ZARZĄDZENIE NR 13/2018

STAROSTY PISKIEGO

z dnia 25 maja 2018 r.

w sprawie wprowadzenia Polityki Ochrony Danych

Na podstawie art. 24 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), publ. Dz. Urz. UE L Nr 119, s. 1, zarządza się, co następuje:

§ 1

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

§ 2

Traci moc Zarządzenie nr 28/2013 Starosty Piskiego z dnia 22 maja 2013 r. w sprawie wprowadzenia „Polityki Bezpieczeństwa Informacji w zakresie przetwarzania danych osobowych w Starostwie Powiatowym w Piszu".

§ 3

Upoważnienia pracowników do przetwarzania danych osobowych wydane przed 25 maja 2018 r. tracą moc.

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA

mgr Andrzej Nowicki

POLITYKA OCHRONY DANYCH

Spis treści

1 Informacje wstępne

Polityka ochrony danych zwana dalej „Polityką" jest dokumentem wewnętrznym Starostwa Powiatowego w Piszu i jest objęta obowiązkiem zachowania w poufności przez wszystkie osoby, którym zostanie ujawniona.

Każda osoba mająca dostęp do danych osobowych zobowiązana jest zapoznać się z niniejszym dokumentem oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści, wg ***załącznika nr 1*** do niniejszej Polityki - Oświadczenie o zapoznaniu się z Polityką.

2 Cel wdrożenia Polityki Ochrony Danych

Celem opracowania i wdrożenia Polityki jest zdefiniowanie ogólnych wymagań i zasad ochrony, które będą fundamentem dla wszystkich dokumentów związanych z ochroną danych osobowych.

Ponadto niniejsza Polityka dotyczy realizacji celów związanych z projektami finansowanymi ze środków zewnętrznych.

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 Podstawa prawna

Polityka została przygotowana w oparciu o:

1) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, zwane w dalszej części Polityki „RODO";
2) Ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000).

5 Definicje

1) **Administrator** – Starosta Piski 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, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
4) **Dane dotyczące zdrowia** oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;
5) **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;

6) **Ograniczenie przetwarzania** oznacza przechowywanie danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
7) **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;
8) **Podmiot przetwarzający** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
9) **Pseudonimizacja** oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
10) **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;
11) **Użytkownik** - osoba posiadająca dostęp do systemu informatycznego przetwarzającego dane osobowe,
12) **Zgoda** oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczące jej danych osobowych;
13) **Zbiór danych** oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

6 Podmioty odpowiedzialne za ochronę i przetwarzanie danych osobowych

6.1 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 osobowych.

6.2 Inspektor Ochrony Danych /IOD/

1) informuje Administratora oraz użytkowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy obowiązujących przepisów, kodeksów postępowania i zatwierdzonych mechanizmów certyfikacji;
2) prowadzi szkolenia z zakresu ochrony danych osobowych;
3) aktualizuje i sprawuje nadzór nad dokumentacją z zakresu ochrony danych osobowych;
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 Podstawy przetwarzania danych osobowych

Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy zostanie spełniona jedna z przesłanek wynikających z art. 6 RODO w przypadku przetwarzania danych zwykłych. Dane osobowe w jednostce przetwarzane są gdy:

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 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 odwołaniu zgody na przetwarzanie danych osobowych.

7.1 Obowiązek informacyjny przy przetwarzaniu danych

Obowiązek informacyjny spoczywający na administratorze w myśl art. 13 i 14 RODO jest realizowany poprzez przekazanie osobie, której dane są przetwarzane informacji dotyczących pozyskiwania danych osobowych, a także ich dalszego przetwarzania. Obowiązek informacyjny jest realizowany zarówno w przypadku zbierania danych od osoby, której dane dotyczą, jak również z innych źródeł.

Jedną z form spełniania obowiązku informacyjnego jest ***załącznik nr 4*** do niniejszego dokumentu, stanowiący jego integralną część.

Administrator realizuje obowiązek informacyjny 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 i 14 RODO.

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 2018 r. o ochronie danych osobowych.

Powyższy obowiązek należy spełnić w momencie zbierania danych.

7.2 Prawa osób, których dane dotyczą

Prawo dostępu do danych, o którym mowa w art. 15 RODO jest realizowane przez Administratora poprzez potwierdzenie faktu przetwarzania danych w miarę możliwości przy użyciu tożsamych środków komunikacji jakie zostały wykorzystane przez osobę kierującą żądanie. W przypadku, gdy przetwarzanie danych w odniesieniu do osoby, której dane dotyczą ma miejsce, wówczas Administrator realizuje uprawnienia dotyczące udzielenia informacji z art. 15 ust. 1 RODO, jak również dostarcza kopię danych, o czym mowa w ustępie 3 ww. artykułu. Szczegółowe informacje dotyczące ww. uprawnienia opisane są w procedurze dostępu do danych stanowiącej ***załącznik nr 5*** do niniejszej Polityki.

Prawo do sprostowania danych, o którym mowa w art. 16 RODO jest wykonywane w wyniku żądania osoby, której dane są przetwarzane. Realizacja uprawnienia dotyczy przypadków przetwarzania danych nieprawidłowych, bądź też niekompletnych. Administrator bez zbędnej zwłoki dokonuje sprostowania danych w związku z żądaniem osoby, które może być ponadto potwierdzone poprzez przedłożenie dodatkowego oświadczenia. Szczegółowe informacje dotyczące ww. uprawnienia opisane są w procedurze prawa do sprostowania danych stanowiącej ***załącznik nr 6*** do niniejszej Polityki.

Prawo do usunięcia danych spoczywające na administratorze danych jest realizowane, o ile zachodzi jedna z okoliczności, o których mowa w art. 17 ust. 1 lit. a) – f) RODO. Administrator bez zbędnej zwłoki dokonuje usunięcia danych, o ile dalsze przetwarzanie nie jest niezbędne, o czym stanowi art. 17 ust. 3 RODO. Realizacja prawa do usunięcia danych

wiąże się również z przekazaniem informacji o konieczności spełnienia żądania przez innych administratorów w sytuacji, gdy dane zostały upublicznione. Administrator weryfikując dostępną technologię oraz koszt realizacji podejmuje rozsądne działania mające na celu poinformowanie innych administratorów. Wykonywanie uprawnień osoby, której dane dotyczą jest zainicjowane żądaniem tej osoby. Szczegółowe informacje dotyczące ww. uprawnienia opisane są w procedurze prawo do bycia zapomnianym stanowiącej ***załącznik nr 7*** do niniejszej Polityki.

Prawo do przenoszenia danych jest realizowane w przypadku zaistnienia przesłanek z art. 20 RODO. Wykonywanie uprawnienia, które przysługuje podmiotowi danych jest inicjowane żądaniem tej osoby. Szczegółowe informacje dotyczące ww. uprawnienia opisane są w procedurze prawo do przenoszenia danych stanowiącej ***załącznik nr 8*** do niniejszej Polityki.

Prawo do sprzeciwu w stosunku do przetwarzanych danych jest realizowane w przypadku zaistnienia przesłanek z art. 21 RODO. Szczegółowe informacje dotyczące ww. uprawnienia opisane są w procedurze prawo do sprzeciwu przetwarzania danych stanowiącej ***załącznik nr 9*** do niniejszej Polityki.

7.3 Zasady dokonywania anonimizacji danych osobowych w dokumentach publikowanych w Biuletynie Informacji Publicznej

1) Użytkownik, sporządzający dokumenty, które mają zostać umieszczone w Biuletynie Informacji Publicznej zobowiązany jest do wstępnej oceny przedmiotowego dokumentu pod względem dopuszczalności publikacji danych osobowych osób fizycznych niepełniących funkcji publicznych lub kierowniczych.
2) W sytuacji stwierdzenia obecności danych osobowych osób fizycznych w dokumentach, o których mowa w pkt. 1, użytkownik zobowiązany jest do dokonania analizy legalności publikacji danych osobowych w przedmiotowym dokumencie oraz dokonania anonimizacji zawartych w nich danych osobowych osób fizycznych tj. imion, nazwisk, adresu, nr PESEL, wieku, numeru telefonu, stanu zdrowia itp.

