ZARZĄDZENIE NR 40/2024
STAROSTY SŁUPSKIEGO

z dnia 17 lipca 2024 r.

w sprawie Polityki Ochrony Danych Osobowych

Na podstawie art. 34 ust. 1 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2024 r. poz. 107) oraz 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) (Dz. U. UE. L. 2016.119. 1) zarządza się, co następuje:

§ 1. Wprowadza się „Politykę Ochrony Danych Osobowych", stanowiącą załącznik do niniejszego zarządzenia.

§ 2. Wykonanie zarządzenia powierza się naczelnikom wydziałów i osobom na samodzielnych stanowiskach pracy.

§ 3. Traci moc zarządzenie Nr 72/2022 Starosty Słupskiego z dnia 26 października 2022 r. w sprawie Polityki Ochrony Danych Osobowych, zmienione zarządzeniem Nr 39/2023 Starosty Słupskiego z dnia 27 kwietnia 2023 r.

§ 4. Zarządzenie wchodzi z życie z dniem podpisania.

Starosta Słupski

Paweł Lisowski

Załącznik do zarządzenia Nr 40/2024
Starosty Słupskiego
z dnia 17 lipca 2024 r.

POLITYKA OCHRONY DANYCH OSOBOWYCH

ROZDZIAŁ I

Wyjaśnienie pojęć

§ 1. Użyte w „Polityce ochrony danych osobowych” pojęcia oznaczają:

1) Administrator danych osobowych, administrator, ADO – Starosta Słupski, który decyduje o celach i sposobach przetwarzania danych;
2) bezpieczeństwo przetwarzania danych osobowych – zachowanie poufności, integralności i rozliczalności danych osobowych;
3) dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
4) dane wrażliwe – dane podlegające szczególnej ochronie wymienione w art. 9 ust. 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) (Dz. U. UE. L. 2016.119. 1), tj. dane osobowe określające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej;
5) eKancelaria – system elektronicznego obiegu dokumentów;
6) hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi;
7) identyfikator – ciąg znaków jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
8) integralność danych – właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
9) IOD – Inspektor Ochrony Danych;
10) naruszenie ochrony danych osobowych - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych;
11) podmiot przetwarzający, procesor – organizacja lub osoba, której administrator powierzył przetwarzanie danych osobowych;

12) polityka - niniejsza „Polityka ochrony danych osobowych”, o ile co innego nie wynika wyraźnie z kontekstu;

13) poufność – właściwość polegająca na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom;

14) pracownicy – osoby zatrudnione w Starostwie Powiatowym w Słupsku oraz na potrzeby niniejszej polityki także stażyści, praktykanci, wolontariusze oraz inne osoby wykonujące prace w ramach zawieranych umów lub pełnionych funkcji;

15) pracodawca – Starostwo Powiatowe w Słupsku, reprezentowane przez Starostę Słupskiego;

16) profilowanie danych osobowych, profilowanie – dowolna forma zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

17) przetwarzanie danych osobowych, przetwarzanie – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, w tym wykonywane w systemach informatycznych;

18) RCP - rejestr czynności przetwarzania;

19) RKCP – rejestr kategorii czynności przetwarzania;

20) RODO - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. 2016.119. 1);

21) rozliczalność - zdolność do wykazania przestrzegania przepisów w zakresie ochrony danych osobowych;

22) Starostwo – Starostwo Powiatowe w Słupsku.

ROZDZIAŁ II

Cel wprowadzenia polityki ochrony danych osobowych

§ 2. 1. Polityka ma na celu zapewnienie ochrony danych osobowych przetwarzanych w Starostwie lub dla których administratorem jest Starosta Słupski.

2. Politykę stosuje się także do przetwarzanych w Starostwie danych osobowych, których administratorem nie jest Starosta Słupski, chyba, że zawarte w tym zakresie umowy stanowią inaczej.

3. Wprowadzenie polityki wynika z realizacji obowiązków określonych w art. 32 RODO.

4. Polityka określa zasady przetwarzania danych osobowych oraz ich zabezpieczania. Stanowi spisany zestaw praw, reguł i zaleceń, regulujących sposób zarządzania ochroną danych wewnątrz Starostwa oraz stosowanych w kontaktach z otoczeniem.
5. Polityka dotyczy zarówno danych osobowych przetwarzanych papierowo, jak i w systemach informatycznych.

ROZDZIAŁ III

Ogólne zasady przetwarzania danych

§ 3. Dane osobowe przetwarza się:

1) zgodnie z prawem (zgodność z prawem);
2) w sposób rzetelny i przejrzysty dla osób, których dane dotyczą (rzetelność, przejrzystość);
3) adekwatnie, stosownie i w sposób ograniczony do tego, co niezbędne do celów, w których są przetwarzane (minimalizacja danych);
4) prawidłowe i w razie potrzeby uaktualnione (prawidłowość);
5) w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów przetwarzania (ograniczenie przechowywania);
6) w sposób zapewniający odpowiednie bezpieczeństwo (integralność i poufność);
7) w sposób, który umożliwia administratorowi wykazanie, że przestrzega przepisów RODO (rozliczalność).

ROZDZIAŁ IV

System ochrony danych

§ 4. 1. Administrator zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych wskutek przetwarzania danych osobowych.

2. W Starostwie stosuje się następujące rozwiązania organizacyjne:

1) dokonywana jest analiza ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii poprzez analizę możliwych scenariuszy naruszeń danych osobowych oraz prawdopodobieństwo i powagę ich wystąpienia;
2) do przetwarzania danych osobowych upoważnieni są wyłącznie pracownicy posiadających upoważnienia nadane przez ADO;
3) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych;
4) zapewniony jest odpowiedni stan wiedzy osób, które przetwarzają dane osobowe o zapewnieniu bezpieczeństwa danym osobowym;
5) osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązano do zachowania ich w tajemnicy;
6) przetwarzanie danych osobowych prowadzone jest w warunkach zabezpieczających je przed dostępem osób nieupoważnionych;
7) stosuje się pisemne umowy powierzenia przetwarzania danych osobowych przy

współpracy z podmiotami przetwarzającymi dane osobowe, dla których administratorem jest Starosta Słupski;
8) opracowany i prowadzony jest RCP;
9) opracowany i prowadzony jest RKCP;
10) zapewnia się dbałość o stosowanie podstaw legalizujących przetwarzanie danych oraz wyszczególnia je w RCP;
11) w odpowiedni sposób zarządza się wyrażonymi zgodami na przetwarzanie danych;
12) realizuje się obowiązki informacyjne oraz zapewnia możliwość dochodzenia swoich praw przez osoby, których dane dotyczą;
13) przeprowadza się analizy ryzyka dla czynności przetwarzania danych;
14) przeprowadza się oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;
15) stosuje się procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych Osobowych – zarządzanie incydentami;
16) stosuje się Instrukcję Zarządzania Systemem Informatycznym, określoną odrębnym zarządzeniem.

3. W ramach zabezpieczenia danych osobowych ochronie podlegają następujące aktywa:
1) sprzęt komputerowy — serwer, komputery osobiste, drukarki i inne urządzenia zewnętrzne;
2) oprogramowanie — kody źródłowe, programy użytkowe, systemy operacyjne, narzędzia wspomagające i programy komunikacyjne;
3) dane zapisane na dyskach oraz dane podlegające przetwarzaniu w systemie;
4) hasła użytkowników;
5) pliki dziennych operacji systemowych i baz danych, kopie zapasowe i archiwa;
6) użytkownicy i administratorzy, którzy obsługują i używają system;
7) dokumentacja zawierająca dane systemu, opisująca jego zastosowanie, przetwarzane informacje, itp. oraz wydruki, związana z przetwarzaniem danych dokumentacja papierowa, z której dane są wprowadzane do systemu informatycznego lub też funkcjonują autonomicznie od niego.

