WÓJT GMINY
Zbójno
woj. kujawsko-pomorskie

Zarządzenie nr 83/2018
Wójta Gminy Zbójno
z dnia 10 grudnia 2018 r.

w sprawie wprowadzenia dokumentacji ochrony danych osobowych przetwarzanych w Urzędzie Gminy Zbójno

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2017 r. poz. 1875 z późn. zm.), w związku z motywem 78, 83 i 84 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, Dz. Urz. UE. z dnia 4 maja 2016 r.), zarządzam co następuje:

§1. Wprowadzam następującą dokumentację ochrony danych osobowych przetwarzanych w Urzędzie Gminy Zbójno:

1) politykę bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno stanowiącą załącznik nr 1 do zarządzenia;

2) instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Zbójno stanowiącą załącznik nr 2 do zarządzenia;

3) instrukcję postępowania w przypadku zagrożenia bezpieczeństwa danych osobowych oraz instrukcję postępowania w przypadku incydentów bezpieczeństwa danych osobowych w Urzędzie Gminy Zbójno stanowiącą załącznik nr 3 do zarządzenia;

4) procedura zarządzania oprogramowaniem komputerowym w Urzędzie Gminy Zbójno stanowiąca załącznik nr 4 do zarządzenia;

5) procedura privacy by design i privacy by default w Urzędzie Gminy Zbójno stanowiąca załącznik nr 5 do zarządzenia;

6) regulamin użytkowania komputerów przenośnych Urzędu Gminy Zbójno stanowiący załącznik nr 6 do zarządzenia.

§2. Traci moc zarządzenie nr 1/2016 Wójta Gminy Zbójno z dnia 5 stycznia 2016 r. w sprawie przyjęcia polityki bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno oraz instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Zbójno.

§3. Zobowiązuje wszystkich pracowników Urzędu Gminy Zbójno do zapoznania się z niniejszą dokumentacją oraz przestrzegania jej postanowień.

§4. Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT
mgr Katarzyna Kukielska

Załącznik nr 1 do zarządzenia nr 83/2018 Wójta Gminy Zbójno z dnia 10 grudnia 2018 r. w sprawie wprowadzenia dokumentacji przetwarzania danych osobowych w Urzędzie Gminy Zbójno.

Polityka bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno

ROZDZIAŁ I
Wprowadzenie do polityki.

1. Polityka bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno *(zwana dalej polityką)* jest to zbiór opracowań, instrukcji i wzorów określających nadrzędny cel – bezpieczeństwo informacji oraz sposobów ich zabezpieczenia w Urzędzie Gminy Zbójno.

Polityka posiada trzy fazy:

1) planowanie – określenie celów, analiza ryzyka;
2) wdrażanie – akceptacja rozwiązań, realizacja planów, szkolenie i edukacja;
3) eksploatacje – nadzór, kontrola, monitoring aktywów, plany awaryjne, przegląd zarządzania.

Polityka powinna zawierać:

1) definicje i objaśnienia;
2) zasady gromadzenia danych;
3) sposób udzielania informacji;
4) zasady rejestracji operacji przetwarzania danych osobowych;
5) podział odpowiedzialności;
6) dokument polityki jest opracowaniem, które nie zawiera szczegółów technicznych;
7) reglamentowanie dostępu użytkowników;
8) systematyczne przypominanie o zasadach ochrony danych;
9) sposób i zasady przeprowadzania audytów bezpieczeństwa.

2. Wójt Gminy Zbójno, świadomy wagi zagrożeń prywatności, w tym zwłaszcza zagrożeń dla danych osobowych przetwarzanych w związku z wykonywaniem zadań administratora danych, deklaruje podejmowanie wszelkich możliwych działań koniecznych do zapobiegania zagrożeniom, m. in. takim jak:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. pożar, zalanie pomieszczeń, katastrofa budowlana, napad, kradzież, włamanie, działania terrorystyczne, niepożądana ingerencja ekipy remontowej;
2) niewłaściwe parametry środowiska zakłócające pracę urządzeń komputerowych (nadmierna wilgotność lub bardzo wysoka temperatura, oddziaływanie pola elektromagnetycznego i inne);
3) awarie sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne naruszenia ochrony danych, niewłaściwe działanie serwisantów, w tym pozostawienie serwisantów bez nadzoru, a także przyzwolenie na naprawę sprzętu zawierającego dane poza siedzibą administratora danych;