7.4 Procedura nadawania upoważnień do przetwarzania danych osobowych

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

1) 1. Administrator zleca przygotowanie upoważnienia do przetwarzania danych osobowych na podstawie wniosku skierowanego przez naczelnika wydziału lub bezpośredniego przełożonego. Wzór wniosku stanowi ***załącznik nr 10***, natomiast wzór upoważnienia stanowi ***załącznik nr 11*** do niniejszej Polityki ochrony danych.

   2. Inspektor ds. kadr jest odpowiedzialny za przygotowanie upoważnień do przetwarzania danych osobowych dla pracowników jednostki na podstawie wniosku o nadanie upoważnienia do przetwarzania danych/uprawnienia do pracy w systemie informatycznym skierowanego przez naczelnika wydziału lub bezpośredniego przełożonego wg wzoru stanowiącego ***załącznik nr 10*** do niniejszej Polityki.
2) Upoważnienia o których mowa w punkcie 1 zatwierdza Administrator, podpisuje wnioskodawca - naczelnik wydziału lub bezpośredni przełożony oraz upoważniony pracownik.
3) Zatwierdzone przez Administratora upoważnienie do przetwarzania danych osobowych inspektor ds. kadr wpisuje do Rejestru wydanych upoważnień i pełnomocnictw RODO - stanowiący odrębną ewidencję - wzór stanowi ***załącznik nr 12*** do niniejszej Polityki.
4) W przypadku zmiany stanowiska, zakresu obowiązków lub w sytuacji, która wpływa bezpośrednio na rodzaj i zakres przetwarzanych danych osobowych, inspektor ds. kadr po uzyskaniu nowego wniosku od naczelnika wydziału lub bezpośredniego przełożonego - wzór wniosku stanowi ***załącznik nr 10***, jest zobowiązany do przygotowania nowego upoważnienia lub jego aktualizacji – procedurę stosuje się odpowiednio.

8 Środki techniczne i organizacyjne zapewniające bezpieczeństwo przetwarzanych danych

Środki techniczne i organizacyjne są opisane w ***załączniku nr 13*** do niniejszej Polityki.

9 Obowiązki po stronie użytkowników

Ze względów bezpieczeństwa przetwarzanych danych użytkowników zobowiązuje się do:

1) **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,
2) **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,
3) bieżącego niszczenia w niszczarce niepotrzebnej dokumentacji papierowej oraz przechowywania pozostałej dokumentacji papierowej w szafach zamykanych na klucz,
4) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej,
5) zachowania w poufności wszelkich informacji w tym danych osobowych poprzez złożenie stosownego oświadczenia stanowiącego wzór zawarty w ***załączniku nr 14*** do niniejszej Polityki.

10 Przenośne nośniki danych oraz komputery przenośne służące do przetwarzania danych osobowych

Użytkownicy mogą korzystać wyłącznie z elektronicznych nośników (w szczególności pendriv-y, dysków zewnętrznych, CD-R, DVD) oraz komputerów przenośnych przeznaczonych do użytku służbowego.

Użytkownik korzystający z ww. urządzeń zobowiązany jest do:

1) przechowywania przedmiotowych danych na dysku szyfrowanym, zabezpieczonym hasłem co najmniej 8 - znakowym zawierającym: małe, wielkie litery, znaki specjalne lub cyfry,
2) transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia,
3) zdecydowanego i skutecznego uniemożliwienia korzystania z komputera osobom nieuprawnionym (np. rodzinie, dzieciom, znajomym).

Informatycy prowadzą inwentaryzację nośników i komputerów przenośnych służących do przetwarzania danych osobowych.

11 Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz nośników kopii zapasowych

Dane osobowe przechowywane są w postaci elektronicznej na:

1) nośnikach elektronicznych wbudowanych w sprzęt informatyczny lub stanowiących element tego systemu,
2) przenośnych nośnikach elektronicznych.

Dane mogą być przechowywane na nośnikach przenośnych jedynie w przypadkach, gdy jest to konieczne, przez czas niezbędny do spełnienia celu, w jakim zostały one na nośniku zapisane.

Po ustaniu czasu przechowywania zawartość nośnika podlega skasowaniu przy użyciu narzędzi zaakceptowanych do użycia w jednostce, a w przypadku nośników optycznych stosuje się niszczarki umożliwiające niszczenie tego typu nośników.

Przenośne elektroniczne nośniki informacji zawierające dane osobowe powinny być przechowywane przez użytkowników w sposób minimalizujący ryzyko ich uszkodzenia lub zniszczenia, w szczególności w zamykanych szafach lub zamykanych meblach biurowych.

W przypadku wycofania sprzętu komputerowego z użycia dane osobowe na nim zapisane powinny być kasowane przy użyciu dedykowanego oprogramowania do bezpiecznego usuwania danych zaakceptowanego do użycia w jednostce. W przypadku braku możliwości programowego usunięcia danych nośniki danych (w tym dysk) podlega fizycznemu zniszczeniu. Zniszczenie nośnika powinno być potwierdzane protokołem zniszczenia.

Możliwe jest powierzenie niszczenia nośników danych wyspecjalizowanym podmiotom zewnętrznym, pod warunkiem:

1) zawarcia umowy, o której mowa w art. 28 RODO,
2) umożliwienia prowadzenia nadzoru nad procesem niszczenia nośników przez Administratora lub osobę przez niego wyznaczoną
3) udokumentowania faktu zniszczenia nośników protokołem.

12 Praca w systemach informatycznych

12.1 Procedura nadawania i odbierania uprawnień dla użytkowników w systemie informatycznym

1) Informatycy nadają uprawnienia użytkownikom do pracy w systemach informatycznych na podstawie okazanego upoważnienia o którym mowa w rozdziale 7.4.
2) Informatycy dokonują modyfikacji, zmiany lub wyrejestrowania uprawnień użytkowników systemów informatycznych na podstawie informacji otrzymanej od naczelnika wydziału lub bezpośredniego przełożonego. Wyrejestrowanie, o którym mowa w pkt 3, może mieć charakter czasowy lub trwały.
3) Wyrejestrowanie następuje poprzez:
   a) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
   b) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).

12.2 Metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

W przypadku dostępu do systemów informatycznych (dziedzinowych i operacyjnych) Użytkownik powinien stosować co najmniej dwuetapową metodę uwierzytelnienia poprzez wpisanie indywidualnego identyfikatora/ login'u oraz hasła. Identyfikator jest przydzielany wg zasady przyjętej w jednostce. W identyfikatorze pomija się polskie znaki diakrytyczne.

W przypadku dublowania się identyfikatorów powinien być on rozszerzany o kolejne litery lub cyfry.

Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz znaki specjalne. Zmiana hasła powinna następować nie rzadziej niż co 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione osobie nieuprawnionej. Użytkownik zobowiązany jest do zachowania hasła w poufności i niezapisywania haseł w sposób jawny.

Hasła administracyjne do urządzeń i systemów informatycznych winny być przechowywane w miejscu wskazanym przez Administratora. Powyższa ewidencja powinna zawierać nazwę użytkownika (administratora), hasło, sposób dostępu, adres IP serwera urządzenia. Hasła te podlegają zmianie w cyklu półrocznym oraz w sytuacji, gdy dochodzi do zmian personalnych wśród osób, które miały do nich dostęp lub je znały. Powinny cechować się one właściwą złożonością tzn. co najmniej 12 znaków, 3 z 4 grup znaków (małe litery, duże litery, cyfry, znaki specjalne).

12.3 Sposoby zabezpieczania 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 Informatyków jest nadzór nad aktualizacją oprogramowania antywirusowego. Użytkownik jest obowiązany każdorazowo zawiadomić Informatyków o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem – wirusa lub w przypadku sygnalizowanych problemów z działaniem oprogramowania antywirusowego.

12.4 Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

Informatycy są odpowiedzialni za dokonywanie przeglądu i konserwacji systemów oraz nośników służących do przetwarzania danych.

12.5 Zasady bezpiecznego użytkowania sprzętu IT

Użytkownik zobowiązany jest korzystać ze sprzętu IT w sposób zgodny z jego przeznaczeniem i chronić go przed jakimkolwiek zniszczeniem lub uszkodzeniem. Użytkownik ma obowiązek natychmiast zgłosić utratę lub zniszczenie powierzonego sprzętu IT. Samowolne otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączenie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione. Użytkownicy nie mogą bez zgody Administratora korzystać z prywatnego sprzętu IT (np. laptopów, telefonów, aparatów fotograficznych, nośników typu pendrive) do wykonywania zadań służbowych.

