

POLITYKA

OCHRONY DANYCH OSOBOWYCH

Miejskiej Strefy Kultury w Łodzi
z siedzibą w Łodzi, przy ulicy Krzemienieckiej 2a

Data wprowadzenia:	23.02.2022
Wersja:	2
Data aktualizacji:	25.11.2024
Opracował:	Inspektor Ochrony Danych Maciej Wara-Wąsowski
Zatwierdził:	

SPIS TREŚCI

INFORMACJE OGÓLNE	3
1. Definicje.....	3
2. Cele Polityki ochrony danych osobowych	5
3. Zakres informacji objętych Polityką ochrony danych osobowych oraz zakres zastosowania	6
OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH	7
Struktura organizacji ochrony danych osobowych.....	7
1.1. Administrator Danych.....	7
1.2. Inspektor Ochrony Danych	9
1.3. Administrator Systemów Informatycznych	10
1.4. Osoby upoważnione do przetwarzania danych osobowych	11
ZASADY PRZETWARZANIA DANYCH OSOBOWYCH.....	12
1. Ogólne zasady przetwarzania danych osobowych.....	12
2. Zakres przetwarzanych danych osobowych.....	13
3. Dopuszczenie osób do przetwarzania danych osobowych	15
4. Powierzenie przetwarzania danych osobowych	16
5. Udostępnienie danych osobowych	18
6. Przekazywanie danych osobowych do państw trzecich.....	19
7. Współadministrowanie danymi osobowymi.....	21
8. Audyty zgodności przetwarzania danych osobowych.....	22
9. Realizacja praw osób, których dane dotyczą	23
10. Ochrona danych osobowych w fazie projektowania	24
11. Ocena skutków dla ochrony danych osobowych (data protection impact assessment).....	25
12. Incydenty ochrony danych osobowych.....	26
13. Ogólne zasady bezpieczeństwa ochrony danych osobowych.....	27
14. Przeglądy i aktualizacja Polityki ochrony danych osobowych.....	29
ZAŁĄCZNIKI	30

INFORMACJE OGÓLNE

1. DEFINICJE

1. **Administrator Danych (ADO)** – Miejska Strefa Kultury w Łodzi, osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; (dalej: ADO lub MSK)
2. **Administrator Systemów Informatycznych (ASI)** – osoba wyznaczona przez Administratora Danych, koordynująca działania związane z zapewnieniem bezpieczeństwa systemów informatycznych, w tym również odpowiadająca za nadzór nad zabezpieczeniem danych osobowych przetwarzanych w systemach informatycznych wykorzystywanych przez Administratora Danych,
3. **dane osobowe** – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”), gdzie poprzez możliwą do zidentyfikowania osobę fizyczną rozumie się osobę, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej,
4. **DPIA** – ocena skutków dla ochrony danych osobowych (*data protection impact assessment*),
5. **Inspektor Ochrony Danych (IOD)** – osoba wyznaczona przez Administratora Danych, koordynująca procesy związane z przestrzeganiem zasad ochrony danych osobowych w ramach procesów przetwarzania danych osobowych zachodzących w strukturze Administratora Danych,
6. **organ nadzorczy** – niezależny organ publiczny powołany w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych oraz ułatwiania swobodnego przepływu danych osobowych w Unii, powołany w każdym państwie członkowskim Unii, którego podstawowym zadaniem jest monitorowanie stosowania RODO,
7. **państwo trzecie** – państwo spoza Europejskiego Obszaru Gospodarczego.
8. **podmiot przetwarzający** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora Danych,
9. **PODO, Polityka** – niniejsza Polityka ochrony danych osobowych,
10. **pracownik** – osoba współpracująca z Administratorem Danych na podstawie umowy o pracę lub umowy cywilnoprawnej,

11. **przetwarzanie** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,
12. **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),
13. **Unia** – Unia Europejska,
14. **Ustawa** – Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2019 r., poz. 1781 ze zm.)

2. CELE POLITYKI OCHRONY DANYCH OSOBOWYCH

Polityka ochrony danych osobowych została opracowana i wdrożona w strukturze Administratora Danych w celu zapewnienia zgodności przetwarzania danych osobowych z wymogami polskich i europejskich aktów prawnych, w szczególności:

1. 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),
2. Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jedn. Dz. U. z 2019 r., poz. 1781 ze zm.)

Polityka ochrony danych osobowych ma zastosowanie do wszystkich pracowników Administratora Danych, którzy w zakresie swoich obowiązków służbowych przetwarzają dane osobowe, jak również do innych osób, które z upoważnienia Administratora Danych uzyskały dostęp do danych osobowych. Każda z tych osób została zapoznana z najważniejszymi procedurami bezpieczeństwa danych opisanymi w Polityce ochrony danych osobowych i zobowiązana do ich przestrzegania w zakresie wynikającym z przydzielonych zadań. Osoby, o których mowa złożyły oświadczenie o zapoznaniu się z procedurami bezpieczeństwa danych oraz zobowiązały się do ich stosowania. Oświadczenie stanowi załącznik nr 2.5 do niniejszej polityki.

Wszelkie wątpliwości dotyczące sposobu interpretacji zapisów Polityki ochrony danych osobowych, powinny być rozstrzygane na korzyść zapewnienia możliwie najwyższego poziomu ochrony danych osobowych oraz realizacji praw osób, których dane dotyczą.

3. ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ OCHRONY DANYCH OSOBOWYCH ORAZ ZAKRES ZASTOSOWANIA

Polityka ochrony danych osobowych opisuje zasady i procedury przetwarzania danych osobowych. Jest to zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych wewnątrz Administratora Danych. Polityka odnosi się całościowo do problemu zabezpieczenia danych osobowych, tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych.

Politykę ochrony danych osobowych stosuje się do wszelkich czynności, stanowiących w myśl RODO, przetwarzanie danych osobowych. Bez względu na źródło pochodzenia danych osobowych, ich zakres, cel zebrania, sposób przetwarzania lub czas przetwarzania, stosowane są zasady ujęte w Polityce.

Rygorowi Polityki podlegają także dane powierzone Administratorowi Danych do przetwarzania na podstawie umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego oraz dane osobowe, które zostały Administratorowi Danych udostępnione.

Przetwarzanie danych osobowych odbywa się na obszarach wskazanych przez Administratora Danych zgodnie z rejestrem czynności przetwarzania danych osobowych stanowiącym załącznik nr 4.5 do niniejszej Polityki.

Przetwarzanie danych odbywa się w budynkach lub/i pomieszczeniach wskazanych w ewidencji budynków i pomieszczeń, stanowiącej załącznik nr 4.3 do Polityki

OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

STRUKTURA ORGANIZACJI OCHRONY DANYCH OSOBOWYCH

Za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami RODO, Ustawy, Polityki oraz procedur wewnętrznych z zakresu ochrony danych osobowych wdrożonych w strukturze Administratora Danych, odpowiadają:

1. Administrator Danych - dyrekcja Miejskiej Strefy Kultury w Łodzi
2. Inspektor Ochrony Danych – powołany i zgłoszony do PUODO
3. Administrator Systemów Informatycznych – osoba wskazana w załączniku nr 2.3 do PODO
4. Osoby upoważnione do przetwarzania danych osobowych – pracownicy i współpracownicy Administratora

1.1. ADMINISTRATOR DANYCH

1. Administrator Danych wyznacza:
 - 1.1. IOD,
 - 1.2. Administratora Systemów Informatycznych.
2. Administrator Danych jest odpowiedzialny za:
 - 2.1. zapewnienie odpowiednich środków organizacyjnych i technicznych w celu zapewnienia i wykazania przetwarzania danych osobowych zgodnie z określonymi w RODO zasadami przetwarzania danych osobowych,
 - 2.2. wdrożenie odpowiednich procedur ochrony danych osobowych,
 - 2.3. jeśli uzna to za konieczne, stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji, jako element dla stwierdzenia przestrzegania przez Administratora Danych ciężących na nim obowiązków,
 - 2.4. zapewnienie środków umożliwiających prawidłową realizację praw osób, których dane dotyczą,
 - 2.5. prowadzenie rejestru czynności przetwarzania danych osobowych,
 - 2.6. prowadzenie rejestru kategorii przetwarzania dokonywanych w imieniu innego administratora,
 - 2.7. współpracę z organem nadzorczym w ramach wykonywania przez niego swoich zadań,

- 2.8. wdrożenie odpowiednich środków organizacyjnych i technicznych, aby zapewnić stopień bezpieczeństwa odpowiadający istniejącemu ryzyku naruszenia praw lub wolności osób, których dane dotyczą,
- 2.9. zgłaszanie naruszenia ochrony danych osobowych właściwemu organowi nadzorczemu, a w przypadku, gdy zajdą ku temu odpowiednie przesłanki, również osobie, której dane dotyczą,
- 2.10. dokumentowanie wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia, jego skutków oraz podjętych działań zaradczych,
- 2.11. zapewnienie odpowiednich środków w celu dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych w sytuacji, jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w tym, jeżeli zajdą ku temu odpowiednie przesłanki, konsultację z organem nadzorczym,
- 2.12. nadawanie upoważnień do przetwarzania danych osobowych oraz prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
- 2.13. zapewnienie legalności przekazywania danych osobowych do podmiotów trzecich,
- 2.14. w stosunku do IOD:
 - 2.14.1. zapewnienie, że jest on właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych,
 - 2.14.2. wspieranie IOD w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej,
 - 2.14.3. zagwarantowanie by IOD nie działał pod wpływem presji i nie otrzymywał instrukcji dotyczących wykonywania swoich zadań,
 - 2.14.4. publikację danych kontaktowych IOD oraz zawiadomienie o nich organu nadzorczego.
3. Administrator Danych każdorazowo wyraża zgodę oraz ostateczną akceptację na kluczowe z perspektywy organizacji działania IOD oraz ASI, w które zaangażowane są podmioty trzecie. Do zaakceptowania tych działań, wystarczająca jest zgoda wyrażona w formie wiadomości e-mail.
4. Wszelkie obowiązki i uprawnienia Administratora Danych wynikają z przepisów prawa (RODO) oraz z wewnętrznych procedur organizacyjnych.

