„WYCIĄG DLA KONTRAHENTA

Z POLITYKI OCHRONY DANYCH OSOBOWYCH

I BEZPIECZEŃSTWA INFORMACJI

URZĘDU MIEJSKIEGO WROCŁAWIA”

Wersja 1.1 (K17/21)

Wrocław, 30.04.2021 r.

Celem dokumentu jest zapoznanie kontrahenta z kluczowymi zasadami funkcjonowania systemu zarządzania bezpieczeństwem informacji w Urzędzie Miejskim Wrocławia, a w szczególności z zasadami ochrony danych osobowych.

Wykorzystywanie lub udostępnianie w celu innym niż wskazany jest zabronione.

Spis treści

Po wydrukowaniu dokument nienadzorowany.

SEBASTIAN PATRYK SOBECKI

Elektronicznie podpisany przez SEBASTIAN PATRYK SOBECKI
Data: 2021.05.25 11:31:11 +02'00'

Preambuła

Realizując konstytucyjne prawo każdej osoby do ochrony życia prywatnego oraz przepisy 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) (Dz. U. UE L 119 z 4 maja 2016 r., s. 1 z późn. zm.) w celu zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ww. rozporządzenia oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, wprowadza się do stosowania w Urzędzie Miejskim Wrocławia rozwiązania organizacyjno- techniczne i prawne w celu określonym w niniejszym dokumencie.

Administrator danych wdraża oraz deklaruje gotowość i zamiar przestrzegania i kontroli przestrzegania przez pracowników postanowień niniejszej polityki oraz jej ciągłego doskonalenia.

Dział 1
Definicje

§ 1. Użyte w niniejszym zarządzeniu definicje i skróty oznaczają:

1) administrator danych – administrator, w rozumieniu art. 4 pkt 7 RODO. O ile co innego nie wynika z PODOiBI przez administratora danych należy rozumieć: w Urzędzie - Prezydenta Wrocławia, Gminę Wrocław, Urząd Miejski Wrocławia, a w Radzie Miejskiej – Radę Miejską;
2) administrator CUI – pracownik Centrum Usług Informatycznych nadzorującego pracę systemu informatycznego oraz wykonujący w systemach informatycznych czynności wymagające specjalnych uprawnień pozwalających na m.in.: zakładanie kont, modyfikowanie zakresu uprawnień, czasowe blokowania oraz usuwanie kont oraz wykonywanie innych czynności administracyjnych oraz realizujący zadania wynikające z Porozumienia nr 1/2018 z dnia 25 maja 2018 r.;
3) anonimizacja – takie przetworzenie danych osobowych, w wyniku, którego dane te stają się danymi osobowymi zanonimizowanymi w sposób, o którym mowa w motywie 26 RODO;
4) BBI – Biuro ds. Bezpieczeństwa Informacji w Urzędzie Miejskim Wrocławia;
5) CPD – (skrót od Centrum Przetwarzania Danych) centralne miejsce w sieci komputerowej, w którym zgromadzone są kluczowe systemy informatyczne CUI, Urzędu oraz innych jednostek organizacyjnych Gminy Wrocław;
6) CUI – Centrum Usług Informatycznych we Wrocławiu - miejska jednostka organizacyjna Gminy Wrocław powołana uchwałą nr XLIX/1221/13 Rady Miejskiej Wrocławia z dnia 17 października 2013 r. (ze zm.);
7) czynności przetwarzania danych osobowych – zespół powiązanych operacji na danych osobowych, wykonywanych przez jedną lub kilka osób, które można określić w sposób zbiorczy, w związku z celem, w jakim te czynności są podejmowane np. rekrutacja pracowników, prowadzenie księgowości, przechowywanie danych w chmurze;
8) dane osobowe – dane osobowe, w rozumieniu art. 4 pkt 1 RODO;
9) DPIA – (skr. od ang. Data Protection Impact Assessment) ocena skutków planowanych operacji przetwarzania dla ochrony danych osobowych, o której mowa w art. 35 RODO;
10) Dyrektor BBI – osoba upoważniona przez administratora danych do wykonywania w jego imieniu określonych zadań, kierująca Biurem ds. Bezpieczeństwa Informacji w Urzędzie Miejskim Wrocławia;
11) Dyrektor CUI – osoba, która w oparciu o pełnomocnictwo Prezydenta Wrocławia kieruje Centrum Usług Informatycznych we Wrocławiu;
12) incydent bezpieczeństwa informacji – potencjalne lub faktyczne naruszenie bezpieczeństwa danych, w szczególności danych osobowych, ze względu na ich integralność, dostępność, poufność, rozliczalność, autentyczność, niezaprzeczalność, niezawodność. Incydentem bezpieczeństwa informacji są w szczególności potencjalne lub faktyczne naruszenia postanowień PODOiBI;
13) infrastruktura – cały sprzęt, oprogramowanie, sieci, wyposażenie itp., które są wymagane do rozwoju, testowania, monitorowania, kontroli lub obsługi aplikacji i usług

informatycznych. Określenie to obejmuje wszystkie technologie informatyczne, ale nie dotyczy ludzi, procesów i dokumentacji;
14) instrukcje i procedury – lista dokumentów dostępnych w Bazie Wiedzy (zakładka „Rozwiązania" w HelpDesk w Urzędzie);
15) IOD – inspektor ochrony danych, w rozumieniu art. 37-39 RODO. O ile co innego nie wynika z PODOiBI przez IOD należy rozumieć IOD Urzędu;
16) kategorie czynności przetwarzania – rodzaj usług świadczonych na rzecz administratora danych np. usługa prowadzenia dokumentacji księgowej, przechowywanie danych administratora danych;
17) kierownictwo Urzędu – Prezydent Wrocławia, Wiceprezydenci Wrocławia, Sekretarz Miasta Wrocławia oraz Skarbnik Miasta Wrocławia;
18) komórka organizacyjna Urzędu – wyodrębniony element struktury organizacyjnej Urzędu, w szczególności: Departament, Wydział, Biuro, Zespół;
19) Konsultant BBI – osoba imiennie wskazana przez dyrektora komórki organizacyjnej Urzędu, posiadająca wiedzę w zakresie ochrony danych osobowych, nadzorująca procesy ochrony danych w konkretnej komórce organizacyjnej, oddelegowana do kontaktu i współpracy z BBI i IOD w obszarze ochrony danych osobowych;
20) naruszenie ochrony danych osobowych – naruszenie ochrony danych osobowych, w rozumieniu art. 4 pkt 12 RODO. Naruszenie ochrony danych stanowi szczególny przypadek incydentu bezpieczeństwa;
21) odbiorca danych – odbiorca, w rozumieniu art. 4 pkt 9 RODO;
22) ograniczenie przetwarzania – oznaczenie przechowywanych danych osobowych w celu ich przetwarzania w węższym zakresie;
23) OPD – (skr. od Obszar Przetwarzania Danych) miejsca, w których pracownicy Urzędu przetwarzają dane osobowe oraz siedziby podmiotów przetwarzających, w których przetwarzane są dane osobowe. ***Wykaz OPD*** zawiera ***Załącznik nr 15 do PODOiBI (Wykaz Obszarów Przetwarzania Danych w Urzędzie Miejskim Wrocławia)***;
24) organ nadzorczy – organ nadzorczy, w rozumieniu art. 4 ust. 21 RODO. W Polsce organem nadzorczym jest Prezes Urzędu Ochrony Danych Osobowych;
25) osoba upoważniona – osoba upoważniona przez administratora danych do przetwarzania danych osobowych, nad którą administrator danych sprawuje bezpośrednią kontrolę w procesie przetwarzania danych realizowanym przez tę osobę;
26) państwo trzecie – państwo nienależące do Europejskiego Obszaru Gospodarczego;
27) podmiot przetwarzający – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora danych;
28) PODOiBI – Polityka Ochrony Danych Osobowych i Bezpieczeństwa Informacji Urzędu Miejskiego Wrocławia, określona w niniejszym dokumencie;
29) Porozumienie – Porozumienie nr 1/2018 z dnia 25 maja 2018 r. zawarte pomiędzy Gminą Wrocław Urzędem Miejskim Wrocławia a Centrum Usług Informatycznych we Wrocławiu;
30) praca zdalna - alternatywna forma pracy w Urzędzie, polegająca na świadczeniu pracy określonej w umowie o pracę poza lokalizacją Urzędu, na warunkach wynikających z odrębnych przepisów;
31) pracownik – osoba zatrudniona/współpracująca z Urzędem w ramach:
    a) stosunku pracy,
    b) odbywanego stażu absolwenckiego lub praktyki zawodowej,
    c) wolontariatu;
    d) umowy cywilnoprawnej (zlecenia, o dzieło i innych),
    e) osoby powiązane z administratorem danych innym stosunkiem prawnym (niebędące jednak przetwarzającym/procesorem, ani jego pracownikiem), działające na polecenie (upoważnienie) administratora danych i pod jego nadzorem (np. zewnętrzni eksperci powoływani przez administratora danych w ramach zespołów zadaniowych);
32) privacy by default – tzw. prywatność z definicji, domyślna ochrona prywatności. Jedna z zasad ochrony prywatności bazująca na założeniu domyślnej ochrony prywatności jako wartości nadrzędnej. Ujawnienie danych z obszaru prywatnego danej osoby wymaga jej wyraźnych i świadomych działań;
33) privacy by design – tzw. prywatność wbudowana w projekt, prywatność w fazie projektowania. Zasada proaktywnego uwzględniania prywatności w projektach, architekturze systemów informatycznych i praktykach biznesowych od samego początku przez cały okres „życia danych";
34) profilowanie – profilowanie, w rozumieniu art. 4 pkt 4 RODO;
35) przetwarzanie danych – przetwarzanie, w rozumieniu art. 4 pkt 2 RODO;