4) podejmowanie pracy w systemie z przełamaniem lub zaniechaniem stosowania procedur ochrony danych, np. praca osoby, która nie jest upoważniona do przetwarzania danych osobowych, próby stosowania nie swojego hasła i identyfikatora przez osoby upoważnione;

5) celowe lub przypadkowe rozproszenie danych w Internecie z ominięciem zabezpieczeń systemu lub wykorzystaniem błędów systemu informatycznego administratora danych;

6) ataki z Internetu;

7) naruszenia zasad i procedur określonych w dokumentacji z zakresu ochrony danych osobowych przez osoby upoważnione do przetwarzania danych osobowych, związane z nieprzestrzeganiem procedur ochrony danych, w tym zwłaszcza:

a) niezgodne z procedurami zakończenie pracy lub opuszczenie stanowiska pracy (nieprawidłowe wyłączenie komputera, niezablokowanie wyświetlenia treści pracy na ekranie komputera przed tymczasowym opuszczeniem stanowiska pracy, pozostawienie po zakończeniu pracy nieschowanych do zamykanych na klucz szaf i biurek dokumentów zawierających dane osobowe, niezamknięcie na klucz biura po jego opuszczeniu, nieoddanie klucza do sekretariatu);

b) naruszenie bezpieczeństwa danych osobowych przez nieautoryzowane ich przetwarzanie;

c) ujawnienie osobom nieupoważnionym procedur ochrony danych osobowych stosowanych u administratora danych;

d) ujawnienie osobom nieupoważnionym danych przetwarzanych przez administratora danych, w tym również nieumyślne ujawnienie danych osobom postronnym, przebywającym bez nadzoru lub niedostatecznie nadzorowanym w pomieszczeniach administratora danych;

e) niewykonywanie stosownych kopii zapasowych;

f) przetwarzanie danych osobowych w celach prywatnych;

g) wprowadzanie zmian do systemu informatycznego administratora danych i instalowanie programów bez zgody administratora systemu.

ROZDZIAŁ II

Cel polityki, zakres zastosowania.

3. Wdrożenie polityki u administratora danych ma na celu zabezpieczenie przetwarzanych przez niego danych osobowych, w tym danych przetwarzanych w systemie informatycznym i poza nim, poprzez wykonanie obowiązków wynikających z przepisów prawa krajowego i Unii Europejskiej w zakresie ochrony danych osobowych.

4. W związku z tym, że system informatyczny administratora danych jest połączony z siecią publiczną, niniejsza polityka służy zapewnieniu wysokiego poziomu bezpieczeństwa danych osobowych. Niniejszy dokument opisuje niezbędny do uzyskania tego bezpieczeństwa zbiór procedur i zasad dotyczących przetwarzania danych osobowych oraz ich zabezpieczenia.

5. Polityka dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny, tj. w formie papierowej jak i w systemach informatycznych.

6. Polityka obowiązuje w Urzędzie Gminy Zbójno.

7. Procedury i zasady określone w polityce stosuje się do wszystkich osób, zarówno zatrudnionych na podstawie umowy o pracę, powołania, wyboru, umów cywilno-prawnych, jak i innych, np. praktykantów, stażystów, pracowników interwencyjnych i robotników publicznych.

ROZDZIAŁ III

Podstawy prawne, przepisy ogólne, definicje i objaśnienia.

8. Zasady przetwarzania danych osobowych w szczególności regulują:

1) 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;

2) ustawa o ochronie danych osobowych z dnia 10 maja 2018 r.;

3) ustawa o świadczeniu usług drogą elektroniczną z dnia 18 lipca 2002 r.;

4) opinie i wytyczne Grupy Roboczej ds. Ochrony Osób Fizycznych w zakresie przetwarzania danych osobowych powołanej na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r., uwzględniając art. 29 i art. 30 wspomnianej dyrektywy;

5) wytyczne w zakresie opracowania i wdrożenia polityki bezpieczeństwa Prezesa Urzędu Ochrony Danych Osobowych.