Administrator ma prawo do monitorowania sprzętu służbowego wykorzystywanego przez pracowników, 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 pracownika, nie później niż 14 dni przed jego uruchomieniem.

Załącznik nr 15 stanowi wzór oświadczenia o monitorowaniu sprzętu komputerowego, na którym pracują użytkownicy.

12.6 Zasady korzystania z oprogramowania

Użytkownik zobowiązany jest do korzystania wyłącznie z oprogramowania dopuszczonego do stosowania w jednostce. Użytkownicy nie mają prawa do instalowania ani używania oprogramowania innego, niż przekazane lub udostępnione im przez Administratora. Zakaz dotyczy między innymi instalacji oprogramowania z zakupionych płyt CD, programów ściąganych ze stron internetowych, a także odpowiadania na samoczynnie pojawiające się reklamy internetowe.

12.7 Zasady korzystania z Internetu

Dopuszcza się korzystanie przez pracowników ze stron Internetowych w celach służbowych, a także okazjonalnie w celach prywatnych. Podczas korzystania z sieci internetowych niedozwolone jest przeglądanie, a także ściąganie materiałów, których treści są prawnie zakazane, naruszają dobre obyczaje lub uznawane są za obraźliwe. Od pracowników wymaga się także zachowania szczególnej ostrożności w przypadku żądania lub prośby podania kodów, PIN-ów, hasła, numerów kart płatniczych przez Internet, w szczególności tyczy się to żądania podania takich informacji przez rzekomy bank.

W zakresie dozwolonym przepisami prawa, Administrator zastrzega sobie prawo kontrolowania sposobu korzystania przez użytkownika z Internetu pod kątem wyżej opisanych zasad oraz ma prawo blokować dostęp do wybranych stron internetowych.

12.8 Zasady korzystania z poczty elektronicznej

Użytkownik jest zobowiązany do korzystania z przyznanego mu adresu mailowego wyłącznie w celu prowadzenia korespondencji związanej z działalnością jednostki. Podczas przesyłania danych należy zachować szczególną ostrożność przy wpisywaniu adresu odbiorcy dokumentu. Zaleca się, aby użytkownik podczas przesyłania danych osobowych pocztą elektroniczną zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.

W przypadkach gdy wiadomość jest kierowana jednocześnie do kilku adresatów należy używać metody „Ukryte do wiadomości-UDW".

Zabrania się także rozsyłania za pośrednictwem poczty elektronicznej „łańcuszków szczęścia", itp.

Użytkownicy powinni okresowo kasować niepotrzebne wiadomości (tj. spam, oferty handlowe).

Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.

12.9 Zasady korzystania z bankowości elektronicznej

Użytkownicy, którzy w zakresie obowiązków maja za zadanie korzystania z bankowości elektronicznej, zobowiązani są do regularnej zmiany hasła oraz nieprzechowywania go w formie pisemnej wraz z loginem. Zabrania się opuszczania stanowiska pracy bez wylogowania się i zamknięcia przeglądarki. Użytkownik logujący się do bankowości elektronicznej nie powinien korzystać z nieznanych sieci bezprzewodowych. W celu zalogowania się do systemu bankowości elektronicznej pracownik nie powinien wchodzić na stronę internetową banku za pośrednictwem linków znajdujących się w korespondencji elektronicznej.

13 Sposób postępowania z dokumentami papierowymi zawierającymi dane osobowe

W stosunku do dokumentów papierowych stanowiących wydruki z systemu obowiązują następujące środki ostrożności:

1) wydruki i dokumentacja powinny być niedostępne dla osób postronnych,
2) nie mogą być pozostawione w drukarce ogólnodostępnej,
3) wydruki niepotrzebne i nieprzydatne powinny być na bieżąco niszczone za pomocą niszczarki.

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.

14 Przesyłanie dokumentów za pośrednictwem poczty elektronicznej

Dokumenty przesyłane drogą elektroniczną, które nie stanowią informacji publicznej powinno zabezpieczać się przy pomocy środków ochrony kryptograficznej. Ochrona kryptograficzna systemu lub sieci teleinformatycznej polega na stosowaniu metod i środków zabezpieczających dane, przez ich szyfrowanie oraz stosowanie innych mechanizmów kryptograficznych, gwarantujących integralność i zabezpieczenie przed nieuprawnionym ujawnieniem tych danych lub uwierzytelnienie podmiotów lub uwierzytelnienie informacji.

Klucze kryptograficzne (hasła, kody, certyfikaty, karty), powinny być zabezpieczone w sposób uniemożliwiający dostęp osobom nieuprawnionym. Rodzaj i model urządzenia kryptograficznego objęty jest zachowaniem poufności w związku z faktem, iż stanowi on element systemu zabezpieczającego.

15 Szkolenia z ochrony danych osobowych

Inspektor Ochrony Danych przeprowadza okresowe szkolenia dla pracowników jednostki zgodnie z poniższymi zasadami:

1) szkolenia wewnętrzne są przeprowadzane w przypadku każdej istotnej zmiany zasad lub przepisów dotyczących ochrony danych osobowych,
2) nowi użytkownicy mają obowiązek samodzielnie zaznajomić się z przepisami prawa w zakresie danych osobowych oraz treścią Polityki ochrony danych.

Administrator informuje Inspektora Ochrony Danych o konieczności przeprowadzenia szkolenia dla pracowników i stażystów.

16 Umowy powierzenia

Umowa powierzenia przetwarzania danych osobowych zawierana jest pomiędzy Administratorem oraz podmiotem przetwarzającym, który przetwarza dane w imieniu Administratora. Szczegółowe zasady dotyczące zawierania umów powierzenia są uregulowane w RODO.

Umowa powierzenia powinna być zawarta przed rozpoczęciem przetwarzania danych przez podmiot przetwarzający.

Wzór umowy powierzenia stanowi ***załącznik nr 16*** do niniejszej Polityki, natomiast wzór rejestru umów powierzenia stanowi ***załącznik nr 17*** do niniejszej Polityki.

17 Procedura zgłaszania naruszeń ochrony danych osobowych

Procedura zgłaszania naruszeń ochrony danych jest opisana w ***załączniku nr 18*** do niniejszej Polityki.

18 Bezpieczeństwo informacji

18.1 Kontrola uprawnień

Informatycy przeprowadzają okresową kontrolę uprawnień i kont użytkowników co najmniej raz na pół roku w celu weryfikacji czy użytkownicy posiadają uprawnienia adekwatne do wykonywanej pracy w systemach informatycznych. Z przeprowadzonej kontroli ww. osoba sporządza notatkę służbową wg wzoru stanowiącego ***załącznik nr 22*** do niniejszej Polityki.

18.2 Inwentaryzacja sprzętu i oprogramowania służącego do przetwarzania informacji

Komisja doraźna powołana przez Administratora w skład której wchodzą Informatycy, odpowiedzialna jest za prowadzenie inwentaryzacji, przeglądu - sprzętu komputerowego i programowania oraz utrzymywanie jej w aktualności.

18.3 Ochrona przetwarzanych informacji

Monitorowanie dostępu do informacji może być realizowane za pomocą: logów aplikacji dziedzinowych oraz logów systemów operacyjnych. Informacje te zawierają: identyfikator i/lub adres IP komputera, dokładną datę, zakres dostępu (przydzielony/odrzucony) oraz opis wykonanej lub zablokowanej akcji.

Czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji realizowane są przez ochronę antywirusową.

Wprowadzenie blokady bezpośredniego dostępu stacji roboczych do sieci Internet:

1) umożliwia zablokowanie bezpośredniego połączenia złośliwego oprogramowania z sieci Internet,
2) utrudnia ominięcie systemów zabezpieczeń,
3) umożliwia kontrolę dostępu i rozliczalność działań użytkowników.

19 Przeprowadzanie okresowych analiz ryzyka w zakresie bezpieczeństwa informacji

Głównym celem analizy ryzyka bezpieczeństwa informacji jest wyznaczenie właściwych kierunków działania kierownictwa oraz określenie priorytetów dla zarządzania ryzykami i zabezpieczeniami. Wyniki analizy ryzyka prowadzą do opracowania planu postępowania z ryzykiem obejmującego wprowadzenie rozwiązań umożliwiających odpowiednio: unikanie tych ryzyk, ograniczanie ich do akceptowanego poziomu, przeniesienie lub świadomą ich akceptację.