36) pseudonimizacja – pseudonimizacja, w rozumieniu art. 4 pkt 5 RODO;
37) rejestr czynności przetwarzania danych osobowych – dokument, o którym mowa w art. 30 ust. 1 RODO, prowadzony w formie pisemnej, w tym elektronicznej przez administratora danych, udostępniany organowi nadzorczemu na jego żądanie;
38) rejestr kategorii czynności przetwarzania – dokument, o którym mowa w art. 30 ust. 2 RODO, prowadzony w formie pisemnej, w tym elektronicznej przez podmiot przetwarzający, udostępniany organowi nadzorczemu na jego żądanie;
39) 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) (Dz. Urz. UE L 119 z 4 maja 2016 r. z późn. zm.);
40) rodzaj przetwarzania – charakter, zakres, cele i kontekst przetwarzania oraz wykorzystywane systemy informatyczne (proces/czynność i sposób ich realizacji);
41) statut CUI – Statut Centrum Usług Informatycznych we Wrocławiu, powołanego uchwałą Rady Miejskiej Wrocławia nr XXX/601/16 z dnia 15 września 2016 r. w sprawie ustanowienia Centrum Usług Wspólnych dla jednostek organizacyjnych Gminy Wrocław pod nazwą Centrum Usług Informatycznych oraz nadania Statutu (ze zm.);
42) system informacyjny – zbiór procedur i narzędzi służących zbieraniu, przechowywaniu, przetwarzaniu, archiwizowaniu oraz przesyłaniu informacji, celem wspomagania i usprawniania zarządzania, podejmowania decyzji i kontroli. Elementem tego systemu może być w szczególności system informatyczny;
43) system informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
44) system informatyczny Urzędu – system informatyczny funkcjonujący w Urzędzie;
45) środki techniczne i organizacyjne – środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych;
46) telepraca – forma dostępu do danych gromadzonych w domenie polegająca na zdalnym podłączeniu się do domeny z wykorzystaniem technologii teleinformatycznych i usługi wirtualnej sieci prywatnej (z ang. virtual private network, w skr. VPN);
47) umowa powierzenia – umowa powierzenia przetwarzania danych osobowych, o której mowa w art. 28 ust. 3 RODO;
48) upoważnienie – oświadczenie administratora danych lub osoby przez niego upoważnionej wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym upoważnieniu, nad którą administrator danych sprawuje bezpośrednią kontrolę w procesie przetwarzania danych realizowanym przez tę osobę;
49) Urząd – Urząd Miejski Wrocławia;
50) usuwanie danych osobowych – zniszczenie danych osobowych (w tym ich anonimizacja);
51) użytkownik – osoba bezpośrednio i leganie korzystającą z danych gromadzonych w systemach informatycznych; użytkownikami systemu obok pracowników mogą być procesorzy danych oraz ich pracownicy, którzy przetwarzają dane na polecenia administratora danych;
52) właściciel zasobu informacyjnego – dyrektor komórki organizacyjnej Urzędu, do której merytorycznych zadań przypisano zasób informacyjny. Właściciele poszczególnych zasobów informacyjnych wymienieni są m.in. w rejestrze czynności przetwarzania prowadzonym przez IOD;
53) WOK – Wydział Organizacyjny i Kadr w Urzędzie;
54) współadministratorzy – współadministratorzy, w rozumieniu art. 26 RODO;
55) zabezpieczenie danych w systemie informatycznym – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
56) Zastępca Dyrektora BBI – osoba upoważniona przez administratora danych do wykonywania w jego imieniu określonych zadań w ramach zastępstwa Dyrektora BBI podczas jego nieobecności lub w innych sytuacjach, zgodnie z ustaleniami wewnętrznymi BBI;
57) Zastępca IOD – osoba wykonująca zadania Inspektora Ochrony Danych w zakresie z nim ustalonym, a w czasie jego nieobecności - w pełnym zakresie zadań i uprawnień. Ilekroć w niniejszej polityce mowa o IOD, należy przez to rozumieć również Zastępcę IOD, w okresie gdy zastępuje on IOD;

58) zasób informacyjny – dawniej zbiór danych osobowych. Uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
59) zgoda osoby, której dane dotyczą – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, w którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

Dział 2
Zakres Polityki Ochrony Danych i Bezpieczeństwa Informacji

§ 2. 1. Zakres PODOiBI dotyczy przetwarzania danych, w szczególności danych osobowych, przetwarzanych w sposób tradycyjny w księgach, rejestrach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych.

2. PODOiBI:

1) zawiera zasady bezpiecznego użytkowania systemów informacyjnych w Urzędzie,
2) wyjaśnia kluczowe zagadnienia wynikające z ochrony danych gromadzonych i przetwarzanych w postaci elektronicznej i papierowej;
3) wskazuje na podstawowe zagadnienia związane z obowiązkami pracownika oraz CUI;
4) określa warunki przetwarzania danych, w szczególności danych osobowych;
5) jest oparta na przepisach RODO i innych powszechnie obowiązujących przepisach.

§ 3. 1. Procedury i zasady określone w PODOiBI stosuje się do wszystkich osób przetwarzających dane, w szczególności dane osobowe, w Urzędzie. Obowiązek przestrzegania tajemnicy danych osobowych dotyczy wszystkich, którzy mają do nich dostęp.

2. Zasady określone w PODOiBI mają zastosowanie do wszelkiego rodzaju zawieranych zobowiązań umownych i innych zdarzeń prawnych, jeśli ich przedmiot dotyczy przetwarzania danych, zwłaszcza danych osobowych.

Dział 3
Role i odpowiedzialności – pracownicy, dyrektorzy i CUI

§ 4. 1. Pracownik przed dopuszczeniem go do pracy zapoznawany jest z informacjami m.in. o: zakresie, celach, podstawach prawnych i zasadach przetwarzania jego danych osobowych, w związku z realizacją obowiązku określonego w art. 12 i następnych RODO. Dokument potwierdzający fakt zapoznania się z tymi informacjami dołącza się do akt osobowych pracownika (w rozumieniu kodeksu pracy). Zmiana stanowiska lub miejsca pracy nie wymaga ponownego składania ww. dokumentu do akt osobowych.

2. Pracownik przetwarzający dane osobowe działa na polecenie administratora danych w oparciu o wydane przez administratora danych w tym zakresie upoważnienie, stanowiące integralną cześć Karty Zakresu i Rodzaju Pracy Pracowników Samorządowych Urzędu Miejskiego Wrocławia.

3. **Pracownik przetwarzający dane osobowe na polecenie (upoważnienie) administratora danych zobowiązany jest do:**

1) zapoznania się oraz ścisłego przestrzegania przepisów prawa w zakresie ochrony danych osobowych oraz tajemnic prawnie chronionych;
2) stosowania określonych przez administratora danych zasad, procedur oraz rekomendacji IOD mających na celu właściwe i adekwatne przetwarzanie danych, w szczególności danych osobowych;
3) należytego zabezpieczenia danych, w szczególności danych osobowych, przed ich ujawnieniem osobom nieupoważnionym;
4) zachowania w tajemnicy treści danych, w szczególności danych osobowych, i innych tajemnic prawnie chronionych;
5) zachowania szczególnej staranności w trakcie dokonywania operacji przetwarzania danych, w szczególności danych osobowych, w celu ochrony interesów osób, których dane dotyczą;
6) współpracy z IOD, w szczególności w sytuacji wystąpienia incydentów bezpieczeństwa informacji oraz podczas prowadzonych audytów zgodności przetwarzania danych osobowych z przepisami dotyczącymi ochrony danych osobowych.

§ 5. (…) 3. Dyrektorzy komórek organizacyjnych Urzędu ponoszą odpowiedzialność za dane przetwarzane w kierowanych przez nich komórkach, w szczególności dane osobowe, i sprawują nadzór nad przestrzeganiem zasad ich przetwarzania.

§ 6. 1. Dyrektor CUI zobowiązany jest do ścisłej współpracy z:
1) dyrektorami Departamentów i ich zastępcami;
2) dyrektorami oraz kierującymi komórkami organizacyjnymi Urzędu;
3) IOD Urzędu w pełnym zakresie obowiązków wynikających z przepisów dot. ochrony danych osobowych, w szczególności w ramach incydentów bezpieczeństwa informacji oraz prowadzonych audytów zgodności przetwarzania danych osobowych z przepisami dot. ochrony danych osobowych oraz opracowania w tym zakresie raportu dla administratora danych.

2. Dyrektor CUI opracowuje, gromadzi i udostępnia dyrektorom komórek organizacyjnych Urzędu dokumentację dot. funkcjonujących w Urzędzie systemów informatycznych.

3. Dyrektor CUI realizuje zadania i czynności wynikające z PODOiBI i jest za nie odpowiedzialny, a ponadto zobowiązany jest do bieżącego śledzenia wprowadzanych nowelizacji jej dotyczących oraz stosowania aktualnej PODOiBI w zakresie przewidzianym Statutem CUI.

4. IOD CUI oraz IOD Urzędu zobowiązani są do ścisłej współpracy w zakresie realizacji zadań i obowiązków, jakie nakładają na nich i na administratora danych obowiązujące przepisy ochrony danych osobowych.

Dział 4
Administrator danych

§ 7. 1. Administrator danych uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO,

(…)

Dział 6
Zasady przetwarzania danych i środki zabezpieczeń

§ 9. Ochronę danych, w szczególności danych osobowych, gromadzonych w sposób tradycyjny i w systemach informatycznych, zabezpieczają środki organizacyjne, techniczne, fizyczne i personalne. Ważnym elementem ochrony danych jest świadomość praw i obowiązków wynikających z obowiązujących przepisów ochrony danych osobowych wszystkich pracowników uczestniczących bezpośrednio w gromadzeniu i przetwarzaniu danych. Obowiązkiem kadry kierowniczej Urzędu jest podnoszenie świadomości ochrony danych wśród podlegających im pracowników i reagowanie na wszelkie naruszenia PODOiBI.

Rozdział 1
Zasady przetwarzania danych

§ 10. 1. Administrator danych określa i wdraża zasady ochrony dostępu do danych, w szczególności danych osobowych oraz postępowanie z danymi podczas ich przetwarzania określone w PODOiBI wraz z załącznikami i dokumentami powiązanymi.

2. **Określa się następujące, podstawowe zasady bezpieczeństwa obowiązujące pracowników:**
1) zasada wiedzy koniecznej – ograniczanie dostępu jedynie do tych danych, które są niezbędne do wykonywania obowiązków;
2) zasada zgłaszania incydentów bezpieczeństwa informacji – każdy pracownik zobowiązany jest do zgłaszania zdarzeń związanych z bezpieczeństwem informacji, zgodnie z trybem określonym w Dziale 8 PODOiBI;
3) zasada odpowiedzialności za zasoby – pracownik jest odpowiedzialny za dane, które przetwarza i zobowiązany jest przestrzegać ustanowionych procedur bezpieczeństwa w tym zakresie;
4) zasada celowego wykorzystywania zasobów – dane mogą być przetwarzane wyłącznie w celach służbowych, w środkach przetwarzania dopuszczonych do wykorzystania w Urzędzie (autoryzowanych). W szczególności, bez zgody administratora danych lub osoby przez niego upoważnionej zabrania się korzystania w tym celu z prywatnych środków

(sprzętu i oprogramowania) przetwarzania danych. Zabrania się wykorzystywania służbowego komputera stacjonarnego, przenośnego, telefonów, smartfonów, tabletów, innych urządzeń oraz oprogramowania do celów prywatnych; (…)

