ZARZĄDZENIE NR OR.0050.12.2019
Burmistrza Miasta Łaskarzew
z dnia 06 marca 2019 r.

w sprawie wprowadzenia Polityki Ochrony Danych.

Na podstawie art. 24 ust. 2 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), publ. Dz. Urz. UE L Nr 119, s. 1. zarządzam, co następuje:

§ 1

Wprowadza się Politykę Ochrony Danych stanowiącą załącznik nr 1 do niniejszego zarządzenia.

§ 2

Traci moc Zarządzenie Nr OR.0050.41.2016 Burmistrza Miasta Łaskarzew z dnia 30 września 2016 roku w sprawie wprowadzenia Polityki bezpieczeństwa informacji w Urzędzie Miasta Łaskarzew

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

Burmistrz Miasta Łaskarzew
Anna Laskowska

POLITYKA OCHRONY DANYCH OSOBOWYCH

Spis treści

1 Informacje wstępne

Polityka ochrony danych osobowych zwana dalej „Polityką" jest dokumentem wewnętrznym **Miasta Łaskarzew** opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań:

1. Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s. 1) - zwane dalej RODO,
2. Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000),
3. Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2017 poz. 2247),
4. Przepisy szczególne, regulujące funkcjonowanie jednostki,
5. Dobre praktyki w dziedzinie bezpieczeństwa informacji oraz ochrony danych osobowych.

Każda osoba mająca dostęp do danych osobowych zobowiązana jest zapoznać się z niniejszym dokumentem oraz potwierdzić ten fakt na wykazie, którego wzór stanowi **załącznik nr 1** do niniejszej Polityki -Wykaz osób zapoznanych z Polityką.

Polityka zawiera wartość normatywną w zakresie oceny zachowania osób zatrudnionych w jednostce oraz świadczących na jej rzecz pracę na podstawie innej, niż umowa o pracę, pod kątem realizacji obowiązków pracowniczych lub umownych oraz wyciągania na tym polu konsekwencji dyscyplinarnych oraz umownych.

2 Zakres stosowania Polityki

Polityka jest stosowana do danych osobowych przetwarzanych w systemach informatycznych oraz w postaci papierowej.

3 Deklaracja stosowania

Administrator ustanawia Politykę oraz deklaruje:

- podejmowanie wszystkich działań niezbędnych dla zapewnienia legalności przetwarzanych danych,
- stałe podnoszenie świadomości oraz kwalifikacji osób przetwarzających dane w zakresie problematyki bezpieczeństwa tychże danych,
- stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanym danym,
- dążenie do zapewnienia poufności, dostępności oraz integralności informacji chronionych w tym szczególnie danych osobowych.

4 Definicje

1. **Administrator** – Miasto Łaskarzew; ustala cele i sposoby przetwarzania danych osobowych,
2. **Inspektor Ochrony Danych /IOD/** - osoba, wyznaczona przez Administratora lub podmiot przetwarzający, posiadająca odpowiednie kwalifikacje zawodowe (wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności wymagane do wypełniania zadań związanych z ochroną tych danych,
3. **Dane osobowe** oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej,
4. **Dane szczególnych kategorii** oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej (w tym o korzystaniu z usług opieki zdrowotnej)ujawniające informacje o stanie jej zdrowia; dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne (przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej) oraz dane

dotyczące seksualności lub orientacji seksualnej osoby fizycznej,

5. **Kopia zapasowa** – kopia danych lub oprogramowania. Celem jej wykonania jest odtworzenia systemu po awarii,
6. **Naruszenie ochrony danych osobowych** oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych,
7. **Obsługa informatyczna-** osoba lub podmiot wyznaczony przez Administratora do realizacji zadań w zakresie zarządzania, bieżącego nadzoru nad systemami informatycznymi oraz serwisu sprzętu komputerowego,
8. **Odbiorca** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania,
9. **Ograniczenie przetwarzania** oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania,
10. **Podmiot przetwarzający** oznacza osobę fizyczną lub prawną, organ publiczny,
11. jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
12. **Polityka** oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.,
13. **Przetwarzanie** oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie 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,

14. **RODO** oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1),
15. **Użytkownik**- osoba posiadająca dostęp do systemu informatycznego przetwarzającego dane osobowe oraz dokumentacji papierowej,
16. **Zgoda** oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych,
17. **Zbiór danych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie (wedle art. 4 pkt. 6 RODO).

5 Podmioty odpowiedzialne za ochronę i przetwarzanie danych osobowych

5.1 Administrator

1. Wdraża odpowiednie środki techniczne i organizacyjne, mające na celu zabezpieczanie przetwarzanych danych oraz zapewnianie poufności, integralności i dostępności danych.
2. Wyznacza Inspektora Ochrony Danych, o czym zawiadamia Prezesa Urzędu Ochrony Danych Osobowych.
3. Podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia przetwarzanych danych zgodnie z procedurą stanowiącą integralną część niniejszej Polityki.
4. Upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie.
5. Podejmuje decyzje dotyczące przeprowadzenia oceny skutków planowanych operacji przetwarzania danych po konsultacji z Inspektorem Ochrony Danych.

6. Wdraża rejestr czynności przetwarzania danych osobowych.
7. Wdraża Politykę ochrony danych.

5.2 Inspektor Ochrony Danych /IOD/

1. Sprawuje nadzór nad przestrzeganiem przepisów o ochronie danych osobowych i informuje Administratora oraz wszystkie osoby przetwarzające dane o obowiązkach na nich spoczywających.
2. Prowadzi szkolenia z zakresu ochrony danych osobowych.
3. Aktualizuje i sprawuje nadzór nad dokumentacją z zakresu ochrony danych osobowych, tj. Polityką ochrony danych.
4. Opracowuje rejestr czynności przetwarzania danych i dokonuje jego bieżącej aktualizacji.
5. Współpracuje z Administratorem w zakresie oceny skutków planowanych operacji przetwarzania danych.
6. Pełni funkcję punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem danych osobowych.
7. Sprawuje nadzór nad naruszeniami ochrony danych osobowych.
8. Opiniuje wpływające wnioski pod kątem ochrony danych osobowych,
9. Sprawuje nadzór nad procesem wydawania upoważnień i uprawnień do przetwarzania danych osobowych oraz systemów informatycznych.
10. Prowadzi sprawy w zakresie udostępniania kopii przetwarzanych danych osobowych, udziela odpowiedzi na wniosek o cel, zakres, ujawnienie oraz okres przechowywania danych.
11. Realizuje procedury dotyczące: sprostowania/uzupełniania, usuwania, danych osobowych, przenoszenia oraz sprzeciwu w zakresie przetwarzania danych osobowych.
12. Opiniuje umowy powierzenia przetwarzania danych osobowych.

Administrator publikuje dane kontaktowe Inspektora Ochrony Danych i zawiadamia o nich organ nadzorczy, zgodnie z art. 37 ust. 7 RODO. Publikacja danych kontaktowych odbywa się w ten sposób, że Administrator udostępnia w sposób publicznie dostępny informacje o: imieniu i nazwisku Inspektora, numerze kontaktowym i/lub adresie e-mail,

zgodnie z art. 11 w zw. z art. 10 ust. 1 ustawy z dnia 10 maja 2018r. o ochronie danych osobowych (Dz. U. 2018, poz. 1000).

5.3 Obsługa informatyczna

1. Przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa lub wyłącza konta użytkowników zgodnie z zasadami określonymi w niniejszej Polityce.
2. Sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane chronione.
3. Podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.
4. Wykonuje kopie zapasowe danych lub oprogramowania.
5. Prowadzi inwentaryzację sprzętu komputerowego i oprogramowania.
6. W sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje Inspektora Ochrony Danych o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia.

5.4 Użytkownicy

Osoby upoważnione przez Administratora do przetwarzania danych osobowych, zobowiązane są do:

1) udziału w wewnętrznym szkoleniu dotyczącym ochrony danych osobowych,
2) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych,
3) stosowania określonych przez Administratora procedur i środków mających na celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, w szczególności:
   a) **polityki „czystego biurka”** - w trakcie pracy użytkownik powinien mieć na biurku tylko te materiały, które są niezbędne do wykonywania obowiązków służbowych. W przypadku opuszczenia stanowiska pracy materiały zawierające dane,

wymagające szczególnej ochrony powinny być zabezpieczone przed dostępem osób nieuprawnionych. Po zakończeniu dnia pracy każdy użytkownik zobowiązany jest do zabezpieczenia wszelkich dokumentów i nośników zawierających istotne dane, w celu uniemożliwienia dostępu do nich osób nieupoważnionych;

b) **polityki „czystego ekranu"** - w przypadku chwilowego opuszczenia stanowiska pracy użytkownik zobowiązany jest do wylogowania się z systemu bądź zablokowania dostępu do pulpitu stacji roboczej w celu uniemożliwienia dostępu do systemu operacyjnego lub aplikacji przez osoby niepowołane. Ponadto w trakcie pracy użytkownik powinien mieć otwarte tylko te aplikacje, które są niezbędne do wykonywania obowiązków służbowych;

c) bieżącego niszczenia w niszczarce niepotrzebnej dokumentacji papierowej oraz przechowywania pozostałej dokumentacji papierowej w szafach zamykanych na klucz;

d) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej;

e) zachowania w poufności wszelkich informacji w tym danych osobowych poprzez złożenie stosownego oświadczenia stanowiącego wzór zawarty w **załączniku nr 2** do niniejszej Polityki.

6 Podstawy przetwarzania danych osobowych

Przetwarzanie danych osobowych zwykłych dopuszczalne jest tylko wtedy, gdy zostanie spełniona jedna z przesłanek wynikających z art. 6 ust. 1 RODO, tj.:

1) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów,
2) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy,
3) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze,
4) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,

5) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

W przypadku przetwarzania danych osobowych na podstawie zgody osoby, której dane dotyczą, należy stosować oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych, którego wzór stanowi **załącznik nr 3** do niniejszej Polityki, natomiast **załącznik nr 4** stanowi wzór oświadczenia o cofnięciu zgody na przetwarzanie danych osobowych.

Z art. 9 ust. 2 RODO wynikają przesłanki legalizujące przetwarzanie danych dotyczących stanu zdrowia, tj.:

1) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach;
2) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem;
3) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
4) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;
5) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
6) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;

7) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, realizowanych na podstawie przepisów prawa, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;
8) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie przepisów prawa;
9) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;
10) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, na podstawie przepisów prawa, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

6.1 Obowiązek informacyjny przy przetwarzaniu danych

Obowiązek informacyjny spoczywający na Administratorze w myśl art. 13 RODO jest realizowany poprzez przekazanie osobie, której dane dotyczą informacji dotyczących pozyskiwania danych osobowych, a także ich dalszego przetwarzania.