1.2. INSPEKTOR OCHRONY DANYCH

1. Funkcję IDO pełni osoba wyznaczona przez Administratora Danych. Uzasadnienie powołania IOD w Miejskiej Strefie Kultury w Łodzi znajduje się w załączniku nr 1.1 do Polityki
2. Wzory dokumentów wyznaczenia oraz odwołania IOD znajdują się w Załączniku nr 2.1 do Polityki.
3. IOD jest wyznaczany przez Administratora Danych na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia swoich zadań.
4. Do zadań IOD należy:
 - 4.1. informowanie o obowiązkach wynikających z RODO oraz innych właściwych przepisów Unii lub państw członkowskich o ochronie danych osobowych oraz doradzanie w tym zakresie,
 - 4.2. monitorowanie przestrzegania RODO oraz innych właściwych przepisów Unii lub państw członkowskich o ochronie danych osobowych,
 - 4.3. monitorowanie przestrzegania wdrożonych procedur ochrony danych osobowych,
 - 4.4. doradztwo w zakresie podziału obowiązków (np. między współadministratorami, Administratorem Danych a podmiotem przetwarzającym lub pomiędzy pracownikami Administratora Danych),
 - 4.5. działania zwiększające świadomość pracowników Administratora Danych w zakresie obowiązków wynikających z RODO lub przyjętych procedur,
 - 4.6. szkolenia dla pracowników Administratora Danych uczestniczących w operacjach przetwarzania danych,
 - 4.7. przeprowadzanie audytów w zakresie przestrzegania RODO i wdrożonych procedur ochrony danych osobowych,
 - 4.8. udzielanie na żądanie zaleceń, co do oceny skutków dla ochrony danych osobowych oraz monitorowanie jej wykonania,
 - 4.9. współpraca z organem nadzorczym oraz pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych,
 - 4.10. pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

1.3. ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

1. Funkcję ASI pełni osoba wyznaczona przez Administratora Danych.
2. Oświadczenie o wyznaczeniu ASI stanowi Załącznik nr 2.3. do Polityki.
3. Do zadań ASI należy:
 - 3.1. Sporządzenie oraz nadzór nad procedurą i rejestrem nadanych uprawnień do systemów informatycznych
 - 3.2. sporządzenie oraz nadzór nad instrukcjami zarządzania systemami (załącznik nr 1.6 do Polityki)
 - 3.3. sporządzenie oraz nadzór nad ewidencją systemów przetwarzających dane osobowe,
 - 3.4. opracowywanie oraz aktualizacja opisu technicznych środków bezpieczeństwa wdrożonych w strukturze Administratora Danych,
 - 3.5. nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,
 - 3.6. podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,
 - 3.7. identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych,
 - 3.8. sprawowanie nadzoru nad kopiami zapasowymi;
 - 3.9. inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych,
 - 3.10. ścisła współpraca z IOD w zakresie bezpieczeństwa i zasad przetwarzania danych osobowych w systemach informatycznych.

1.4. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Każda osoba, która uzyskała upoważnienie do przetwarzania danych, zobowiązana jest do ich ochrony w sposób zgodny z przepisami RODO, Ustawy oraz postanowieniami Polityki.
2. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia. Stosowny zapis o przyjęciu zobowiązania do zachowania w tajemnicy przetwarzanych danych osobowych zawiera upoważnienie, którego wzór znajduje się w Załączniku nr 2.4 do Polityki.
3. Naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy skutkuje poniesieniem odpowiedzialności karnej na podstawie przepisów Ustawy oraz stanowi ciężkie naruszenie obowiązków pracowniczych i może być podstawą rozwiązania stosunku pracy w trybie art. 52 Ustawy Kodeks Pracy (tekst jedn. Dz.U. 2023, poz. 1465 z), bądź rozwiązania stosunku cywilnoprawnego.
4. Upoważnienie do przetwarzania danych zostaje nadane pracownikowi lub współpracownikowi Administratora danych po ukończeniu szkolenia RODO zgodnie z procedurą szkoleń i nadawania upoważnień, stanowiącą załącznik nr 1.4 do Polityki

ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. OGÓLNE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. Przetwarzanie danych osobowych w strukturze Administratora Danych odbywa się zgodnie z ogólnymi zasadami przetwarzania danych osobowych określonymi w art. 5 RODO (*zasada rozliczalności*). Oznacza to, że dane osobowe przetwarzają się:
 - 1.1 zgodnie z prawem, w oparciu o co najmniej jedną przesłankę legalności przetwarzania danych osobowych wskazaną w art. 6 lub 9 RODO (*zasada legalności*),
 - 1.2 w sposób rzetelny przy uwzględnieniu interesów i rozsądnych oczekiwań osób, których dane dotyczą (*zasada rzetelności*),
 - 1.3 w sposób przejrzysty dla osób, których dane dotyczą (*zasada przejrzystości*),
 - 1.4 w konkretnych, wyraźnych i prawnie uzasadnionych celach (*zasada ograniczenia celu*),
 - 1.5 w zakresie adekwatnym, stosownym oraz niezbędnym dla celów, w których są przetwarzane (*zasada minimalizacji danych*),
 - 1.6 przy uwzględnieniu ich prawidłowości i ewentualnego uaktualniania (*zasada prawidłowości*),
 - 1.7 przez okres nie dłuższy, niż jest to niezbędne dla celów, w których są przetwarzane (*zasada ograniczenia przechowywania*),
 - 1.8 w sposób zapewniający odpowiednie bezpieczeństwo (*integralność i poufność*).
2. Administrator Danych gwarantuje, że określone decyzje odnoszące się do procesów przetwarzania danych osobowych zostały przeanalizowane z punktu widzenia zgodności z ogólnymi zasadami przetwarzania danych, a przede wszystkim, że są z nimi zgodne.
3. Zgodnie z zasadą przejrzystości oraz spełniając wymagania art. 13 i 14 RODO, Administrator stosuje odpowiednie klauzule informacyjne, opisujące m.in. tożsamość administratora danych, podstawy prawne przetwarzania danych, cele przetwarzania, retencje danych oraz prawa osób których dane dotyczą.
4. Wzory klauzul informacyjnych stosowanych w Miejskiej Strefie Kultury w Łodzi, stanowią załączniki do Polityki: 2.10 (ogólna klauzula informacyjna), 2.11 (klauzula informacyjna dotycząca zawieranych umów, 2.12 (klauzula informacyjna dla pracowników MSK), 2.13 (klauzula informacyjna dotycząca monitoringu wizyjnego)