Zaleca się, by zarządzanie ryzykiem w bezpieczeństwie informacji zapewniało:

1) zidentyfikowanie ryzyka,
2) oszacowanie ryzyka z punktu widzenia następstw dla działalności oraz prawdopodobieństwa wystąpienia,
3) informowanie o prawdopodobieństwie i następstwach ryzyka oraz zrozumienie tych informacji,
4) ustanowienie priorytetów postępowania z ryzykiem,
5) określenie priorytetów dla działań podjętych w celu zredukowania ryzyka,
6) regularne monitorowanie i przegląd różnych typów ryzyka oraz procesu zarządzania ryzykiem,
7) zbieranie informacji w celu doskonalenia podejścia do zarządzania ryzykiem,
8) szkolenie kierownictwa w zakresie ryzyka oraz działań podejmowanych w celu postępowania z ryzykiem.

20 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, bowiem utrzymywanie wysokiego poziomu bezpieczeństwa informacji, wymaga stałego monitorowania i okresowego badania stanu zabezpieczenia wszystkich elementów tego systemu.

21 Aktualizacja Polityki Ochrony Danych

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).

Celem przeglądów polityki jest zapewnienie jej rozliczalności w stosunku do realizowanych zadań oraz możliwości obsługi interesantów w każdych warunkach niezależnie od okoliczności i zmian.

22 Wykaz załączników

Nr 1- Wzór oświadczenia o zapoznaniu się z Polityką Ochrony Danych,
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 wniosku o nadanie upoważnienia do przetwarzania danych osobowych/ uprawnienia do pracy w systemie informatycznym,
Nr 11- Wzór upoważnienia do przetwarzania danych osobowych,
Nr 12- Wzór ewidencji osób upoważnionych do przetwarzania danych,
Nr 13- Opis środków technicznych i organizacyjnych,
Nr 14- Wzór oświadczenia o zachowaniu w poufności danych,
Nr 15- Oświadczenie o monitorowaniu komputerów służbowych,
Nr 16- Wzór umowy powierzenia,
Nr 17- Wzór rejestru umów powierzenia przetwarzania danych osobowych,

Nr 18- Procedura zgłaszania naruszeń ochrony danych osobowych,

Nr 19- Wzór rejestru naruszeń ochrony danych,

Nr 20- Wzór zgłoszenia naruszenia ochrony danych organowi nadzorczemu,

Nr 21- Wzór zawiadomienia o naruszeniu danych osobowych,

Nr 22- Wzór notatki z kontroli uprawnień.

STAROSTA
mgr Andrzej Nowicki

Zał. nr 1 do Polityki ochrony danych	**Wzór oświadczenia o zapoznaniu się z Polityką Ochrony Danych**

Ja, niżej podpisany..... oświadczam, iż zapoznałam/zapoznałem się z treścią Polityki Ochrony Danych obowiązującą w Starostwie Powiatowym w Piszu wprowadzoną Zarządzeniem nr 13/2018 Starosty Piskiego z dnia 25 maja 2018 r.

(podpis osoby składającej oświadczenie)

Zał. nr 2 do Polityki ochrony danych	**Wzór oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych**

Wyrażam zgodę na przetwarzanie moich danych osobowych zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), publ. Dz. Urz. UE L Nr 119, s. 1 w celach ....

.....

(data, podpis)

Administratorem danych osobowych przetwarzanych ww. celach jest.....

Zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), publ. Dz. Urz. UE L Nr 119, s. 1 osobie, której dane dotyczą przysługuje prawo:

- żądania dostępu do danych osobowych;

- sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych;

- wniesienia sprzeciwu;

- cofnięcia zgody w każdym momencie, jednak bez wpływu na zgodność z prawem przetwarzania danych osobowych, którego dokonano na podstawie zgody przed jej cofnięciem;

- wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00 – 193 Warszawa.

Zapoznałam/-em się z treścią powyższego.

.....

(data, podpis)

Zał. nr 3 do Polityki ochrony danych	**Wzór odwołania zgody na przetwarzanie danych osobowych**

Zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), publ. Dz. Urz. UE L Nr 119, s. 1 odwołuje wyrażoną przeze mnie zgodę na przetwarzanie danych osobowych w celach

.....

przez.....

.....

(data, podpis)

Zał.nr 4 do Polityki ochrony danych	**Wzór klauzuli informacyjnej**

Zgodnie z art. 13 ust. 1 i ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. informuję, iż:

1. Administratorem Pani/Pana danych osobowych jest

2. W sprawach z zakresu ochrony danych osobowych mogą Państwo kontaktować się z Inspektorem Ochrony Danych pod adresem e-mail: inspektor@cbi24.pl.

3. Dane osobowe będą przetwarzane w celu realizacji obowiązków prawnych ciążących na Administratorze.

4. Dane osobowe będą przetwarzane przez okres niezbędny do realizacji ww. celu z uwzględnieniem okresów przechowywania określonych w przepisach odrębnych, w tym przepisów archiwalnych.

5. Podstawą prawną przetwarzania danych jest art. 6 ust. 1 lit. c) ww. Rozporządzenia.

6. Odbiorcami Pani/Pana danych będą podmioty, które na podstawie zawartych umów przetwarzają dane osobowe w imieniu Administratora.

7. Osoba, której dane dotyczą ma prawo do:

- dostępu do treści swoich danych oraz możliwości ich poprawiania, sprostowania, ograniczenia przetwarzania, a także - w przypadkach przewidzianych prawem - prawo do usunięcia danych i prawo do wniesienia sprzeciwu wobec przetwarzania Państwa danych.

- wniesienia skargi do organu nadzorczego w przypadku gdy przetwarzanie danych odbywa się z naruszeniem przepisów powyższego rozporządzenia tj. Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00-193 Warszawa.

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

Zał. nr 5 do Polityki ochrony danych	**Procedura realizacji uprawnienia: prawo dostępu do danych**

1. Cel procedury

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

Każdej osobie fizycznej przysługuje prawo do uzyskania wyczerpujących informacji od Administratora, w postaci potwierdzenia, czy dane są faktycznie przetwarzane przez Administratora.

Prawo dostępu do danych osobowych jest realizowane poprzez wydanie kopii przetwarzanych danych osobie, której dane dotyczą.

2. Prawa osoby fizycznej, której dane są przetwarzane

Osoba fizyczna, której dane są przetwarzane ma prawo do uzyskania informacji o:

1) celach, w jakich przetwarzane są dane osobowe;
2) kategoriach danych osobowych, które podlegają przetwarzaniu;
3) odbiorcach lub kategoriach odbiorców;
4) planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, kryteriach ustalania okresu przechowywania danych;
5) prawie do żądania sprostowania swoich danych osobowych;
6) prawie do usunięcia lub ograniczenia przetwarzania danych osobowych;
7) prawie do wniesienia sprzeciwu wobec konkretnego przetwarzania swoich danych;
8) prawie do wniesienia skargi do organu nadzorczego, na przetwarzanie swoich danych, jeśli są one przetwarzane niezgodnie z obowiązującymi przepisami;
9) w sytuacji, gdy dane osobowe nie zostały zebrane od osoby, której one dotyczą – wszelkich dostępnych informacje o źródle, z którego administrator pozyskał te dane;
10) zautomatyzowanym podejmowaniu decyzji, jeżeli takie administrator realizuje wobec konkretnej osoby fizycznej taki sposób przetwarzania, w tym informacji o profilowaniu (art. 22 ust. 1 i 4 RODO), jak również wszelkie istotne informacje o zasadach podejmowania takich decyzji oraz

o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby fizycznej, której przetwarzane dane i decyzje dotyczą.

3. Realizacja uprawnienia dostępu do danych

Osoba fizyczna otrzymuje dostęp do swoich danych osobowych poprzez uzyskanie **kopii przetwarzanych danych osobowych.**

Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.

Pierwsza kopia i jej przekazanie odbywa się **bezpłatnie**, lecz za wszelkie kolejne kopie, o które zwróci się podmiot danych, Administrator będzie miał prawo pobrać „opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych" (art. 15 ust. 3 RODO) związanych z jej wytworzeniem (według stawek obowiązujących u Administratora).

