Tytuł
Polityka ochrony danych osobowych
Gmina Krokowa

POLITYKA OCHRONY DANYCH OSOBOWYCH

Gmina Krokowa

Polityka ochrony danych osobowych
Gmina Krokowa

Spis treści

Polityka ochrony danych osobowych
Gmina Krokowa

1 Informacje wstępne

Polityka ochrony danych osobowych zwana dalej „Polityką” jest dokumentem wewnętrznym **Gminy Krokowa** 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** – Gmina Krokowa ul. Żarnowiecka 29, 84-110 Krokowa, reprezentowana przez Wójta Gminy; 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. **Biuro obsługi informatycznej -** 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, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
11. **Polityka** oznacza niniejszą Politykę ochrony danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.,
12. **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,

13. **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),
14. **Użytkownik**- osoba posiadająca dostęp do systemu informatycznego przetwarzającego dane osobowe oraz dokumentacji papierowej,
15. **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,
16. **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

Użytkownik systemu przetwarzania Danych Osobowych – każdy pracownik, który wykonując czynności służbowe, przetwarza Dane Osobowe, tzn. wykonuje na nich operacje takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie niezależnie czy odbywa się to w zbiorach tradycyjnych czy systemie IT.
Użytkownicy systemu są odpowiedzialni za zapewnienie bezpieczeństwa systemu ochrony Danych Osobowych w tym przetwarzanych w systemie IT, a w szczególności są zobowiązani 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 13** do niniejszej Polityki,
   f) sporządzanie kopii zapasowych zgodnie z procedurą opisaną w pkt. 11.3 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 2** do niniejszej Polityki, natomiast **załącznik nr 3** 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 4** 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 5 do 9** 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 10** do niniejszej Polityki ochrony danych;
2) zatwierdzone upoważnienie do przetwarzania danych osobowych Administrator wpisuje do ewidencji nadanych upoważnień - stanowiącej **załącznik nr 11** 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 oraz rozkodowania systemu alarmowego przed rozpoczęciem pracy urzędu.
Osoby, którym zostały powierzone klucze oraz kod cyfrowy do systemu alarmowego zobowiązani są do nieudostępniania kluczy oraz kodu cyfrowego do systemu alarmowego osobom trzecim.

Klucze do poszczególnych pomieszczeń pracownicy pobierają i zdają po zakończonym dniu pracy do informacji. 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 17** 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 12** 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) obsługa informatyczna na wniosek bezpośredniego przełożonego nadaje uprawnienia użytkownikom do pracy w systemach informatycznych
2) obsługa informatyczna jednostki przeprowadza okresową kontrolę uprawnień i kont użytkowników co najmniej raz na dwa lat w celu weryfikacji czy użytkownicy posiadają uprawnienia adekwatne do wykonywanej pracy w systemach informatycznych.
3) 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) kopią zapasową objęte są dokumenty i programy zainstalowane w komputerach umieszczonych w pokojach pracowników Urzędu Gminy.
3) użytkownicy we własnym zakresie odpowiadają za sporządzanie kopii zapasowych dokumentów znajdujących się na lokalnych dyskach twardych;
4) po wykonaniu kopii zapasowej zaleca się ich weryfikację poprzez dokonanie próby odtworzeniowej.

11.4 Procedura zarządzania sprzętem komputerowym i oprogramowaniem

1. Użytkownik zobowiązany jest korzystać ze sprzętu komputerowego 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 komputerowego (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.
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 komputerowego 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 komputerowego i nośników danych

1. Obsługa informatyczna dokonuje przeglądu i konserwacji sprzętu komputerowego 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 wyrażeniu zgody na przetwarzanie danych osobowych,
Nr 3- Wzór odwołania zgody na przetwarzanie danych osobowych,
Nr 4- Wzór klauzuli informacyjnej,
Nr 5- Procedura prawo dostępu do danych,
Nr 6- Procedura prawo do sprostowania danych do danych,
Nr 7- Procedura prawo do bycia zapomnianym,
Nr 8- Procedura prawo do przenoszenia danych,
Nr 9- Procedura prawo do sprzeciwu,
Nr 10- Wzór upoważnienia do przetwarzania danych osobowych,
Nr 11- Wzór ewidencji osób upoważnionych do przetwarzania danych,
Nr 12- Opis środków technicznych stosowanych do zabezpieczania danych,
Nr 13 – wzór oświadczenia o zachowaniu w poufności danych,
Nr 14 – oświadczenie o monitorowaniu komputerów służbowych
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,