4. W celu ochrony danych osobowych stosuje się następujące zabezpieczenia fizyczne:
1) umieszczenie komputerów w odpowiednio zabezpieczonych pomieszczeniach;
2) zabezpieczenie dostępu do pomieszczeń, w których odbywa się przetwarzanie danych osobowych przed osobami postronnymi drzwiami wyposażonymi w zamki;
3) wyposażenie budynku w monitoring i system alarmowy;
4) umieszczenie gaśnic w pobliżu obszarów przetwarzania danych;
5) zamykanie pomieszczeń po godzinach pracy;
6) składowanie w zamykanych szafach dokumentów i nośników zawierających dane osobowe.

5. Ochrona danych osobowych niezinformatyzowanych:
1) zbiory nieinformatyczne są odpowiednio zabezpieczone przed nieuprawnionym dostępem i zniszczeniem;

2) dokumenty i wydruki, zawierające dane osobowe, przechowuje się w zamykanych szafach;
3) wydruki robocze, błędne lub zdezaktualizowane są niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie lub zanonimizowanie.

6. Ustala się następujące minimalne zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe:

1) zamykanie drzwi do pomieszczeń na klucz;
2) zamykanie zawartości szaf i biurek, zawierającej dane osobowe, na klucz;
3) zamykanie okien po zakończeniu pracy;
4) monitorowanie korytarzy przez całą dobę, we wszystkie dni roku.

7. W razie potrzeby w Starostwie wdrażane są takie środki, jak pseudonimizacja, anonimizacja i szyfrowanie danych osobowych.

8. Starostwo rejestruje w RCP przypadki przekazywania danych poza Europejski Obszar Gospodarczy.

ROZDZIAŁ V

Administrator danych osobowych

§ 5. Administrator zobowiązuje się do podjęcia odpowiednich kroków, mających na celu zapewnienie prawidłowej ochrony danych osobowych, w szczególności do zapewnienia, że przez cały okres ich przetwarzania, dane będą:

1) przetwarzane zgodnie z prawem;
2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami;
3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania;
5) zabezpieczone środkami technicznymi i organizacyjnymi, które zapewniają rozliczalność, integralność oraz poufność danych;
6) przetwarzane w systemach informatycznych Administratora, w których stosuje się wysoki poziom bezpieczeństwa.

ROZDZIAŁ VI

Inspektor Ochrony Danych

§ 6. 1. W celu bieżącego monitorowania powszechnie obowiązujących przepisów prawa oraz dokumentów aktów wewnętrznych Starostwa ADO powołuje IOD.
2. Do zadań IOD należy w szczególności:

1) informowanie administratora, podmiotu przetwarzającego oraz pracowników przetwarzających dane osobowe o obowiązkach spoczywających na nich na mocy przepisów o ochronie danych osobowych i doradzanie im w tej sprawie;
2) prowadzenie RCP oraz RKCP i zapewnienie informacji o tych rejestrach;
3) prowadzenie rejestru upoważnień do przetwarzania danych osobowych oraz powierzeń przetwarzania danych osobowych;
4) monitorowanie przestrzegania przepisów i polityk wewnętrznych administratora (współadministratora lub podmiotów przetwarzających dane osobowe) w zakresie ochrony danych osobowych;
5) prowadzenie szkoleń pracowników z zakresu ochrony danych osobowych;
6) zapewnienie realizacji obowiązku informacyjnego wynikającego z przepisów o ochronie danych osobowych;
7) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
8) współpraca z organem nadzorczym - Prezesem Urzędu Ochrony Danych Osobowych;
9) pełnienie roli punktu kontaktowego dla osób, których dane dotyczą we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy przepisów o ochronie danych osobowych;
10) kontrolowanie treści dokumentów przeznaczonych do publikacji w Biuletynie Informacji Publicznej pod względem ich zgodności z przepisami z zakresu ochrony danych osobowych;
11) monitorowanie Biuletynu Informacji Publicznej pod kątem zawartości danych osobowych, z uwzględnieniem dokonania minimum dwukrotnie w ciągu roku przeglądu wybranej części zasobów pod kątem zapewnienia przetwarzania danych zgodnie z zasadą ograniczenia przechowania.

3. IOD posiada uprawnienia do:
1) wydawania poleceń pracownikom przetwarzającym dane pod zwierzchnictwem ADO w zakresie stosowania określonych zabezpieczeń tych danych;
2) czasowego wstrzymania przetwarzania danych osobowych przez pracownika ADO na zasadach określonych w polityce – w przypadku naruszenia bezpieczeństwa danych osobowych skutkującego wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, których dotyczą.

4. Osoby, których dane są przetwarzane, posiadają możliwość skontaktowania się z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy zapisów zawartych w RODO. Dane kontaktowe IOD są zamieszczone na stronie internetowej administratora oraz w innych miejscach, w których osoby te mogą się z nimi zapoznać.

5. W trakcie realizacji swoich zadań IOD posiada, w niezbędnym zakresie, dostęp do wszystkich danych osobowych przetwarzanych w Starostwie.

ROZDZIAŁ VII

Dostęp do przetwarzania danych osobowych

§ 7. 1. Przetwarzanie danych osobowych jest możliwe wyłącznie po udzieleniu upoważnienia do przetwarzania danych osobowych, wystawionego przez administratora.
2. W tym celu, przed dopuszczeniem pracownika do pracy przy przetwarzaniu danych osobowych:

1) bezpośredni przełożony pracownika lub osoba odpowiedzialna za realizację umowy, w ramach której mają być przetwarzane dane osobowe pismem wewnętrznym przekazanym za pomocą eKancelarii wnioskuje do IOD o przeszkolenie i przygotowanie upoważnienia w zakresie przetwarzania danych osobowych dla osoby zatrudnionej w Starostwie (załącznik nr 1), mającej odbyć staż, praktykę, wolontariat lub wykonującej pracę w ramach zawieranych umów lub pełnionych funkcji (załącznik nr 2);
2) IOD zapoznaje pracownika z przepisami dotyczącymi ochrony danych osobowych oraz uregulowaniami wewnętrznymi w tym zakresie i przyjmuje od osoby zatrudnionej
   w Starostwie (załącznik nr 3) mającej odbyć staż, praktykę, wolontariat lub wykonującej pracę w ramach zawieranych umów lub pełnionych funkcji (załącznik nr 4) podpisane oświadczenie;
3) ADO udziela upoważnienia do przetwarzania danych osobowych, sporządzane według wzoru stanowiącego załącznik nr 5 do polityki, które zostaje zaewidencjonowane w rejestrze upoważnień prowadzonym przez IOD, w uzasadnionych przypadkach dopuszcza się stosowanie innego wzoru;
4) przez IOD przekazana zostaje informacja o zakończeniu szkolenia do bezpośredniego przełożonego pracownika oraz kadr, co pozwala przełożonemu za pomocą pisma wewnętrznego wnioskować do właściwego administratora systemu informatycznego o nadanie uprawnień.

§ 8. 1. Zakres upoważnienia do przetwarzania danych osobowych obejmuje:

1) poziom [1] – uprawnienia tylko do zbierania, utrwalania, porządkowania, przechowywania, pobierania, przeglądania, dopasowywania lub łączenia;
2) poziom [2] – uprawnienia do adaptowania lub modyfikowania, organizowania, wykorzystywania;
3) poziom [3] – uprawnienia do ujawniania poprzez przesłanie, rozpowszechniania lub innego rodzaju udostępniania;
4) poziom [4] – uprawnienia do usuwania lub niszczenia, ograniczania.

2. Wyższe poziomy uprawnień, o których mowa w ust. 3, uwzględniają uprawnienia poziomów niższych.
3. Rejestr wydanych upoważnień do przetwarzania danych osobowych prowadzony jest w formie elektronicznej, przy pomocy eKancelarii.
4. Dostęp do czynności przetwarzania organizowany jest w odniesieniu do stanowiska służbowego pracownika.