5) zasada zapisywania i archiwizacji dokumentów w formie elektronicznej – wszystkie dokumenty wytwarzane na zasobach sieciowych Urzędu stanowią dane Urzędu, użytkownicy, mają obowiązek zapisywania ich na dyskach sieciowych K: lub M:, w miejscach wyznaczonych dla poszczególnych komórek organizacyjnych lub realizowanych zadań. Zabrania się permanentnego przechowywania dokumentów zawierających dane osobowe na dyskach lokalnych komputerów - dokumenty zawierające dane osobowe mogą być przechowywane na dyskach lokalnych komputerów jedynie tymczasowo, w celu wytworzenia dokumentów w wersjach finalnych;
6) zasada autoryzowanych portów – gniazda umożliwiające włączanie urządzeń komputerowych do sieci wewnętrznej Urzędu są domyślnie nieaktywne (porty urządzeń sieciowych nie są skrosowane), uaktywnienie gniazd odbywa się na wniosek za pośrednictwem zgłoszenia HelpDesk w związku z uzasadnioną potrzebą podłączenia służbowego urządzenia do gniazda; do portów komputerów, w szczególności portów USB nie wolno podłączać żadnych nieautoryzowanych prywatnych urządzeń (np.: pendrive, telefon, dysk zewnętrzny itp.), które umożliwiają zapis danych zgromadzonych w infrastrukturze i systemach informatycznych Urzędu; do aktywnego gniazda lub portu można podłączyć dowolne służbowe (autoryzowane) urządzenie;
7) zasada legalności oprogramowania – zakaz samodzielnego instalowania oprogramowania, w tym w szczególności przechowywania na komputerze treści naruszających prawa autorskie oraz innych nielegalnych danych;
8) zasada prywatności kont w systemach – każdy użytkownik zobowiązany jest do pracy w systemach teleinformatycznych na przypisanych mu kontach. Bezwzględnie zabronione jest udostępnianie kont osobom, które nie zostały do nich przypisane;
9) zasada poufności haseł i kodów dostępu – zachowanie poufności i nieprzekazywanie osobom nieuprawnionym haseł i kodów dostępu. W szczególności zasada ta dotyczy osobistych haseł dostępu do systemów teleinformatycznych i stref chronionych;
10) zasada prywatności ekranu - monitory, na których wyświetlane są dane osobowe, należy zabezpieczyć folią prywatyzującą lub ustawić w taki sposób, aby uniemożliwić wgląd osobom postronnym w wyświetlane dane, pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, należy chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych; powyższą zasadę należy stosować w odniesieniu do wszelkiego typu wyświetlaczy (także np. wpłatomaty, wyświetlacze urządzenia kolejkowego itp.);
11) zasada czystego pulpitu – na pulpicie komputera mogą znajdować się jedynie ikony standardowego oprogramowania i aplikacji służbowych oraz skróty do folderów pod warunkiem, że w nazwie nie zawierają danych, w szczególności danych osobowych, które mogą zostać w sposób niekontrolowany ujawnione (np. podczas prezentacji);
12) zasada nazewnictwa plików i folderów – nazwy plików lub folderów oraz ich metadane nie mogą zawierać danych osobowych;
13) zasada blokowania komputera – blokowanie komputera, zgodnie z obowiązującym ustawieniem wygaszacza ekranu, a także przed każdym opuszczeniem pomieszczenia. W przypadku dłuższej nieobecności w pomieszczeniu konieczne jest wylogowanie się z systemu;
14) zasada czystej drukarki/kserokopiarki – zabieranie dokumentów z drukarek zaraz po ich wydrukowaniu, w szczególności zasada ta dotyczy dokumentów pozostawianych w drukarkach znajdujących się w innym pomieszczeniu. Dla drukarek znajdujących się w przestrzeni ogólnodostępnej wymagane jest stosowanie indywidualnych zasad dostępu umożliwiających emisję wydruku jedynie podczas obecności zlecającego wydruk;
15) zasada zamkniętego pomieszczenia – niepozostawianie osób postronnych samych w pomieszczeniu (pod nieobecność pracownika), stosowanie adekwatnych zasad nadzoru na osobami przebywającymi w różnych strefach Urzędu, bezwzględne zamykanie pomieszczeń na klucz przy ich opuszczaniu i niepozostawianie kluczy w zamkach;
16) zasada czystego biurka – niepozostawianie bez nadzoru dokumentów papierowych oraz nośników danych (płyt CD, DVD, pamięci flash USB itp.);
17) zasada czystej tablicy – po zakończonym spotkaniu w pomieszczeniach ogólnodostępnych (sale konferencyjne itp.) należy uprzątnąć wszystkie materiały oraz wyczyścić tablice (flipchart itp.);

18) zasada czystego kosza – dokumenty papierowe z wyjątkiem materiałów promocyjnych powinny być na bieżąco niszczone w niszczarkach lub – w przypadku niszczenia dużych ilości dokumentów - za pośrednictwem firmy zewnętrznej.

Rozdział 2
Środki zabezpieczeń - organizacyjne

§ 11. 1. Administrator danych stosuje niżej podane środki zabezpieczeń, które dotyczą wszystkich pracowników przetwarzających dane, w tym dane osobowe . W szczególności administrator danych zobowiązuje pracowników do:

1) **zapoznania się i przestrzegania przepisów dotyczących ochrony danych osobowych oraz przepisów w zakresie zabezpieczeń systemów informatycznych, z których korzystają (w tym przestrzegania postanowień PODOiBI, w szczególności zasad przetwarzania danych osobowych);**
2) zachowania danych, w tym danych osobowych, w tajemnicy oraz podpisania stosowanych oświadczeń w tym zakresie; (…).

2. Administrator danych wyznacza IOD oraz może wyznaczyć Zastępcę IOD, dysponujących niezbędnymi zasobami oraz wymaganym poziomem wiedzy fachowej.

3. Administrator danych wdraża procedury i zasady postępowania w zakresie dostępu do stref przetwarzania danych, w szczególności:

1) procedurę zarządzania kluczami do pomieszczeń stanowiącą ***Załącznik nr 2 do PODOiBI (Polityka kluczy)***, obszarów, szaf oraz w zakresie poruszania się i przebywania w zdefiniowanych strefach, w których są przetwarzane dane;
2) pracownicy, którzy przetwarzają dane reagują na stwierdzoną obecność osób postronnych w strefach 3a lub 3b; szczegółowy opis stref zawiera ***Załącznik nr 3 do PODOiBI (Opis stref Urzędu)***;
3) użytkownicy, którzy przetwarzają dane, reagują na stwierdzoną obecność osób postronnych bez nadzoru osób uprawnionych w strefach 2a lub 2b.

4. Administrator danych zdefiniował zasoby informacyjne oraz wprowadził klasyfikację danych osobowych, (…)

5. Administrator danych wdraża **procedury reagowania osób odpowiedzialnych za ochronę danych w przypadku zagrożenia lub faktycznej utraty lub ujawnienia danych**, w szczególności:

1) w razie awarii sprzętu informatycznego pracownicy niezwłocznie powiadamiają CUI poprzez rejestrację zgłoszenia w HelpDesk (zasady zgłaszania awarii znajdują się w instrukcjach i procedurach HelpDesku);
2) w razie awarii sprzętu nieinformatycznego pracownicy niezwłocznie powiadamiają właściwego administratora obiektu (budynku Urzędu) poprzez zgłoszenie telefoniczne lub informację przesłaną pocztą elektroniczną, (zgodnie z zasadami zgłaszania awarii nieinformatycznych funkcjonującymi w Urzędzie);
3) procedurę i zasady w zakresie zgłaszania i obsługi incydentów bezpieczeństwa informacji w razie ich wystąpienia, zobowiązującą pracowników do aktywnych działań z wykorzystaniem określonych kanałów zgłoszeniowych zgodnie z Działem 8 PODOiBI i *Procedurą zarządzania incydentami bezpieczeństwa informacji w Urzędzie Miejskim Wrocławia)*;
4) zobowiązuje się podmioty, o których mowa w § 14 ust. 2 PODOiBI do zgłaszania stwierdzonych słabości systemu zabezpieczeń lub podejrzeń wystąpienia takich słabości, za pośrednictwem kanałów kontaktu z IOD;
5) realizacja wniosków, zaleceń i rekomendacji sformułowanych w wyniku analizy zdarzeń nieplanowanych (m.in. incydentów bezpieczeństwa informacji) jest monitorowana i weryfikowana.

6. Administrator danych wprowadza procedury i instrukcje nadawania i odbierania uprawnień w systemach informatycznych (…)

9. Powierzenie przetwarzania danych osobowych innym podmiotom odbywa się wyłącznie na podstawie pisemnych umów powierzenia / porozumień, w stosunku, do których wzorcowa treść, sposób negocjowania treści, akceptacja ostatecznej treści odbywają się we współdziałaniu pomiędzy: dyrektorem komórki organizacyjnej, radcą prawnym i IOD.

10. Administrator danych określił i weryfikuje wymagania co do poziomu bezpieczeństwa, jakie zobowiązuje się zapewnić podmiot przetwarzający. Weryfikacja faktycznie stosowanych zabezpieczeń jest możliwa w drodze audytu lub kontroli przeprowadzanych przez Urząd lub

podmiot zewnętrzny. Wszystkie zdarzenia dotyczące powierzenia danych są ewidencjonowane w ramach rejestru czynności przetwarzania. (…)

12. Wdrożenia nowych projektów w Urzędzie np. informatycznych lub istotne modyfikacje istniejących, obejmujących między innymi przetwarzanie danych osobowych, odbywają się z uwzględnieniem zasady ochrony prywatności w fazie projektowania (z ang. „privacy by design") oraz domyślnej ochrony danych (z ang. „privacy by default") w rozumieniu RODO, w szczególności:

1) dokumentacja projektowa systemów Urzędu i CUI uwzględnia kluczowe aspekty ochrony danych osobowych i prywatności osób, których dane są/będą przetwarzane;
2) dokumentacja dotycząca udzielania zamówień publicznych uwzględnia kluczowe aspekty ochrony danych osobowych i prywatności osób, których dane są/będą przetwarzane;
3) dokumentacja systemów informatycznych zawiera dedykowane części opracowane zgodnie ze standardem CUI w zakresie dokumentacji ochrony danych osobowych; (…)

13. Administrator danych eksploatuje, rozwija i serwisuje systemy i procesy przetwarzania, w szczególności:

1) adekwatne zabezpieczenia oraz ochrona prywatności osób są utrzymywane i monitorowane w ciągu całego czasu życia procesu/systemu;
2) stosuje się metodologię proaktywnego uwzględnienia prywatności w technologiach informatycznych, praktykach biznesowych i infrastrukturze;
3) przetwarzanie wyłącznie tych danych osobowych, które są niezbędne dla każdego sprecyzowanego celu przetwarzania, z minimalizacją ilości zbieranych danych, zakresu przetwarzania, okresu przetwarzania oraz ich dostępności;
4) prywatność osób jest domyślnym sposobem działania Urzędu przy jednoczesnym utrzymaniu pełnej funkcjonalności oraz bezpieczeństwa;
5) interesy osób są chronione za pomocą ustawień domyślnych, odpowiednich powiadomień - klauzul informacyjnych i przyjaznych użytkownikowi możliwości. (…)

Rozdział 3
Środki zabezpieczeń - personalne

Oddział 1
Upoważnienia

§ 12. Administrator danych stosuje środki personalne wskazane w niniejszym Rozdziale.