Umożliwienie wglądu do danych konkretnej osobie fizycznej nie może powodować naruszenia praw innych osób lub też tajemnic prawnie chronionych.

Uzyskując wgląd do swoich danych osoba fizyczna nie może mieć nieuzasadnionego dostępu do danych innych osób fizycznych, lub do danych stanowiących tajemnicę przedsiębiorstwa.

W przypadku, gdy przetwarzana jest duża ilość informacji o osobie, która chce skorzystać z prawa dostępu do swoich danych, Administrator kieruje do tej osoby żądanie sprecyzowania do jakich konkretnie danych lub też informacji o czynnościach przetwarzania jej danych chciałaby ona uzyskać dostęp.

<u>Terminy na udzielenie odpowiedzi na żądanie:</u>

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

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

Wzór odpowiedzi na skierowany wniosek:

Na podstawie art. 15 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, Administrator potwierdza, że Pana/Pani dane osobowe są przetwarzane i jednocześnie informuje, że:

1) celem przetwarzania Pani/Pana danych osobowych jest …;
2) (administrator) przetwarza Pani/Pana dane osobowe w zakresie … (należy wskazać kategorię danych osobowych);
3) dane osobowe będą ujawniane … (należy wskazać odbiorcę lub kategorie odbiorców);
4) dane osobowe będą przechowywane przez okres …;
5) przysługuje Panu/Pani prawo do sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych, a także prawo do wniesienia sprzeciwu oraz skargi do organu nadzorczego;
6) (administrator) uzyskał Pani/Pana dane osobowe z … (należy wskazać źródło, o ile dane nie zostały pozyskane od osoby, której dotyczą);
7) (należy dodać informacje dotyczące zautomatyzowanego podejmowania decyzji, w tym profilowania, o ile znajduje to zastosowanie).

_____

(data, podpis)

Zał. nr 6 do Polityki ochrony danych	**Procedura: prawo do sprostowania danych osobowych**

1. Cel procedury

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

2. Prawa osoby fizycznej, której dane są przetwarzane

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

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

3. Procedura rozpatrywania żądań o sprostowanie danych osobowych

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

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

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

Działania podejmowane na podstawie żądania o sprostowanie lub uzupełnienie danych są zwolnione z opłat (art. 12 ust. 5 RODO), lecz jeżeli żądania osoby, której dane dotyczą są ewidentnie nieuzasadnione

lub nadmierne (np. ze względu na swój ustawiczny charakter) Administratorowi przysługują dwa uprawnienia:

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

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

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

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

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

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

Terminy na udzielenie odpowiedzi na żądanie:

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

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

Zał. nr 6 do Polityki ochrony danych	**Procedura: prawo do sprostowania danych osobowych**

Wzór wniosku o sprostowanie/uzupełnienie

danych osobowych

.....

Imię i nazwisko

.....

Adres zamieszkania / adres poczty elektronicznej

wnioskuję o dokonanie sprostowanie / uzupełnienie moich danych osobowych, w postaci: _____

/należy wymienić o jakie kategorie danych osobowych chodzi oświadczającemu/wnioskującemu/

Podstawa do dokonania sprostowania / uzupełnienia:_____

_____

(np. decyzja administracyjna, inny akt prawny, dokument (do wglądu) osobie przyjmującej oświadczenie / wniosek* upoważnionej do tej czynności przez Administratora)

_____

/data i czytelny podpis osoby składającej wniosek /

Zał. nr 7 do Polityki ochrony danych	**Procedura: prawo do usunięcia danych osobowych („prawo do bycia zapomnianym")**

1. Cel procedury

Celem procedury jest realizacja uprawnienia osoby fizycznej prawa usunięcia swoich danych osobowych („prawo do bycia zapomnianym") przetwarzanych przez Administratora.

2. Prawa osoby fizycznej, której dane są przetwarzane

I. Każdej osobie fizycznej przysługuje jednakowe prawo żądania usunięcia jego danych osobowych przetwarzanych przez Administratora.

Składa się ono z następujących uprawnień:

1) możliwości żądania przez osobę, której dane dotyczą, usunięcia jej danych osobowych przez Administratora danych,
2) możliwości żądania, aby Administrator danych poinformował innych administratorów danych, którym upublicznił dane osobowe, że osoba, której dane dotyczą, żąda, by ci administratorzy usunęli wszelkie łącza do tych danych lub ich kopie, czy ich replikacje.

Obowiązek poinformowania innych administratorów danych może być ograniczony przez:

1) dostępną technologię,
2) koszty,
3) konieczność ograniczenia się Administratora do „rozsądnych działań".

Administrator, w przypadku podjęcia decyzji, o ograniczeniu poinformowania innych administratorów danych ma obowiązek wykazania takich ograniczeń w ewentualnym postępowaniu przed organem nadzorczym.

II. Każdemu podmiotowi danych przysługuje jednakowe prawo do „bycia zapomnianym."

Prawo to można wykonać, jeżeli spełniona jest choć jedna z następujących przesłanek:

1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
2) osoba, której dane dotyczą, wycofała zgodę na przetwarzanie danych osobowych i nie istnieje inna podstawa przetwarzania danych;
3) osoba, której dane dotyczą, zgłosiła sprzeciw wobec przetwarzania swoich danych w związku ze swoją szczególną sytuacją albo wobec przetwarzania danych dla celów marketingowych;
4) dane osobowe były przetwarzane w sposób „niezgodny z prawem";

5) dane osobowe „muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega Administrator";
6) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego bezpośrednio dziecku.

W przypadku wykonania prawa do bycia zapomnianym, Administrator zaprzestaje przetwarzania danych osobowych i usuwa dane osoby, która złożyła stosowne oświadczenie/ wniosek, chyba że zachodzą szczególne przypadki ograniczające prawo do bycia zapomnianym:

1) istnieje przepis prawa, który nakazuje przetwarzanie danych osobowych,
2) istnieje sytuacja, w której przetwarzanie jest niezbędne do ustalenia dochodzenia lub obrony roszczeń.

Wzór wniosku o usunięcie danych osobowych (prawo do bycia zapomnianym)

.....

Imię i nazwisko

.....

Adres zamieszkania / adres poczty elektronicznej

/ wnioskuję* o dokonanie usunięcia moich danych osobowych, w postaci:_____

/należy wymienić o jakie kategorie danych osobowych chodzi wnioskującemu/

.....

/ czytelny podpis osoby składającej wniosek

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

1. Cel procedury

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

2. Prawa osoby fizycznej, której dane są przetwarzane

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

Prawo do przenoszenia danych to, w szczególności prawo do:

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

Prawo do przeniesienia danych może zostać wykonane, gdy:

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

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

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

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

Wzór wniosku o przeniesienie danych osobowych

.....

Imię i nazwisko

.....

Adres zamieszkania / adres poczty elektronicznej

Wnioskuję o dokonanie przeniesienia moich danych osobowych, w postaci_____

_____

/należy wymienić o jakie kategorie danych osobowych chodzi oświadczającemu/wnioskującemu/

(np. decyzja administracyjna, inny akt prawny, dokument (do wglądu), opis sytuacji, mającej podstawę do usunięcia danych osobowych okazane osobie przyjmującej oświadczenie / wniosek* upoważnionej do tej czynności przez Administratora)

Nazwa podmiotu, do którego należy przenieść dane osobowe wymienione w pkt. 2. : _____

_____

_____

/data i czytelny podpis /

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

1. Cel procedury

Celem procedury jest realizacja uprawnienia osoby fizycznej prawa do sprzeciwu do przetwarzania swoich danych osobowych przez Administratora.

2. Prawa osoby fizycznej, której dane są przetwarzane

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

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

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

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

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

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

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

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

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

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

Profilowanie to szczególny rodzaj przetwarzania danych osobowych, który:

- odbywa się w sposób automatyczny,
- ma na celu ocenę osoby fizycznej lub przewidywanie jej zachowania.

Profilowanie zawsze wymaga poinformowania (w sposób możliwy do zweryfikowania) o nim osób, które są profilowane.

Profilowanie może być wykorzystywane jako narzędzie dla tzw. automatycznego podejmowania decyzji Administratora wobec osób, których dane dotyczą.

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

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

Jeżeli profilowanie miałoby się odbywać w oparciu o szczególne kategorie danych osobowych, wówczas jedyną podstawą prawną, która mogłaby takie profilowanie zalegalizować, może być szczególny przepis prawa.