5. Oświadczenia i upoważnienia, o których mowa powyżej przechowuje się wraz z dokumentacją pracowniczą lub w aktach spraw dotyczących zawarcia i wykonania umowy.
6. Odwołania lub zmiany upoważnienia dokonuje ADO na wniosek osoby odpowiedzialnej za realizację umowy, w ramach której mają być przetwarzane dane osobowe, naczelnika, samodzielnego stanowiska pracy lub bezpośredniego przełożonego pracownika.

ROZDZIAŁ VIII

Szkolenia

§ 9. 1. Szkolenia przeprowadzane są zgodnie z planem rocznym lub na żądanie ADO, gdy zaistnieje taka potrzeba.
2. Szczegółowy zakres szkolenia w odniesieniu do stanowisk ustala IOD.

ROZDZIAŁ IX

Rejestr czynności przetwarzania

§ 10. 1. RCP stanowi formę dokumentowania czynności przetwarzania danych oraz umożliwia realizację zasady rozliczalności.
2. Prowadzenie RCP powierzone zostało przez administratora IOD. Przy jego pomocy ADO inwentaryzuje i kontroluje sposób, w jaki w przetwarza się dane osobowe.
3. W RCP, dla każdej czynności przetwarzania danych, która uznana została za odrębną, odnotowuje się co najmniej:

1) imię i nazwisko, dane kontaktowe administratora oraz IOD;
2) nazwy czynności przetwarzania;
3) właścicieli czynności przetwarzania;
4) cele przetwarzania;
5) kategorie osób, których dane dotyczą;
6) kategorie danych osobowych;
7) planowane terminy usunięcia danych;
8) nazwę oraz dane kontaktowe współadministratorów;
9) nazwę podmiotu przetwarzającego i dane kontaktowe;
10) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione;
11) opis technicznych i organizacyjnych środków bezpieczeństwa;
12) informację o transferze danych do kraju trzeciego lub organizacji międzynarodowej oraz wskazanie odpowiednich zabezpieczeń w przypadku takiego transferu.

4. RCP, prowadzony w formie elektronicznej, może zawierać także kolumny nieobowiązkowe, w których informacje uzupełniane są w miarę wiedzy i możliwości.
5. Dane w RCP umieszczane, zmieniane i usuwane są na podstawie informacji przekazywanych pismem wewnętrznym przez naczelników wydziałów i samodzielne stanowiska pracy do IOD. Po uzyskaniu akceptacji wnioskowanych zmian przez ADO w eKancelarii są one wprowadzane do RCP.

ROZDZIAŁ X

Rejestr kategorii czynności przetwarzania

§ 11. 1. RKCP stanowi formę dokumentowania kategorii czynności przetwarzania danych w imieniu administratora.

2. Prowadzenie RKCP powierzone zostało przez administratora IOD.

3. W RKCP, dla każdej kategorii przetwarzania danych, która uznana została za odrębną, odnotowuje się co najmniej:

1) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
2) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa;
3) imię i nazwisko lub nazwę oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający,
4) nazwę i dane kontaktowe przedstawiciela administratora oraz IOD;
5) informację o transferze danych do kraju trzeciego lub organizacji międzynarodowej oraz wskazanie odpowiednich zabezpieczeń w przypadku takiego transferu.

4. RKCP może zawierać także kolumny nieobowiązkowe, w których informacje uzupełniane są w miarę wiedzy i możliwości.

5. Dane w RKCP umieszczane, zmieniane i usuwane są na podstawie informacji przekazywanych w formie elektronicznej przez naczelników wydziałów i samodzielne stanowiska pracy IOD. Po uzyskaniu akceptacji wnioskowanych zmian przez ADO w eKancelarii są one wprowadzane do RKCP.

ROZDZIAŁ XI

Obowiązki informacyjne

§ 12. 1. W Starostwie:

1) dba się o czytelność i prosty styl przekazywanych informacji osobom, których dane są przetwarzane oraz dba się o dotrzymywanie prawnych terminów realizacji obowiązków względem tych osób;
2) określa się zgodne z prawem i efektywne sposoby wykonywania obowiązków informacyjnych oraz ich treść;
3) informuje się odbiorców danych o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych, jeśli nie wymaga to niewspółmiernie dużego wysiłku i jest możliwe;
4) bez zbędnej zwłoki zawiadamia się osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby;
5) określa się sposób informowania osób o przetwarzaniu danych niezidentyfikowanych, m.in. poprzez tabliczki informacyjne.

2. Za prawidłową realizację obowiązków określonych w ust. 1 odpowiadają naczelnicy, kierownicy oraz samodzielne stanowiska pracy.

§ 13. 1. Osoby, których dane są przetwarzane informowane są o:

1) przedłużeniu ponad jeden miesiąc terminu na rozpatrzenie żądania tej osoby;
2) przetwarzaniu jej danych, przy pozyskiwaniu danych od tej osoby;
3) przetwarzaniu jej danych, przy pozyskiwaniu danych o tej osobie niebezpośrednio od niej;
4) planowanej zmianie celu przetwarzania danych;
5) uchyleniu ograniczenia przetwarzania zanim ono nastąpi;
6) prawie sprzeciwu względem przetwarzania danych najpóźniej przy pierwszym kontakcie z tą osobą.

2. Za prawidłową realizację obowiązków określonych w ust. 1 odpowiadają naczelnicy, kierownicy oraz samodzielne stanowiska pracy.

ROZDZIAŁ XII

Realizacja praw osób, których dane dotyczą

§ 14. 1. Przy przetwarzaniu danych osobowych uwzględniane są następujące prawa osób, których dane dotyczą:

1) prawo dostępu do danych - na żądanie osoby, po uprzedniej weryfikacji tożsamości tej osoby, informuje się ją o tym, czy jej dane są przetwarzane oraz o szczegółach przetwarzania, które wynikają z treści art. 15 RODO. Administrator spełnia ten obowiązek poprzez dostarczenie bezpłatnie jednej kopii jej danych osobowych. Za każdą kolejną kopię pobrana zostaje opłata w trybie i wysokości określonych w procedurze Systemu Zarządzania Starostwem dotyczącej tego zagadnienia. W przypadku możliwego naruszenia praw i wolności innych osób, odmawia się wydania kopii danych;
2) prawo do sprostowania danych – osoba, której dane dotyczą, ma prawo żądania niezwłocznego sprostowania tych danych osobowych, jeśli są nieprawidłowe lub uzupełnienia niekompletnych danych, jeśli jest to zgodne z celem ich przetwarzania;
3) prawo do usunięcia danych („prawo do bycia zapomnianym”) – osoba, której dane dotyczą, ma prawo żądania usunięcia jej danych osobowych w szczególnych okolicznościach:
    a) dane nie są niezbędne do celów, w których zostały zebrane, ani przetwarzane w innych zgodnych z prawem celach;
    b) zgoda na ich przetwarzanie została cofnięta, a nie ma innej legalnej podstawy ich przetwarzania;
    c) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych;
    d) dane były przetwarzane niezgodnie z prawem;
    e) konieczność usunięcia wynika z obowiązku prawnego, któremu podlega administrator.

    Jeśli zachodzi jedna z wyżej wymienionych przesłanek, administrator usuwa te dane niezwłocznie. Zapewnione zostały procedury, które mają na celu efektywną realizację prawa do usunięcia danych. Wdraża się sposoby postępowania, które mają na celu

sprawdzenie, czy nie zachodzi jeden z wyjątków, które wyłączają prawo do bycia zapomnianym, a mianowicie, gdy przetwarzanie tych danych jest niezbędne do:

a) korzystania z prawa do wolności wypowiedzi i informacji;
b) wywiązania się z prawnego obowiązku, który leży na administratorze lub wykonania zadania publicznego lub w ramach władzy publicznej;
c) celów archiwalnych w interesie publicznym, celów badań naukowych, historycznych i statystycznych;
d) ustalenia, dochodzenia lub obrony roszczeń.

W przypadku usunięcia danych informuje się osobę, której dane dotyczą, o odbiorcach danych na żądanie tej osoby. Jeśli dane, które mają zostać usunięte zostały przez administratora upublicznione, to, jeśli jest to możliwe, podejmuje on działania, aby poinformować innych administratorów o żądaniu usunięcia tych danych.