§ 13. 1. Kierownictwo Urzędu wykonuje czynności przetwarzania danych osobowych w zakresie swoich kompetencji i zadań (…)

4. Pracownik dokonuje czynności przetwarzania danych osobowych w zakresie:

1) indywidualnych obowiązków pracowniczych, określonych w Karcie Rodzaju i Zakresu Pracy Pracownika Samorządowego;
2) czynności określonych w umowie cywilnoprawnej (zlecenia, o dzieło lub innej);
3) zadań określonych dla stażysty;
4) programu praktyk zawodowych;
5) zadań określonych dla wolontariusza;
6) obowiązków określonych w zarządzeniach Prezydenta, w tym określających funkcjonowanie zespołów zadaniowych.

5. Każda osoba działająca z upoważnienia i mająca dostęp do danych osobowych przetwarza je wyłącznie na polecenie administratora danych.

§ 14. 1. Upoważnienie do przetwarzania danych osobowych wraz z oświadczeniem, których wzór zawarto w ***Załączniku nr 4 do PODOiBI (Wzór upoważnienia do przetwarzania danych osobowych wraz z oświadczeniem upoważnionego)*** stanowią:

1) dla osób, o których mowa w § 1 pkt 30 lit. a – nieodłączną część Karty Rodzaju i Zakresu Pracy Pracownika Samorządowego,
2) dla osób o których mowa w § 1 pkt 30 lit. b-d – nieodłączną część umowy o praktyki/staż/wolontariat lub innego dokumentu, na podstawie, którego, osoba upoważniona ma świadczyć czynności na rzecz Urzędu.

2. Pracownik zostaje upoważniony do przetwarzania danych osobowych przez administratora danych oraz składa oświadczenie, o którym mowa w ust. 1, przed rozpoczęciem przetwarzania tych danych.

3. Stosując zasadę określoną w ust. 2, upoważnienie wydawane jest w trzech egzemplarzach, w tym jeden dla pracownika (z wyłączeniem osób, o których mowa w § 1 pkt 30 lit. d-e), jeden dla administratora danych, jeden dla dyrektora komórki organizacyjnej, na rzecz, której realizowane są czynności związane z przetwarzaniem danych. **W stosunku do osób, o których mowa w § 1 pkt 30 lit. d-e, upoważnienie wydawane jest w dwóch egzemplarzach, jeden dla upoważnionego, drugi dla dyrektora komórki organizacyjnej, który nadzoruje wykonanie zadań.**

4. Każda zmiana stanowiska, zmiana zakresu obowiązków pracowniczych, wymaga aktualizacji w zakresie upoważnienia do przetwarzania danych osobowych i powiązanego z nim oświadczenia, o którym mowa w ust. 1.

§ 15. Upoważnienia do przeprowadzenia: kontroli, audytów, wykonania czynności służbowych, pełnienia funkcji członka zespołu/komisji, etc., wydawane są przez dyrektorów komórek organizacyjnych Urzędu, pod egidą których, ze względu na zakres zadań, osoby upoważnione realizują czynności zgodnie ze wzorem stanowiącym ***Załącznik nr 4 do PODOiBI (Wzór upoważnienia do przetwarzania danych osobowych wraz z oświadczeniem upoważnionego).*** Wraz z upoważnieniem należy przekazać klauzulę informacyjną dostosowaną do charakteru czynności osoby upoważnionej (zleceniobiorca, stażysta, praktykant etc.).

§ 16. 1. (…)

3. Zakończenie stosunku pracy / stażu / wolontariatu / praktyki / umowy cywilnoprawnej /innego stosunku prawnego, o którym mowa w § 1 pkt 30 lit. e, w okresie obwiązywania upoważnienia, powoduje wygaśnięcie upoważnienia wraz z dniem ustania stosunku pracy/stażu/wolontariatu/praktyki/umowy cywilnoprawnej/innego stosunku prawnego, o którym mowa w § 1 pkt 30 lit. e.

§ 17. 1. Ewidencje osób upoważnionych do przetwarzania danych osobowych, o których mowa w § 15, prowadzone są we właściwych komórkach organizacyjnych, przez Konsultantów BBI.

2. IOD, WOK oraz CUI współpracują z Konsultantami BBI w zakresie aktualizacji ewidencji, o której mowa w ust. 1.

Oddział 2
Przygotowanie i szkolenie

§ 18. 1. Każdy pracownik przed dopuszczeniem do pracy z danymi, w szczególności danymi osobowymi, zobowiązany jest do uczestnictwa w szkoleniu i zapoznania z przepisami z zakresu ochrony danych osobowych i PODOiBI.

2. Każda zmiana stanowiska, która wiąże się ze znaczącą zmianą sposobu lub zakresu przetwarzania danych przez pracownika skutkuje koniecznością ponownego uczestnictwa w szkoleniu, o którym mowa w ust. 1.

§ 19. 1. Szkolenia prowadzi IOD (…), w tym przygotowuje tematykę i zakres merytoryczny oraz ewidencję osób w nich uczestniczących.

2. Udział w szkoleniu jest potwierdzany podpisem na liście obecności.

Oddział 3
Pozostałe

§ 20. Pracownicy przetwarzający dane osobowe zapoznają się z PODOiBI i stosują ją w praktyce. Potwierdzenie zapoznania się z PODOiBI pracownicy potwierdzają podpisując stosowne oświadczenie, którego wzór stanowi *Załącznik nr 5 do PODOiBI (Wzór oświadczenia o zapoznaniu się z PODOiBI)*.

§ 21. Zasady określające obowiązki pracownika w ramach przetwarzania danych są stosowane: powszechnie w odniesieniu do wszystkich kategorii osób i adekwatnie do czasu trwania zadań/obowiązków/umowy.

§ 22. Administrator danych zapewnia zastępowalność pracowników, z uwzględnieniem faktycznie nadanych uprawnień, kompetencji i wiedzy wraz z rozliczalnością ich działań.

§ 23. Administrator danych dysponuje personelem bezpieczeństwa tj. osobami, które są przeszkolone, nadzorowane, a w razie konieczności posiadają odpowiednie uprawnienie dostępu do informacji i które wykonują czynności związane z: fizyczną ochroną informacji, w tym kontrolą dostępu do pomieszczeń lub obszarów, w których przetwarzane są informacje, nadzorem nad systemem dozoru wizyjnego, reagowaniem na alarmy lub sygnały awaryjne oraz prowadzeniem lub uczestnictwem w audytach weryfikujących faktycznie stosowane środki zabezpieczeń.

Rozdział 4
Środki zabezpieczeń - fizyczne i techniczne (systemowe)

§ 24. 1. Dane w postaci elektronicznej przetwarzane są przy użyciu infrastruktury i systemów informatycznych Urzędu pracujących we wspólnej domenie. (…)

§ 25. 1. Serwery oraz kluczowa infrastruktura sieciowa (m.in. firewall'e, przełączniki, routery) znajdują się w wydzielonych pomieszczeniach z ograniczonym dostępem. Większość, w tym wszystkie kluczowe serwery sieciowe, znajdują się w CPD. Ze względu na liczbę i znaczenie gromadzonych i przetwarzanych danych w CPD, tylko w tym miejscu zastosowane zostały rozszerzone środki techniczne, w celu utrzymania integralności, poufności, rozliczalności i dostępności danych, w szczególności danych osobowych. (…) Wejście do CPD jest możliwe tylko dla uprawnionych osób posiadających karty elektroniczne z odpowiednimi uprawnieniami i których obowiązki służbowe wymagają wizyt w pomieszczeniu CPD. Szczegółowe warunki wejścia do CPD określa odrębna instrukcja. W CPD zainstalowany jest system monitoringu wizyjnego wraz z rejestracją w cyklu ciągłym, na okres minimum 1 tygodnia. CPD posiada środki bezpieczeństwa w postaci czujników zalania wodą, czujników wtargnięcia, systemu automatycznego wykrywania, systemu automatycznego gaszenia pożaru, systemu klimatyzacyjnego, systemu podtrzymania zasilania oraz niezależnego zasilania. (…).

§ 26. W Urzędzie funkcjonuje monitoring wizyjny. Zasady funkcjonowania monitoringu wizyjnego w Urzędzie Miejskim Wrocławia (w tym: cel i zakres przetwarzania danych osobowych, podstawy prawne przetwarzania, miejsca monitorowane, wykaz istniejących systemów kontroli i dozoru oraz wykaz rozmieszczenia kamer) określone zostały w ***Załączniku nr 13 do PODOiBI (Zasady funkcjonowania monitoringu wizyjnego w Urzędzie Miejskim Wrocławia).***

Dział 7
Podejście oparte na ryzyku, prywatność w fazie projektowania i domyślna ochrona danych

§ 29. Dyrektor komórki organizacyjnej Urzędu planując i realizując wszystkie rodzaje przetwarzania danych osobowych stosuje podejście oparte na ryzyku.

§ 30. Analizę ryzyka dla konkretnego rodzaju przetwarzania (proces/czynność przetwarzania/zadanie/zasób informacyjny) przeprowadza każdorazowo właściciel zasobu informacyjnego w oparciu o *stosowne zarządzenie Prezydenta* (którym na dzień sporządzenia niniejszego PODOiBI jest „Zarządzenie Prezydenta Wrocławia nr K/17/20 w sprawie zarządzania ryzykiem związanym z przetwarzaniem danych osobowych w Urzędzie Miejskim Wrocławia"). Właściciel zasobu informacyjnego przeprowadzając analizę ryzyka obowiązany jest skonsultować się w tej materii z IOD.

(…)

§ 33. W każdym przypadku realizacji nowych zadań, w ramach, których przetwarzane są dane osobowe, dyrektor komórki organizacyjnej Urzędu, będący właścicielem zasobu informacyjnego, uwzględnia prawa osób, których dane dotyczą, na każdym kluczowym etapie projektowania i wdrażania oraz kieruje się zasadą domyślnej ochrony danych. Czynności powyższe konsultuje z IOD.

Dział 8
Incydenty bezpieczeństwa informacji

§ 34. Administrator danych ewidencjonuje zdarzenia dotyczące bezpieczeństwa informacji (w tym naruszenia ochrony danych osobowych).

§ 35. 1. Wszystkie zgłoszone incydenty bezpieczeństwa informacji, w tym naruszenia ochrony danych, są ewidencjonowane w wewnętrznym rejestrze incydentów bezpieczeństwa informacji prowadzonym w systemie komputerowym HelpDesk. System HelpDesk stanowi jeden z elementów dokumentacji, o której mowa w art. 33 ust. 5 RODO.

2. Wszystkie działania wykonywane w ramach obsługi incydentów bezpieczeństwa informacji są dokumentowana przez IOD, Dyrektora BBI lub upoważnionych pracowników BBI.