Zwolnienie z realizacji obowiązku informacyjnego znajduje zastosowanie w sytuacji, gdy dane pozyskiwane są od osoby, której te dane dotyczą a podmiot ten dysponuje już informacjami, o których mowa w art. 13 RODO oraz w zakresie uregulowanym przez przepisy krajowe, w szczególności przez ustawę z dnia 10 maja 2018r. o ochronie danych osobowych.

Powyższy obowiązek należy spełnić w momencie zbierania danych.

Administrator realizuje obowiązek informacyjny w sposób uznany za najbardziej dogodny, poprzez wykorzystanie odpowiednich środków, które umożliwią w zwięzłej, przejrzystej i łatwo dostępnej formie udzielenie osobie, której dane dotyczą wszelkich informacji, o których mowa w art. 13 RODO.

Wzór klauzuli informacyjnej wynikającej z art. 13 RODO stanowi **załącznik nr 5** do niniejszej Polityki.

6.2 Prawa osób, których dane dotyczą

Osobie, której dane są przetwarzane, przysługuje:

1) prawo dostępu do danych, które realizowane jest na podstawie art. 15 RODO poprzez potwierdzenie faktu przetwarzania danych, z użyciem formy wykorzystanej przez osobę kierującą żądanie;
2) prawo do sprostowania danych, które realizowane jest na podstawie art. 16 RODO, w wyniku żądania osoby, której dane są przetwarzane (dotyczy przypadków przetwarzania danych nieprawidłowych, bądź też niekompletnych);
3) prawo do usunięcia danych, tzw. „prawo do bycia zapomnianym", które realizowane jest na podstawie przesłanek wynikających z art. 17 ust. 1 RODO i w trybie w tym przepisie określonym;
4) prawo do ograniczenia przetwarzania danych, które realizowane jest na podstawie przesłanek wynikających z art. 18 ust. 1 RODO;
5) prawo do przenoszenia danych tj. prawo do otrzymania w ustrukturyzowanym, powszechnie używanym formacie (nadającym się do odczytu maszynowego) danych osobowych jej dotyczących, które dostarczyła Administratorowi, jak również przesłanie tychże danych innemu Administratorowi, realizowane jest na podstawie przesłanek wynikających art. 20 RODO;
6) na podstawie art. 19 RODO Administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać

niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

Szczegółowe zasady realizowania w/w uprawnień opisane są w procedurach stanowiących **załączniki od 6 do 10** do niniejszej Polityki.

6.3 Procedura nadawania upoważnień do przetwarzania danych osobowych

Do przetwarzania danych osobowych mogą mieć dostęp osoby posiadające pisemne upoważnienia do przetwarzania danych osobowych.

1) Administrator przygotowuje upoważnienie do przetwarzania danych osobowych. wzór upoważnienia stanowi **załącznik nr 11** do niniejszej Polityki ochrony danych;
2) zatwierdzone przez Administratora upoważnienie do przetwarzania danych osobowych pracownik ds. kadr wpisuje do ewidencji nadanych upoważnień - stanowiącej **załącznik nr 12** do niniejszej Polityki;
3) w przypadku zmiany stanowiska, zakresu obowiązków lub w sytuacji, która wpływa bezpośrednio na rodzaj i zakres przetwarzanych danych osobowych, Administrator jest zobowiązany do przygotowania nowego upoważnienia lub jego aktualizacji – procedurę stosuje się odpowiednio.

7 Środki techniczne i organizacyjne zapewniające bezpieczeństwo przetwarzanych danych

Administrator, działając w oparciu o art. 24 ust. 1 i art. 32 ust. 1 RODO, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

Administrator wyznaczył osoby, które są upoważnione do otwierania drzwi wejściowych. Osoby, którym zostały powierzone klucze zobowiązani są do nieudostępniania kluczy osobom trzecim.

Klucze do poszczególnych pomieszczeń pracownicy pobierają i zdają po zakończonym dniu pracy do skrzynki znajdującej się Sekretariacie. Od momentu pobrania kluczy do momentu

ich zdania na użytkownikach spoczywa pełna odpowiedzialność za ich zabezpieczenie. Po otwarciu pomieszczeń biurowych, przed przystąpieniem do pracy, użytkownicy sprawdzają stan zastosowanych zabezpieczeń. W przypadku stwierdzenia nieprawidłowości należy postępować zgodnie z procedurą naruszeń stanowiącą **załącznik nr 16** do niniejszej Polityki.

Zabrania się pozostawiania kluczy do pomieszczeń obszaru przetwarzania danych w drzwiach lub w miejscach ogólnie dostępnych, pomieszczenia zamyka się na czas nieobecności wszystkich użytkowników w sposób uniemożliwiający dostęp osobom nieupoważnionym.

Użytkownicy po godzinach pracy jednostki mogą w nim przebywać jedynie za zgodą Administratora.

W przypadkach przebywania pracowników w pomieszczeniach obszaru przetwarzania danych po wyznaczonych godzinach pracy, godzinach pełnienia obowiązków, wykonywania zadań na rzecz Administratora należy upewnić się czy zamknięto drzwi wejściowe do obszaru przetwarzania danych osobowych. Dodatkowo opuszczając obszar przetwarzania danych należy sprawdzić czy zamknięto wszystkie okna oraz drzwi wejściowe do pomieszczeń.

Szczegółowe skatalogowanie środków technicznych opisane jest w **załączniku nr 13** do niniejszej Polityki.

8 Szkolenia z zakresu ochrony danych osobowych

Administrator lub osoba przez niego wyznaczona przeprowadza wewnętrzne szkolenia z zakresu ochrony danych osobowych dla osób mających dostęp do danych.

Szkolenia wewnętrzne powinny być przeprowadzane w przypadku każdej istotnej zmiany zasad lub przepisów dotyczących ochrony danych osobowych.

W przypadku przeprowadzenia szkolenia wskazane jest jego udokumentowanie i potwierdzenie uczestnictwa przez osoby biorące w nim udział.

9 Przetwarzanie danych osobowych przez podmioty trzecie

Administrator może przekazać podmiotowi trzeciemu przetwarzane przez siebie dane osobowe w ramach:

1) udostępnienia, jeżeli jest to przewidziane w powszechnie obowiązujących przepisach prawa,

2) powierzenia, jeżeli podmiot trzeci przetwarza dane w imieniu i na polecenie Administratora.

W sytuacji powierzenia przetwarzania danych konieczne jest zawarcie umowy powierzenia przetwarzania danych osobowych pomiędzy Administratorem oraz podmiotem przetwarzającym, który przetwarza dane w imieniu Administratora.

Szczegółowe zasady dotyczące zawierania umów powierzenia są uregulowane w art. 28 ust. 3 RODO.

Administrator przyjął minimalne wymagania co do umowy powierzenia przetwarzania danych stanowiące **załącznik nr 15** do Polityki.

Administrator prowadzi rejestr zawartych umów powierzenia według wzoru stanowiącego **załącznik nr 16** do Polityki.

10 Procedura zgłaszania naruszeń ochrony danych osobowych

Procedura zgłaszania naruszeń ochrony danych jest opisana w **załączniku nr 17** do niniejszej Polityki.

11 Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych

11.1 Procedura zarządzania uprawnieniami użytkowników w systemach informatycznych

1) Administrator nadaje uprawnienia użytkownikom do pracy w systemach informatycznych - **wzór wniosku stanowi załącznik nr 11 do** Polityki ochrony danych,
2) Administrator dokonuje modyfikacji, zmiany lub wyrejestrowania uprawnień użytkowników systemów informatycznych.
3) Administrator jednostki przeprowadza okresową kontrolę uprawnień i kont użytkowników co najmniej raz na rok w celu weryfikacji czy użytkownicy posiadają uprawnienia adekwatne do wykonywanej pracy w systemach informatycznych.
4) z przeprowadzonej kontroli ww. osoba sporządza notatkę służbową wg wzoru stanowiącego **załącznik nr 18** do niniejszej Polityki.

11.2 Procedura dostępu do systemów informatycznych

1) w przypadku dostępu użytkowników do systemów informatycznych (dziedzinowych i operacyjnych) należy stosować metodę uwierzytelnienia poprzez wpisanie indywidualnego identyfikatora/ login'u oraz hasła;
2) identyfikator jest przydzielany wg zasady przyjętej w jednostce (np. pierwsza litera imienia i nazwisko). W identyfikatorze należy pomijać polskie znaki diakrytyczne,
3) w przypadku dublowania się identyfikatorów powinien być on rozszerzany o kolejne litery lub cyfry;
4) hasło powinno składać się z unikalnego zestawu znaków, zawierających małe i wielkie litery, cyfry oraz znaki specjalne. Hasła powinny być regularnie zmieniane przez użytkowników oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione osobie nieuprawnionej;
5) użytkownik zobowiązany jest do zachowania hasła w poufności i niezapisywania haseł w sposób jawny;
6) hasła administracyjne do urządzeń i systemów informatycznych w tym baz danych winny być przechowywane w miejscu wskazanym przez Administratora.

11.3 Procedura wykonywania kopii bezpieczeństwa

1) w celu zwiększenia poziomu bezpieczeństwa oraz zapewnienia ciągłości działania jednostki tworzy się kopie zapasowe danych;
2) za sporządzenie kopi zapasowych odpowiedzialna jest obsługa informatyczna jednostki;
3) kopią zapasową objęte są: systemy informatyczne mające wpływ w szczególności na zachowanie ciągłości działania, w których gromadzone są dane istotne dla Administratora.
   Do archiwizacji służy dedykowana aplikacja FerroBackupSystem 4.8 zainstalowana na serwerze znajdującym się w serwerowni. Archiwizacja wykonywana jest od poniedziałku do piątku w 2 trybach:
   1. Bazy danych aplikacji w trybie pełnym po godzinach pracy jednostki
   2. Pliki użytkowników ok. 2 razy w tygodniu w trybie przyrostowym (co 30 dni wykonywana jest archiwizacja pełna) – w trakcie pracy.

   Dostępnych jest 5 ostatnich kopii baz danych i 2 ostatnie kopie plików użytkowników. Od Poniedziałku do Piątku wykonywana jest replikacja kopii na oddzielny serwer który również znajduje się w serwerowni.
4) użytkownicy we własnym zakresie odpowiadają za sporządzanie kopii zapasowych

dokumentów znajdujących się na lokalnych dyskach twardych;

5) po wykonaniu kopii zapasowej zaleca się ich weryfikację poprzez dokonanie próby odtworzeniowej.