2. ZAKRES PRZETWARZANYCH DANYCH OSOBOWYCH

1. Polityka ma zastosowanie w stosunku do wszystkich danych osobowych przetwarzanych przez Administratora Danych, niezależnie od formy ich przetwarzania (elektroniczna lub papierowa) oraz tego, czy są to dane przetwarzane w zbiorach danych, w zestawach czy stanowią one pojedyncze informacje osobowe.
2. Administrator Danych prowadzi:
 - 2.1 rejestr czynności przetwarzania danych osobowych, których jest administratorem w rozumieniu RODO (załącznik nr 4.5 Polityki)
 - 2.2 rejestr kategorii czynności przetwarzania dokonywanych w imieniu administratorów, którzy powierzyli mu przetwarzanie danych (załącznik nr 4.6 do Polityki)
3. Rejestr, o którym mowa w pkt 2.1. zawiera co najmniej następujące informacje:
 - 3.1 nazwę oraz dane kontaktowe Administratora Danych oraz wszelkich współadministratorów
 - 3.2 gdy ma to zastosowanie imię, nazwisko lub nazwę oraz dane kontaktowe swojego przedstawiciela
 - 3.3 imię i nazwisko oraz dane kontaktowe IOD,
 - 3.4 cele przetwarzania,
 - 3.5 opis kategorii osób, których dane dotyczą,
 - 3.6 opis kategorii danych osobowych,
 - 3.7 kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,
 - 3.8 gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,
 - 3.9 jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
 - 3.10 ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.
4. Rejestr, o którym mowa w pkt 2.2. zawiera co najmniej następujące informacje:
 - 4.1 nazwę oraz dane kontaktowe Administratora Danych,
 - 4.2 imię i nazwisko lub nazwę oraz dane kontaktowe każdego administratora, w imieniu którego działa Administrator Danych,
 - 4.3 gdy ma to zastosowanie, imię, nazwisko lub nazwę oraz dane kontaktowe przedstawiciela każdego administratora, w imieniu którego działa Administrator Danych,
 - 4.4 gdy ma to zastosowanie, imię i nazwisko oraz dane kontaktowe IOD każdego administratora, w imieniu którego działa Administrator Danych,

- 4.5 kategorie przetwarzań dokonywanych w imieniu każdego z administratorów,
 - 4.6 gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń,
 - 4.7 ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.
- 5. Administrator Danych prowadzi i aktualizuje rejestry, o których mowa w pkt 2 w formie elektronicznej.
 - 6. Wyłączone z obowiązku prowadzenia rejestru są podmioty zatrudniające mniej niż 250 osób. Wyłączenie to nie ma zastosowania jeżeli przetwarzanie, którego dokonują:
 - a) może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego;
 - b) obejmuje szczególne dane wrażliwe, genetyczne lub biometryczne;
 - c) obejmuje dane osobowe dotyczące wyroków skazujących i naruszeń prawa.
 - 7. W przypadku zgłoszenia przez uprawniony organ nadzoru żądania w tym zakresie, Administrator Danych udostępnia mu prowadzone przez siebie rejestry.

3. DOPUSZCZENIE OSÓB DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator Danych realizując Politykę, w zakresie udostępniania danych osobowych w ramach własnej (wewnętrznej) struktury, zezwala na ich przetwarzanie w systemie informatycznym lub w wersji papierowej wyłącznie osobom, które uzyskały uprzednie, stosowne upoważnienie do przetwarzania danych osobowych.
2. Upoważnienie do przetwarzania danych osobowych nadawane jest po przeprowadzeniu szkolenia e-learningowego, stacjonarnego lub zaznajomieniu w innej formie, osoby upoważnianej z zasadami ochrony danych osobowych obowiązującymi w strukturze Administratora Danych, zgodnie z procedurą opisaną w załączniku nr 1.4 Polityki.
3. Upoważnienie do przetwarzania danych osobowych, nadawane jest indywidualnie.
4. Elementem upoważnienia jest oświadczenie o zachowaniu poufności.
5. Administrator Danych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, której wzór stanowi Załącznik nr 4.4. do Polityki.
6. Szczegółowa Procedura szkoleń oraz nadawania upoważnień do przetwarzania danych osobowych jest każdorazowo omawiana z IOD i dopasowywana do potrzeb Administratora Danych.

4. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator Danych realizując Politykę dopuszcza, by dane osobowe, których jest administratorem były przetwarzane poza własnymi strukturami organizacyjnymi. Może się to odbywać wyłącznie na drodze powierzenia danych, w określonym celu i zakresie, podmiotowi przetwarzającemu na mocy umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego.
2. Podstawowym warunkiem dopuszczalności powierzenia przetwarzania danych w imieniu administratora jest poddanie planowanego outsourcingu analizie, która powinna zapewnić, że wybór podmiotu przetwarzającego został uzależniony od zapewnienia wystarczających gwarancji ochrony danych.
3. Zawierana przez Administratora Danych umowa powierzenia przetwarzania danych osobowych (wzór umowy znajduje się w załączniku nr 2.6 do Polityki) musi być zgodna z postanowieniami art. 28 RODO tj. w szczególności określać:
 - 3.1. przedmiot powierzenia,
 - 3.2. czas trwania powierzenia,
 - 3.3. charakter i cel przetwarzania,
 - 3.4. rodzaj powierzanych danych osobowych,
 - 3.5. kategorie osób, których dane dotyczą,
 - 3.6. warunki podpowierzenia przetwarzania danych
 - 3.7. obowiązki i prawa Administratora Danych,
 - 3.8. obowiązki podmiotu przetwarzającego.
4. Umowa powierzenia może zostać zawarta w formie pisemnej, w tym elektronicznej.
5. W przypadku, gdy elementy powierzenia przetwarzania danych wskazane w pkt 3 znajdują się już w zawartej z danym podmiotem umowie, nie ma konieczności sporządzania dodatkowej umowy powierzenia przetwarzania danych osobowych.
6. Za zawieranie umów powierzenia przetwarzania danych osobowych odpowiadają pracownicy wyznaczeni przez Administratora Danych.
7. Pracownik wyznaczony przez Administratora Danych przed planowanym rozpoczęciem współpracy z podmiotem przetwarzającym, jest zobowiązany poinformować o tym IOD oraz skonsultować z nim postanowienia zawieranej umowy w zakresie powierzenia przetwarzania danych osobowych. Powierzenie przetwarzania danych może odbyć się wyłącznie na podstawie postanowień zaakceptowanych przez IOD.
8. Umowa powierzenia przetwarzania danych osobowych podpisywana jest zgodnie z zasadami reprezentacji Administratora Danych lub udzielonymi pełnomocnictwami.

9. Każdorazowe dokonanie powierzenia danych osobowych musi zostać obligatoryjnie odnotowane w rejestrze czynności przetwarzania danych osobowych.
10. Administrator Danych ma prawo kontroli podmiotów przetwarzających, którym powierzył przetwarzanie danych osobowych.
11. Administrator Danych w zakresie prowadzonej przez siebie działalności może przetwarzać również dane osobowe powierzone przez podmioty, na rzecz których świadczy usługi. Przyjęcie danych w powierzenie przez Administratora Danych musi zostać obligatoryjnie odnotowane w rejestrze kategorii czynności przetwarzania danych osobowych.
12. Administrator Danych dla celów dowodowych powinien prowadzić rejestr zawieranych umów powierzenia przetwarzania.

5. UDOSTĘPNIENIE DANYCH OSOBOWYCH

1. Udostępnienie danych osobowych może nastąpić tylko w oparciu o co najmniej jedną przesłankę spośród wskazanych w art. 6 RODO i / lub art. 9 RODO.
2. Każdorazowe udostępnienie danych których administratorem w rozumieniu RODO jest Miejska Strefa Kultury w Łodzi, powinno być skonsultowane z powołanym Inspektorem Ochrony Danych
3. Administrator Danych realizując Politykę dopuszcza, by dane osobowe, których jest administratorem były przekazywane innym administratorom w formie udostępnienia danych.

6. PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH

1. Przekazywanie danych, których administratorem jest Administrator Danych do państw trzecich i organizacji międzynarodowych, może się odbywać wyłącznie po spełnieniu warunków przewidzianych w Rozdziale V RODO.
2. Przekazywanie danych do państw trzecich może mieć formę zarówno powierzenia przetwarzania danych osobowych oraz udostępnienia danych osobowych, co oznacza, że w zależności od rodzaju przekazania, należy wziąć również pod uwagę postanowienia podrozdziałów 4 i 5 Polityki.
3. Przekazanie danych osobowych, których administratorem jest Administrator Danych do państwa trzeciego może nastąpić w sytuacji, jeżeli Komisja Europejska wydała decyzję, że dane państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Takie przekazanie nie wymaga specjalnego zezwolenia.
4. W przypadkach braku decyzji Komisji Europejskiej, o której mowa w pkt 3, dokonanie przekazania danych osobowych do państwa trzeciego jest możliwe, gdy Administrator Danych samodzielnie zapewni odpowiednie zabezpieczenia i pod warunkiem, że będą obowiązywały egzekwowalne prawa osób, których dane dotyczą i skuteczne środki ochrony prawnej. Odpowiednie zabezpieczenia Administrator Danych może zapewnić za pomocą:
 - 4.1. prawnie wiążącego i egzekwowalnego instrumentu między organami lub podmiotami publicznymi,
 - 4.2. wiążących reguł korporacyjnych zatwierdzonych przez organ nadzorczy, mających zastosowanie do każdego z członków grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą,
 - 4.3. standardowych klauzul ochrony danych przyjętych lub zatwierdzonych przez Komisję Europejską,
 - 4.4. standardowych klauzul ochrony danych przyjętych przez organ nadzorczy i zatwierdzonych przez Komisję Europejską,
 - 4.5. zatwierdzonego kodeksu postępowania wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą, lub
 - 4.6. zatwierdzonego mechanizmu certyfikacji wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą.
5. Z zastrzeżeniem zezwolenia właściwego organu nadzorczego odpowiednie zabezpieczenia, o których mowa w pkt 4 Administrator Danych może zapewnić w szczególności za pomocą:

- 5.1. klauzul umownych między Administratorem Danych lub podmiotem przetwarzającym a Administratorem Danych, podmiotem przetwarzającym lub odbiorcą danych osobowych w państwie trzecim lub organizacji międzynarodowej, lub
 - 5.2. postanowień uzgodnień administracyjnych między organami lub podmiotami publicznymi, w których przewidziane będą egzekwowlalne i skuteczne prawa osób, których dane dotyczą.
6. W szczególnych przypadkach, dopuszcza się przekazanie danych osobowych przez Administratora Danych do państwa trzeciego pomimo braku decyzji Komisji Europejskiej, o której mowa w pkt 3 oraz zapewnienia odpowiednich zabezpieczeń, o których mowa w pkt 4 i 5. Do tych szczególnych przypadków zalicza się przekazanie danych pod warunkiem, że:
- 6.1. osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którymi może się dla niej wiązać proponowane przekazanie, wyrazi na nie wyraźną zgodę,
 - 6.2. przekazanie jest niezbędne do wykonania umowy zawartej z osobą, której dane dotyczą,
 - 6.3. przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, której dane dotyczą,
 - 6.4. przekazanie jest niezbędne ze względu na ważne względy interesu publicznego,
 - 6.5. przekazanie jest niezbędne ze względu na posiadane roszczenia,
 - 6.6. przekazanie jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą lub
 - 6.7. przekazanie nastąpi z publicznego rejestru.
7. Administrator Danych przed planowanym przekazaniem danych do państwa trzeciego, jest zobowiązany poinformować o tym IOD oraz skonsultować z nim warunki przekazania tych danych. Przekazanie danych może odbyć się wyłącznie na podstawie warunków i postanowień zaakceptowanych przez IOD.

7. WSPÓŁADMINISTROWANIE DANYMI OSOBOWYMI

1. Administrator Danych w zakresie przetwarzanych przez siebie danych osobowych dopuszcza możliwość przyjęcia modelu współadministrowania danymi osobowymi zgodnie z art. 26 RODO.
2. Współadministrowanie danymi może zachodzić wówczas, jeżeli Administrator Danych oraz co najmniej jeden inny podmiot, wspólnie ustalają cele i sposoby przetwarzania danych osobowych. Oznacza to, że w danym procesie przetwarzania danych osobowych muszą zostać spełnione równocześnie trzy warunki, tj. Administrator Danych oraz co najmniej jeden inny podmiot muszą:
 - 2.1. być administratorami w rozumieniu art. 4 pkt 7 RODO,
 - 2.2. muszą wspólnie ustalić cele przetwarzania danych,
 - 2.3. muszą wspólnie ustalić sposoby (techniczne i organizacyjne) przetwarzania danych osobowych.
3. W przypadku spełnienia warunków, o których mowa w pkt 2 Administrator Danych oraz co najmniej jeden inny podmiot stają się współadministratorami danych w zakresie danego procesu przetwarzania danych osobowych.
4. W przypadku przyjęcia modelu współadministrowania danymi, współadministratorzy danych w drodze wspólnych uzgodnień, w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO.
5. W sytuacji, kiedy w zakresie zachodzących w strukturze Administratora Danych procesów przetwarzania danych osobowych pojawią się procesy, wobec których istnieje prawdopodobieństwo za współadministrowania danymi, Administrator Danych informuje o tym fakcie IOD.
6. IOD dokonuje oceny, czy dany proces przetwarzania spełnia warunki współadministrowania danymi.
7. W przypadku, kiedy wynik oceny, o której mowa w pkt 6 wskazuje na współadministrowanie danymi osobowymi, IOD, przy współudziale pozostałych współadministratorów, opracowuje wspólne uzgodnienia, o których mowa w pkt 4.
8. Przykładowy wzór umowy o współadministrowaniu danymi osobowymi znajduje się w załączniku nr 2.14 do Polityki

8. AUDYTY ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

1. Audyty zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz procedurami wdrożonymi w strukturze Administratora Danych przeprowadzane są przez IOD.
2. IOD przeprowadza audyt według opracowanego planu audytów (załącznik nr 3.1 do Polityki)
3. IOD przygotowuje plan audytów na okres nie dłuższy niż rok z zaznaczeniem, że plan musi obejmować co najmniej jeden audyt celowy rocznie.
4. Plan audytów IOD przygotowuje w formie elektronicznej i przedstawia Administratorowi Danych nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem.
5. W planie audytów IOD uwzględnia, w szczególności:
 - 5.1. przedmiot, zakres oraz termin przeprowadzenia poszczególnych audytów oraz sposób i zakres ich dokumentowania,
 - 5.2. procesy przetwarzania danych osobowych objęte audytem,
 - 5.3. konieczność weryfikacji zgodności przetwarzania danych osobowych z:
 - 5.3.1. zasadami przetwarzania danych osobowych,
 - 5.3.2. zasadami dotyczącymi zabezpieczenia danych osobowych,
 - 5.3.3. zasadami przekazywania danych osobowych.
6. W toku audytu IOD wykonuje i dokumentuje czynności, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania.
7. Po zakończeniu audytu, IOD przygotowuje dla Administratora Danych, sprawozdanie w tym zakresie. Sprawozdanie sporządzane jest w postaci elektronicznej albo w postaci papierowej.
8. IOD przekazuje Administratorowi Danych sprawozdanie nie później niż w terminie 30 dni od zakończenia audytu.
9. Sprawozdanie z audytu sporządzone w dwóch kopiach powinno być podpisane przez IOD i Administratora