3. Dokumentacja dotycząca incydentów bezpieczeństwa informacji przechowywana jest w Biurze ds. Bezpieczeństwa Informacji i jest udostępniana IOD, administratorowi danych i organowi nadzorczemu na żądanie.

§ 36. W przypadku pozyskania informacji o incydencie bezpieczeństwa, każda osoba zobowiązana do stosowania PODOiBI, ma obowiązek zgłosić ten fakt IOD, Dyrektorowi BBI oraz swojemu bezpośredniemu przełożonemu zgodnie z procedurą opisaną w *Załączniku nr 16 do PODOiBI (Procedura zarządzania incydentami bezpieczeństwa informacji w Urzędzie Miejskim Wrocławia).* W sytuacji, gdy osoba, zobowiązana do stosowania PODOiBI, nie ma pewności co do charakteru zdarzenia (tj. czy stanowi ono incydent bezpieczeństwa informacji, czy też go nie stanowi) powinna zgłosić dane zdarzenie jako incydent bezpieczeństwa informacji.

§ 37. W każdym przypadku wystąpienia incydentu bezpieczeństwa informacji administrator danych konsultuje z IOD, czy incydent ten stanowił naruszenie ochrony danych osobowych, a jeżeli tak to czy naruszenie to skutkowało ryzykiem (w szczególności wysokim ryzykiem) naruszenia praw lub wolności osób fizycznych, a także podejmuje decyzję o dalszym trybie postępowania w zakresie powiadomienia właściwych organów oraz podjęcia innych, szczególnych czynności zabezpieczających system informatyczny, bądź zapewnienia dodatkowych środków ochrony.

§ 38. W przypadkach, gdy incydent bezpieczeństwa informacji realizuje jednocześnie hipotezy norm zawartych w art. 33 lub art. 34 RODO, administrator bezpieczeństwa podejmuje działania opisane w tych przepisach (w szczególności powiadamia organ nadzorczy lub osoby których dane dotyczą).

§ 39. 1. Działaniami dodatkowymi związanymi z incydentem bezpieczeństwa informacji, niebędącymi integralną częścią jego obsługi, mogą być: przeprowadzenie audytu doraźnego lub wydanie rekomendacji podjęcia określonych działań zaradczych lub naprawczych (w tym wykonanie szacowania ryzyka).

2. Decyzję o zastosowaniu działań dodatkowych podejmuje zgodnie ze swoją właściwością Dyrektor BBI (w odniesieniu do wszystkich incydentów bezpieczeństwa informacji; przy czym w odniesieniu do incydentów z obszaru danych osobowych w porozumieniu z IOD) lub IOD (w odniesieniu do incydentów bezpieczeństwa informacji z obszaru danych osobowych).

3. Podjęcie powyższych działań przez IOD lub Dyrektora BBI nie wyklucza podjęcia przez administratora danych działań wynikających z przepisów prawa cywilnego (w szczególności przepisów prawa pracy dotyczących odpowiedzialności odszkodowawczej i porządkowej pracowników) lub karnego.

§ 40. Szczegółowe informacje dotyczące procesu zarządzania incydentami bezpieczeństwa informacji w UMW (w szczególności sposób zgłaszania tych incydentów) zawarte są w *Procedurze zarządzania incydentami bezpieczeństwa informacji w Urzędzie Miejskim Wrocławia.*

Dział 9
Inspektor Ochrony Danych, Zastępca Inspektora Ochrony danych, Konsultanci BBI

§ 41. 1. Administrator danych wyznacza w Urzędzie IOD oraz może wyznaczyć Zastępcę IOD.

2. Do pełnienia funkcji IOD administrator danych wyznacza na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych osobowych.

3. Szczegółowe zasady powoływania i funkcjonowania IOD w Urzędzie określa *Regulamin organizacyjny IOD w Urzędzie Miejskim Wrocławia.*

§ 42. Administrator danych publikuje dane kontaktowe IOD w BIP oraz wywiesza informacje w miejscach ogólnie dostępnych w Urzędzie oraz zawiadamia o powołaniu IOD organ nadzorczy.

§ 43. 1. Administrator danych zapewnia IOD właściwe i niezwłoczne włączanie go w sprawy dotyczące ochrony danych w Urzędzie.

2. Administrator danych wspiera IOD w wypełnianiu przez niego zadań, zapewniając mu niezbędne do wykonania tych zadań narzędzia oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej. Administrator danych zapewnia, aby IOD nie otrzymywał wytycznych i instrukcji dotyczących wykonywania przez niego zadań, mogących mieć wpływ na podejmowanie przez niego decyzji naruszających zasady ochrony danych osobowych. IOD nie może być odwoływany ani karany przez administratora danych za wypełnianie swoich zadań,

3. IOD podlega bezpośrednio najwyższemu kierownictwu administratora danych. (…)

§ 45. Osoby, których dane dotyczą, mogą kontaktować się z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

§ 46. Inspektor Ochrony Danych jest zobowiązany do zachowania tajemnicy i poufności, co do wykonywania swoich zadań.

§ 47. 1. Inspektor Ochrony Danych w szczególności:

1) działa w oparciu m.in. o *Regulamin organizacyjny IOD w Urzędzie Miejskim Wrocławia*;
2) bierze udział w planowaniu wszystkich nowych procesów i projektów obejmujących przetwarzanie danych osobowych i modyfikowaniu już istniejących;
3) posiada bezpośrednie wsparcie pracowników BBI;
4) posiada pośrednie wsparcie w postaci Konsultantów BBI.

2. Inspektor Ochrony Danych jest również uprawniony do podejmowania względem pracowników Urzędu Miejskiego Wrocławia oraz innych osób przetwarzających dane na podstawie upoważnienia Prezydenta Wrocławia (np. stażystów) wszelkich dopuszczalnych prawem działań, niezbędnych do ustalenia czy doszło do zagrożenia lub naruszenia bezpieczeństwa przetwarzanych danych osobowych oraz wyjaśnienia przyczyn tego zagrożenia lub naruszenia i roli osób uczestniczących w tym zagrożeniu lub naruszeniu (w szczególności Inspektor Ochrony Danych może żądać złożenia przez pracownika ustnych lub pisemnych wyjaśnień oraz wnioskować do przełożonego służbowego danego pracownika lub do pracodawcy, o podjęcie stosownych kroków wynikających z przepisów prawa pracy).

§ 48. 1. Zastępca IOD wykonuje zadania wskazane przez IOD, a w czasie jego nieobecności – realizuje je w pełnym zakresie zadań i uprawnień IOD.

2. Do Zastępcy IOD stosuje się odpowiednio postanowienia dotyczące IOD.

§ 49. Konsultant BBI (w odniesieniu do komórki organizacyjnej Urzędu, przy której działa) wspiera BBI i IOD w zakresie realizowanych przez nich obowiązków oraz wykonuje zadania wskazane przez Dyrektora BBI oraz IOD (lub ich zastępców). (…)

Dział 12
Obowiązek informacyjny oraz zgoda na przetwarzanie danych

§ 62. 1. W każdym przypadku zbierania danych osobowych bezpośrednio od osoby, której dane dotyczą, administrator danych spełnia obowiązek informacyjny wobec osoby, której dane dotyczą.

2. Przekazane informacje muszą być przejrzyste, wyraźnie odróżniać się od innych informacji niezwiązanych z ochroną prywatności i formułowane w możliwie najprostszy sposób, unikając nadmiernie specjalistycznego języka. Informacje powinny być konkretne i nie pozostawiać miejsca na różne interpretacje. W szczególności, należy się upewnić, że dla osoby, której dane dotyczą, cele i podstawa prawna przetwarzania danych osobowych są wystarczająco jasne.

3. Komórka organizacyjna Urzędu biorąc pod uwagę specyfikę realizowanych czynności przetwarzania dopasowuje do nich informacje zawarte w klauzuli informacyjnej. Ogólny wzór stanowi *Załącznik nr 9 do PODOiBI (Wzór klauzuli informacyjnej).* Dostosowana klauzula informacyjna konsultowana jest z IOD.

4. Wzór klauzuli informacyjnej dla pracownika Urzędu, określa *Załącznik nr 10 do PODOiBI (Wzór klauzuli informacyjnej dla pracownika Urzędu)*.

5. Wzory klauzul informacyjnych dla stażystów, praktykantów i zleceniobiorców Urzędu Miejskiego Wrocławia dostosowywane są przez komórkę organizacyjną Urzędu realizującą zadanie.

§ 63. 1. W każdym przypadku pozyskiwania danych osobowych z innych źródeł niż od osoby, której dane dotyczą, administrator danych spełnia obowiązek informacyjny wobec osoby, której dane dotyczą, niezwłocznie, jednak nie później niż przy pierwszym kontakcie z osobą, której dane dotyczą. Przekazane informacje muszą spełniać wymogi wskazane w § 62 ust. 2. Komórka organizacyjna Urzędu dostosowuje formułę informacji, której ogólny wzór stanowi *Wzór klauzuli informacyjnej dla pracowników Urzędu Miejskiego Wrocławia,* do merytoryki i specyfiki wykonywanych przez nią czynności przetwarzania. Dostosowana klauzula informacyjna konsultowana jest z IOD.

(…)

Dział 13
Postanowienia końcowe

§ 65. Wszelkie zasady opisane w PODOiBI są przestrzegane przez pracowników przetwarzających dane osobowe, którzy uwzględniają w tym zakresie prawa i wolności osób, których dane te dotyczą.

§ 66. Ocena potrzeby aktualizacji PODOiBI (i jej ewentualna aktualizacja) przeprowadzana będzie przynajmniej raz na rok, a ponadto w każdym przypadku, gdy zostanie to uznane za konieczne (w szczególności: w przypadku zmaterializowania się nowych, niezdiagnozowanych wcześniej ryzyk, które mają wpływ na jej treść).

Dział 14
Załączniki

§ 67. Integralną część „WYCIĄGU DLA KONTRAHENTA Z POLITYKI OCHRONY DANYCH OSOBOWYCH I BEZPIECZEŃSTWA INFORMACJI URZĘDU MIEJSKIEGO WROCŁAWIA” stanowią następujące załączniki PODOiBI:

Załącznik nr 2 – Polityka kluczy;
Załącznik nr 3 – Opis stref Urzędu;
Załącznik nr 4 – Wzór upoważnienia do przetwarzania danych osobowych wraz z oświadczeniem upoważnionego;
Załącznik nr 5 – Wzór oświadczenia o zapoznaniu się z PODOiBI;
Załącznik nr 13 – Zasady funkcjonowania monitoringu wizyjnego w Urzędzie Miejskim Wrocławia;
Załącznik nr 15 – Wykaz Obszarów Przetwarzania Danych w Urzędzie Miejskim Wrocławia;

Załącznik nr 2
do Polityki Ochrony Danych Osobowych
i Bezpieczeństwa Informacji Urzędu Miejskiego Wrocławia

POLITYKA KLUCZY

§ 1. Ilekroć w niniejszym dokumencie mowa o pracowniku Urzędu należy przez to rozumieć pracownika w rozumieniu kodeksu pracy.