4) prawo do ograniczenia przetwarzania danych – osoba, której dane dotyczą, ma prawo żądać od administratora ograniczenia przetwarzania danych w następujących sytuacjach:
   a) kwestionowana jest prawidłowość danych (na okres pozwalający sprawdzić prawidłowość tych danych);
   b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
   c) administrator nie potrzebuje już danych osobowych w celu przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
   d) osoba, której dane dotyczą wniosła sprzeciw wobec przetwarzania (do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą).

   Jeżeli przetwarzanie danych zostało skutecznie ograniczone, przechowywanie lub przetwarzanie danych może wystąpić wyłącznie w celu ustalenia, dochodzenia, obrony roszczeń, jednakże inne przetwarzanie dozwolone jest wyłącznie za zgodą osoby, której dane dotyczą. W razie uchylenia ograniczenia przetwarzania osoba, której dane dotyczą jest o tym fakcie informowana. W przypadku ograniczenia przetwarzania danych informuje się osobę o odbiorcach danych, na żądanie tej osoby.
5) prawo do przenoszenia danych – osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie, który nadaje się do odczytu maszynowego, dane osobowe jej dotyczące, które dostarczyła administratorowi oraz ma prawo żądać by te dane zostały przesłane innemu administratorowi, jeśli przetwarzanie odbywa się w sposób zautomatyzowany na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy;
6) prawo do sprzeciwu – osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw związany z jej szczególną sytuacją wobec przetwarzania danych osobowych, które oparte jest na powierzeniu administratorowi realizacji zadania publicznego lub wykonywania władzy publicznej lub w oparciu o prawnie uzasadniony interes. Administrator musi uwzględnić ten sprzeciw, 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 i obrony roszczeń;

7) prawo do niepodlegania zautomatyzowanemu podejmowaniu decyzji – osoba, której dane dotyczą, ma prawo do tego, żeby nie podlegać decyzjom, które opierają się wyłącznie na zautomatyzowanym przetwarzaniu (w tym profilowaniu) i wywołują wobec tej osoby skutki prawne lub wpływają na nią w istotny sposób. Zapewnione zostało prawo do interwencji ludzkiej, chyba że wyżej wspomniana decyzja jest:
   a) niezbędna do zawarcia umowy między osobą, której dane dotyczą, a administratorem;
   b) dozwolona przepisami prawa;
   c) oparta na wyraźnej zgodzie osoby, której dane dotyczą;
8) prawa osób trzecich - realizując prawa osób, których dane dotyczą, wprowadzane są gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste). Administrator może się zwrócić do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

2. W razie żądania realizacji praw przez osobę, której dane nie są przetwarzane w Starostwie, należy poinformować taką osobę o nieprzetwarzaniu jej danych.
3. W razie odmowy spełnienia żądania, administrator informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.
4. Za prawidłową realizację praw osób, których dane dotyczą określonych w ust. 1 odpowiadają naczelnicy, kierownicy oraz samodzielne stanowiska pracy.

ROZDZIAŁ XIII

Powierzenie przetwarzania danych

§ 15. 1. Administrator przed powierzeniem danych osobowych ustala z każdym podmiotem zasady takiego powierzenia.
2. Zapisy dotyczące powierzenia przetwarzania danych osobowych mogą stanowić odrębną umowę w stosunku do umowy głównej, normującej kwestie wykonania usługi, dostawy, roboty budowlanej lub stanowić jej element.
3. Umowa powierzenia danych osobowych powinna zawierać zapisy dotyczące:

1) przedmiotu przetwarzania;
2) czasu trwania przetwarzania;
3) charakteru przetwarzania;
4) celu przetwarzania;
5) rodzaju danych osobowych;
6) kategorii osób, których dane dotyczą;
7) obowiązków i praw administratora danych;
8) obowiązków, aby:

a) przetwarzane dane osobowe były wyłącznie na udokumentowane polecenie administratora,
b) osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,
c) procesor podejmował wszelkie środki wymagane na mocy art. 32 RODO,
d) procesor przestrzegał warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w art. 28 ust. 2 i 4 RODO,
e) procesor pomagał 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 rozdziale III RODO,
f) procesor pomagał administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO,
g) procesor po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych
h) procesor udostępniał administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków,
i) procesor umożliwiał administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów i przyczyniał się do nich.

4. Wzór umowy powierzenia danych osobowych stanowi załączniki nr 6 do polityki. Dopuszcza się stosowanie zewnętrznych druków umów. Umowy rejestrowane są w systemie eKancelaria.
5. Jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający korzystać będzie z usług innego podmiotu przetwarzającego, wówczas niezbędne jest wyrażenie zgody na podpowierzenie oraz zobowiązanie podmiotu przetwarzającego do zawarcia analogicznej umowy powierzenia jak ta, którą zawarł administrator z tym podmiotem przetwarzającym.
6. Maksymalny czas zgłoszenia naruszenia danych osobowych przez podmiot przetwarzający wynosi 24 godziny.

ROZDZIAŁ XIV

Procedura oceny kontrahentów

§ 16. 1. W przypadku, gdy przetwarzanie ma być dokonywane przez podmiot trzeci w imieniu administratora korzysta on wyłącznie z usług takich podmiotów, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
2. Po ustaleniu, że w danym procesie dochodzi do powierzenia przetwarzania danych osobowych, właściciel czynności przetwarzania obowiązany jest do dokonania oceny czy podmiot, któremu mają zostać powierzone dane osobowe zapewnia wystarczające gwarancje

wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
3. W stosunku do podmiotów, którym ma być podpowierzone przetwarzanie danych osobowych, stosuje się te same zasady, co w stosunku do podmiotów, którym są te dane powierzane.
4. Ocena realizacji wymagania bezpieczeństwa, przez podmiot któremu administrator zamierza powierzyć dane osobowe w dokonywana jest za pomocą odebrania od osoby reprezentującej podmiot, któremu zamierza się powierzyć dane osobowe, oświadczenia o stosowaniu odpowiednich środków technicznych i organizacyjnych, które realizują wymogi RODO oraz zapewniają ochronę danych osób, których dane dotyczą, w szczególności zapewniających poufność, integralność oraz dostępność danych osobowych.

ROZDZIAŁ XV

Postępowanie w przypadku naruszenia lub podejrzenia naruszenia danych osobowych

§ 17. 1. Poniższe postanowienia mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych przetwarzanych w systemach informatycznych, jak i formie papierowej.
§ 18. Za okoliczności, które uznaje się za naruszenie lub podejrzenie naruszenia ochrony systemu przetwarzającego dane osobowe, uważa się w szczególności:

1) nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują;
2) nieuprawnione naruszenie lub próby naruszenia poufności, integralności i rozliczalności danych i systemu;
3) niezamierzoną zmianę lub utratę danych zapisanych na kopiach zapasowych;
4) nieuprawniony dostęp do danych osobowych wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu;
5) udostępnienie osobom nieupoważnionym danych osobowych;
6) inny stan systemu informatycznego lub pomieszczeń, niż pozostawiony przez użytkownika po zakończeniu pracy;
7) wydarzenia losowe, obniżające poziom ochrony systemu (np. brak zasilania lub pożar);
8) kradzież lub zagubienie sprzętu informatycznego lub nośników zewnętrznych zawierających dane osobowe (np. wydruków komputerowych, płyt CD, dysków twardych, pamięci zewnętrznych).

§ 19. Przed przystąpieniem do pracy pracownicy dokonują sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy. Pracownicy zwracają szczególną uwagę, czy nie zaszły okoliczności wskazujące na naruszenie lub próby naruszenia ochrony danych osobowych.
§ 20. 1. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie ochrony danych osobowych pracownik bezzwłocznie powiadamia o tym fakcie swojego bezpośredniego przełożonego, administratora oraz IOD.