11.4 Procedura zarządzania sprzętem elektronicznym i oprogramowaniem

1. Użytkownik zobowiązany jest korzystać ze sprzętu elektronicznego w sposób zgodny z jego przeznaczeniem i chronić go przed jakimkolwiek zniszczeniem lub uszkodzeniem.
2. Użytkownik ma obowiązek niezwłocznie zgłosić utratę lub zniszczenie powierzonego sprzętu Administratorowi.
3. Użytkownik nie może bez zgody Administratora instalować dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączać niezatwierdzonych urządzeń do systemu informatycznego.
4. Użytkownik nie może bez zgody Administratora korzystać z prywatnego sprzętu elektronicznego (np. laptopów, telefonów, aparatów fotograficznych, nośników typu pendrive) do wykonywania zadań służbowych.
5. Administrator ma prawo do monitorowania sprzętu służbowego wykorzystywanego przez użytkowników, regulacje w tym zakresie wynikają z ustawy o ochronie danych osobowych z 10 maja 2018 roku Dz.U. z 2018 r. poz. 1000). O fakcie monitorowania Administrator zobowiązany jest powiadomić użytkowników, nie później niż 14 dni przed jego uruchomieniem. **Załącznik nr 19** stanowi wzór oświadczenia o monitorowaniu sprzętu komputerowego, na którym pracują użytkownicy.
6. Użytkownik zobowiązany jest do korzystania wyłącznie z oprogramowania dopuszczonego do stosowania w jednostce.
7. Użytkownik nie może instalować ani używać oprogramowania innego, niż przekazane lub udostępnione przez Administratora.

11.5 Procedura korzystania z poczty elektronicznej

1. Użytkownik jest zobowiązany do korzystania z przyznanego mu adresu mailowego wyłącznie w celu prowadzenia korespondencji służbowej.
2. Użytkownik nie może używać służbowego adresu mailowego do celów prywatnych,

w szczególności do rejestracji na portalach społecznościowych, dokonywania zakupów w sklepach internetowych.

3. Użytkownik nie może używać służbowego adresu mailowego w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
4. Użytkownik powinien zachować szczególną ostrożność przy wpisywaniu adresu odbiorcy wiadomości.
5. Użytkownik podczas wysyłania maili do wielu adresatów jednocześnie, powinien użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości".
6. Użytkownik podczas przesyłania danych osobowych pocztą elektroniczną powinien zawrzeć prośbę o potwierdzenie zapoznania się z informacją przez adresata.
7. Użytkownik powinien zastosować zabezpieczenia kryptograficzne przy przesyłaniu załączników do wiadomości. Zabezpieczenia kryptograficzne mogą polegać na przesłaniu za hasłowanych plików w formie załącznika, niemniej hasło powinno być przekazane adresatowi sms bądź podczas rozmowy telefonicznej po uprzednim zweryfikowaniu tożsamości adresata.
8. Użytkownik powinien zachować szczególną ostrożność podczas odbierania poczty elektronicznej, a w szczególności nie powinien otwierać plików i linków w niej zawartych, ani otwierać załączników, jeżeli nie ma pewności co do autentyczności adresata wiadomości. Tego typu maile większości przypadków mogą zawierać załączniki ze szkodliwym kodem, które po „kliknięciu" infekują komputer użytkownika oraz może istnieć realne ryzyko zaimplementowania kodu w pozostałych komputerach sieci wewnętrznej jednostki.
9. W wyniku działania takiego szkodliwego oprogramowania może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowaniem przez kryptowirusy. W takim przypadku użytkownik powinien poinformować o zdarzeniu Administratora.
10. Użytkownik powinien regularnie usuwać niepotrzebne wiadomości pocztowe i opróżniać folder elementów usuniętych.

Administrator jako pracodawca w świetle art. 22^3 § 1 ustawy z dnia 26 czerwca 1974r. - Kodeks pracy (Dz. U. z 2018 r. poz. 917) może wprowadzić kontrolę służbowej poczty elektronicznej pracownika, jeżeli jest to niezbędne do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych użytkownikowi narzędzi pracy.

W przypadku rozwiązania stosunku pracy z użytkownikiem, osoba wyznaczona przez Administrator zobowiązana jest zablokować konto poczty i usunąć dane.

11.6 Procedura korzystania z Internetu

1. Użytkownik powinien korzystać z dostęp do sieci Internetu wyłącznie w celach niezbędnych do wykonywania zadań służbowych.
2. Użytkownik nie powinien otwierać stron zawierających treści nie związanych bezpośrednio z merytoryką pracy, ze względu na możliwość przypadkowego pobrania złośliwego kodu, który może automatycznie zainfekować system operacyjny komputera.
3. Użytkownik ponosi pełną odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu,
4. Użytkownik nie może korzystać ze stron, na których prezentowane są treści o charakterze przestępczym, hackerskim, pornograficznym lub innym zakazanym przez prawo (na większości stron tego typu może być zaimplementowany złośliwy kod, który może automatycznie zainfekować system operacyjny komputera w sposób niewidoczny dla użytkownika.).
5. Użytkownik nie może oglądać/słuchać materiałów multimedialnych zawartych w Internecie, co może w znacznym stopniu wysycić łącze internetowe i uniemożliwić pracę innym użytkownikom.
6. Użytkownik nie może pobierać aplikacji z sieci Internet bez wcześniejszej zgody Administratora.
7. Użytkownik w przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, powinien zwrócić uwagę na pojawienie się odpowiedniej ikony (kłódka) oraz adresu www rozpoczynającego się frazą "https:". Dla pewności należy „kliknąć" na ikonkę

kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.

8. Użytkownik powinien zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet.

11.7 Procedura korzystania z bankowości elektronicznej

1. Użytkownik, który wykonuje przelewy bankowe zobowiązany jest do regularnej zmiany hasła oraz nieprzechowywania go w formie pisemnej wraz z loginem.
2. Użytkownik nie może opuścić stanowiska pracy bez wylogowania się i zamknięcia przeglądarki.
3. Użytkownik logujący się do bankowości elektronicznej nie powinien korzystać z nieznanych sieci bezprzewodowych.
4. W celu zalogowania się do systemu bankowości elektronicznej użytkownik nie powinien wchodzić na stronę internetową banku za pośrednictwem linków znajdujących się w korespondencji elektronicznej.

11.8 Procedura pracy na odległość i mobilnego przetwarzania danych

Administrator dopuszcza możliwość pracy zdalnej pod warunkiem stosowania się do poniższych zasad bezpieczeństwa.

1. Komunikacja z zewnętrz powinna być realizowana tylko poprzez mechanizmy zapewniające odpowiednie bezpieczeństwo (np. VPN, Team Viewer).W przypadku firm zewnętrznych dokonujących czynności serwisowych (np. aktualizacja oprogramowania dziedzinowego) dostęp taki jest nadzorowany przez obsługę informatyczną oraz każdorazowo powinien być poprzedzony autoryzacją (np. podaniem hasła do Team Viewer, które wygasa po skończonej sesji).
2. Administrator wprowadza obowiązek logowania połączeń wykonywanych za pomocą sieci bezprzewodowej w celu rejestracji działań użytkowników w sieci i zmniejszenia ryzyka użytkowania sieci niezgodnie z przeznaczeniem.
3. Komunikację należy prowadzić tylko za pomocą bezpiecznych metod transmisji, w tym włączenie transmisji szyfrowanej lub przeniesienie usług sieciowych na serwer

posiadający taką możliwość.

4. Administrator dopuszcza możliwość pracy z urządzeń mobilnych wyłącznie z urządzeń przeznaczonych do użytku służbowego.
5. Urządzenia mobilne służące do łączenia się systemami i sieciami zarządzanymi przez Administratora muszą być zgłoszone do obsługi informatycznej, celem zabezpieczenia ich odpowiednimi środkami uwierzytelniania, jakimi jak np. PIN-y, do zainstalowania odpowiedniego oprogramowania antywirusowego, zaszyfrowania.
6. Obsługa informatyczna prowadzi ewidencję udostępnionych urządzeń mobilnych.
7. Administrator zabrania wykorzystywania służbowych urządzeń mobilnych do celów prywatnych oraz udostępniania ich osobom trzecim, jak również instalowania aplikacji, które nie są niezbędne do wykonywania obowiązków danego pracownika.
8. Administrator zabrania korzystania z publicznych sieci WIFI oraz pozostawiać urządzenia bez nadzoru pracownika, w szczególności w miejscach ogólnodostępnych dla szerokiego grona osób trzecich.

Jeżeli użytkownicy korzystają ze służbowych urządzeń mobilnych poza miejscem pracy, zobowiązani są do przestrzegania poniższych zasad bezpiecznego korzystania z urządzeń mobilnych:

1) Nie wolno pozostawiać zostawiać urządzenia bez opieki i nigdy nie wolno go pożyczać osobie trzeciej.
2) Należy używać kodu blokady otrzymanego od Administratora znanego wyłącznie osobie, która dysponuje urządzeniem.
3) Należy na bieżąco (lub z ustalonym przez obsługę informatyczną harmonogramem) zgłaszać się do obsługi informatycznej w celu wykonania aktualizacji systemu oraz aplikacji zainstalowanych w urządzeniu.
4) Jeżeli urządzenie posiada Wi-Fi lub Bluetooth, należy je wyłączać, jeśli nie są w danym czasie wykorzystywane.
5) Nie wolno łączyć się z nieznanymi sieciami bezprzewodowymi.
6) Nie wolno otwierać nieznanych linków lub załączników i nie należy akceptować nieoczekiwanych instalacji aplikacji i/lub wtyczek – o fakcie zaistnienia takich

okoliczności należy każdorazowo poinformować Informatyka.

7) Potrzebne do pracy aplikacje należy pobierać tylko ze znanych i zaufanych źródeł.
8) Z siecią firmową należy łączyć się tylko za pośrednictwem urządzeń zaakceptowanych przez Administratora.
9) Należy zawsze używać rozwiązań posiadających silne mechanizmy szyfrowania transmisji i ochrony danych.

12 Procedura postępowania z dokumentami papierowymi zawierającymi dane osobowe

1. W stosunku do dokumentów papierowych stanowiących wydruki z systemu obowiązują następujące środki ostrożności:
   a) wydruki i dokumentacja powinny być niedostępne dla osób postronnych,
   b) nie mogą być pozostawione w drukarce ogólnodostępnej,
   c) wydruki niepotrzebne i nieprzydatne powinny być na bieżąco niszczone za pomocą niszczarki,
   d) dokumenty, których nie można zniszczyć z przyczyn technicznych lub formalnych, powinny być składowane w miejscu z ograniczonym dostępem, systematycznie weryfikowane, a następnie archiwizowane zgodnie z obowiązującymi w tym zakresie przepisami.

13 Procedura zabezpieczania sprzętu elektronicznego i systemu informatycznego

1. Komputery stacjonarne i przenośne powinny być zabezpieczone programem antywirusowym, który sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu.
2. Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie powinno odbywać się przy wykorzystaniu ww. oprogramowania zainstalowanego na stacjach roboczych oraz komputerach przenośnych.
3. Obowiązkiem obsługi informatycznej jest nadzór nad aktualizacją oprogramowania antywirusowego.
4. Użytkownik jest obowiązany każdorazowo zawiadomić obsługę informatyczną o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem – wirusa lub w przypadku sygnalizowanych problemów z działaniem oprogramowania antywirusowego.