§ 2. Dostęp do pomieszczeń we wszystkich lokalizacjach Urzędu mają tylko osoby, dla których dostęp ten jest niezbędny do realizacji zadań na rzecz Urzędu (np. pracownicy Urzędu, stażyści, praktykanci, osoby świadczące usługi na podstawie umów innych niż umowa o pracę) oraz – w przypadku budynku przy ul. Strzegomskiej 148 we Wrocławiu – pracownicy służb ratunkowych.

§ 3. 1. Za określenie uprawnień dostępu do pomieszczeń dla osób, dla których dostęp ten jest niezbędny do realizacji zadań na rzecz Urzędu, odpowiada dyrektor komórki organizacyjnej Urzędu (w odniesieniu do pomieszczeń będących w dyspozycji rzeczonej komórki organizacyjnej Urzędu).

2. Dyrektor komórki organizacyjnej Urzędu odpowiada za przygotowanie i aktualizację list osób upoważnionych do dostępu do pomieszczeń. Aktualne listy przekazywane są administratorowi obiektu w danej lokalizacji.

3. Dyrektor Wydziału Bezpieczeństwa i Zarządzania Kryzysowego Urzędu odpowiedzialny za pracę Centrum Zarządzania Kryzysowego, zobowiązany jest do przedkładania administratorowi obiektu aktualnego wykazu pracowników służb ratunkowych, uprawnionych do poboru kluczy do pomieszczeń w obiekcie mieszczącym się we Wrocławiu przy ul. Strzegomskiej 148.

4. Na podstawie list, o których mowa w ust. 2, pracownikom Urzędu wydawane są przez administratorów obiektów imienne identyfikatory do pobierania i zdawania kluczy („**identyfikator**") lub nadawane są dla ich kart Urbancard uprawnienia do pobierania kluczy z i zdawania kluczy do depozytora kluczy („**autoryzacja karty Urbancard**").

5. W przypadku rozwiązania umowy o pracę lub dłuższej nieobecności (np. urlop macierzyński, urlop bezpłatny) pracownika Urzędu posiadającej identyfikator lub autoryzowaną kartę Urbancard, dyrektor komórki organizacyjnej Urzędu, w której ten pracownik jest zatrudniony, , zobowiązany jest do odebrania identyfikatora i przekazania go administratorowi obiektu albo unieważnienia identyfikatora poprzez przekazanie stosownej informacji administratorowi obiektu albo do zlecenia wycofania autoryzacji dla karty Urbancard.

§ 4. 1. Wydawanie i zdawanie kluczy odbywa się w pomieszczeniach portierni lub bezpośrednio z / do elektronicznych depozytorów kluczy w budynkach Urzędu. Klucz może zostać pobrany i zdany przez pracownika Urzędu, pracownika służb, o których mowa w § 3 ust. 3 lub inne osoby („**użytkownik klucza**").

2. Pobranie klucza:

1) przez pracownika Urzędu następuje po okazaniu imiennego identyfikatora wraz z kartą Urbancard (w przypadku pobierania klucza z portierni) lub za pomocą autoryzowanej karty Urbancard (w przypadku pobierania klucza z depozytora kluczy),
2) w przypadku pracowników służb, o których mowa w § 3 ust. 3 – po zweryfikowaniu danych osoby w wykazie pracowników służb ratunkowych,
3) przez inne osoby, niż wymienione w pkt 2 i 3 – po okazaniu pisemnego zezwolenia wydanego przez dyrektora komórki organizacyjnej Urzędu (w przypadku pobierania klucza z portierni).

3. W wypadkach szczególnych możliwe będzie:

1) na pisemne polecenie Dyrektora komórki organizacyjnej Urzędu – nadanie przez administratora obiektu konkretnej osobie uprawnień do pobierania i zdawania klucza bez potrzeby aktualizacji listy, o której mowa w § 3 ust. 2,
2) pobranie klucza przez użytkownika klucza, po weryfikacji przez osobę dozorującą obiekt (pracownika ochrony lub strażnika miejskiego) tożsamości użytkownika klucza oraz sprawdzeniu czy znajduje się on na liście, o której mowa w § 3 ust. 2, lub czy zostało wydane polecenie, o którym mowa w pkt 1, dotyczące tego użytkownika klucza i jaka jest jego treść.

4. Fakt pobrania i zdania klucza użytkownik klucza potwierdza czytelnym wpisem w książce wydawania kluczy (w przypadku pobierania klucza z portierni) lub fakty te potwierdzane są automatycznie przy odczytywaniu danych autoryzowanej karty Urbancard przez czytnik depozytora kluczy (w przypadku pobierania klucza z depozytora kluczy).

5. W przypadku zgubienia klucza lub karty Urbancard, administrator obiektu lub użytkownik klucza, w zależności, które z nich stwierdzi wcześniej tą okoliczność, niezwłocznie zgłasza incydent bezpieczeństwa zgodnie z procedurą opisaną w Dziale 8 PODOiBI.

6. Każde wydanie klucza zapasowego do pomieszczenia musi być odnotowane w książce raportów prowadzonej przez administratora obiektu.

7. W przypadku elektronicznych systemów kontroli dostępu, w sytuacji zgubienia / kradzieży klucza elektronicznego (identyfikatora) należy niezwłocznie zgłosić ten fakt za pomocą aplikacji HelpDesk lub telefonicznie na nr 9090 oraz zgłosić incydent bezpieczeństwa informacji zgodnie z procedurą opisaną w Dziale 8 PODOiBI.

§ 5. Bezwzględnie zakazuje się użytkownikom kluczy samodzielnego dorabiania kluczy do pomieszczeń Urzędu oraz przekazywania kluczy osobom nieuprawnionym.

§ 6. Wydział Obsługi Urzędu informuje właściwe komórki organizacyjne - z co najmniej dwutygodniowym wyprzedzeniem - o zmianie sposobu przechowywania kluczy z tradycyjnego na przechowywanie w depozytorach.

Załącznik nr 3 #
do Polityki Ochrony Danych Osobowych #
i Bezpieczeństwa Informacji Urzędu Miejskiego Wrocławia #
#

OPIS STREF URZĘDU #

Strefa 1 #

A Ogólnodostępny obszar dla klientów i pracowników #

Korytarze, hole, klatki schodowe, toalety, dziedzińce wewnętrzne #

B Dedykowane obszary obsługi klienta (np. Centrum Obsługi Podatnika, Centrum Obsługi Mieszkańca, kasy) #

Osoby z zewnątrz mogą przebywać w strefach bez nadzoru. #

#

Strefa 2 #

A Pokoje #

Pokoje pracowników zamykane na klucz #

B "Open space" w TCOM #

C Piwnice i strychy #

D Sale konferencyjne i szkoleniowe #

E Pomieszczenia z ksero i drukarkami na korytarzach ("szklane boksy") #

Dostęp do pomieszczeń realizowany jest zgodnie z "Polityką kluczy". #

Rozliczalność dostępu realizowana w formie "książki kluczy", możliwość pobrania klucza wyłącznie przez wskazane imiennie osoby ; #

Osoby z zewnątrz mogą przebywać w strefie wyłącznie pod bezpośrednim nadzorem upoważnionych pracowników administratora lub podmiotu dozorującego (np. straż miejska, pracownicy ochrony. #

F Pomieszczenia w których dostępne są monitory rejestratorów monitoringu wizyjnego w budynkach Urzędu (portiernie) #

Dostęp do pomieszczeń mają wyłącznie uprawnieni pracownicy Wydziału Obsługi Urzędu (administratorzy budynków) oraz pracownicy podmiotów dozorujących. W sytuacjach tego wymagających za zgodą administratora budynku dostęp do pomieszczeń jest udzielany innym osobom. Fakt ten jest każdorazowo odnotowywany w książce przebiegu służby podmiotu dozorującego. #

Strefa 3 #

A Budynkowe/kondygnacyjne punkty dystrybucyjne (BPD/KPD) #

B Centra Przetwarzania Danych (CPD) #

C Miejsca przechowywania kopii zapasowych #

D Miejsca pracy administratorów systemów informatycznych #

E Magazyny: ul. Strzegomska 148 pok. 26, ul. Świdnicka 53 pok. 115 # (magazyn DCPD, magazyn DMSTD) #

Dostęp do pomieszczeń wyłącznie zgodnie z Instrukcją 06/006; #

Osoby z zewnątrz mogą przebywać w strefie wyłącznie pod bezpośrednim nadzorem pracowników administratora lub podmiotu dozorującego (np. straż miejska,# pracownicy ochrony; #

Istnieją aktualizowane na bieżąco rejestry użytkowników (pracowników); #

Rozliczalność dostępu realizowana automatycznie poprzez elektroniczny system rejestracji . #

Załącznik nr 4
do Polityki Ochrony Danych Osobowych i Bezpieczeństwa
Informacji Urzędu Miejskiego Wrocławia

WZÓR UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH WRAZ Z OŚWIADCZENIEM UPOWAŻNIONEGO

Pani/Pan
Imię i nazwisko ……
Stanowisko/Funkcja/Rola* ……
*niepotrzebne skreślić

OŚWIADCZENIE

Oświadczam, że zostałam/em zapoznana/y z przepisami dotyczącymi ochrony danych osobowych oraz regulacjami wewnętrznymi wprowadzonymi i wdrożonymi do stosowania przez Administratora Danych (Prezydenta Wrocławia), także w zakresie dotyczącym bezpieczeństwa informacji i zobowiązuję się do:

1) zachowania w tajemnicy danych osobowych, jak również innych informacji chronionych na podstawie przepisów prawa lub regulacji wewnętrznych Urzędu oraz zachowania w tajemnicy sposobów ich zabezpieczania, także po ustaniu zatrudnienia/powołania/wyznaczenia;
2) niewykorzystywania danych osobowych oraz innych informacji uzyskanych w związku z realizacją obowiązków służbowych w celach pozasłużbowych;
3) korzystania ze sprzętu IT oraz oprogramowania wyłącznie w związku z wykonywaniem obowiązków służbowych;
4) wykorzystywania jedynie oprogramowania pochodzącego udostępnionego przez Urząd;
5) należytej dbałości o ww. sprzęt i oprogramowanie zgodnie z regulacjami wewnętrznymi Urzędu;
6) nieudostępniania sprzętu służbowego, w szczególności urządzeń mobilnych, osobom trzecim.

Przyjmuję do wiadomości, że postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane przez Urząd za ciężkie naruszenie obowiązków pracowniczych w rozumieniu postanowień Kodeksu Pracy lub naruszenie przepisów karnych w rozumieniu przepisów dotyczących informacji prawnie chronionych.

…… ……
data podpis oświadczającego

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

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, upoważniam Pana/Panią: …… …… na okres ..... do przetwarzania danych osobowych, administrowanych lub powierzonych do przetwarzania Administratorowi Danych (Prezydentowi Wrocławia), w postaci papierowej oraz w ramach nadanych dostępów do systemów informatycznych, zgodnie z powierzonymi Pani/Panu zadaniami w ramach:

.....