2. Do czasu przybycia administratora lub osoby wyznaczonej przez administratora do zbadania sprawy, zgłaszający:

1) powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów;
2) zabezpiecza elementy systemu informatycznego lub dokumentacji papierowej, przede wszystkim poprzez uniemożliwienie dostępu do nich osobom nieupoważnionym;
3) podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.

3. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, administrator lub osoba wyznaczona przez administratora do zbadania sprawy po przybyciu na miejsce:

1) ocenia zastałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane osobowe oraz stan urządzeń, a także szacuje wielkość negatywnych następstw incydentu;
2) wysłuchuje relacji osoby, która dokonała powiadomienia oraz innych osób związanych z incydentem;
3) podejmuje decyzje o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych.

4. Osoba dokonująca czynności, o których mowa powyżej, sporządza raport z przebiegu zdarzenia, w którym powinny się znaleźć w szczególności informacje o:

1) osobie powiadamiającej o zaistniałym zdarzeniu;
2) dacie i godzinie powiadomienia;
3) godzinie pojawienia się w pomieszczeniach, w których przetwarzane są dane;
4) sytuacji, jaką zastała;
5) przyczynach wystąpienia zdarzenia;
6) podjętych działaniach i ich uzasadnieniu;
7) stanie systemu informatycznego lub dokumentacji papierowej po podjęciu działań naprawczych;
8) wnioskach dotyczących ograniczenia możliwości ponownego wystąpienia naruszenia ochrony danych osobowych.

5. Wzór raportu stanowi załącznik nr 7 do polityki.
6. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik może kontynuować pracę dopiero po otrzymaniu pozwolenia od administratora lub osoby przez niego wyznaczonej.
7. W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej dyscypliny pracy administrator wyjaśnia wszystkie okoliczności incydentu i podejmuje stosowne działania wobec osób, które dopuściły się wskazanego naruszenia.
8. Po zakończeniu czynności naprawczych system informatyczny powinien utrzymać poziom ochrony nie niższy niż przed wystąpieniem incydentu związanego z naruszeniem ochrony danych osobowych.

§ 21. W przypadku odebrania zgłoszenia nieuprawnionego ujawnienia danych osobowych mogącego stanowić naruszenie sporządzany jest raport. Wzór raportu stanowi załącznik nr 8 do polityki.

ROZDZIAŁ XVI

Zgłoszenie naruszenia danych osobowych PUODO

§ 22. 1. Administrator wszelkimi sposobami dąży do zapobiegania sytuacjom skutkującym naruszeniem danych osobowych oraz zminimalizowania powstałych szkód, mając na uwadze, że w przypadku braku odpowiedniej i szybkiej reakcji naruszenie ochrony danych osobowych może skutkować: powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych, takich jak: utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne.
2. W przypadku naruszenia ochrony danych osobowych administrator, dokonuje dwóch zgłoszeń:

1) bez zbędnej zwłoki, jednak nie później niż w czasie 72 godzin po stwierdzeniu naruszenia, zgłasza to organowi nadzorczemu - Prezesowi Urzędu Ochrony Danych Osobowych - chyba że mało prawdopodobne jest, by to naruszenie skutkowało ryzykiem ingerencji w prawa lub wolności osób fizycznych. Jeśli zgłoszenie przekazywane jest później niż w ciągu 72 godzin, dołącza się do niego wyjaśnienie przyczyn opóźnienia;
2) w przypadku zdarzeń naruszających bezpieczeństwo sieci zgłasza incydent niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT).

3. Termin „bez zbędnej zwłoki” ustalany jest z uwzględnieniem w szczególności charakteru i wagi naruszenia ochrony danych osobowych, jego konsekwencji oraz niekorzystnych skutków dla osoby, której dane dotyczą.
4. Zgłoszenie, o którym mowa w ust. 2 pkt. 1 zawiera co najmniej:

1) opis charakteru naruszenia ochrony danych osobowych, w tym wskazanie kategorii i przybliżonej liczby osób, których dane dotyczą oraz kategorii i przybliżonej liczby wpisów danych, których dotyczy naruszenie;
2) dane kontaktowe IOD lub innego podmiotu kontaktowego, który posiada wiedzę na temat naruszenia;
3) opis możliwych konsekwencji tego naruszenia;
4) środki zastosowane lub proponowane przez administratora w celu usunięcia naruszenia lub zmniejszenia jego negatywnych skutków.

5. W Starostwie prowadzony jest rejestr oraz dokumentacja wszelkich naruszeń ochrony danych osobowych (okoliczności, skutki, podjęte działania zaradcze), zgodnie z zasadą rozliczalności.

6. Administrator wdraża wszelkie odpowiednie techniczne środki ochrony i wszelkie odpowiednie środki organizacyjne, które umożliwiają jak najszybsze stwierdzenie naruszenia ochrony danych osobowych i poinformowanie organu nadzorczego oraz osoby, której dane dotyczą, zgodnie z treścią rozdziału XVII.

ROZDZIAŁ XVII

Zawiadamianie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych

§ 23. 1. W przypadku, w którym administrator, zgodnie z zasadą rozliczalności stwierdzi, że naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, informuje bez zbędnej zwłoki osobę, której dane dotyczą, o takim naruszeniu. Zawiadomienie to musi zawierać minimalnie informacje określone w § 19 ust. 4 pkt. 2-4.

2. Zawiadomienie to nie jest wymagane, gdy:

1) zastosowano odpowiednie środki techniczne i organizacyjne ochrony, jak np. szyfrowanie danych, które uniemożliwiają odczyt danych osobom nieuprawnionym;
2) zastosowano po naruszeniu środki eliminujące wysokie ryzyko naruszenia praw lub wolności osób fizycznych;
3) konieczne byłoby włożenie niewspółmiernie dużego wysiłku, aby taką osobę poinformować, w takim przypadku wystarczający jest publiczny komunikat lub podobny środek, aby poinformować taką osobę w równie skuteczny sposób.

3. Zawiadomienie, o którym mowa w ust. 2, może zostać przekazane również w formie elektronicznej.

ROZDZIAŁ XVIII

Nadzorowanie zgodności

§ 24. 1. W celu utrzymania zgodności z RODO oraz niniejszej polityki, IOD tworzy roczny plan audytów, dopuszcza się możliwość przeprowadzenia audytu poza planem na polecenie ADO.

2. Wzór planu audytu stanowi załącznik nr 9 do polityki.

3. Zakres, sposób przeprowadzenia audytu oraz sposób dokumentowania ustaleń audytu określany jest przez IOD.

4. Po zakończeniu audytu sporządzany jest raport audytowy.

5. Raport, o którym mowa w ust. 1 powinien zawierać:

1) pełną nazwę administratora i adres jego siedziby;
2) imię i nazwisko IOD;
3) wykaz czynności podjętych przez IOD w toku sprawdzenia oraz imiona, nazwiska i stanowiska osób biorących udział w tych czynnościach;
4) datę rozpoczęcia i zakończenia audytu;
5) określenie przedmiotu i zakresu audyt;

6) opis stanu faktycznego stwierdzonego w toku sprawdzenia oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych;
7) stwierdzone nieprawidłowości w zakresie objętym audytem wraz z planowanymi lub podjętymi działaniami przywracającymi stan zgodny z RODO oraz zapisami niniejszej polityki;
8) wyszczególnienie załączników stanowiących składową część audytu;
9) datę i miejsce sporządzenia oraz podpis IOD i osoby audytowanej.

6. Raport przekazany zostaje do podpisania osobie audytowanej, która w terminie 7 dni może odnieść się do jego treści.
7. Po przeanalizowaniu i rozpatrzeniu uwag dokument zostaje uzupełniony stosowną adnotacją.
8. W przypadku wydania zaleceń podlegają one sprawdzeniu przez IOD poprzez odebranie pisemnych informacji o sposobie ich wykonania. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenie ochrony danych osobowych stosuje się zasady opisane w rozdziałach od XV do XVII polityki.