Jeżeli zgoda na profilowanie została pobrana przy pomocy dedykowanej strony internetowej, odwołanie zgody musi być możliwe w ten sam sposób.

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

4. Realizacja prawa do sprzeciwu

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

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

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

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

Aby dane osobowe zostały całkowicie usunięte konieczne jest skorzystanie przez osobę, której dane przetwarza Administrator konieczne jest skorzystanie z prawa do usunięcia danych osobowych – prawa do bycia zapomnianym.

Zał. nr 10 do Polityki ochrony danych	**Wzór wniosku o nadanie upoważnienia do przetwarzania danych osobowych/uprawnienia do pracy w systemie informatycznym**

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

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

Zatrudnionemu/onej w .....

Na stanowisku.....

☐ do przetwarzania danych osobowy w zakresie:

1. .....

2. .....

3. .....

☐ do pracy w systemach informatycznych:

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

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

.....
(data i podpis osoby składającej wniosek)

Zał.nr 11 do Polityki ochrony danych	**Wzór upoważnienia do przetwarzania danych osobowych**

……..,dnia……roku

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE upoważniam:

Pana/ Panią ……

Zatrudnionego/zatrudnioną w ……Na stanowisku……do przetwarzania danych osobowych w następujących celach:

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

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

(podpis Naczelnika Wydziału)

(pieczęć i podpis Administratora)

(podpis Pracownika)

REJESTR WYDANYCH UPOWAŻNIEŃ I PEŁNOMOCNICTW - RODO

Lp.	Data wydania	Imię i nazwisko osoby upoważnionej	Zajmowane stanowisko służbowe	Zakres upoważnienia	Okres obowiązywania

Zał.nr 13 do Polityki ochrony danych	**Opis środków technicznych i organizacyjnych**

Środki zabezpieczające obiekt Starostwa Powiatowego w Piszu - Warszawska 1:

Monitoring wizyjny wewnętrzny i zewnętrzny, alarm pożarowy, alarm antywłamaniowy, drzwi i zamki antywłamaniowe w drzwiach wejściowych, w newralgicznych pomieszczeniach obiektu znajdują się drzwi z kontrolą dostępu na osobiste karty magnetyczne pracowników. Obiekt jest również chroniony przez firmę zewnętrzną powiadamianą o zdarzeniach w trybie automatycznym drogą radiową.

Wykaz systemów informatycznych służących do przetwarzania danych osobowych:

1. Wydział Finansowy:
    a. Płatnik
    b. System firmy Progman: Kadry, Płace, Przelewy, Zlecone
    c. System firmy Progman: FK, Rozrachunki, Zbiorczy Vat, Wyposażenie
2. Wydział Organizacyjny:
    a. System firmy Progman: Kadry, Płace
3. Wydział Geodezji, Kartografii i Katastru:
    a. Systemy Firmy Geobid: EwOpis, Ośrodek
    b. System archiwalny EGiB
4. Wydział Gospodarki Nieruchomościami:
    a. Systemy Firmy Geobid: Mienie, EwOpis
5. Wydział Komunikacji i Transportu:
    a. System archiwalny Zeto Katowice: Kierowca, Pojazd
6. Wydział Zagospodarowania Przestrzennego i Budownictwa:
    a. Systemy Firmy Geobid: EwOpis
7. Wydział Rolnictwa, Leśnictwa, Rybactwa Śródlądowego, Ochrony Środowiska i Gospodarki Wodnej:
    a. Systemy Firmy Geobid: EwOpis
8. Powiatowy Rzecznik Konsumentów:
    a. Rejestr w formie arkusza Excel z danymi prowadzonych spraw
9. Wszystkie wydziały:
    a. Każdy pracownik posiada na swoim komputerze lokalne dane programu pocztowego zawierające potencjalnie dane osobowe
    b. Pliki aplikacji biurowych np. Word, Excel znajdujące się lokalnie na komputerze pracownika lub na dostępnych dla niego zasobach sieciowych

Kopie zapasowe

Dane osobowe przetwarzane w formie elektronicznej, w szczególności w systemach informatycznych podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiadają Informatycy.

Kopią zapasową objęte są:

	Częstotliwość wykonywania kopii zapasowej	Rodzaj nośnika na jakim wykonano kopię zapasową	Sposób wykonywania kopii	Miejsce przechowywania nośnika na którym zapisano kopię
Bazy danych	Codziennie	NAS	Automatyczna	NAS
Serwery	Codziennie	NAS	Automatyczna	NAS
Pliki	Codziennie	NAS	Automatyczna	NAS

Sposób postępowania z kluczami do pomieszczeń biurowych

Administrator wyznaczył pracowników, którzy są upoważnieni do otwierania głównych drzwi wejściowych do budynku oraz do rozkodowywania systemu alarmowego przed rozpoczęciem pracy jednostki. Pracownik, któremu zostały powierzone klucze oraz kod cyfrowy do systemu alarmowego zobowiązany jest do nie udostępniania kluczy oraz kodu cyfrowego do systemu alarmowego osobom trzecim.

Klucze do poszczególnych pomieszczeń pracownicy pobierają i zdają po zakończonym dniu pracy do Punktu Obsługi Klienta. Od momentu pobrania kluczy do momentu ich zdania na pracownikach spoczywa pełna odpowiedzialność za ich zabezpieczenie. Po otwarciu pomieszczeń biurowych, przed przystąpieniem do pracy, pracownicy sprawdzają stan zastosowanych zabezpieczeń. W przypadku stwierdzenia nieprawidłowości należy postępować zgodnie z procedurą naruszeń stanowiącą ***załącznik nr 18*** 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 pracowników w sposób uniemożliwiający dostęp osobom nieupoważnionym.

Pracownicy 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.

Zał. nr 14 do Polityki ochrony danych	**Wzór oświadczenia o zachowaniu w poufności danych**

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

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

.....

(podpis pracownika)

Zał.nr 15 do Polityki ochrony danych	**Oświadczenie o monitorowaniu komputerów służbowych**

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

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

(podpis osoby składającej oświadczenie)

* - niepotrzebne skreślić

Zał.nr 16 do Polityki ochrony danych	**Wzór umowy powierzenia**

UMOWA
POWIERZENIA DANYCH OSOBOWYCH DO PRZETWARZANIA

zawarta w dniu _____ r. w _____
pomiędzy:

_____ _____ _____
z siedzibą w _____. (___ - _____),
ul. _____ ,
NIP _____, reprezentowaną przez:
_____ – *(funkcja)*
_____ – *(funkcja)*
zwaną w treści Umowy „**Administratorem**",

a

_____ _____ _____
z siedzibą w _____. (___ - _____),
ul. _____ , NIP
_____, reprezentowaną przez:
_____ – *(funkcja)*
_____ – *(funkcja)*
zwaną w treści Umowy **„Procesorem"** lub **„Przetwarzającym",**
w dalszej części Umowy Administrator i Procesor są nazywani łącznie „**Stronami**" lub każde oddzielnie „**Stroną**".

§ 1

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

1. Umowa ma charakter umowy powierzenia danych osobowych w rozumieniu art. 28 ust. 1 i 3 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych; Dz. U. UE. L. 2016, poz. 119.1), zwanego w dalszej części Umowy jako: „Rozporządzenie".
2. Procesor uprawniony jest do przetwarzania danych osobowych wyłącznie w celu wykonania umowy głównej, tj. umowy z dnia _____ , której przedmiotem jest _____, które będzie zwane w dalszej części Umowy jako „przetwarzanie" .
3. Przetwarzanie dotyczyć będzie (*wskazać kategorie osób oraz rodzaj danych,)*

§ 2

Czas trwania Umowy

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

§ 3

Warunki powierzenia danych osobowych do przetwarzania

1. Procesor przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora oraz:
   a) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
   b) podejmuje odpowiednie środki techniczne oraz organizacyjne, mające na celu zapewnienia bezpieczeństwa danych osobowych;
   c) nie korzysta z usług innego podmiotu przetwarzającego, bez uprzedniej pisemnej zgody Administratora;
   d) w miarę możliwości pomaga Administratorowi, poprzez odpowiednie środki techniczne i organizacyjne, wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w art. 12-23 Rozporządzenia;
   e) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32-36 Rozporządzenia;
   f) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji Administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, w tym również te, zawarte na nośnikach danych, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;
   g) udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia oraz umożliwia Administratorowi