5. Użytkownik, który posiada dostęp do systemów informatycznym powinien mieć zablokowaną możliwość instalowania nieautoryzowanego oprogramowania.

13.1 Procedura korzystania z elektronicznych nośników danych oraz komputerów przenośnych

1. Użytkownik może korzystać wyłącznie z elektronicznych nośników danych w szczególności pendriv-y, dysków zewnętrznych, CD-R, DVD oraz komputerów przenośnych przeznaczonych do użytku służbowego.
2. Użytkownik korzystający z elektronicznych nośników danych oraz komputerów przenośnych jest w całym okresie użytkowania odpowiedzialna za bezpieczeństwo danych i oprogramowania na nim zainstalowanego.
3. Użytkownik korzystający z ww. urządzeń zobowiązany jest do:
   a) przechowywania danych na dysku szyfrowanym zabezpieczonym hasłem,
   b) transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia oraz stosownego zabezpieczenia komputera przed uszkodzeniem,
   c) zdecydowanego i skutecznego uniemożliwienia korzystania z komputera osobom nieuprawnionym (np. rodzinie, dzieciom, znajomym).

Obsługa informatyczna jest odpowiedzialna za prowadzenie inwentaryzacji sprzętu elektronicznego i oprogramowania oraz utrzymywanie jej w aktualności.

13.2 Procedura wykonywania przeglądów i konserwacji sprzętu elektronicznego i nośników danych

1. Obsługa informatyczna dokonuje przeglądu i konserwacji sprzętu elektronicznego i nośników danych.
2. Użytkownik nie może samodzielne dokonywać napraw sprzętu elektronicznego, wymiany jego podzespołów oraz wykonywanie innych czynności nie związanych bezpośrednio z jego eksploatacją lub nie dopuszczonych do wykonywania przez producenta sprzętu w instrukcji obsługi.
3. Użytkownik ma obowiązek niezwłocznie powiadomić obsługę informatyczną o wszelkich nieprawidłowościach i awariach sprzętu informatycznego, mogących

prowadzić do próby naruszenia lub naruszenia bezpieczeństwa danych osobowych.

4. W przypadku awarii systemu informatycznego i utraty informacji lub w przypadku zaistnienia możliwości uszkodzenia informacji obsługa informatyczna jest zobowiązana do:

a) przetestowania sieci informatycznej, systemu informatycznego oraz aplikacji służącej do przetwarzania danych,

b) ocenić zasadność odtworzenia danych przy wykorzystaniu aktualnej kopii zapasowej lub kilku kopii zapasowych, a w przypadku uzasadnionej konieczności odtworzyć dane przy wykorzystaniu aktualnej kopii zapasowej lub kilku kopii zapasowych.

13.3 Procedura utylizacji i serwisu sprzętu elektronicznego

1. W przypadku wycofania sprzętu elektronicznego z użycia, dane osobowe na nim zapisane powinny być kasowane przy użyciu dedykowanego oprogramowania do bezpiecznego usuwania danych, najlepiej za pomocą certyfikowanego urządzenia np.: demagnetyzera.
2. W przypadku braku możliwości programowego usunięcia danych ze sprzętu elektronicznego podlega on fizycznemu zniszczeniu.
3. Zniszczenie sprzętu elektronicznego powinno być potwierdzane protokołem zniszczenia.
4. W przypadku przekazywania stacji roboczej z dyskiem albo innych nośników danych do naprawy, dysk lub nośnik powinien zostać zdemontowany lub pozbawiany danych, naprawa powinna być dokonywana w obecności osoby upoważnionej przez Administratora lub powinna zostać zawarta umowa powierzenia przetwarzania danych.

14 Procedura zarządzania ryzykiem

1. Administrator analizuje możliwe sytuacje i naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia,
2. Administrator przeprowadza analizy ryzyka naruszenia praw lub wolności osób

fizycznych dla czynności przetwarzania danych lub ich kategorii,

3. Analiza ryzyka powinna zapewniać:
   a) zidentyfikowanie ryzyka,
   b) oszacowanie ryzyka z punktu widzenia następstw dla działalności oraz prawdopodobieństwa wystąpienia,
   c) informowanie o prawdopodobieństwie i następstwach ryzyka oraz zrozumienie tych informacji,
   d) ustanowienie priorytetów postępowania z ryzykiem,
   e) regularne monitorowanie i przegląd różnych typów ryzyka oraz procesu zarządzania ryzykiem,
   f) zbieranie informacji w celu doskonalenia podejścia do zarządzania ryzykiem.
4. Administrator dokumentuje wykonaną analizę ryzyka.
5. Administrator dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych tam, gdzie zgodnie z analizą ryzyka ryzyko naruszenia praw i wolności osób jest wysokie.

15 Audyt wewnętrzny w zakresie bezpieczeństwa informacji

Podmioty realizujące zadania publiczne zobowiązane są do przeprowadzenia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji nie rzadziej niż raz na rok, zgodnie z § 20 ust. 2 pkt 14 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, bowiem utrzymywanie wysokiego poziomu bezpieczeństwa informacji, wymaga stałego monitorowania i okresowego badania stanu zabezpieczenia wszystkich elementów tego systemu.

16 Aktualizacja Polityki

Niniejsza polityka podlega regularnym (nie rzadziej niż raz na rok) przeglądom dokonywanym przez Inspektora Ochrony Danych. W zależności od potrzeb mogą zostać przeprowadzone przez niego także dodatkowe przeglądy po stwierdzeniu istotnego naruszenia

bezpieczeństwa, pojawieniu się zasadniczych zmian w jednostce, jego strukturze lub jego otoczeniu (nowe zagrożenia, technologie).

17 Wykaz załączników

Nr 1- Wykaz osób zapoznanych z Polityką ochrony danych osobowych,

Nr 2-Wzór oświadczenia o zachowaniu w poufności danych,

Nr 3-Wzór oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych,

Nr 4- Wzór odwołania zgody na przetwarzanie danych osobowych,

Nr 5- Wzór klauzuli informacyjnej,

Nr 6- Procedura prawo dostępu do danych,

Nr 7- Procedura prawo do sprostowania danych do danych,

Nr 8- Procedura prawo do bycia zapomnianym,

Nr 9- Procedura prawo do przenoszenia danych,

Nr 10- Procedura prawo do sprzeciwu,

Nr 11- Wzór wniosku o nadanie upoważnienia do przetwarzania danych osobowych/ uprawnienia do pracy w systemie informatycznym,

Nr 12- Wzór upoważnienia do przetwarzania danych osobowych,

Nr 13- Wzór ewidencji osób upoważnionych do przetwarzania danych,

Nr 14- Opis środków technicznych stosowanych do zabezpieczania danych,

Nr 15- Wzór umowy powierzenia,

Nr 16- Wzór rejestru umów powierzenia przetwarzania danych osobowych,

Nr 17- Procedura zgłaszania naruszeń ochrony danych osobowych,

Nr 18- Wzór notatki z kontroli uprawnień,

Nr 19- Oświadczenie o monitorowaniu komputerów służbowych.

Zał. nr 1 do Polityki ochrony danych	**Wykaz osób zapoznanych z Polityką ochrony danych osobowych**

Lp.	**Imię i nazwisko pracownika**	**Podpis**
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		
21.		
22.		
23.		
24.		

Zał. nr 2 do Polityki ochrony danych	**Wzór oświadczenia o zachowaniu w poufności danych**

_____, _____

(miejscowość) (data)

Ja niżej podpisany/podpisana* ..... zobowiązuję się do zachowania w tajemnicy danych osobowych, do których mam lub będę miała/miał* dostęp w związku z wykonywaniem przeze mnie zadań służbowych i obowiązków pracowniczych, zarówno w trakcie obowiązującego stosunku pracy, jak i bezterminowo po ustaniu zatrudnienia.

Ponadto oświadczam, że zostałem/zostałam* zapoznany/zapoznana* z przepisami dotyczącymi ochrony danych osobowych, w szczególności 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) oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000 z późn. zm.).

_____

(czytelny podpis, data)

* - niepotrzebne skreślić

Zał. nr 3 do Polityki ochrony danych	**Wzór oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych**

_____, _____

(miejscowość) (data)

Wyrażam zgodę na przetwarzanie moich danych osobowych w celach .....zgodnie z art. 6 ust. 1 lit a) Rozporządzeniem 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 (publ. Dz. Urz. UE L Nr 119, s. 1).

_____

(czytelny podpis, data)

1. Administratorem Pani/Pana danych osobowych jest .....
2. W sprawach z zakresu ochrony danych osobowych mogą Państwo kontaktować się z Inspektorem Ochrony Danych pod adresem e-mail: **inspektor@cbi24.pl.**
3. Dane osobowe będą przetwarzane ww. celu.
4. Dane osobowe będą przetwarzane do czasu cofnięcia zgody na przetwarzanie danych osobowych.
5. Podstawą prawną przetwarzania danych jest art. 6 ust. 1 lit. a) ww. Rozporządzenia.
6. Odbiorcami Pani/Pana danych będą podmioty, które na podstawie zawartych umów przetwarzają dane osobowe w imieniu Administratora.
7. Osoba, której dane dotyczą ma prawo do:

a. żądania dostępu do danych osobowych oraz ich sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych,
b. cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
c. wniesienia skargi do organu nadzorczego w przypadku gdy przetwarzanie danych odbywa się z naruszeniem przepisów powyższego rozporządzenia tj. Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa,

Ponadto informujemy, iż w związku z przetwarzaniem Pani/Pana danych osobowych nie podlega Pan/Pani decyzjom, które się opierają wyłącznie na zautomatyzowanym

przetwarzaniu, w tym profilowaniu, o czym stanowi art. 22 ogólnego rozporządzenia o ochronie danych osobowych.

Zał. nr 4 do Polityki ochrony danych	**Wzór oświadczenia o cofnięciu zgody na przetwarzanie danych osobowych**

_____ , _____

(miejscowość) (data)

Oświadczenie

o cofnięciu zgody na przetwarzanie danych osobowych

Na mocy przysługującego mi uprawnienia, wynikającego z art. 7 ust. 3 zd. 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; tzw. „RODO"), dobrowolnie cofam wyrażoną przeze mnie zgodę na przetwarzanie danych osobowych w postaci _____, w celach: _____, przetwarzanych przez: _____.