…… …… data podpis administratora danych

Załącznik nr 5
do Polityki Ochrony Danych Osobowych i Bezpieczeństwa
Informacji Urzędu Miejskiego Wrocławia
(ZMODYFIKOWANY NA POTRZEBY KONTRAHENTA UMW)

…….
(KONTRAHENT UMW)

WZÓR OŚWIADCZENIA O ZAPOZNANIU SIĘ Z WYCIĄGIEM Z PODOiBI

Zgodnie z postanowieniami § 20 Polityki Ochrony Danych Osobowych i Bezpieczeństwa Informacji w Urzędzie Miejskim Wrocławia, stanowiącej załącznik do zarządzenia nr K/16/21 Prezydenta Wrocławia z dnia 30 kwietnia 2021 r. w sprawie Polityki Ochrony Danych Osobowych i Bezpieczeństwa Informacji w Urzędzie Miejskim Wrocławia, oraz postanowieniami ……. oświadczam, że zapoznałam/zapoznałem się szczegółowo z treścią WYCIĄGU DLA KONTRAHENTA Z POLITYKI OCHRONY DANYCH OSOBOWYCH I BEZPIECZEŃSTWA INFORMACJI URZĘDU MIEJSKIEGO WROCŁAWIA".

KONTRAHENT UMW: ……

L.p.	**Imię i nazwisko** (drukowane litery)	**Data**	**Podpis**
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13.			
14.			
15.			

Załącznik nr 13
do Polityki Ochrony Danych Osobowych
i Bezpieczeństwa Informacji Urzędu Miejskiego Wrocławia

ZASADY FUNKCJONOWANIA MONITORINGU WIZYJNEGO W URZĘDZIE MIEJSKIM WROCŁAWIA

Wstęp

Niniejszy dokument określa zasady funkcjonowania monitoringu wizyjnego w budynkach Urzędu Miejskiego Wrocławia wraz z ich otoczeniem pozostającym w zasobach Gminy Wrocław, w tym miejsca instalacji kamer tego systemu, reguły rejestracji i zapisu informacji oraz sposób zabezpieczenia i udostępniania zgromadzonych danych o zdarzeniach.

Urząd Miejski Wrocławia w zakresie zastosowania monitoringu kieruje się zasadą adekwatności, tj. administrator danych osobowych może pozyskiwać jedynie te dane, co do których istnieje uzasadnienie formalnoprawne ich pobierania oraz zasadą proporcjonalności w doborze zastosowanej technologii monitoringu w danym obiekcie.

System monitoringu wizyjnego jest stosowany, ponieważ inne środki prewencyjne, ochrony i bezpieczeństwa o charakterze fizycznym i logicznym, niewymagające pozyskania obrazu, są niewystarczające dla realizacji prawnie uzasadnionych celów w zakresie ochrony dużych powierzchniowo nieruchomości. Zasadność stosowania monitoringu była również wielokrotnie potwierdzana przez organy ścigania. Administrator uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, zdecydował w efekcie przeprowadzonej oceny ryzyka dla ochrony danych osobowych (DPIA), zgodnie z artykułem 35 RODO, stosować w budynkach i wokół budynków Urzędu Miejskiego Wrocławia monitoring wizyjny, na określonych poniżej zasadach, jako niezbędny dla zapewnienia bezpieczeństwa osób przebywających w budynku, ochrony mienia, nadzoru nad pracownikami i infrastrukturą, zgodny z zasadami przetwarzania danych osobowych oraz niegenerujący wysokiego ryzyka dla praw i wolności osób objętych tym monitoringiem.

Przed wejściem w życie niniejszej wersji dokumentu przeanalizowano następujące aspekty:
1) nadzór eksploatacyjny,
2) bezpieczeństwo fizyczne oprogramowania jak i urządzeń systemu monitoringu wizyjnego,
3) zapewnienie adekwatnych środków technicznych i organizacyjnych w celu bezpiecznego przechowywania oraz archiwizacji nagrań z systemu monitoringu wizyjnego,
4) przeprowadzono ocenę skutków dla ochrony danych (DPIA) w opisywanym zakresie przetwarzania.

Rozdział I: Słownik

Określenia użyte w niniejszym dokumencie oznaczają:
1) administrator obiektu – pracownik Wydziału Obsługi Urzędu obowiązany i uprawniony do: podejmowania wszelkich działań zmierzających do funkcjonowania obiektu zgodnie z jego przeznaczeniem i jego ochrony (np. wydawania upoważnień umożliwiających dostęp do pomieszczeń);
2) monitoring wewnętrzny – monitoring rejestrujący obraz wewnątrz obiektów Urzędu;
3) monitoring zewnętrzny – monitoring rejestrujący obraz w bezpośrednim otoczeniu obiektów Urzędu;
4) obiekt – pomieszczenie lub budynek;
5) system monitoringu wizyjnego – zespół powiązanych ze sobą urządzeń (np. kamer, urządzeń rejestrująco-odtwarzających, nośników danych) i oprogramowania, służący do rejestracji i przechowywania obrazu.

Rozdział II: Cel i zakres przetwarzania

System monitoringu wizyjnego obejmuje monitoring:

1) wewnętrzny stosowany w celu: zapewnienia bezpieczeństwa pracowników, ochrony mienia oraz zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić Gminę Wrocław Urząd Miejski Wrocławia na szkodę,
2) zewnętrzny stosowany w celu: zapewnienia bezpieczeństwa publicznego i bezpieczeństwa klientów oraz ochrony przeciwpożarowej w obszarze przestrzeni publicznej wokół obiektów Urzędu, w szczególności ograniczenia zachowań nagannych i innych zachowań niepożądanych zagrażających zdrowiu i bezpieczeństwu użytkowników obiektu.

Zakres przetwarzania obejmuje przetwarzanie (bez dźwięku) wizerunku postaci i twarzy klientów Urzędu, pracowników Urzędu oraz osób postronnych (przechodniów, funkcjonariuszy publicznych itp.), w miejscach, o których mowa w rozdziale IV, za pomocą urządzeń, o których mowa w rozdziale V, w sposób określonych w tych rozdziałach.

Rozdział III: Podstawy prawne przetwarzania

Urząd korzysta z systemu monitoringu wizyjnego zgodnie z art. 22^2 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2019 r. poz. 1040 z późn. zm.) oraz na podstawie art. 9a ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2019 r., poz. 506 z późn. zm.). Powyższe podstawy prawne zostały wprowadzone przepisami ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000 z późn. zm.) w związku z wdrożeniem rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dziennik Urzędowy Unii Europejskiej z dnia 14 maja 2016 r. L 119/1, s. 1 z późn. zm.).

Podstawą prawną przetwarzania danych w ramach wizyjnego monitoringu wewnętrznego jest prawnie uzasadniony interes administratora polegający na potrzebie zapewnienia bezpieczeństwa na terenie Urzędu i jego placówek oraz możliwości identyfikacji osób znajdujących się na ich terenie. W przypadku wizyjnego monitoringu zewnętrznego, podstawą prawną przetwarzania jest wykonanie zadania realizowanego w interesie publicznym przez administratora polegającego na potrzebie zapewnienia bezpieczeństwa publicznego i bezpieczeństwa klientów oraz ochrony przeciwpożarowej w obszarze przestrzeni publicznej wokół obiektów Urzędu.

Nagrania obrazu zawierające dane osobowe przetwarza się wyłącznie do celów, dla których zostały zebrane, wskazanych w rozdziale I, i przechowuje w okresie do 3 miesięcy od dnia nagrania. Urząd zapewnia ścisłą kontrolę praw dostępu osób uprawnionych do nagrań.

Rozdział IV: Miejsca monitorowane

Wykaz budynków Urzędu Miejskiego Wrocławia objętych systemem monitoringu wizyjnego:

1) ul. Bernardyńska 5,
2) ul. Wojciecha Bogusławskiego 8,10,
3) ul. Hubska 8-16,
4) al. Karkonoska 45,
5) ul. Kotlarska 41,
6) al. Marcina Kromera 44,
7) pl. Nowy Targ 1-8,
8) Rynek 13,
9) Sukiennice 9 (w tym Sukiennice 8, Rynek Ratusz 7-9 oraz Przejście Żelaźnicze 1),
10) Sukiennice 10,
11) ul. Świdnicka 53,
12) ul. Pawła Włodkowica 20,
13) ul. Gabrieli Zapolskiej 4.

Kamery są umieszczone w różnych punktach budynków Urzędu Miejskiego Wrocławia, zapewniając widok m.in. na ciągi komunikacyjne, hole, windy, klatki schodowe, dziedzińce, parkingi, kasy, centra obsługi mieszkańców.

Lokalizacja kamer w poszczególnych budynkach przedstawiona jest na schematach, stanowiących załącznik nr 2 do niniejszego dokumentu.

Kamery w Urzędzie zlokalizowane są w taki sposób, aby ograniczyć do minimum monitorowanie tych obszarów, które nie są istotne dla zakładanych celów. Urząd nie monitoruje więc miejsc, w których oczekuje się większej prywatności (m.in. miejsc, o których mowa w art. 22^2 § 1^1 i § 2 zd. 1 kodeksu pracy oraz art. 9a ust. 2 ustawy o samorządzie gminnym).

Obiekty objęte systemem monitoringu wizyjnego są oznaczone informacją o monitoringu w sposób widoczny i czytelny, za pomocą piktogramów ze znaczkiem kamery.

Rozdział V: Informacje techniczne na temat funkcjonowania systemu monitoringu wizyjnego

System monitoringu wizyjnego składa się z następujących elementów:
1) zespołu kamer rejestrujących zdarzenia poprzez odbiór obrazu w przestrzeni znajdującej się w polu widzenia kamer monitorowanego obszaru. Urząd nie używa kamer internetowych do celów wideoochrony,
2) urządzeń przesyłowych, w tym monitorów pozwalających na podgląd,
3) urządzeń rejestrująco-odtwarzających na urządzeniu twardodyskowym,
4) elektronicznych nośników danych oraz
5) oprogramowania wykorzystywanego w celu osiągnięcia określonej funkcjonalności w zakresie monitoringu.

Zainstalowane kamery umożliwiają jedynie rejestrację i zapis obrazu bez rejestracji dźwięku oraz bez możliwości automatycznej analizy obrazu wykorzystywanej do identyfikacji osób obserwowanych.

Funkcjonujący system monitoringu wizyjnego nie przetwarza „danych biometrycznych", czyli danych szczególnych kategorii w rozumieniu art. 9 ust. 1 RODO (w szczególności nie umożliwia automatycznego rozpoznawania osób monitorowanych w oparciu o cechy biometryczne).

Wszystkie kamery działają całodobowo, siedem dni w tygodniu.