(lub upoważnionemu przez niego audytorowi) przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

2. Jeżeli powierzone dane osobowe są przetwarzane w formie elektronicznej na serwerach i nośnikach danych Procesora, te serwery i nośniki nie mogą znajdować się poza obszarem Unii Europejskiej i Europejskiego Obszaru Gospodarczego.
3. Procesor zobowiązuje się do każdorazowego i niezwłocznego informowania Administratora o przypadkach naruszenia przepisów prawa dotyczących ochrony powierzonych danych osobowych, w tym w szczególności przepisów Rozporządzenia, zaistniałych w okresie obowiązywania niniejszej Umowy.
4. W przypadku stwierdzenia naruszenia ochrony danych osobowych, o którym mowa w art. 33 Rozporządzenia, Procesor zgłasza je Administratorowi bez zbędnej zwłoki. Zgłoszenie naruszenia ochrony danych osobowych Administratorowi powinno nastąpić w formie pisemnej lub elektronicznej.
5. Na wypadek zawinionego naruszenia przez Procesora zasad przetwarzania danych osobowych (określonych w przepisach powszechnie obowiązującego prawa, Rozporządzenia oraz niniejszej Umowy), skutkującego zobowiązaniem Administratora na mocy prawomocnego orzeczenia sądu, ugody sądowej bądź porozumienia mediacyjnego do wypłaty odszkodowania, zadośćuczynienia lub kary pieniężnej, Procesor zobowiązuje się zrekompensować Administratorowi udokumentowane straty z tego tytułu w pełnej wysokości. Zobowiązanie Procesora, o którym mowa powyżej, powstanie pod warunkiem pisemnego powiadomienia go o każdym przypadku wystąpienia przez osoby trzecie z roszczeniem wobec Administratora z podaniem podstaw prawnych i faktycznych, w terminie 3 dni od daty dowiedzenia się Administratora o takim roszczeniu.
6. Procesor jest zwolniony z odpowiedzialności za szkody spowodowane przetwarzaniem przez niego danych naruszającym przepisy prawa, jeżeli nie można mu przypisać winy za zdarzenie, które doprowadziło do powstania szkody.
7. Procesor zapewnia, że dane osobowe nie będą udostępniane jego pracownikom i zleceniobiorcom przed podpisaniem przez nich oświadczeń lub umów o zachowaniu poufności. Zachowanie poufności nie ustaje po rozwiązaniu lub wygaśnięciu stosunku pracy lub umowy cywilnoprawnej, niezależnie od przyczyny tego rozwiązania lub wygaśnięcia.
8. Procesor zobowiązuje się do monitorowania i stosowania przepisów prawa, powszechnie dostępnych wskazówek i zaleceń organu nadzorczego oraz unijnych organów doradczych, zajmujących się ochroną danych osobowych, w zakresie przetwarzania powierzonych mu

danych, po uprzednim uzgodnieniu wpływu tych regulacji na przetwarzanie danych z Administratorem.

§ 4

Kontrola przetwarzania danych powierzonych

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

§ 5

Podpowierzenie danych

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

§ 6

Przetwarzanie powierzonych danych po rozpoczęciu stosowania ogólnego rozporządzenia o ochronie danych (Rozporządzenia)

1. Strony zgodnie postanawiają, iż począwszy od dnia rozpoczęcia stosowania Rozporządzenia (tj. od 25 maja 2018 r.), bez uszczerbku dla pozostałych postanowień niniejszej Umowy, zastosowanie znajdą postanowienia zawarte w § 3 Umowy.

2. Procesor oświadcza, iż jest świadomy zmiany przepisów dotyczących ochrony danych osobowych na skutek wejścia w życie Rozporządzenia i tym w związku z tym oświadcza, że przetwarzanie powierzonych mu danych osobowych, najpóźniej od dnia 25 maja 2018 r. będzie odbywało się z poszanowaniem przepisów Rozporządzenia oraz krajowych przepisów polskich z zakresu ochrony danych osobowych.
3. Strony postanawiają, że zawarcie niniejszej Umowy stanowi udokumentowane polecenie Administratora, o którym stanowi art. 28 ust. 3 lit. a Rozporządzenia.

§ 7
Poufność

1. Procesor zobowiązuje się do zachowania w tajemnicy wszelkich danych osobowych, informacji i materiałów przekazanych lub udostępnionych mu lub o których wiedzę powziął w związku z realizacją Umowy, a także powstałych w wyniku jej wykonania informacji i materiałów w formie pisemnej, graficznej lub jakiejkolwiek innej formie. Informacje i materiały są objęte tajemnicą nie mogą być bez uprzedniej pisemnej zgody Administratora udostępniane jakiejkolwiek osobie trzeciej, ani też ujawnione w inny sposób, chyba że w dniu ich ujawnienia były powszechnie znane albo muszą być ujawnione zgodnie z powszechnie obowiązującymi przepisami prawa, orzeczeniem sądu lub organu państwowego.
2. Procesor zapewnia, że osoby upoważnione do przetwarzania danych osobowych będą obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia. Obowiązek zachowania tajemnicy nie ustaje po zaprzestaniu przetwarzania danych z jakiejkolwiek podstawy. Przepis § 3 ust. 6 Umowy stosuje się odpowiednio.

§ 8
Współpraca Stron

1. Strony ustalają, że podczas realizacji Umowy powierzenia będą ze sobą ściśle współpracować, informując się wzajemnie o wszystkich okolicznościach mających lub mogących mieć wpływ na wykonanie powierzenia danych osobowych.
2. Strony będą dokonywały uzgodnień i podejmowały decyzje operacyjne poprzez swoich przedstawicieli odpowiedzialnych za realizację Umowy w formie ustnej, pisemnej lub elektronicznej.

3. Strony zobowiązują się, że wszelkie decyzje dotyczące polubownego zakończenia sporu z osobą fizyczną na skutek naruszenia ochrony jej danych osobowych, w szczególności fakt i wysokość wypłaty ewentualnego odszkodowania, podejmą wspólnie.

§ 9

Wypowiedzenie umowy

1. Każdej ze Stron przysługuje uprawnienie do rozwiązania Umowy z zachowaniem miesięcznego terminu wypowiedzenia ze skutkiem na koniec miesiąca kalendarzowego, w którym oświadczenie o wypowiedzeniu zostało doręczone drugiej stronie.
2. Administrator ma prawo wypowiedzieć Umowę w trybie natychmiastowym, w przypadku rażącego naruszenia postanowień Umowy przez Procesora, który:
   a) wykorzystał dane osobowe w sposób niezgodny z Umową, w szczególności przetwarzał je dla własnych celów lub celów innych podmiotów, a także celów niezgodnych z powszechnie obowiązującymi przepisami prawa lub postanowieniami niniejszej Umowy;
   b) wykonuje Umowę niezgodnie z obowiązującymi w tym zakresie przepisami prawa lub instrukcjami Administratora w tym zakresie;
   c) nie zaprzestał niewłaściwego przetwarzania danych osobowych mimo uprzedniego wezwania Administratora do usunięcia naruszeń i bezskutecznego upływu wyznaczonego terminu 14 dni na zaniechanie naruszeń.

§ 10

Postanowienia Końcowe

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

_____ _____

(Administrator) **(Procesor)**

Zał. nr 17 do Polityki ochrony danych	**Wzór rejestru umów powierzenia przetwarzania danych osobowych**

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

Zał. nr 18 do Polityki ochrony danych	**Procedura zgłaszania naruszeń ochrony danych osobowych**

1. Cel procedury

Celem procedury jest zminimalizowanie mogących wystąpić nieprawidłowości w funkcjonowaniu Zakładu, spowodowanych nieuprawnionym ujawnieniem danych osobowych, udostępnieniem lub umożliwieniem dostępu do nich osobom nieupoważnionym, zabraniem danych przez osobę nieupoważnioną, uszkodzeniem lub usunięciem, a w szczególności:

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

2. Klasyfikacja naruszeń

Naruszenia ze względu na ich występowanie możemy podzielić na:

1. zdarzenia losowe **zewnętrzne**, których występowanie może doprowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej, zakłócenia ciągłości pracy systemów (np. klęski żywiołowe, przerwy w zasilaniu);
2. zdarzenia losowe **wewnętrzne**, których występowanie może doprowadzić do zniszczenia danych, zakłócenia ciągłości pracy systemu, może nastąpić naruszenie poufności danych (np. niezamierzone pomyłki operatorów, administratorów, awarie sprzętowe, błędy w oprogramowaniu);
3. zdarzenia zamierzone, celowe i świadome, niepowodujące uszkodzenia infrastruktury technicznej i zakłóceń ciągłości pracy możemy podzielić na:
    a) nieuprawniony dostęp do bazy danych z zewnątrz
    b) nieuprawniony dostęp do bazy danych z sieci wewnętrznej
    c) nieuprawniony transfer danych
    d) pogorszenie funkcjonowania sprzętu i oprogramowania np. działania wirusów
    e) bezpośrednie zagrożenie materialnych składników systemu np. kradzież sprzętu.