_____

(czytelny podpis, data)

Zał.nr 5 do Polityki ochrony danych	**Wzór obowiązku informacyjnego z art. 13**

Obowiązek informacyjny stosowany w przypadku gdy podstawa prawną przetwarzania jest przepis prawa

Zgodnie z art. 13 ust. 1 i ust. 2 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) ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. informuję, iż:

1. Administratorem Pani/Pana danych osobowych jest .....
2. W sprawach z zakresu ochrony danych osobowych mogą Państwo kontaktować się z Inspektorem Ochrony Danych pod adresem e-mail: inspektor@cbi24.pl.
3. Dane osobowe będą przetwarzane w celu realizacji obowiązków prawnych ciążących na Administratorze.
4. Dane osobowe będą przetwarzane przez okres niezbędny do realizacji ww. celu z uwzględnieniem okresów przechowywania określonych w przepisach odrębnych, w tym przepisów archiwalnych.
5. Podstawą prawną przetwarzania danych jest art. 6 ust. 1 lit. c) ww. Rozporządzenia.
6. Odbiorcami Pani/Pana danych będą podmioty, które na podstawie zawartych umów przetwarzają dane osobowe w imieniu Administratora.
7. Osoba, której dane dotyczą ma prawo do:

a. dostępu do treści swoich danych oraz możliwości ich poprawiania, sprostowania, ograniczenia przetwarzania, a także - w przypadkach przewidzianych prawem - prawo do usunięcia danych i prawo do wniesienia sprzeciwu wobec przetwarzania Państwa danych.
b. wniesienia skargi do organu nadzorczego w przypadku gdy przetwarzanie danych odbywa sięz naruszeniem przepisów powyższego rozporządzenia tj. Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

Ponadto informujemy, iż w związku z przetwarzaniem Pani/Pana danych osobowych nie podlega Pan/Pani decyzjom, które się opierają wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, o czym stanowi art. 22 ogólnego rozporządzenia o ochronie danych osobowych.

Zał.nr 5 do Polityki ochrony danych	**Wzór obowiązku informacyjnego z art. 13**

Obowiązek informacyjny stosowany w przypadku gdy podstawa prawną przetwarzania jest umowa

Zgodnie z art. 13 ust. 1 i ust. 2 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) ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. informuję, iż:

1. Administratorem Pani/Pana danych osobowych jest
   .....
2. W sprawach z zakresu ochrony danych osobowych mogą Państwo kontaktować się z Inspektorem Ochrony Danych pod adresem e-mail: inspektor@cbi24.pl.
3. Dane osobowe będą przetwarzane w celu realizacji umowy cywilnoprawnej.
4. Dane osobowe będą przetwarzane przez okres niezbędny do realizacji ww. celu z uwzględnieniem okresów przechowywania określonych w przepisach odrębnych, w tym przepisów archiwalnych.
5. Podstawą prawną przetwarzania danych jest art. 6 ust. 1 lit. b) ww. rozporządzenia.
6. Odbiorcami Pani/Pana danych będą podmioty, które na podstawie zawartych umów przetwarzają dane osobowe w imieniu Administratora.
7. Osoba, której dane dotyczą ma prawo do:

a. dostępu do treści swoich danych oraz możliwości ich poprawiania, sprostowania, ograniczenia przetwarzania oraz do przenoszenia swoich danych, a także - w przypadkach przewidzianych prawem - prawo do usunięcia danych i prawo do wniesienia sprzeciwu wobec przetwarzania Państwa danych.
b. wniesienia skargi do organu nadzorczego w przypadku gdy przetwarzanie danych odbywa się z naruszeniem przepisów powyższego rozporządzenia tj. Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa

Podanie danych osobowych jest warunkiem zawarcia umowy cywilnoprawnej. Konsekwencją niepodania danych osobowych jest brak możliwości zawarcia umowy.

Ponadto informujemy, iż w związku z przetwarzaniem Pani/Pana danych osobowych nie podlega Pan/Pani decyzjom, które się opierają wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, o czym stanowi art. 22 ogólnego rozporządzenia o ochronie danych osobowych.

Zał. nr 6 do Polityki ochrony danych	**Procedura realizacji uprawnienia do danych osobowych, o którym mowa w art. 15 RODO**

I. Cel ustanowienia procedury

Celem procedury jest realizacja prawa dostępu do danych przez osobę fizyczną w oparciu o art. 15 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; tzw. ogólne rozporządzenie o ochronie danych).

II. Unormowania ogólne

Osoba fizyczna posiada uprawnienie do potwierdzenia od Administratora faktu, czy dane jej dotyczącej są przez niego (przez nią) przetwarzane oraz dostępu do tych danych. W miarę możliwości Administrator powinien umożliwić udzielenie zdalnego dostępu do bezpiecznego systemu, który zapewni osobie, której dane dotyczą, bezpośredni dostęp do jej danych osobowych.

Administrator zobowiązany jest do udzielenia osobie, której dane dotyczą, informacji dotyczących:

1. celu przetwarzania,
2. kategorii odnośnych danych osobowych,
3. odbiorców lub kategorii odbiorców, którym dane osobowe zostały lub zostaną ujawnione (w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych),
4. planowanego okresu przechowywania danych osobowych (gdy nie jest to możliwe – podanie kryteriów ustalania tego okresu),
5. uprawnienia do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczących osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania,
6. uprawnienia do wniesienia skargi do organu nadzorczego,
7. dostępnych informacji o ich źródle (jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkich),
8. zautomatyzowanego podejmowania decyzji (w tym o profilowania) oraz istotnych informacji o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

III. Forma realizacji uprawnienia

1. realizacja uprawnienia dostępu do danych następuje poprzez złożenie wniosku:
a. na piśmie (w tym – w drodze wiadomości e-mail),
b. ustnie, jeżeli osoba, której dane dotyczą tego zażąda, o ile innymi sposobami potwierdzi się tożsamość tej osoby,
2. Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się w powszechnie stosowanej formie elektronicznej,
3. realizacja uprawnienia dostępu do danych jest wolna od opłat w zakresie uzyskania uprawnienia do pierwszej kopii danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, Administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych,
4. Administrator może odmówić podjęcia działań w związku z żądaniem, jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, co Administrator ma obowiązek wykazać,
5. prawo do uzyskania kopii danych osobowych (pkt. 1) nie może niekorzystnie wpływać na prawa i wolności innych (np. w zakresie praw autorskich), naruszać tajemnic prawnie chronionych etc,
6. Administrator może żądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą (art. 12 ust. 6 RODO). Realizacji uprawnienia dostępu do danych jest wyłączona gdy nie jest możliwe zidentyfikowanie osoby, od której żądanie pochodzi (art. 12 ust. 2 RODO).

IV. Termin realizacji uprawniania dostępu do danych

1. Administrator realizuje uprawnienie dostępu do danych niezwłocznie; termin ten nie może być dłuższy, niż miesiąc od dnia otrzymania żądania (art. 12 ust. 3 RODO).
2. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W taki przypadku Administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu,

z podaniem przyczyn opóźnienia na piśmie, bądź elektronicznie, chyba że osoba, której dane dotyczą zażąda innej formy.

3. Jeżeli Administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie, przy czym nie później niż w terminie miesiąca od otrzymania żądania, informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem (art. 12 ust. 4 RODO).

Zał. nr 7 do Polityki ochrony danych	**Procedura realizacji uprawnienia do „bycia zapomnianym", o którym mowa w art. 17 RODO**

I. Cel ustanowienia procedury

Celem procedury jest realizacja prawa osoby fizycznej do usunięcia swoich danych osobowych („prawo do bycia zapomnianym") przetwarzanych przez Administratora, którą utworzono w oparciu o art. 17 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; tzw. ogólne rozporządzenie o ochronie danych).

II. Unormowania ogólne

Osobie fizycznej przysługuje prawo żądania usunięcia jej danych osobowych przetwarzanych przez Administratora tj.:

1. możliwości żądania przez osobę, której dane dotyczą, niezwłocznego ich usunięcia,
2. możliwości żądania, aby Administrator danych poinformował innych administratorów danych, którym upublicznił dane osobowe, że osoba, której dane dotyczą, żąda, by ci Administratorzy usunęli wszelkie łącza do tych danych lub ich kopie, bądź replikacje.

Administrator informuje o usunięciu danych osobowych każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda (art. 19 RODO). Administrator, w przypadku podjęcia decyzji, o ograniczeniu poinformowania innych administratorów danych ma obowiązek wykazania takich ograniczeń w ewentualnym postępowaniu przed organem nadzorczym.

III. Realizacja uprawnienia do „bycia zapomnianym"

Przesłanki realizacji „prawa do bycia zapomnianym":

1. dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane (art. 17 ust. 1 pkt. a RODO),
2. osoba, której dane dotyczą, wycofała zgodę, o której mowa w art. art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a), na przetwarzanie danych osobowych i nie istnieje inna podstawa przetwarzania danych (art. 17 ust. 1 pkt. b RODO),

3. osoba, której dane dotyczą, zgłosiła sprzeciw wobec przetwarzania swoich danych i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania (art. 17 ust. 1 pkt. c RODO),
4. dane osobowe były przetwarzane w sposób niezgodny z prawem (art. 17 ust. 1 pkt. d RODO),
5. dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator (art. 17 ust. 1 pkt. e RODO),
6. dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego bezpośrednio dziecku w warunkach określonych w art. 8 ust. 1 RODO (art. 17 ust. 1 pkt. f RODO).

IV. Ograniczenie realizacji uprawnienia do „bycia zapomnianym"

W przypadku wykonania prawa do bycia zapomnianym, Administrator danych zaprzestaje przetwarzania danych osobowych i usuwa dane osoby, która złożyła stosowny wniosek, chyba że zachodzą szczególne przypadki ograniczające „prawo do bycia zapomnianym", tj. gdy przetwarzanie jest niezbędne:

1. do korzystania z prawa do wolności wypowiedzi i informacji (art. 17 ust. 3 lit. a RODO),
2. do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (art. 17 ust. 3 lit. b RODO),
3. z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3 (art. 17 ust. 3 lit. c RODO),
4. do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile prawdopodobne jest, że realizacja uprawnienia do „bycia zapomnianym", uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania (art. 17 ust. 3 lit. d RODO),
5. do ustalenia, dochodzenia lub obrony roszczeń (art. 17 ust. 3 lit. e RODO).

Administrator, w przypadku podjęcia decyzji, o ograniczeniu prawa do bycia zapomnianym ma obowiązek wykazania takich cech w ewentualnym postępowaniu przed organem nadzorczym.