9. Przez użyte w treści polityki sformułowania należy rozumieć:

1) dane osobowe – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizyczne;

2) zbiór danych osobowych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

3) przetwarzanie danych osobowych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

4) usuwanie danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

5) administrator danych - rozumie się przez to Wójta Gminy Zbójno;

6) inspektor ochrony danych - rozumie się przez to pracownika urzędu wyznaczonego przez administratora danych do nadzorowania przestrzegania zasad ochrony oraz wymagań w zakresie ochrony, wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych;

7) administrator systemu - osoba zatrudniona na stanowisku informatyka zarządzająca systemem informatycznym w Urzędzie Gminy Zbójno;

8) system informatyczny – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

9) zabezpieczenia systemu – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

10) osoby zatrudnione przy przetwarzaniu danych osobowych – rozumie się przez to pracowników pracujących na zbiorach danych osobowych;

11) upoważnienie - dokument upoważniający pracownika, stażystę, praktykanta, zleceniobiorcę i innych do przetwarzania danych osobowych zgromadzonych w Urzędzie Gminy Zbójno;

12) urząd - należy przez to rozumieć Urząd Gminy Zbójno;

13) rozporządzenie - należy przez to rozumieć rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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);

14) poufność (ang. confidentiality) – funkcja bezpieczeństwa wskazująca obszar, w którym dane nie powinny być udostępniane lub ujawniane nieuprawnionym osobom, procesom lub innym podmiotom;

15) integralność danych, także spójność (ang. data integrity) – funkcja bezpieczeństwa polegająca na tym, że dane nie zostały zmienione, dodane lub usunięte w nieautoryzowany sposób;

16) rozliczalność (ang. accountability) - jedna z podstawowych funkcji bezpieczeństwa zapewniająca, że określone działanie dowolnego podmiotu może być jednoznacznie przypisane temu podmiotowi; funkcja ta jest realizowana najczęściej za pomocą różnych form rejestrowania zdarzeń (logowania) w połączeniu z ochroną integralności, niezaprzeczalności oraz autentyczności zapisów w rejestrze.

10. Administrator danych przetwarza dane znajdujące się w zbiorach danych tylko wtedy, gdy przetwarzanie jest zgodne z prawem i wyłącznie w przypadkach w jakich spełniony jest co najmniej jeden z warunków opisanych w art. 6 rozporządzenia.

11. Osoby zatrudnione przy przetwarzaniu danych osobowych są zobowiązane do przetwarzania danych osobowych we właściwych zbiorach nie dłużej niż jest to niezbędne dla osiągnięcia celu ich przetwarzania.

12. Osoby zatrudnione przy przetwarzaniu danych są zobowiązane powiadomić inspektora ochrony danych o ewentualnych naruszeniach bezpieczeństwa systemu ochrony danych osobowych.

13. Zabrania się przetwarzania danych osobowych ujawniających:

1) pochodzenie rasowe lub etniczne;

2) poglądy polityczne;

3) przekonania religijne lub filozoficzne;

4) przynależność wyznaniową;

5) przynależność partyjną lub związkową;

6) stan zdrowia, kod genetyczny, nałogi lub fakty z życia seksualnego,

lub inne dane o charakterze wrażliwym, chyba, że pozwalają na to obowiązujące przepisy prawa lub osoba, której powyższe dane dotyczą wyraziła na to pisemną zgodę.

14. Pracownik, który:

1) przetwarza w zbiorze danych osobowych:

a) dane osobowe, do których przetwarzania nie jest uprawniony,

b) dane osobowe, których przetwarzanie jest zabronione,

c) dane osobowe niezgodne z celem stworzenia zbioru danych osobowych;

2) udostępnia lub umożliwia dostęp do danych osobowych osobom nieupoważnionym;

3) nie zgłasza inspektorowi ochrony danych zbiorów danych podlegających rejestracji lub nie dokonuje aktualizacji zbiorów już zgłoszonych;

4) nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o przysługujących jej prawach;

5) uniemożliwia osobie, której dane dotyczą, korzystanie z przysługujących jej praw;

6) nie stosuje się do obowiązujących instrukcji, regulaminów i innych przepisów prawnych w zakresie ochrony danych osobowych lub bezpieczeństwa informacji;

7) nie dopełnia obowiązku informacyjnego (nie stosuje klauzul),

podlega odpowiedzialności prawnej na zasadach określonych w powszechnie obowiązujących przepisach prawa.

ROZDZIAŁ IV

Gromadzenie danych osobowych.

15. Dane osobowe mogą być uzyskiwane:

1) bezpośrednio od osoby, której te dane dotyczą;

2) z innych źródeł, w granicach dozwolonych przepisami prawa.

16. Zbierane dane osobowe muszą być wykorzystane tylko do celów, w jakich są lub będą przetwarzane.

ROZDZIAŁ V

Obowiązek informacyjny administratora danych.