ROZDZIAŁ XIX

Obowiązki pracowników

§ 25. 1. Pracownicy zobowiązani są do:
1) przetwarzania danych osobowych zgodnie z RODO, ustawą o ochronie danych osobowych, wszystkimi regulacjami wewnętrznymi w tym zakresie oraz celem ich przetwarzania;
2) zachowania w tajemnicy danych osobowych oraz sposobu ich zabezpieczenia, także po ustaniu zatrudnienia lub innego zobowiązania wynikającego z zawartych umów;
3) zabezpieczenia danych osobowych przed ich utratą, uszkodzeniem, zniszczeniem, zmianą lub udostępnieniem osobom nieupoważnionym przez:
   a) właściwe użytkowanie systemów informatycznych, w tym nieujawnianie identyfikatorów i haseł dostępu,
   b) zabezpieczenie papierowej dokumentacji m.in. poprzez przechowywanie jej w miejscach niedostępnych dla osób postronnych
   - także w przypadku pracy zdalnej;
4) niszczenia wszystkich niepodlegających archiwizacji danych osobowych, zgodnie z zasadami opisanymi w Rozdziale XX polityki;
5) uczestniczenia w szkoleniach z zakresu ochrony danych osobowych;
6) współpracy z IOD w zakresie ochrony danych osobowych;
7) stosowania polityk czystego:
   a) biurka – polegającej na zabezpieczaniu dokumentów i nośników na stanowisku pracy przed wglądem osób nieupoważnionych,
   b) ekranu – polegającej na uniemożliwieniu osobom niepowołanym wglądu do danych wyświetlanych na ekranach,

c) kosza - polegającej na niewyrzucaniu dokumentów do kosza na śmieci i niszczeniu ich w taki sposób, aby odczytanie treści nie było możliwe,
d) wydruku – polegającej na zabieraniu materiałów z urządzeń zaraz po ich wydrukowaniu, skserowaniu lub zeskanowaniu;

8) wylogowania się z systemu informatycznego i wyłączenia sprzętu komputerowego, a także zabezpieczenia stanowiska pracy poprzez umieszczenie dokumentów i nośników zawierających dane osobowe w zamykanych szafach oraz zamknięcie okien i drzwi przed opuszczeniem stanowiska pracy;
9) zapewnienia odpowiedniego okresu przechowywania informacji zgromadzonych w Biuletynie Informacji Publicznej i stosowania zasady ograniczenia przechowywania danych osobowych, w szczególności poprzez określenie okresu niezbędnego do osiągnięcia celu przetwarzania oraz terminu usunięcia danych z BIP;
10) zgłoszenia drogą e-mailową Oddziałowi Obsługi Informatycznej stwierdzonych nieścisłości w informacjach opublikowanych w Biuletynie Informacji Publicznej Powiatu Słupskiego.

2. Za naruszenie obowiązków w zakresie danych osobowych pracownicy podlegają odpowiedzialności dyscyplinarnej lub porządkowej, bądź wynikającej z zawartych umów lub innych dokumentów, na podstawie których przetwarzają dane osobowe.

ROZDZIAŁ XX
Retencja danych

§ 26. 1. Administrator podejmuje starania, aby dane osobowe były adekwatne, stosowne oraz ograniczone do tego, co niezbędne w stosunku do celów, w których są przetwarzane.

2. Pracownicy zobowiązani są do stosowania terminów usuwania danych określonych w RCP i RKCP.

3. Usuwanie danych osobowych następuje:

1) w przypadku dokumentów papierowych oraz optycznych nośników danych (płyty CD/DVD) - za pomocą niszczarki do papieru lub korzystając z usług wyspecjalizowanych firm, oferujących usługi w tym zakresie;

2) w przypadku sprzętu komputerowego - zgodnie z zapisami zarządzenia nr 73/2022 Starosty Słupskiego z dnia 26 października 2022 r. w sprawie Instrukcji Zarządzania Systemem Informatycznym;

3) w przypadku danych zamieszczonych w Biuletynie Informacji Publicznej Powiatu Słupskiego – poprzez ich usunięcie po zrealizowaniu celu przetwarzania danych osobowych;

4) w przypadku innych nośników danych (np. pendrivy i telefony komórkowe) - poprzez czyszczenie ich przez pracowników merytorycznych lub korzystając z usług wyspecjalizowanych firm, oferujących usługi w tym zakresie.

Z przeprowadzonej czynności sporządza się notatkę służbową.

ROZDZIAŁ XXI

Praca zdalna

§ 27 1. W przypadku wykonywania pracy zdalnej pracownik zobowiązany jest do:

1) wykorzystywania podczas pracy zdalnej sprzętu komputerowego przekazanego przez pracodawcę;

2) właściwego zabezpieczenia danych osobowych przed zniszczeniem oraz utratą i przetwarzania ich wyłącznie w celach służbowych, zabronione jest wykonywanie skanów i wydruków w miejscu pracy zdalnej;

3) zabezpieczenia dostępu do sprzętu służbowego oraz posiadanych danych i informacji, także na nośnikach papierowych przed osobami postronnymi, w tym wspólnie z nim zamieszkującymi;

4) zachowania poufności informacji, w szczególności podczas służbowych rozmów telefonicznych i wideokonferencji;

5) wyłączenia opcji nagrywania i przechowywania - w przypadku korzystania z programów z funkcją wideokonferencji;

6) przetwarzania danych osobowych zgodnie z przepisami powszechnie obowiązującego prawa, w szczególności RODO i ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781) oraz wprowadzonych i wdrożonych do stosowania procedur postępowania i wewnętrznych polityk.

2. Na wniosek naczelnika, samodzielnego stanowiska pracy lub bezpośredniego przełożonego pracownika IOD przeprowadza instruktaż i szkolenie w zakresie stosowania procedur ochrony danych osobowych w czasie wykonywania pracy zdalnej. Szkolenie takie może odbyć się w formie wideokonferencji.

3. Kontrola przestrzegania wymogów w zakresie bezpieczeństwa i ochrony informacji ma charakter zdalny i polega na monitorowaniu korzystania przez pracownika ze służbowego sprzętu.

4. Pracodawca może w każdym czasie przeprowadzić kontrolę doraźną wykonywania pracy zdalnej u pracownika, w ustalonym miejscu jej świadczenia. Przepisy zarządzenia Nr 63/2019 Starosty Słupskiego z dnia 7 czerwca 2019 r. w sprawie ustalenia Regulaminu działalności kontrolnej wykonywanej przez Starostwo Powiatowe w Słupsku stosuje się odpowiednio.

5. Pracodawca zapewnia w pełnym zakresie zdalną instalację, konserwację, aktualizację oprogramowania i serwis powierzonego pracownikowi sprzętu komputerowego. W przypadku braku możliwości uzyskania wsparcia zdalnie pracownik zobowiązuje się do stawienia w siedzibie pracodawcy, wraz z użytkowanym sprzętem, w uprzednio ustalonym terminie.

6. Pracownik ma prawo do uzyskania wsparcia technicznego poprzez zgłoszenie wszelkich uzasadnionych potrzeb w tym zakresie za pośrednictwem modułu Helpdesk w aplikacji Statlook Assistant lub telefonicznie.

7. W przypadku przeprowadzanej inwentaryzacji pracownik zobowiązany jest do dostarczenia sprzętu komputerowego do siedziby pracodawcy na jego polecenie.

ROZDZIAŁ XXII

Postanowienia końcowe

§ 28. 1. Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w polityce może być podstawą rozwiązania stosunku pracy bez wypowiedzenia z osobą, która dopuściła się naruszenia.
2. W sprawach nieuregulowanych w polityce mają zastosowanie przepisy aktów prawnych dotyczących ochrony danych osobowych, w szczególności RODO.

3. Pracownicy zobowiązani są do zapoznania z treścią tego dokumentu i potwierdzają ten fakt poprzez odczyt treści komunikatu zawierającego niniejszy dokument w eKancelarii.

Załącznik nr 1
do Polityki Ochrony Danych
Osobowych

....., ……. r.