V. Forma realizacji uprawnienia

1. realizacja uprawnienia do bycia zapomnianym następuje poprzez złożenie wniosku:
a) na piśmie (w tym – w drodze wiadomości e-mail),
b) ustnie, jeżeli osoba, której dane dotyczą tego zażąda, o ile innymi sposobami potwierdzi się tożsamość tej osoby,
2. realizacja uprawnienia do bycia zapomnianym jest wolna od opłat. Administrator,
3. może pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo odmówić podjęcia działań w związku z żądaniem, jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, co Administrator ma obowiązek wykazać,
4. Administrator może żądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą (art. 12 ust. 6 RODO). Realizacji uprawnienia „do bycia zapomnianym" jest wyłączona, gdy nie jest możliwe zidentyfikowanie osoby, od której żądanie pochodzi (art. 12 ust. 2 RODO).

VI. Termin realizacji uprawniania do „bycia zapomnianym"

1. Administrator realizuje uprawnienie do „bycia zapomnianym" niezwłocznie; termin ten nie może być dłuższy, niż miesiąc od dnia otrzymania żądania (art. 12 ust. 3 RODO).
2. w razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W taki przypadku Administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia na piśmie, bądź elektronicznie, chyba że osoba, której dane dotyczą zażąda innej formy.
3. jeżeli administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie, przy czym nie później niż w terminie miesiąca od otrzymania żądania, informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o

możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem (art. 12 ust. 4 RODO).

Zał. nr 8 do Polityki ochrony danych	**Procedura: prawo do przenoszenia danych**

1. Cel procedury

Celem procedury jest realizacja uprawnienia osoby fizycznej prawa do przeniesienia swoich danych osobowych przetwarzanych przez Administratora.

2. Prawa osoby fizycznej, której dane są przetwarzane

Prawo do przenoszenia danych może być wykonane wyłącznie wtedy, gdy osoba, której dane dotyczą uprzednio dostarczyła Administratorowi dane jej dotyczące, lub wyraziła zgodę na pozyskanie przez Administratora tych danych, w inny sposób, określony uprzednio odpowiednim oświadczeniem.

Prawo do przenoszenia danych to, w szczególności prawo do:

1. otrzymania przez osobę, której dane dotyczą, w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, danych osobowych jej dotyczących, które dostarczyła Administratorowi,
2. prawo przesłania przez osobę, której dane dotyczą, danych osobowych jej dotyczących, które dostarczyła administratorowi, innemu administratorowi, bez przeszkód ze strony administratora danych, o ile jest to technicznie możliwe.

Prawo do przeniesienia danych może zostać wykonane, gdy:

1. przetwarzanie danych odbywa się na podstawie zgody osoby, lub w celu wykonania umowy,
2. przetwarzanie danych odbywa się w sposób zautomatyzowany - prawo do przenoszenia danych obejmuje tylko te dane osobowe, które są przetwarzane przy użyciu systemów informatycznych i nie obejmuje ono tradycyjnych, manualnych papierowych zbiorów danych.

Prawo do przenoszenia danych obejmuje dane osobowe dotyczące osoby, która wykonuje to prawo i które to dane ta osoba dostarczyła Administratorowi. Wykonywanie tego prawa nie może ono niekorzystnie wpływać na praw i wolności innych osób.

+Prawo do przenoszenia danych nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi.

Zał.nr 9 do Polityki ochrony danych	**Procedura: prawo do sprzeciwu**

1. **Cel procedury**

Celem procedury jest realizacja prawa osoby fizycznej do sprzeciwu wobec przetwarzania jej danych osobowych przez Administratora.

2. **Prawa osoby fizycznej, której dane są przetwarzane**

Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw z przyczyn związanych z jej szczególną sytuacją wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f) RODO, w sytuacji, w której:

1. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi;
2. przetwarzanie jest niezbędne do celów, wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą jest dzieckiem.

Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie, do złożenia sprzeciwu wobec powyższego przetwarzania jej danych osobowych, oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji.

W sytuacji, gdy Administrator przetwarza dane osobowe na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym również profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.

Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, to Administratorowi nie wolno już przetwarzać tych danych osobowych do takich celów.

Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, osoba, której dane dotyczą, ma prawo

wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

Jeżeli dane osobowe są przetwarzane do celów marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo wnieść bezpłatnie sprzeciw do Administratora, w dowolnym momencie, wobec tego konkretnego przetwarzania, pierwotnego lub dalszego (w tym profilowania), o ile jest ono powiązane z marketingiem bezpośrednim.

Prawo do sprzeciwu musi zostać przez Administratora wyraźnie podane do wiadomości osobie, której dane dotyczą, jak również musi być przedstawione jasno i oddzielnie od wszelkich innych informacji.

3. Szczególne uprawnienia związane z procesami zautomatyzowanego przetwarzania danych - w tym z profilowaniem

Profilowanie to szczególny rodzaj przetwarzania danych osobowych, który odbywa się w sposób automatyczny, ma na celu ocenę osoby fizycznej lub przewidywanie jej zachowania.

Profilowanie zawsze wymaga poinformowania (w sposób możliwy do zweryfikowania) o nim osób, które są profilowane. Profilowanie może być wykorzystywane jako narzędzie dla tzw. automatycznego podejmowania decyzji Administratora wobec osób, których dane dotyczą.

Jeżeli automatyczne podejmowanie decyzji wywołuje skutki prawne wobec osób, których dane dotyczą, lub w podobny istotny sposób wpływa na te osoby, Administrator może mechanizm ten stosować wyłącznie wtedy, gdy spełniony jest jeden z następujących warunków:

1. osoba profilowana wyrazi na to wyraźną zgodę,
2. profilowanie jest niezbędne do zawarcia lub wykonywania umowy z tą osobą,
3. profilowanie jest dopuszczalne przez szczególne przepisy prawa.

Jeżeli profilowanie miałoby się odbywać w oparciu o szczególne kategorie danych osobowych, wówczas jedyną podstawą prawną, która mogłaby takie profilowanie

zalegalizować, może być szczególny przepis prawa. W przypadku gdy zgoda na profilowanie została pobrana przy pomocy dedykowanej strony internetowej, odwołanie zgody musi być możliwe w ten sam sposób.

Odwołanie zgody wywołuje wyłącznie skutki na przyszłość – oznacza to, że od chwili otrzymania oświadczenia o odwołaniu zgody, nie można już opierać na zgodzie przetwarzania danych.

4. Realizacja prawa do sprzeciwu

Administrator, po wniesieniu sprzeciwu przez osobę, której dane przetwarzał, powinien zaprzestać przetwarzania tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

Nawet jeżeli dane osobowe mogą być przetwarzane zgodnie z prawem, gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi lub ze względu na prawnie uzasadnione interesy administratora lub strony trzeciej, każdej osobie, której dane dotyczą, przysługuje prawo sprzeciwu wobec przetwarzania danych osobowych dotyczących jej szczególnej sytuacji.

Wykazanie zaistnienia ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń, jest obowiązkiem leżącym po stronie Administratora, i ma on obowiązek wykazania powyższego, w ewentualnym postępowaniu przed organem nadzorczym.

Wykorzystanie prawa do sprzeciwu nie prowadzi do automatycznego usunięcia wszystkich danych osobowych przez Administratora. Oznacza ono, że Administrator, z chwilą otrzymania sprzeciwu wobec przetwarzania danych osobowych, zaprzestaje z nich korzystać.

Zał. nr 10 do Polityki ochrony danych	**Procedura: prawo do sprostowania danych osobowych**

1. Cel procedury

Celem procedury jest realizacja uprawnienia osoby fizycznej do sprostowania/uzupełnienia swoich danych przetwarzanych przez Administratora.

2. Prawa osoby fizycznej, której dane są przetwarzane

Każdej osobie fizycznej przysługuje jednakowe prawo do niezwłocznego sprostowania/uzupełnienia dotyczących go danych osobowych, które są nieprawidłowe lub nieaktualne. Uwzględniając cele przetwarzania, osoba, której dane dotyczą ma prawo do żądania od Administratora uzupełnienia niekompletnych danych osobowych, poprzez przedstawienie odpowiedniego oświadczenia Administratorowi.

Jeżeli osoba fizyczna zażąda uzupełnienia katalogu dotyczących go danych osobowych o te, które nie są niezbędne Administratorowi do działania, to taki wniosek nie musi zostać pozytywnie rozpatrzony przez Administratora dla osoby, której dane dotyczą.

3. Procedura rozpatrywania żądań o sprostowanie danych osobowych

Komunikacja z osobą, której dane dotyczą powinna być prowadzona w zwięzłej, przejrzystej, zrozumiałej i dostępnej formie.

Osoba składająca wniosek o sprostowanie/uzupełnienie danych osobowych oświadcza, że jest osobą możliwą do zidentyfikowania, na podstawie dobrowolnie podanych danych osobowych, umożliwiających jej jednoznaczną identyfikację.

W przypadku, gdy Administrator nie jest w stanie zidentyfikować osoby składającej wniosek o sprostowanie/uzupełnienie danych osobowych, ma prawo na podstawie obowiązujących przepisów prawa odmówić rozpatrzenia żądania, uprzednio podejmując wszelkie możliwe środki w celu zidentyfikowania osoby, która z nim wystąpiła.

Działania podejmowane na podstawie żądania o sprostowanie lub uzupełnienie danych są zwolnione z opłat (art. 12 ust. 5 RODO), lecz jeżeli żądania osoby, której dane dotyczą są ewidentnie nieuzasadnione lub nadmierne (np. ze względu na swój ustawiczny charakter) Administratorowi przysługują dwa uprawnienia:

1. pobranie rozsądnej opłaty, która uwzględnia administracyjne koszty prowadzenia komunikacji i podjętych działań (według stawek obowiązujących u Administratora),
2. odmowa podejmowania działań.

Administrator, w przypadku podjęcia decyzji, o nieuzasadnionym lub nadmiernym charakterze żądania ma obowiązek wykazania takich cech żądania (wniosku) w ewentualnym postępowaniu przed organem nadzorczym.

Administrator jest zobowiązany po dokonaniu sprostowania/ uzupełnienia danych osobowych poinformować wszystkich odbiorców którym ujawniono dane podlegające uzupełnieniu/sprostowaniu o fakcie ich uzupełnienia/sprostowania.

W przypadku braku możliwości wykonania powyższego, lub gdy działanie takie wymagałoby niewspółmiernie dużego wysiłku ze strony Administratora, może on podjąć decyzję o nieudzieleniu stosownej informacji odbiorcom, jednakże ma obowiązek wykazania braku tej możliwości lub niewspółmiernie dużego wysiłku w ewentualnym postępowaniu przed organem nadzorczym.

4. Terminy rozpatrywania żądań o sprostowanie/uzupełnienie danych osobowych.

Na podstawie art. 12 ust. 3 RODO, Administrator podejmuje decyzję o przyjęciu/odrzuceniu oświadczenia/wniosku o sprostowanie/uzupełnienie danych osobowych bez zbędnej zwłoki.