3. Zgłaszanie naruszeń związanych z bezpieczeństwem informacji

W przypadku stwierdzenia naruszenia zabezpieczeń lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik przetwarzający dane osobowe zobowiązany jest przerwać czynności i niezwłocznie zgłosić ten fakt bezpośredniemu przełożonemu, a następnie postępować stosownie do podjętej przez niego decyzji.

Pracownicy jednostki mają obowiązek zgłaszać zauważone przez siebie naruszenia oraz notować wszystkie szczegóły związane z naruszeniami.

Zgłoszenie powinno zawierać:

a) imię i nazwisko zgłaszającego,
b) określenie sytuacji i czasu w jakim stwierdzono naruszenie zabezpieczeń danych osobowych;
c) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia;
d) określenie znanych zgłaszającemu sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

Osoba zgłaszająca naruszenie w miarę możliwości powinna zabezpieczyć materiał dowodowy np.: zrobić zdjęcie ekranu komputera, co do którego zaistniało podejrzenie, że jego działanie odbiega od normy. Osobą odpowiedzialną za przyjmowanie zgłoszeń naruszeń w jednostce jest Sekretarz Powiatu.

4. Postępowanie z naruszeniami

Osoba, która otrzymała zgłoszenie dokonuje wstępnej identyfikacji zdarzenia i po konsultacji z Inspektorem Ochrony Danych Osobowych dokonuje jego kwalifikacji jako naruszenie niskie lub wysokie. W przypadku kwalifikacji naruszenia jako niskie należy dokonać wpisu do rejestru naruszeń, którego wzór stanowi ***załącznik nr 19*** do Polityki ochrony danych. Naruszenia zakwalifikowane jako wysokie podlegają zgłoszeniu do organu nadzorczego niezwłocznie, jednak nie później niż po upływie 72 godzin po stwierdzeniu naruszenia. W przypadku wysokiego naruszenia należy powołać Zespół ds. oceny naruszeń powołany Zarządzeniem Starosty w składzie: Sekretarz Powiatu, Naczelnik Wydziału w którym nastąpiło naruszenie, Informatycy oraz Inspektor Ochrony Danych Osobowych.
Zespół dokonuje analizy naruszenia pod kątem

a) charakter incydentu i jego znaczenie związane z naruszeniem bezpieczeństwa fizycznego lub teleinformatycznego,
b) miejsce wystąpienia incydentu - identyfikacja punktu, w którym nastąpiło zdarzenie (lokalizacja, serwer, stacja robocza itp.),
c) liczba referatów/komórek organizacyjnych dotkniętych incydentem,
d) identyfikację zasobów potrzebnych przy dalszych działaniach w ramach postępowania z incydentem związanym z bezpieczeństwem informacji,
e) możliwości rozszerzania się incydentu i sposoby jego ograniczania,
f) szacowany poziom szkód,
g) szacunkowy czas, po którym skutki naruszenia zostaną zlikwidowane, jeżeli nie ma możliwości natychmiastowego usunięcia stanu naruszenia bezpieczeństwa informacji,
h) skutki organizacyjne i prawne (wstępny szacunek).

Po dokonanej analizie Administrator zgłasza naruszenie do organu nadzorczego (wzór zgłoszenia stanowi ***załącznik nr 20*** do Polityki ochrony danych),

oraz jeżeli naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu (wzór zawiadomienia stanowi ***załącznik nr 21*** do Polityki ochrony danych). Zawiadomienie osoby nie jest wymagane jeśli Administrator wdrożył odpowiednie techniczne i organizacyjne środki, które uniemożliwią osobom nieuprawnionym dostęp do danych, zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą. Z zawiadomienia o którym mowa wyżej można nie należy stosować gdy wymagałoby to niewspółmiernie dużego wysiłku. W takim jednak wypadku należy opublikować ogłoszenie, zastosować inny, równie skuteczny środek.

Jeżeli z jakiegokolwiek powodu nie uda się przekazać zgłoszenia w tym terminie, do zgłoszenia należy dołączyć wyjaśnienie przyczyn opóźnienia. Jeżeli Administrator nie zawiadomił jeszcze o naruszeniu osób, których ono dotyczy, organ nadzorczy może mu to nakazać.

Dodatkowo naruszenia mogą być wykorzystywane przez Inspektora Ochrony Danych podczas szkoleń pracowniczych jako przykład tego, co może się wydarzyć, jak unikać ich w przyszłości i jak reagować jak się wydarzą. Podczas wykorzystywania powyższych informacji należy wykazać się daleko idącą ostrożnością w aspekcie zachowywania poufności.

Zał. nr 19 do Polityki ochrony danych	**Wzór rejestru naruszeń ochrony danych**

Lp.	Data Naruszenia	Kategoria Osób	Charakter Naruszenia	Kwalifikacja naruszenia (niskie lub wysokie)	Zastosowane środki zaradcze	Zgłoszenie do organu nadzorczego (dotyczy lub nie dotyczy)	Zawiadomienie osoby której dane dotyczą (dotyczy lub nie dotyczy)	Uzasadnienie zwolnienia z zawiadomienia osoby, której dane zostały naruszone
1.								
2.								
3.								
4.								

Zał. nr 20 do Polityki ochrony danych	**Wzór zgłoszenia naruszenia ochrony danych organowi nadzorczemu**

.....dnia.....

Urząd Ochrony Danych Osobowych

.....

Zgłoszenie o naruszeniu ochrony danych osobowych organowi nadzorczemu

Na podstawie obowiązku wynikającego z art. 33 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

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

.....

(Podpis Administratora)

Zał. nr 21 do Polityki ochrony danych	**Wzór zawiadomienia o naruszeniu danych osobowych**

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

Pan/Pani .....

.....

.....

ZAWIADOMIENIE O NARUSZENIU DANYCH OSOBOWYCH

Na podstawie obowiązku wynikającego z art. 34 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) w związku z naruszeniem Pana/Pani danych osobowych w zakresie ..... Zawiadamiamy co następuje:

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

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

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

.....

(Podpis Administratora)

Zał. 22 do Polityki ochrony danych	**Wzór notatki z kontroli uprawnień**

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

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

1. Użytkownicy pracują na systemach zgodnych z ich uprawnieniami TAK/NIE
   Jeśli NIE, należy wskazać pracowników którym należy nadać lub zabrać upoważnienia:
   .....
   .....
2. Użytkownicy posiadają na stacjach roboczych oprogramowanie na które jednostka posiada licencje
   TAK/NIE
   Jeśli NIE, należy wykazać to oprogramowania oraz nazwy stacji roboczych, na których się ono znajduje
   .....
   .....
3. Na stacjach roboczych pracowników znajduje się oprogramowanie nie związane z pracą służbową np. komunikatory społecznościowe, aplikacje służące do wymiany lub pobierania plików, czytniki prywatnej poczty, oprogramowanie umożliwiające dostęp do prywatnej chmury z danymi itp. portalami społecznościowymi
   TAK/NIE
   Jeśli TAK należy wskazać pracowników oraz stacje robocze, na których zostało zidentyfikowane wyżej wymienione oprogramowanie:
   .....
   .....
4. Czy na stacjach roboczych pracowników znajdują się dokumenty i korespondencja nie związana z czynnościami służbowymi
   TAK/NIE
   Jeśli TAK należy wskazać pracowników oraz stacje robocze na której niezgodności występują:
   .....
   .....
5. Wnioski i zalecenia pokontrolne:
   .....
   .....

.....
(podpis Informatyka)