sieciowa (firewall)

Każdy komputer w organizacji powinien być wyposażony w zaporę sieciową, blokującą niepożądany ruch sieciowy. Reguły zapory winny być centralnie zarządzane przez zespół administratorów. Reguły zezwalające na konkretny ruch (port, protokół, aplikacja) powinny dopuszczać ruch niezbędny do zarządzania stacjami roboczymi, laptopami i serwerami oraz wymagany przez pracownika na danym stanowisku. Każdy nadmiarowy ruch powinien być domyślnie zabroniony.

Aktualizacje systemów i aplikacji

Wszystkie systemy operacyjne i aplikacje powinny być regularnie aktualizowane zgodnie z przyjętą polityką aktualizacji. Aktualizacje łatające wykryte luki zabezpieczeń oznaczone jako krytyczne lub wysokie powinny być wdrożone do 24h od momentu publikacji aktualizacji. Przed produkcyjnym wdrożeniem aktualizacji powinny one być przetestowane na systemach testowych celem sprawdzenia poprawności ich działania. Administratorzy powinni mieć możliwość wygenerowania raportów o statusie aktualizacji dla każdego z systemów.

Utwardzenie konfiguracji systemów

Konfiguracja systemów operacyjnych powinna być maksymalnie utwardzona zgodnie z najlepszymi praktykami producentów oraz niezależnych organizacji (np. CIS, NIST czy CISA), zmniejszając obszar ataku i przełamania zabezpieczeń systemów.
Konfiguracja powinna być regularnie weryfikowana.

Najmniejsze możliwe uprawnienia

Każdy użytkownik systemu powinien pracować na regularnym koncie użytkownika. Nie dopuszcza się pracy na koncie administratora użytkownikom nie będącym członkiem zespołu administratorów IT. Wszystkie nadawane uprawnienia powinny być konfigurowane zgodnie z zasadą najmniejszych możliwych uprawnień.

Rozliczalność użytkowników i logowanie do systemu

Każdy użytkownik powinien być dopuszczony do systemu wyłącznie przez zalogowanie z wykorzystaniem unikalnego identyfikatora (loginu) i hasła zgodnego z przyjętą polityką haseł. W systemach i aplikacjach sklasyfikowanych jako krytyczne wymogiem jest uwierzytelnianie dwuskładnikowe z użyciem kart inteligentnych lub tokenów z kodem jednorazowym. Każda zmiana w systemie lub aplikacji przez użytkownika powinna być możliwa do zidentyfikowania, przez którego użytkownika została wykonana. Nie dopuszcza się współdzielenia kont pomiędzy użytkownikami systemu.

Nadawanie i odbieranie uprawnień

Użytkownicy zostają dopuszczeni do pracy w systemie na wniosek bezpośredniego przełożonego. Przełożony we wniosku określa zestaw uprawnień niezbędny do pracy w systemie na danym stanowisku. Administratorzy systemu na bazie poprawnego wniosku tworzą konto użytkownika, ustawiają początkowe hasło, które musi być zmienione przy pierwszym logowaniu oraz dodają użytkownika do wymaganych grup. Nadają również dostęp do aplikacji. W przypadku, gdy pracownik przestaje świadczyć pracę na rzecz organizacji, jego konto jest natychmiast wyłączane przez administratora na wniosek bezpośredniego przełożonego pracownika lub przedstawiciela działu kadr. Po 90 dniach konto może zostać usunięte permanentnie.

Regularne skany podatnościowe

Organizacja zobowiązana jest do przeprowadzania regularnych skanów podatnościowych, umożliwiających automatyczne wykrywanie brakujących aktualizacji zabezpieczeń na poziomie systemów i aplikacji oraz luk w konfiguracji. Skany podatnościowe winny być wykonywane przynajmniej raz na 3 miesiące; na podstawie wygenerowanego raportu odpowiednie akcje usuwające luki powinny być przeprowadzone przez zespół administratorów.