17. Administrator danych zbierający i przetwarzający dane osobowe jest odpowiedzialny za poinformowanie osób, których dane osobowe przetwarza o:

1) swojej tożsamości i danych kontaktowych oraz tożsamość i danych kontaktowych swojego przedstawiciela, jeżeli istnieje;

2) danych kontaktowych inspektora ochrony danych;

3) celach przetwarzania, do których mają posłużyć dane osobowe;

4) podstawie prawnej przetwarzania;

5) prawnie uzasadnionym interesie realizowanym przez administratora danych lub przez stronę trzecią – jeżeli przetwarzanie odbywa się na podstawie prawnie usprawiedliwionego interesu administratora danych (art. 6 ust. 1 lit. f);

6) odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;

7) transferze danych do państwa trzeciego, w tym o:

a) zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej,

b) stwierdzeniu lub braku stwierdzenia przez komisję odpowiedniego stopnia ochrony lub wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych w przypadku przekazania danych do państwa trzeciego, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi;

8) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

9) prawie do żądania od administratora danych dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub wniesienia sprzeciwu wobec przetwarzania, a także przenoszenia danych;

10) prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem jeżeli przetwarzanie odbywa się na podstawie zgody na przetwarzanie danych zwykłych (art. 6 ust. 1 lit. a rozporządzenia) lub szczególnej kategorii (art. 9 ust. 2 lit. a rozporządzenia);

11) prawie wniesienia skargi do organu nadzorczego;

12) informacji, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;

13) informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 rozporządzenia oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

18. W przypadku gdy administrator danych zbiera dane osobowe z innego źródła niż od osoby której dane dotyczą, zgodnie z art. 14 ust. 1 i 2 rozporządzenia, powinien poinformować ją o:

1) sprawach z punktów od 1 do 11 oraz 13 wskazanych powyżej;

2) kategoriach przetwarzanych danych osobowych;

3) źródle pochodzenia danych osobowych, a jeżeli ma to zastosowanie, o pochodzeniu ich ze źródeł powszechnie dostępnych.

19. W razie wątpliwości co do właściwego przetwarzania danych osobowych oraz zabezpieczania danych osobowych należy kierować pytania do inspektora ochrony danych.

20. Administrator danych i/lub jego pracownicy informują inspektora ochrony danych w szczególności o następujących sprawach:

1) sprawy pracownicze:

a) zatrudnieniu nowego pracownika, zleceniobiorcy, przyjęciu osoby na staż, przyjęciu osoby w celu odbywania praktyki,

b) zwolnieniu lub zakończeniu wykonywania czynności przez osoby wymienione pod lit. a,

c) skargach (związanych z przetwarzaniem danych osobowych) pracowników, byłych pracowników, zleceniobiorców, stażystów, praktykantów,

d) zamiarze udostępnienia danych osobowych osób wymienionych pod lit. a podmiotom zewnętrznym;

2) podmioty zewnętrzne:

a) zamiarze zawarcia umowy z podmiotem zewnętrznym (jeżeli umowa przewiduje przepływ danych osobowych),

b) zamiarze zmiany podmiotu zewnętrznego przetwarzającego dane osobowe,

c) postępowaniu przedstawicieli podmiotów zewnętrznych niezgodnym z zasadami bezpieczeństwa ochrony danych osobowych,

d) zamiarze przydzielenia zdalnych dostępów do systemów informatycznych przedstawicielom firm zewnętrznych;

3) strony internetowe:

a) zamiarze zmiany lub uruchomieniu nowego hostingu serwisów www zbierających lub przesyłających dane osobowe,

b) zamiarze uruchomienia nowej strony internetowej lub modyfikowaniu funkcjonalności już istniejącej (jeżeli dochodzi do przepływu danych za ich pośrednictwem),

c) zamiarze przetwarzania danych osobowych zgromadzonych za pośrednictwem stron internetowych w innym celu niż to wynika z „klauzul zgody",

d) zamiarze umieszczenia (opublikowania) danych osobowych (w tym i zdjęć) na stronie internetowej;

4) działania marketingowe i promocyjne:

a) zamiarze zorganizowania konkursu, programu lub innych działań marketingowych lub promocyjnych wymagających przetwarzania danych osobowych,

b) zamiarze nawiązania współpracy z podmiotem zewnętrznym w zakresie marketingu lub promocji (związanym z przetwarzaniem danych osobowych);

5) usuwanie danych:

a) zamiarze usunięcia większej ilości danych osobowych (zarówno w wersji papierowej jak i w systemach informatycznych),

b) zamiarze przekazania nośników elektronicznych (komputerów/laptopów) zawierających dane osobowe podmiotom zewnętrznym (np. celem ich naprawy),

c) niewłaściwym usuwaniu zbędnych danych osobowych przez współpracowników (zwykłe śmietniki), zepsutym sprzęcie do niszczenia zbędnych dokumentów;