(miejscowość) (data)

Inspektor Ochrony Danych

w miejscu

WNIOSEK

Wnioskuję o przeszkolenie/przygotowanie upoważnienia* dotyczącego udzielenia/zmiany/odwołania* uprawnień do przetwarzania danych osobowych dla Pani/Pana ……

zatrudnionej/zatrudnionego* w Starostwie Powiatowym w Słupsku na stanowisku ……/

z powodu przyjęcia do pracy/przejścia na inne stanowisko/zmiany zakresu obowiązków/zwolnienia z pracy/innego* *(jakiego?)*

……

Wnioskowany zakres upoważnienia *(także czynności w ramach zastępstwa):*

Lp.	Nazwa czynność przetwarzania *(wykazanej w RCP i/lub w RKCP)*	Zakres upoważnienia [1] [2] [3] [4]**	Czas trwania upoważnienia	Udzielenie/zmiana/ odwołanie upoważnienia

……

(Podpis)

* Niepotrzebne skreślić

** Poziom [1] – uprawnienia tylko do zbierania, utrwalania, porządkowania, przechowywania, pobierania, przeglądania, dopasowywania lub łączenia.

Poziom [2] – uprawnienia do adaptowania lub modyfikowania, organizowania, wykorzystywania.

Poziom [3] – uprawnienia do ujawniania poprzez przesłanie, rozpowszechniania lub innego rodzaju udostępniania.

Poziom [4] – uprawnienia do usuwania lub niszczenia, ograniczania.

Wyższe poziomy uprawnień uwzględniają uprawnienia poziomów niższych.

Załącznik nr 2
do Polityki Ochrony Danych
Osobowych

....., ……. r.

(miejscowość) (data)

Inspektor Ochrony Danych

w miejscu

WNIOSEK

Wnioskuję o przeszkolenie/przygotowanie upoważnienia* dotyczącego udzielenia/zmiany/odwołania* uprawnień do przetwarzania danych osobowych Pani/Pana ……

- odbywającej/odbywającego w Starostwie Powiatowym w Słupsku staż/praktykę/wolontariat*
- w związku z zawarciem umowy …….. z dnia …….*
- w związku z objęciem funkcji …….. .

Wnioskowany zakres upoważnienia:

Lp.	Nazwa czynność przetwarzania (wykazanej w RCP i/lub w RKCP)	Zakres upoważnienia [1] [2] [3] [4]**	Czas trwania upoważnienia	Udzielenie/zmiana/ odwołanie upoważnienia

……
(Podpis)

* Niepotrzebne skreślić
** Poziom [1] – uprawnienia tylko do zbierania, utrwalania, porządkowania, przechowywania, pobierania, przeglądania, dopasowywania lub łączenia.
Poziom [2] – uprawnienia do adaptowania lub modyfikowania, organizowania, wykorzystywania.
Poziom [3] – uprawnienia do ujawniania poprzez przesłanie, rozpowszechniania lub innego rodzaju udostępniania.
Poziom [4] – uprawnienia do usuwania lub niszczenia, ograniczania.
Wyższe poziomy uprawnień uwzględniają uprawnienia poziomów niższych.

Załącznik nr 3
do Polityki Ochrony Danych
Osobowych

…….……... …….……..

(imię i nazwisko pracownika) (data)

Oświadczenie

Obowiązki pracownika

Pracownik dopuszczony do przetwarzania danych osobowych zobowiązany jest do:

1) zapoznania się i przestrzegania:
   a) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. 2016.119. 1),
   b) dokumentów wprowadzonych w związku z przetwarzaniem danych osobowych;
2) przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora zadaniach;
3) zapewnienia bezpieczeństwa przetwarzania danych osobowych poprzez ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem;
4) zachowania w tajemnicy danych oraz sposobu ich zabezpieczenia, do których uzyskał dostęp w trakcie zatrudnienia, również po ustaniu zatrudnienia.

Odpowiedzialność pracownika

Za niedopełnienie obowiązków wynikających z niniejszego oświadczenia pracownik ponosi odpowiedzialność na podstawie przepisów Regulaminu Pracy Starostwa Powiatowego w Słupsku, Kodeksu pracy oraz ustawy o ochronie danych osobowych.

Oświadczam, że znane są mi obowiązki wskazane w niniejszym oświadczeniu i zobowiązuję się do ich przestrzegania, ponadto potwierdzam odbiór 1 egzemplarza oświadczenia.

.....

(podpis pracownika)

Załącznik nr 4
do Polityki Ochrony Danych
Osobowych

…….……... …….……..

(imię i nazwisko) (data)

Oświadczenie

Obowiązki

Osoba wykonująca pracę w ramach zawartej umowy lub pełnionej funkcji/stażysta/praktykant/wolontariusz dopuszczony do przetwarzania danych osobowych zobowiązany jest do:

1) zapoznania się i przestrzegania:
   a) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. 2016.119. 1),
   b) dokumentów wprowadzonych w związku z przetwarzaniem danych osobowych;
2) zachowania w poufności informacji uzyskanych w związku z wykonywaniem czynności w miejscu odbywania stażu/praktyki/wolontariatu lub w toku wykonywania pracy w ramach zawartej umowy lub pełnionej funkcji, stanowiących tajemnicę służbową oraz takich, których ujawnienie może narazić pracodawcę na szkodę, z wyłączeniem informacji, które zostały:
   a) opublikowane lub stały się jawne w inny sposób,
   b) ujawnione przez strony trzecie bez naruszania zasad poufności,
   c) ujawnione na podstawie odpowiedniego przepisu prawa, wyroku sądowego lub decyzji administracyjnej;
3) podejmowania pozytywnych działań zmierzających do ochrony informacji, o których mowa w pkt. 2, o ile w trakcie wykonywania zadań mogłoby dojść do ujawnienia takich informacji;
4) zapoznawania się z dokumentami, analizami, zawartością dysków twardych i innych nośników informacji itp. nie związanych z wykonywanymi zadaniami;
5) wykorzystywania własnego sprzętu informatycznego na terenie Starostwa bez wiedzy i zgody pracowników Oddziału Obsługi Informatycznej;
6) zbierania, kopiowania oraz powielania dokumentów i danych, a w szczególności udostępnienia ich osobom trzecim, informowania osób trzecich o danych objętych zakazem.

Odpowiedzialność

Za niedopełnienie obowiązków wynikających z niniejszego oświadczenia osoba wykonująca pracę w ramach zawartej umowy lub pełnionej funkcji/stażysta/praktykant/wolontariusz

ponosi odpowiedzialność na podstawie przepisów Kodeksu postępowania cywilnego oraz ustawy o ochronie danych osobowych.

Oświadczam, że znane są mi obowiązki wskazane w niniejszym oświadczeniu i zobowiązuję się do ich przestrzegania, ponadto potwierdzam odbiór 1 egzemplarza oświadczenia.

.....

(podpis pracownika)

Załącznik nr 5
do Polityki Ochrony Danych
Osobowych

STAROSTA
SŁUPSKI

....., ……. r.

(miejscowość) (data)

Pan/Pani
……..
stanowisko/funkcja
komórka organizacyjna

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. 2016.119. 1)

upoważniam Pana/Panią do:

przetwarzania danych osobowych administrowanych i/lub powierzonych do przetwarzania w ramach czynności/kategorii:
- (*wymienić czynności, zgodnie z RCP i/lub RKCP wraz z oznaczeniem zakresu upoważnienia*);
w postaci papierowej i elektronicznej.

Jednocześnie, wraz z nadanym upoważnieniem, zobowiązuję Pana/Panią do zapewnienia poufności danych i sposobu ich zabezpieczania oraz przestrzegania przepisów dotyczących ochrony danych osobowych ze szczególnym uwzględnieniem 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) i ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781) oraz wprowadzonych i wdrożonych do stosowania procedur postępowania i wewnętrznych polityk udostępnionych do wglądu.

Upoważnienia udziela się na okres zatrudnienia/stażu/praktyki/wolontariatu/pełnienia funkcji.
Upoważnienie może być odwołane w każdym czasie.
**Odwołuję upoważnienie Nr …….. z dnia ……..