Bezpieczna komunikacja

Każda komunikacja sieciowa, na poziomie której przesyłane są dane osobowe, w tym dane wrażliwe, powinna odbywać się z wykorzystaniem protokołów szyfrowanych, celem zapewnienia integralności i poufności danych.

Wykrywanie incydentów bezpieczeństwa

Organizacja powinna wdrożyć technologie i mechanizmy umożliwiające zautomatyzowany sposób reakcji na incydenty bezpieczeństwa w systemach i sieci. Zaleca się wdrożenie technologii typu SIEM i IDS/IPS. Administratorzy powinni mieć wdrożoną konsolę umożliwiającą śledzenie incydentów bezpieczeństwa, na podstawie których mogą podjąć działania niwelujące szkodliwe działania. Organizacja powinna wykryć incydenty bezpieczeństwa najpóźniej do 72 godzin od momentu powstania incydentu.

Kontrola dostępu do Internetu

Dostęp do Internetu powinien być ściśle monitorowany i możliwie ograniczony, najlepiej z wykorzystaniem serwera proxy, na którym wdrożone zostały odpowiednie polityki dostępu. W szczególności blokowane powinny być usługi umożliwiające przesyłanie i składowanie plików na zewnętrze dyski w chmurze, jak Dropbox, OneDrive czy Google Drive. Należy również rozważyć blokadę stron typu social media czy dostępu do prywatnych skrzynek email. Zabrania się bezpośredniego podłączania komputerów do Internetu, sieć wewnętrzna powinna być odseparowana od Internetu dedykowaną zaporą sieciową.

Bezpieczna utylizacja sprzętu

Każdy dysk serwera lub komputera, a także nośniki wymienne/przenośne powinny być utylizowane w sposób bezpieczny, najlepiej przez fizyczne uszkodzenie. W przypadku konieczności oddania komputera do serwisu przekazanie sprzętu nie powinno dotyczyć dysków twardych.

Kontrola dostępu do sieci wewnętrznej

Organizacja powinna zapobiec możliwości podłączenia do sieci wewnętrznej niezidentyfikowanych komputerów, zarówno z wykorzystaniem sieci kablowej jak i bezprzewodowej. Podłączenie nieautoryzowanego komputera powinno skutkować brakiem dostępu do sieci i jej zasobów. O takim fakcie powinien również zostać powiadomiony zespół administratorów.

Archiwizacja danych

Ważne z punktu widzenia dostępności dane powinny być regularnie archiwizowane zgodnie z przyjęta w organizacji polityką archiwizacji. Dotyczy to zarówno systemów i ich konfiguracji, baz danych i aplikacji. Archiwa winny być przechowywane w sposób bezpieczny, uniemożliwiając do nich dostęp osobom postronnym. Należy regularnie wykonywać testy odtworzenia systemów i danych, sprawdzając ich poprawność oraz procedury odzyskiwania. Jedna z kopii danych winna być przechowywana poza strefą, w której znajdują się archiwizowane systemy, jeśli to możliwe w innym budynku. Transport nośników powinien odbywać się w sposób bezpieczny, a kopie przechowywane w miejscu niedostępnym poza administratorami systemu i osobami upoważnionymi.

Blokada ekranu

Ekrany komputerów powinny być automatycznie blokowane po 5min. bezczynności użytkownika. Ponowne odblokowanie powinno się odbywać przez podanie hasła przez pracownika.

Hasła

Hasła winny być zmieniane co najmniej raz na 30 dni, minimalna długość hasło powinna wynosić 8 znaków, zasady haseł powinny spełniać zasady złożoności, a historia haseł blokować co najmniej 12 ostatnio użytych haseł.

Wysoka dostępność systemów i usług

Systemy krytyczne powinny być odporne na awarie, aby zachować ich ciągłość działania. Każdy element mogący ulec uszkodzeniu powinien być zdublowany. Należy wdrożyć techniki umożliwiające zachowanie ciągłości działania, jak klastry, wielokrotne ścieżki dostępu czy replikację danych, niwelując przy tym pojedyncze punkty awarii.

PREZYDENT MIASTA
Daniel Beger