9. REALIZACJA PRAW OSÓB, KTÓRYCH DANE DOTYCZĄ

1. Administrator Danych uwzględnia w zachodzących w jego strukturze procesach przetwarzania danych osobowych, procedury i zasady ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy przepisów RODO, w tym, w szczególności:
 - 1.1. prawo do wycofania wyrażonej zgody (art. 7 ust. 3 RODO),
 - 1.2. prawo dostępu przysługujące osobie, której dane dotyczą (art. 15 RODO),
 - 1.3. prawo do sprostowania danych (art. 16 RODO),
 - 1.4. prawo do usunięcia danych (*prawo do bycia zapomnianym*) (art. 17 RODO),
 - 1.5. prawo do ograniczenia przetwarzania (art. 18 RODO),
 - 1.6. prawo do przenoszenia danych (art. 20 RODO),
 - 1.7. prawo sprzeciwu (art. 21 RODO),
 - 1.8. prawo do niepodlegania decyzjom opartym na zautomatyzowanym przetwarzaniu (art. 22 RODO).
2. Procedura realizacji praw osób, których dane dotyczą stanowi załącznik nr 1.5. do Polityki.
3. Ewidencja realizacji praw osób, których dane dotyczą stanowi załącznik nr 4.2. do Polityki.
4. Raport z realizacji praw osób, których dane dotyczą stanowi załącznik nr. 2.9. do Polityki.
5. Prawa jednostki realizowane są także przy uwzględnieniu przepisów ustaw szczególnych.

10. OCHRONA DANYCH OSOBOWYCH W FAZIE PROJEKTOWANIA

1. Administrator Danych wdraża odpowiednie środki techniczne i organizacyjne, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, nadania przetwarzaniu danych niezbędnych zabezpieczeń oraz zapewnieniu ochrony praw osób, których dane dotyczą.
2. Wdrażając odpowiednie środki techniczne i organizacyjne Administrator Danych uwzględnia:
 - 2.1. stan wiedzy technicznej,
 - 2.2. koszt wdrażania,
 - 2.3. charakter, zakres, kontekst i cele przetwarzania danych,
 - 2.4. ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania.
 - 2.5. W uzasadnionych przypadkach przeprowadzona zostaje analiza ryzyka zgodnie z procedurą określoną w załączniku 3.3 do Polityki aby ocenić ryzyka określone w podpunkcie 2.4
3. Administrator Danych wdraża takie środki techniczne i organizacyjne, aby przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia określonego celu przetwarzania, biorąc pod uwagę: ilość zbieranych danych osobowych, ich zakres, okres ich przechowywania oraz ich dostępność dla innych osób.
4. W szczególności stosowane środki techniczne i organizacje muszą zapewnić, by dane osobowe nie były udostępniane nieokreślonej liczbie osób.
5. W pierwszej kolejności, Administrator Danych rozważa, czy cel jakiego ma służyć projektowane rozwiązanie jest możliwy do osiągnięcia bez konieczności przetwarzania danych osobowych. Jeśli tak, należy wybrać takie rozwiązanie.
6. Administrator Danych zapewnia, aby spełnienie warunków wskazanych w pkt 1-5 (tzw. zasady *privacy by design* i *privacy by default*) było odpowiednio udokumentowane np. w formie notatki, maila, raportu z przeprowadzonych testów systemu informatycznego, wydruku z ekranu systemu.
7. Ogólny opis organizacyjnych i technicznych środków bezpieczeństwa wdrożonych w strukturze Administratora Danych stanowi Załącznik nr 1.2 do Polityki.

11. OCENA SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH (DATA PROTECTION IMPACT ASSESSMENT)

1. W uzasadnionych przypadkach mogących powodować wysokie ryzyko naruszenia praw i wolności osób których dane dotyczą Administrator Danych dokonuje oceny skutków dla ochrony danych (DPIA – data protection impact assessment), w celu opisanego przetwarzania danych osobowych oraz oceny jego konieczności i proporcjonalności, a także w celu wspomaganego zarządzania ryzykiem naruszenia praw i wolności osób fizycznych wynikającym z przetwarzania ich danych osobowych kiedy jest to wymagane .
2. Wzór DPIA stanowi załącznik nr 3.2 do Polityki Ochrony Danych

12. INCYDENTY OCHRONY DANYCH OSOBOWYCH

1. Osobami odpowiedzialnymi za bezpieczeństwo danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do pomieszczeń oraz systemów, w których przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia incydentów ochrony danych osobowych, są: Administrator Danych, IOD oraz ASI (w odniesieniu do danych przetwarzanych w systemach informatycznych).
2. Procedura postępowania z incydentami ochrony danych osobowych stanowi Załącznik nr 1.3. do Polityki.
3. W przypadku zaistnienia incydentu, zgodnie z procedurą, IOD sporządza raport z naruszenia. Załącznik nr 2.8
4. Wszystkie incydenty niezależnie od tego czy pozostają sprawą wewnętrzną czy podlegają zgłoszeniu do Prezesa urzędu ochrony Danych, są odnotowywane w ewidencji naruszeń , prowadzonej przez Inspektora Ochrony Danych. Wzór ewidencji naruszeń stanowi załącznik nr 4.1 do Polityki