Terminy na udzielenie odpowiedzi na żądanie:

1. Administrator zobowiązany jest do udzielenia odpowiedzi na żądanie osoby fizycznej w terminie **miesiąca** od otrzymania tego żądania,
2. jeżeli żądanie ma charakter skomplikowany, lub skierowano dużą liczbę żądań, administrator może wydłużyć czas udzielenia odpowiedzi o kolejne **2 miesiące**, jednakże w takim wypadku jest zobowiązany do przekazania takiej informacji osobie fizycznej w terminie pierwszego miesiąca licząc od momentu wpłynięcia żądania. Musi również w takim wypadku podać przyczyny wydłużenia terminu na udzielenie odpowiedzi (art. 12 ust. 3 RODO).

W przypadku, gdy Administrator nie zamierza udzielić odpowiedzi i działań wobec żądania osoby fizycznej jest zobowiązany do poinformowania tej osoby o powodach niepodjęcia działań, a także możliwości wniesienia skargi do organu nadzorczego oraz skorzystania przez podmiot danych z możliwości wniesienia sprawy do sądu.

Zał. nr 11 do Polityki ochrony danych	**Wzór wniosku o nadanie upoważnienia do przetwarzania danych osobowych/uprawnienia do pracy w systemie informatycznym**

Wnioskuję o nadanie/zmianę / upoważnienia do przetwarzania danych lub/i uprawnień w systemach informatycznych*

Panu/Pani..... .....

Zatrudnionemu/onej w .....

Na stanowisku.....do przetwarzania danych osobowy w następujących w zakresie:

.....

☐ do pracy w systemach informatycznych:

lp.	systemy informatyczne*	uprawnienia*
1.		
2.		
3.		
4.		
5.		
6.		

* niepotrzebne skreślić
* Systemy informatyczne, do których użytkownik ma dostęp
* Uprawnienia:
O-odczyt
W-wydruk
M-modyfikacja (zmiana, wprowadzanie danych)

_____
(podpis osoby składającej wniosek)

Zał.nr 12 do Polityki ochrony danych	**Wzór upoważnienia do przetwarzania danych osobowych**

.....dnia.....roku

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 i 32 ust. 4 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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** .....zatrudnionego/zatrudnioną w ..... na stanowisku:..... do przetwarzania danych osobowych w zakresie:

Ponadto pracownik posiada dostęp do następujących systemów informatycznych przetwarzających dane osobowe:

lp.	**systemy informatyczne**	**uprawnienia***
1.		
2.		
3.		
4.		

* Uprawnienia:
O-odczyt
W-wydruk
M-modyfikacja (zmiana, wprowadzanie danych)

Rozwiązanie stosunku pracy/ umowy w przypadku zleceniobiorców/ skutkuje odwołaniem upoważnienia.

(pieczęć i podpis Administratora)

Niniejszym uprzednio wydane upoważnienie traci moc. *(*niniejsza klauzula ma zastosowanie tylko dla osób którym wcześniej wydano upoważnienie)*

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Imię i nazwisko	Stanowisko	Data nadania	Data ustania

Zał. nr 14 do Polityki ochrony danych	**Opis środków technicznych stosowanych do zabezpieczania danych**

Obszarem przetwarzania danych osobowych są pomieszczeniach w Urzędu Miasta Łaskarzew

Na obszar przetwarzania danych osobowych składają się następujące pomieszczenia biurowe:

Numer pokoju	**Parter/Piętro**

Zał.nr 15 do Polityki ochrony danych	**Wzór umowy powierzenia**

UMOWA

POWIERZENIA DANYCH OSOBOWYCH DO PRZETWARZANIA

zawarta w dniu _____ r. w _____

pomiędzy:

_____

z siedzibą w _____

ul. _____ ,

NIP _____, reprezentowaną przez:

_____ – *(funkcja)*

_____ – *(funkcja)*

zwaną w treści Umowy „**Administratorem**”,

a

_____ _____ _____

z siedzibą w _____

ul. _____,

NIP _____, reprezentowaną przez:

_____ – *(funkcja)*

_____ – *(funkcja)*

zwaną w treści Umowy **„Procesorem”** lub **„Przetwarzającym”,**

w dalszej części Umowy Administrator i Procesor są nazywani łącznie **„Stronami”** lub każde oddzielnie **„Stroną”**.

§ 1

Przedmiot Umowy, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą

1. Umowa ma charakter umowy powierzenia danych osobowych w rozumieniu art. 28 ust. 1 i 3 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. 2016, poz. 119.1), zwanego w dalszej części Umowy jako: „Rozporządzenie”.
2. Procesor uprawniony jest do przetwarzania danych osobowych wyłącznie w celu wykonania umowy głównej, tj. umowy z dnia _____ , której

przedmiotem jest _____, które będzie zwane w dalszej części Umowy jako „przetwarzanie" .

3. Przetwarzanie dotyczyć będzie (*wskazać kategorie osób oraz rodzaj danych,)*

§ 2

Czas trwania Umowy

1. Umowa zostaje zawarta na czas określony od dnia _____ do dnia _____ (*ewentualnie: na czas trwania umowy, o której mowa w § 1 ust. 3*).
2. Procesor nie ma prawa do wykorzystania zgromadzonych na podstawie niniejszej Umowy danych osobowych w jakimkolwiek celu po jej rozwiązaniu, niezależnie od podstawy takiego rozwiązania.

§ 3

Warunki powierzenia danych osobowych do przetwarzania

1. Procesor przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora oraz:

a. zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
b. podejmuje odpowiednie środki techniczne oraz organizacyjne, mające na celu zapewnienia bezpieczeństwa danych osobowych;
c. nie korzysta z usług innego podmiotu przetwarzającego, bez uprzedniej pisemnej zgody Administratora;
d. w miarę możliwości pomaga Administratorowi, poprzez odpowiednie środki techniczne i organizacyjne, wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w art. 12-23 Rozporządzenia;
e. uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32-36 Rozporządzenia;
f. po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji Administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, w tym również te, zawarte na nośnikach danych, chyba że prawo Unii

Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;

g. udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia oraz umożliwia Administratorowi (lub upoważnionemu przez niego audytorowi) przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

2. Jeżeli powierzone dane osobowe są przetwarzane w formie elektronicznej na serwerach i nośnikach danych Procesora, te serwery i nośniki nie mogą znajdować się poza obszarem Unii Europejskiej i Europejskiego Obszaru Gospodarczego.

3. Procesor zobowiązuje się do każdorazowego i niezwłocznego informowania Administratora o przypadkach naruszenia przepisów prawa dotyczących ochrony powierzonych danych osobowych, w tym w szczególności przepisów Rozporządzenia, zaistniałych w okresie obowiązywania niniejszej Umowy.

4. W przypadku stwierdzenia naruszenia ochrony danych osobowych, o którym mowa w art. 33 Rozporządzenia, Procesor zgłasza je Administratorowi bez zbędnej zwłoki. Zgłoszenie naruszenia ochrony danych osobowych Administratorowi powinno nastąpić w formie pisemnej lub elektronicznej.

5. Na wypadek zawinionego naruszenia przez Procesora zasad przetwarzania danych osobowych (określonych w przepisach powszechnie obowiązującego prawa, Rozporządzenia oraz niniejszej Umowy), skutkującego zobowiązaniem Administratora na mocy prawomocnego orzeczenia sądu, ugody sądowej bądź porozumienia mediacyjnego do wypłaty odszkodowania, zadośćuczynienia lub kary pieniężnej, Procesor zobowiązuje się zrekompensować Administratorowi udokumentowane straty z tego tytułu w pełnej wysokości. Zobowiązanie Procesora, o którym mowa powyżej, powstanie pod warunkiem pisemnego powiadomienia go o każdym przypadku wystąpienia przez osoby trzecie z roszczeniem wobec Administratora z podaniem podstaw prawnych i faktycznych, w terminie 3 dni od daty dowiedzenia się Administratora o takim roszczeniu.

6. Procesor jest zwolniony z odpowiedzialności za szkody spowodowane przetwarzaniem przez niego danych naruszającym przepisy prawa, jeżeli nie można mu przypisać winy za zdarzenie, które doprowadziło do powstania szkody.

7. Procesor zapewnia, że dane osobowe nie będą udostępniane jego pracownikom i zleceniobiorcom przed podpisaniem przez nich oświadczeń lub umów o zachowaniu poufności. Zachowanie poufności nie ustaje po rozwiązaniu lub wygaśnięciu stosunku

pracy lub umowy cywilnoprawnej, niezależnie od przyczyny tego rozwiązania lub wygaśnięcia.

8. Procesor zobowiązuje się do monitorowania i stosowania przepisów prawa, powszechnie dostępnych wskazówek i zaleceń organu nadzorczego oraz unijnych organów doradczych, zajmujących się ochroną danych osobowych, w zakresie przetwarzania powierzonych mu danych, po uprzednim uzgodnieniu wpływu tych regulacji na przetwarzanie danych z Administratorem.

§ 4

Kontrola przetwarzania danych powierzonych

1. Administrator przez cały okres obowiązywania Umowy jest uprawniony do kontroli poprawności zabezpieczenia i przetwarzania danych powierzonych Procesorowi. Kontrola może zostać przeprowadzona m.in. w formie bezpośredniej inspekcji polegającej na dopuszczeniu przedstawicieli Administratora do wszystkich obszarów przetwarzania danych osobowych objętych niniejszą Umową we wszystkich lokalizacjach Procesora, w sposób nieutrudniający nadmiernie jego bieżącej działalności. Procesor zobowiązany jest do przedstawienia odpowiednich dokumentów do kontroli oraz wyjaśnień na piśmie na każde wezwanie Administratora,.
2. W przypadku, gdy kontrola, o której mowa w ust. 1, wykaże jakiekolwiek nieprawidłowości Administrator ma prawo żądać od Procesora niezwłocznego wdrożenia zaleceń Administratora wynikających z ustaleń pokontrolnych. Zalecenia te przedstawiane będą w formie ustnej, pisemnej lub elektronicznej.

§ 5

Podpowierzenie danych

1. Procesor może powierzać przetwarzanie powierzonych mu danych osobowych objętych Umową innym podmiotom na stałe współpracującym z Procesorem (tzw. podpowierzenie) wyłącznie po uprzedniej pisemnej zgodzie Administratora.
2. Podpowierzając przetwarzanie danych osobowych innym podmiotom, Procesor jest obowiązany zapewnić w dalszej umowie powierzenia spełnienie przez ten podmiot wszelkich wymogów w zakresie ochrony danych osobowych na poziomie, co najmniej takim samym jak przewidziany w niniejszej Umowie.