System monitoringu wizyjnego jest systemem standardowym i (zasadniczo) statycznym (tj. pole widzenia kamer nie jest dynamicznie dostosowywane). Rejestruje on obrazy cyfrowe i jest wyposażony w detektor ruchu. Rejestruje określone ruchy wykryte przez kamery na monitorowanym obszarze wraz z godziną, datą i miejscem. Ponieważ system monitoringu wizyjnego nie jest synchronizowany z zewnętrznym źródłem czasu, mogą występować nieznaczne różnice między czasem rzeczywistym, a czasem uwidocznionym na materiale z monitoringu.

Zapis z systemu monitoringu wizyjnego przechowywany jest na elektronicznym nośniku przez okresy wskazane osobno dla każdego budynku, jak w załączniku nr 1 do niniejszego dokumentu. Po upływie wskazanego okresu dane ulegają usunięciu poprzez nadpisanie danych na urządzeniu rejestrującym obraz.

Elementy systemu monitoringu wizyjnego w miarę konieczności i możliwości finansowych są udoskonalane, wymieniane i rozszerzane.

W razie potrzeby system monitoringu wizyjnego uzupełnia inne systemy ochrony fizycznej, takie jak system kontroli dostępu czy system antywłamaniowy.

Systemu monitoringu wizyjnego nie stosuje się do żadnych innych celów niż wskazane wcześniej np. do monitorowania pracy urzędników, ani do kontrolowania obecności.

Rozdział VI: Dostęp do zebranych danych osobowych

Dane z systemu monitoringu wizyjnego mogą być udostępniane wyłącznie podmiotom upoważnionym na podstawie przepisów prawa. Warunkiem koniecznym dostępu do zapisanego materiału z systemu monitoringu wizyjnego przez podmiot uprawniony jest podanie (w miarę precyzyjne - dzień, godzina, minuta) okresu, z którego pochodzi zarejestrowany materiał.

Z wyjątkiem sytuacji opisanej w art. 15 RODO, nie udostępnia się nagrań osobom fizycznym, ponieważ mogłoby to naruszyć prawa i wolności innych osób trzecich.

Dostęp do materiałów wideo – zarówno zarejestrowanych, jak i otrzymywanych na żywo – mają jedynie osoby upoważnione, w tym administratorzy obiektów i pracownicy portierni.

Osoby, które mają podgląd w obraz zarejestrowany przez system monitoringu wizyjnego zobowiązane są do przestrzegania przepisów prawa w zakresie ochrony danych osobowych a ich uprawnienie dostępu do tych danych musi wynikać z wyraźnego upoważnienia, np. z treści umowy zawartej na dozór i monitorowanie budynków.

Dostęp do nagrań i struktury technicznej systemu monitoringu wizyjnego zgodnie z zasadą ograniczonego dostępu przysługuje niewielkiej grupie wskazanych osób. Urząd definiuje cel i zakres prawa dostępu – w szczególności określa, kto ma prawo oglądać nagrania w czasie rzeczywistym, oglądać zarejestrowane nagrania, kopiować je, pobierać, usuwać, zmieniać lub udostępniać.

Wszyscy pracownicy Urzędu, w ramach obowiązku informacyjnego, zostaną poinformowani o celach, zakresie oraz sposobie zastosowania systemu monitoringu wizyjnego przed dopuszczeniem ich do pracy. Podobnie, praktykanci, stażyści oraz osoby zatrudnione na podstawie umowy cywilnoprawnej w Urzędzie są informowani, w ramach obowiązku informacyjnego, o celach, zakresie oraz sposobie zastosowania systemu monitoringu wizyjnego.

Informacja na temat funkcjonowaniu systemu monitoringu wizyjnego dla klientów Urzędu jest umieszczona m.in. w gablotach informacyjnych, na stronie Biuletynu Informacji Publicznej oraz w miejscach, których jest zainstalowany monitoring.

Wszelkie przypadki przekazania danych z systemu monitoringu wizyjnego poza Urząd i wszelkie przypadki ich ujawnienia poza Urząd są dokumentowane. Dokładnie oceniana jest konieczność ich przekazania oraz zgodność celów przekazania z pierwotnym celem ich przetwarzania na potrzeby bezpieczeństwa. Do rejestru zatrzymywania i przekazywania danych ma wgląd kierownictwo Wydziału Obsługi Urzędu oraz Inspektor Ochrony Danych w Urzędzie.

Rozdział VII: Ochrona i zabezpieczanie danych osobowych

Aby chronić bezpieczeństwo systemu monitoringu wizyjnego, w tym danych osobowych, wprowadzono następujące rozwiązania techniczne i organizacyjne:

1) rejestratory, na których przechowuje się zarejestrowane obrazy, znajdują się w zabezpieczonych pomieszczeniach na portierniach, chronionych środkami bezpieczeństwa fizycznego. Dostęp do portierni mają administratorzy obiektów oraz upoważnieni pracownicy podmiotów przetwarzających. W sytuacjach szczególnych wejście do pomieszczeń innych osób odbywa się za zgodą administratora obiektu i jest rejestrowane w Książce przebiegu służby. Transmisja obrazu i jego rejestracja odbywa się wyłącznie lokalnie, tj. na drodze pomiędzy rejestratorem, a kamerą. Żadne z urządzeń wchodzących w skład systemu monitoringu wizyjnego nie jest podłączone do sieci Internet;
2) Wydział Obsługi Urzędu na bieżąco aktualizuje listę wszystkich osób, którym przysługują prawa dostępu do systemu i szczegółowo określa te prawa,
3) o udzieleniu prawa dostępu do systemu monitoringu winien być powiadomiony niezwłocznie administrator obiektu i Inspektor Ochrony Danych,
4) przed nabyciem lub instalacją wszelkich nowych systemów wideoochrony należy skonsultować się z Inspektorem Ochrony Danych.

Rozdział VIII: Okres przechowywania danych

Nagrania obrazu zawierające dane osobowe są przechowywane przez okres nieprzekraczający 3 miesięcy od dnia nagrania, o ile przepisy odrębne nie stanowią inaczej. Szczegóły dotyczące okresów przechowywania nagrań w poszczególnych budynkach określono w załączniku nr 1 do niniejszego dokumentu. Po upływie ww. okresu uzyskane w wyniku monitoringu nagrania obrazu zawierające dane osobowe, podlegają zniszczeniu, z wyjątkiem sytuacji, w których nagrania zostały zabezpieczone, zgodnie z odrębnymi przepisami.

Rozdział IX: Prawa osób, których dotyczą dane

Osobom, których dotyczą dane osobowe przechowywane przez Urząd w ramach systemu monitoringu wizyjnego, przysługują następujące prawa związane z przetwarzaniem danych osobowych:

1) prawo dostępu do danych osobowych,
2) prawo żądania sprostowania własnych danych osobowych,
3) prawo żądania usunięcia własnych danych osobowych,
4) prawo żądania ograniczenia przetwarzania własnych danych osobowych,
5) prawo sprzeciwu wobec przetwarzania własnych danych osobowych ze względu na Twoją szczególną sytuację.

Aby skorzystać z powyższych praw, należy skontaktować się z Biurem ds. Bezpieczeństwa Informacji lub z Inspektorem Ochrony Danych (dane kontaktowe w rozdziałach XI i XII poniżej).

Na wniosek osoby, której dane dotyczą, o którym mowa w art. 15 RODO, istnieje możliwość obejrzenia zarejestrowanych obrazów. W tym celu wnioskodawca musi jednoznacznie udowodnić swoją tożsamość oraz wskazać dzień, godzinę, miejsce i okoliczności, w których został zarejestrowany przez kamery.

Rozdział X: Prawo wniesienia skargi

W przypadku nieprawidłowości przy przetwarzaniu danych osobowych w ramach systemu monitoringu wizyjnego, osobie, której prawa zostały naruszone, przysługuje prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych, tj. Prezesa Urzędu Ochrony Danych Osobowych.

Rozdział XI: Administrator Danych Osobowych

Administratorem danych osobowych przetwarzanych w ramach systemu monitoringu wizyjnego jest Gmina Wrocław Urząd Miejski Wrocławia, z siedzibą we Wrocławiu.

Dane kontaktowe:

1) listownie na adres: pl. Nowy Targ 1-8, 50-141 Wrocław,
2) przez e-mail: iod@um.wroc.pl,
3) telefonicznie: +48 71 777 77 77

Rozdział XII: Inspektor Ochrony Danych

W Urzędzie wyznaczono Inspektora Ochrony Danych. Jest nim Sebastian Sobecki. Inspektor to osoba, z którą można się kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych oraz korzystania z przysługujących praw związanych z przetwarzaniem danych osobowych.

Dane kontaktowe:

- listownie na adres: ul. G. Zapolskiej 4, 50-032 Wrocław,
- przez e-mail: iod@um.wroc.pl,
- telefonicznie: +48 717 77 77 24

Rozdział XIII: Dane kontaktowe – administratorzy obiektów

1) pl. Nowy Targ 1-8, ul. Bernardyńska 5, ul. Kotlarska 41 telefoniczne: +48 71 777 75 05 (lub 75 15, 75 55) oraz dyspozytor transportu samochodowego +48 71 777 74 92 ,
2) al. Marcina Kromera 44 telefonicznie: +48 71 777 92 00,
3) Sukiennice 8 i 9, Rynek Ratusz 7-9, Przejście Żelaźnicze 1, Sukiennice 10, ul. Pawła Włodkowica 20, Rynek 13
   telefonicznie: +48 71 777 83 22 (lub 74 78, 83 12),
4) ul. Gabrieli Zapolskiej 4, ul. Świdnicka 53, ul. Wojciecha Bogusławskiego 8,10, al. Karkonoska 45
   telefonicznie: +48 71 777 75 63 (lub 86 01, 76 05),
5) ul. Hubska 8-16 telefonicznie: +48 71 799 67 63

Załącznik nr 15
do Polityki Ochrony Danych Osobowych
i Bezpieczeństwa Informacji Urzędu Miejskiego Wrocławia

WYKAZ OBSZARÓW PRZETWARZANIA DANYCH W URZĘDZIE MIEJSKIM WROCŁAWIA

Obszar przetwarzania danych osobowych obejmuje następujące budynki Urzędu:

1) ul. Bernardyńska 5;
2) ul. Bogusławskiego 8, 10;
3) ul. Hubska 8-16
4) ul. Karkonoska 45;
5) ul. Komuny Paryskiej 39-41;
6) ul. Kotlarska 41;
7) ul. Kuźnicza 15;
8) al. M. Kromera 44;
9) ul. K. Michalczyka 23;
10) pl. Nowy Targ 1-8;
11) Rynek Ratusz 7-9;
12) Rynek 13;
13) ul. Stalowa 62;
14) ul. Strzegomska 148;
15) Sukiennice 8, 9, 10;
16) ul. Świdnicka 53;
17) ul. P. Włodkowica 20;
18) ul. G. Zapolskiej 4;
19) Przejście Żelaźnicze 1;