13. OGÓLNE ZASADY BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

1. Dostęp do danych osobowych mogą mieć tylko pracownicy posiadający upoważnienie do ich przetwarzania.
2. Przebywanie osób nieuprawnionych do przetwarzania danych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania, chyba, że dane te są w odpowiedni sposób zabezpieczone przed dostępem.
3. Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem, w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
4. Pracownicy przechowujący dane osobowe zobowiązani są do zabezpieczenia materiałów zawierających dane w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym.
5. Niedopuszczalnym jest wnoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.
6. Nikomu nie należy udostępniać indywidualnych haseł i identyfikatorów do systemów informatycznych.
7. Wysyłanie seryjnych wiadomości e-mail wymaga zastosowania opcji *kopia ukryta*.
8. Nie można udzielać informacji dotyczących danych osobowych innym podmiotom na podstawie prośby o takie dane skierowanej w formie zapytania telefonicznego.
9. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. *czystego biurka*, która oznacza niepozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników. Nie należy pozostawiać danych osobowych w miejscach ogólnodostępnych takich jak np. biurka, blaty, parapety.
10. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe odbywać się musi w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.
11. Za bezpieczeństwo przetwarzania danych osobowych indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do tego rodzaju danych.
12. W czasie chwilowej nieobecności pracowników w pomieszczeniach, w godzinach pracy jak i po zakończeniu pracy, są oni zobowiązani do zamykania na klucz szafek w których znajdują się dane osobowe lub/i pomieszczeń wchodzących w skład obszarów, w których przetwarzane są dane osobowe.

13. Klucze do pomieszczeń, w których przetwarzane są dane osobowe nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia kluczy przed udostępnieniem ich osobom nieupoważnionym.
14. Przed wyjściem z pomieszczenia, w którym przechowywane są dane osobowe należy upewnić się, że zostało ono odpowiednio zabezpieczone (zamknięte okna, drzwi).
15. Po zakończeniu pracy w systemie informatycznym, w którym przechowywane są dane osobowe, należy wylogować się z systemu.
16. Osoba użytkująca komputer przenośny zawierający dane osobowe zobowiązana jest do zachowania szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarzane są dane osobowe.
17. Na pracowniku pracującym zdalnie spoczywa obowiązek odpowiedniego zabezpieczenia danych tak, aby osoby trzecie nie miały dostępu do danych osobowych.
18. Dane osobowe przesyłane elektronicznie powinny być zabezpieczone hasłem. Hasło to powinno być wysyłane oddzielnym kanałem telekomunikacyjnym.

14. PRZEGLĄDY I AKTUALIZACJA POLITYKI OCHRONY DANYCH OSOBOWYCH

1. Polityka podlega okresowemu przeglądowi pod kątem jej adekwatności, nie rzadziej niż raz do roku.
2. Przeglądu Polityki dokonuje Inspektor Ochrony Danych
3. Przegląd powinien obejmować, w szczególności ocenę adekwatności Polityki do:
 - 3.1. procesów funkcjonujących w strukturach Administratora Danych,
 - 3.2. obowiązujących przepisów prawa odnoszących się do ochrony danych osobowych, którym podlega Administrator Danych.
4. W każdym przypadku, gdy zmianie ulegają przepisy prawa będące źródłem wskazanych w Polityce obowiązków lub zaistnieją istotne zmiany faktyczne w ramach struktury Administratora Danych przegląd Polityki wykonywany jest niezwłocznie.
5. Jeżeli w wyniku przeglądu Polityki stwierdzona zostanie konieczność aktualizacji jej zapisów, Inspektor Ochrony Danych rekomenduje dokonanie aktualizacji Polityki w wymaganym zakresie.

1. Opinie i procedury

- 1.1. Opinia w sprawie powołania Inspektora Ochrony Danych
- 1.2. Opis organizacyjnych i technicznych środków bezpieczeństwa wdrożonych w celu ochrony danych
- 1.3. Procedura postępowania z incydentami dotyczącymi ochrony danych
- 1.4. Procedura szkoleń oraz nadawania upoważnień do przetwarzania danych osobowych
- 1.5. Procedura realizacji praw osób których dane dotyczą
- 1.6. Instrukcja zarządzania systemami informatycznymi

2. Wzory dokumentów

- 2.1. Wzór powołania/zmiany IOD
- 2.2. Dokument potwierdzający powołania Inspektora Ochrony Danych
- 2.3. Oświadczenie o wyznaczeniu Administratora Systemów Informatycznych
- 2.4. Wzór upoważnienia do przetwarzania danych osobowych
- 2.5. Wzór oświadczenia o zapoznaniu się z Polityką Ochrony Danych Osobowych
- 2.6. Wzór umowy powierzenia przetwarzania
- 2.7. Wzór umowy poufności
- 2.8. Raport z naruszenia ochrony danych osobowych (raport z incydentu)
- 2.9. Raport z realizacji praw osób, których dane dotyczą
- 2.10. Klauzula informacyjna MSK (ogólna)
- 2.11. Klauzula informacyjna MSK (umowy)
- 2.12. Klauzula informacyjna MSK (zatrudnienie)
- 2.13. Klauzula monitoring wizyjny MSK
- 2.14. Wzór umowy w sprawie współadministrowania danymi

3. Dokumenty audytowe

- 3.1. Wzór harmonogramu audytów
- 3.2. Wzór oceny skutków dla ochrony danych (DPIA)
- 3.3. Wzór procedury dotyczącej analizy ryzyka

4. Ewidencje, rejestry, wykazy

- 4.1. Ewidencja naruszeń ochrony danych osobowych
- 4.2. Ewidencja realizacji praw osób których dane dotyczą
- 4.3. Ewidencja budynków i pomieszczeń, w których przetwarzane są dane osobowe
- 4.4. Ewidencja upoważnień MSK
- 4.5. Rejestr czynności przetwarzania danych osobowych
- 4.6. Rejestr kategorii czynności przetwarzania