§ 6

Poufność

1. Procesor zobowiązuje się do zachowania w tajemnicy wszelkich danych osobowych, informacji i materiałów przekazanych lub udostępnionych mu lub o których wiedzę powziął w związku z realizacją Umowy, a także powstałych w wyniku jej wykonania informacji i materiałów w formie pisemnej, graficznej lub jakiejkolwiek innej formie. Informacje

   i materiały są objęte tajemnicą nie mogą być bez uprzedniej pisemnej zgody Administratora udostępniane jakiejkolwiek osobie trzeciej, ani też ujawnione w inny sposób, chyba że w dniu ich ujawnienia były powszechnie znane albo muszą być ujawnione zgodnie z powszechnie obowiązującymi przepisami prawa, orzeczeniem sądu lub organu państwowego.
2. Procesor zapewnia, że osoby upoważnione do przetwarzania danych osobowych będą obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia. Obowiązek zachowania tajemnicy nie ustaje po zaprzestaniu przetwarzania danych z jakiejkolwiek podstawy. Przepis § 3 ust. 6 Umowy stosuje się odpowiednio.

§ 7

Współpraca Stron

1. Strony ustalają, że podczas realizacji Umowy powierzenia będą ze sobą ściśle współpracować, informując się wzajemnie o wszystkich okolicznościach mających lub mogących mieć wpływ na wykonanie powierzenia danych osobowych.
2. Strony będą dokonywały uzgodnień i podejmowały decyzje operacyjne poprzez swoich przedstawicieli odpowiedzialnych za realizację Umowy w formie ustnej, pisemnej lub elektronicznej,.
3. Strony zobowiązują się, że wszelkie decyzje dotyczące polubownego zakończenia sporu z osobą fizyczną na skutek naruszenia ochrony jej danych osobowych, w szczególności fakt i wysokość wypłaty ewentualnego odszkodowania, podejmą wspólnie.

§ 8

Wypowiedzenie umowy

1. Każdej ze Stron przysługuje uprawnienie do rozwiązania Umowy z zachowaniem miesięcznego terminu wypowiedzenia ze skutkiem na koniec miesiąca kalendarzowego, w którym oświadczenie o wypowiedzeniu zostało doręczone drugiej stronie=.
2. Administrator ma prawo wypowiedzieć Umowę w trybie natychmiastowym, w przypadku rażącego naruszenia postanowień Umowy przez Procesora, który:

a. wykorzystał dane osobowe w sposób niezgodny z Umową, w szczególności przetwarzał je dla własnych celów lub celów innych podmiotów, a także celów niezgodnych z powszechnie obowiązującymi przepisami prawa lub postanowieniami niniejszej Umowy;

b. wykonuje Umowę niezgodnie z obowiązującymi w tym zakresie przepisami prawa lub instrukcjami Administratora w tym zakresie;

c. nie zaprzestał niewłaściwego przetwarzania danych osobowych mimo uprzedniego wezwania Administratora do usunięcia naruszeń i bezskutecznego upływu wyznaczonego terminu 14 dni na zaniechanie naruszeń.

§ 9

Postanowienia Końcowe

1. Z tytułu wykonywania niniejszej Umowy Procesorowi *przysługuje/nie przysługuje* dodatkowe wynagrodzenie.
2. Wszelkie zmiany niniejszej Umowy wymagają formy pisemnej pod rygorem nieważności.
3. Spory wynikłe z tytułu Umowy będzie rozstrzygał Sąd właściwy dla miejsca siedziby Administratora.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

_____ _____

(Administrator) **(Procesor)**

Zał. nr 16 do Polityki ochrony danych	**Wzór rejestru umów powierzenia przetwarzania danych osobowych**

Lp.	**Numer umowy**	**Data zawarcia umowy**	**Strona umowy**	**Zakres powierzenia**
1.				
2.				

Zał. nr 17 do Polityki ochrony danych	**Procedura zarządzania naruszeniami ochrony danych osobowych**

I. Istota naruszenia ochrony danych

Incydentem w zakresie danych osobowych jest sytuacja powodująca utratę poufności, integralności lub dostępności przetwarzanych danych.

Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

1. nieautoryzowany dostęp do danych,
2. nieautoryzowane modyfikacje lub zniszczenie danych,
3. udostępnienie danych nieautoryzowanym podmiotom,
4. nielegalne ujawnienie danych,
5. pozyskiwanie danych z nielegalnych źródeł.

II. Postępowanie w przypadku naruszenia danych osobowych

1. Użytkownik, który stwierdzi lub podejrzewa fakt naruszenia danych osobowych, jest zobowiązany niezwłocznie zgłosić to swojemu bezpośredniemu przełożonemu. Przełożony zgłasza fakt naruszenia Administratorowi i Inspektorowi ochrony danych.
2. Typowe sytuacje, gdy bezpośredni przełożony powinien powiadomić Administratora i Inspektora ochrony danych:

a. ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
b. dokumentacja jest niszczona bez użycia niszczarki,
c. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,
d. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe, stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.,
e. niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych,

f. ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe,
g. wynoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz firmy bez upoważnienia,
h. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej;
i. stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
j. telefoniczne próby wyłudzenia danych osobowych;
k. kradzież komputerów lub twardych dysków z danymi osobowymi;
l. utrata kontroli nad kopią danych osobowych;
m. maile zachęcające do ujawnienia identyfikatora i/lub hasła;
n. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
o. istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki"
p. hasła do systemów przechowywane są w pobliżu komputera.

3. Użytkownik, który stwierdzi fakt naruszenia danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia .
4. W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Inspektora ochrony danych lub innej osoby upoważnionej przez Administratora danych.

Inspektor ochrony danych podejmuje następujące kroki:

1. zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości i ciągłości pracy,
2. odbiera dokładną relację z zaistniałego naruszenia bezpieczeństwa danych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,
3. nawiązuje kontakt ze specjalistami zewnętrznymi (jeśli zachodzi taka potrzeba).
4. Inspektor ochrony danych dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych sporządzając raport - Załącznik nr 1.

5. Inspektor ochrony danych zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych) - Załącznik nr 2 - rejestr incydentów i działań korygujących i zapobiegawczych.

III. Zgłaszanie naruszenia ochrony danych do Urzędu Ochrony Danych Osobowych

1. W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Urzędowi ochrony danych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Wzór zgłoszenia – Załącznik nr 3.
2. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:

a. opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
b. zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
c. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
d. opisywać środki zastosowane lub proponowane przez Administratora w celu zapobiegania naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach - środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

3. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.
4. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

IV. Zawiadomienie osoby której dane dotyczą, o naruszeniu ochrony danych osobowych

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
2. Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w § 10 ust. 2 lit. b), c) i d).
3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:

a. Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

b. Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1; c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Zał. nr 17 do Polityki ochrony danych	**Procedura zarządzania naruszeniami ochrony danych osobowych**

Załącznik nr 1 Raport naruszenia ochrony danych

1. Data ..... Godzina .....
2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem

   .....

   (imię, nazwisko, stanowisko służbowe,):
3. Lokalizacja zdarzenia .....

   (nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):
4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:

   .....
5. Podjęte działania:

   .....
6. Wstępna ocena przyczyn wystąpienia naruszenia:

   .....
7. Postępowanie wyjaśniające i naprawcze:

   .....

.....
(podpis pracownika)

.....
(data i podpis Inspektora ochrony danych)

Załącznik nr 2 Rejestr naruszeń

Lp.	Data naruszenia	Kategoria osób, których dane zostały naruszone	Kwalifikacja naruszenia (niskie lub wysokie)	Zastosowane środki zaradcze	Zgłoszenie do organu nadzorczego (dotyczy lub nie dotyczy)	Zawiadomienie osoby której dane dotyczą (dotyczy lub nie dotyczy)
1.						
2.						
3.						
4.						

Załącznik nr 3 Zgłoszenie o naruszeniu ochrony danych osobowych organowi nadzorczemu

_____ , _____

(miejscowość) (data)

Urząd Ochrony Danych Osobowych

Ul. Stawki 2

00-193 Warszawa

Na podstawie obowiązku wynikającego z art. 33 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).

Data Naruszenia	
Liczba osób których dane dotyczą	
Liczba wpisów danych osobowych i kategoria tych danych	
Dane Inspektora Danych osobowych	
Dane Organu Nadzorczego	
Charakter Naruszenia:	
Konsekwencje naruszenia:	
Zastosowane i proponowane środki zaradcze:	

_____

(Podpis Administratora)

Załącznik nr: 4 Zawiadomienie o naruszeniu ochrony danych osoby, których dane zostały naruszone

_____ , _____
(miejscowość) (data)

Pan/Pani

_____

_____

Na podstawie obowiązku wynikającego z art. 34 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) w związku z naruszeniem Pana/Pani danych osobowych w zakresie ..... Zawiadamiamy co następuje:

Konsekwencją wyżej wymienionej sytuacji jest podjęcie przez osoby nieupoważnione informacji w zakresie.....

Urząd podjął wszelkie możliwe środki celem minimalizacji skutków naruszenia między innymi: zawiadomienie do organu nadzorczego, zawiadomienie organów ścigania, wcześniejsza szyfryzacja danych.

Celem uzyskania dodatkowych informacji należy kontaktować się z .....

_____
(Podpis Administratora)

Zał. 18 do Polityki ochrony danych	**Wzór notatki z kontroli uprawnień**

_____ , _____

(miejscowość) (data)

W związku z kontrolą uprawnień i kont użytkowników z dnia ..... stwierdzam co następuje:

1. Użytkownicy *pracują/ nie pracują na systemach zgodnych z ich uprawnieniami.
2. Użytkownicy *posiadają/ nie posiadają na stacjach roboczych oprogramowanie na które jednostka posiada licencje.
3. Na stacjach roboczych użytkowników *znajduje/ nie znajduje się oprogramowanie nie związane z pracą służbową np. komunikatory społecznościowe, aplikacje służące do wymiany lub pobierania plików, czytniki prywatnej poczty, oprogramowanie umożliwiające dostęp do prywatnej chmury z danymi itp. portalami społecznościowymi.
4. Na stacjach roboczych pracowników *znajdują/ nie znajdują się dokumenty i korespondencja nie związana z czynnościami służbowymi

Wnioski i zalecenia pokontrolne:

_____

(podpis)

*niepotrzebne skreślić

Zał.nr 19 do Polityki ochrony danych	**Oświadczenie o monitorowaniu komputerów służbowych**

_____ , _____
(miejscowość) (data)

Oświadczam, iż zostałam/zostałem zaznajomiona/zaznajomiony z faktem, iż systemy informatyczne, do których mam dostęp na komputerach służbowych i na których wykonuję obowiązki pracownicze, są monitorowane, w zakresie ilościowego i jakościowego wykorzystania tych systemów.

Oświadczam, że monitoring obejmuje również sposób wykorzystania służbowej poczty elektronicznej. Zobowiązuję się do wykorzystywania jej jedynie w celu realizacji zadań pracowniczych, wynikających ze stosunku pracy.

_____
(podpis)

* - niepotrzebne skreślić