(podpis Administratora)

*Poziom [1] – uprawnienia tylko do zbierania, utrwalania, porządkowania, przechowywania, pobierania, przeglądania, dopasowywania lub łączenia.
Poziom [2] – uprawnienia do adaptowania lub modyfikowania, organizowania, wykorzystywania.
Poziom [3] – uprawnienia do ujawniania poprzez przesłanie, rozpowszechniania lub innego rodzaju udostępniania.
Poziom [4] – uprawnienia do usuwania lub niszczenia, ograniczania.
Wyższe poziomy uprawnień uwzględniają uprawnienia poziomów niższych.

**stosuje się tylko w przypadku dokonania odwołania upoważnienia

ul. Szarych Szeregów 14, 76-200 Słupsk
tel. (+48) 59 841 85 00, tel./fax (+48) 59 842 71 11
e-mail: starostwo@powiat.slupsk.pl

Załącznik nr 6
do Polityki Ochrony Danych
Osobowych

Umowa powierzenia
przetwarzania danych osobowych

zawarta dnia …… pomiędzy:

…….

zwanym w dalszej części Umowy **„Administratorem danych" lub „Administratorem"**

oraz

…….

…….

…….

zwanym w dalszej części Umowy **„Podmiotem przetwarzającym"**

reprezentowanym przez:

…….

§ 1
Powierzenie przetwarzania danych osobowych

1. Administrator danych powierza Podmiotowi przetwarzającemu dane osobowe do przetwarzania, w trybie art. 28 ogólnego 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, z późn. zm.) (zwanego w dalszej części Umowy „Rozporządzeniem" lub „RODO"), na zasadach, w zakresie i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.

§ 2
Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał w formie papierowej oraz przy wykorzystaniu systemów informatycznych, powierzone na podstawie Umowy dane …….……. w postaci: ……...
2. Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji Umowy Nr ……. z dnia ……. zawartej ……

§ 3
Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających zgodność z RODO, w tym adekwatny stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób, których dane dotyczą.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane osobowe, przy czym będą to jedynie osoby, które posiadają odpowiednie przeszkolenie z zakresu ochrony danych osobowych i są niezbędne do w realizacji celu niniejszej Umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić, że osoby, które upoważnia do przetwarzania danych osobowych, w celu realizacji niniejszej Umowy, zobowiążą się do zachowania tajemnicy lub będą podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy, o której mowa w art. 28 ust. 3 pkt b) Rozporządzenia, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu. Podmiot przetwarzający zapewnia ponadto, że osoby o których mowa w niniejszym ustępie będą przetwarzały dane osobowe zgodnie z zasadą wiedzy koniecznej.
5. Podmiot przetwarzający po wykonaniu czynności o których mowa w § 1 Umowy Nr …… z dnia ……. r. zawartej z …… usuwa wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. Podmiot przetwarzający zobowiązuje się przed przystąpieniem do przetwarzania powierzonych przez Administratora danych wdrożyć i utrzymywać przez czas przetwarzania wszelkie środki i zabezpieczenia związane z przetwarzaniem danych,

zgodnie z wymaganiami art. 32 Rozporządzenia.

7. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia. W razie wpływu do Podmiotu przetwarzającego żądania w zakresie realizacji praw osób, których dotyczą powierzone dane, Podmiot przetwarzający niezwłocznie informuje o tym Administratora. Udzielając informacji, Podmiot przetwarzający przekazuje dane nadawcy i treść żądania oraz określa, w jakim zakresie jest w stanie przyczynić się do realizacji żądania.
8. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi w ciągu 24 godzin.

§4
Prawo kontroli

1. Administrator danych zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, mającej na celu weryfikację czy Podmiot przetwarzający spełnia obowiązki wynikające z niniejszej Umowy.
2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum 7-dniowym uprzedzeniem.
3. Prawo do przeprowadzenia kontroli obejmuje: wstęp do pomieszczeń, w których znajdują się zasoby uczestniczące w operacjach przetwarzania powierzonych danych osobowych; żądanie złożenia pisemnych lub ustnych wyjaśnień od osób upoważnionych do przetwarzania powierzonych danych osobowych; wgląd do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z celem kontroli oraz przeprowadzanie oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania powierzonych danych.
4. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli, w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni.

§ 5
Raportowanie

1. Na wniosek Administratora, Podmiot przetwarzający udostępnia wszelkie informacje niezbędne do realizacji lub wykazania spełnienia obowiązków wynikających z RODO.
2. Informacji, o których mowa w ust. 1, udziela się w terminie 7 dni roboczych od dnia doręczenia wniosku, z zastrzeżeniem ust. 3.
3. Jeżeli wniosek, o którym mowa w ust. 1, dotyczy realizacji obowiązku zgłoszenia naruszenia ochrony danych osobowych lub usunięcia jego skutków, Podmiot przetwarzający udziela informacji w najbliższym możliwym terminie, nie później niż w ciągu 24 godzin od doręczenia wniosku.

§ 6

Dalsze powierzenie danych do przetwarzania

Podmiot przetwarzający nie może powierzyć danych osobowych objętych niniejszą Umową do dalszego przetwarzania podwykonawcom.

§ 7

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w Umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Urzędu Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

§ 8

Czas obowiązywania Umowy

Niniejsza Umowa obowiązuje od dnia jej zawarcia przez czas obowiązywania Umowy Nr …….. z dnia ……. zawartej ……

§ 9

Rozwiązanie Umowy

Administrator danych może rozwiązać niniejszą Umowę ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:

a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;

b) przetwarza dane osobowe w sposób niezgodny z Umową;

c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych.

§ 10

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne").
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

§ 11

Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej Umowy będzie sąd właściwy miejscowo dla siedziby Administratora danych.

_____ _____

Administrator danych Podmiot przetwarzający

Załącznik nr 7
do Polityki Ochrony Danych
Osobowych

....., ……. r.

(miejscowość) (data)

Raport z naruszenia bezpieczeństwa danych osobowych

1. Osoba powiadamiająca o zaistniałym zdarzeniu:

(imię, nazwisko, stanowisko służbowe, nazwa użytkownika - jeśli występuje)

.....

2. Data powiadomienia: ..... r. Godzina powiadomienia: .....

3. Godzina pojawienia się w pomieszczeniach, w których przetwarzane są dane: ……

4. Opis zastanej sytuacji:

.....

.....

5. Przyczyny wystąpienia zdarzenia:

.....

.....

.....

6. Podjęte działania i ich uzasadnienie:

.....

.....

7. Stan systemu informatycznego lub dokumentacji papierowej po podjęciu działań naprawczych:

.....

.....

8. Wnioski w sprawie ograniczenia możliwości ponownego wystąpienia naruszenia ochrony danych osobowych:

.....

.....

.....

.....

(podpis Administratora lub IOD)

Załącznik nr 8
do Polityki Ochrony Danych
Osobowych

....., ……. r.

(miejscowość) (data)

Raport z naruszenia bezpieczeństwa danych osobowych

1. Osoba powiadamiająca o zaistniałym zdarzeniu:

(imię, nazwisko)

.....

2. Data powiadomienia: ..... r. Godzina powiadomienia: .....

3. Opis zastanej sytuacji:

.....

.....

4. Przyczyny wystąpienia zdarzenia:

.....

.....

.....

5. Podjęte działania i ich uzasadnienie:

.....

.....

6. Stan systemu informatycznego lub dokumentacji papierowej po podjęciu działań naprawczych:

.....

.....

7. Wnioski w sprawie ograniczenia możliwości ponownego wystąpienia naruszenia ochrony danych osobowych:

.....

.....

.....

.....

(podpis Administratora lub IOD)

Załącznik nr 9
do Polityki Ochrony
Danych Osobowych

Plan audytów na okres ……..

Nr	Przedmiot sprawdzenia	Zakres sprawdzenia	Termin sprawdzenia	Sposób i zakres dokumentowania sprawdzenia
1.				
2.				

……..…… ……...……..

(data i podpis IOD) (data i podpis Administratora)