6) incydenty bezpieczeństwa:

a) wycieku, utracie (zagubieniu) lub udostępnieniu osobie nieupoważnionej danych osobowych,

b) wycieku, utracie (zagubieniu) lub udostępnieniu osobie nieupoważnionej danych osobowych przez podmiot zewnętrzny (kontrahenta),

c) nie działającym zabezpieczeniu danych osobowych (np. niszczarki do dokumentów, zgubione klucze, ujawnione i nie zmienione hasła dostępowe, etc.),

d) nie stosowaniu się do procedur bezpieczeństwa (np. polityka czystego biurka, polityka czystego ekranu, polityka kluczy, etc.);

7) skargi i sygnalizacje:

a) wszelkich skargach osób fizycznych na niezgodne z prawem przetwarzanie danych osobowych,

b) wszelkich pismach przychodzących od jakichkolwiek organów lub urzędów w zakresie ochrony danych osobowych,

c) wszelkiej korespondencji przychodzącej od podmiotów zewnętrznych w zakresie wątpliwości (zgodności) działań z przepisami ochrony danych osobowych;

8) okresowe kontrole:

a) współudziale w okresowych kontrolach (sprawdzeniach) przestrzegania procedur opisanych w dokumentacji wewnętrznej,

b) składanie wyjaśnień, udostępnianie dokumentów oraz systemów informatycznych do kontroli (sprawdzenia);

9) inne sprawy: zamiar przeprowadzki, uruchomienia lub zlikwidowania wydziału/biura/referatu/stanowiska itp., w którym były przetwarzane dane osobowe.

21. Kandydaci do pracy w procesie rekrutacji wyrażają zgodę na przetwarzanie danych osobowych w formie oświadczenia, zgodnie z przepisami Kodeksu pracy. Wzór oświadczenia kandydata do pracy stanowi ***załącznik nr 1 do polityki.***

22. W celu realizacji obowiązku informacyjnego, o którym mowa w pkt 17 i 18, administrator danych opracowuje tzw. klauzule informacyjne dla każdej operacji przetwarzania danych osobowych. Klauzule informacyjne zamieszcza się w biuletynie informacji publicznej gminy Zbójno, na stronie internetowej urzędu, na tablicy ogłoszeń w siedzibie urzędu oraz w miarę możliwości przekazuje się je osobom, których dane osobowe są przetwarzane.

ROZDZIAŁ VI

Udzielanie informacji o przetwarzaniu danych osobowych.

23. Osobom, których dane przetwarza się przysługuje prawo kontroli ich danych osobowych, a w szczególności prawo do uzyskania wyczerpujących informacji na temat tych danych.

24. Każda osoba, która wystąpi z wnioskiem o otrzymanie informacji na temat swoich danych osobowych, musi otrzymać odpowiedź na piśmie w terminie nie przekraczającym 30 dni od daty wpłynięcia wniosku.

25. W przypadku, gdy dane osoby są niekompletne, nieaktualne, nieprawdziwe lub zostały
zebrane z naruszeniem ustawy, albo są zbędne do realizacji celu, dla którego zostały zebrane, inspektor ochrony danych jest zobowiązany do podjęcia działań w celu ich uzupełnienia, uaktualnienia lub sprostowania.

ROZDZIAŁ VII
Rejestracja operacji przetwarzania danych osobowych.

26. Kierownicy komórek organizacyjnych i pracownicy zatrudnieni na samodzielnych stanowiskach pracy w urzędzie, odpowiedzialni za dokonywanie operacji przetwarzania danych osobowych są zobowiązani do niezwłocznego zgłoszenia do rejestru czynności przetwarzania danych osobowych prowadzonego przez inspektora ochrony danych:

1) planowanych operacji przetwarzania danych osobowych;
2) zmian do operacji przetwarzania danych osobowych już zarejestrowanych w rejestrze czynności przetwarzania danych osobowych.

ROZDZIAŁ VIII
Rejestr czynności przetwarzania danych osobowych.

27. Administrator danych prowadzi rejestr czynności przetwarzania danych osobowych. W rejestrze zamieszcza się między innymi następujące informacje:

1) nazwę czynności przetwarzania danych;
2) nazwę jednostki organizacyjnej urzędu (wydział, samodzielne stanowisko itd.), w której przetwarzane są dane osobowe;
3) cel przetwarzania danych osobowych;
4) kategorie osób, których dane osobowe są przetwarzane;
5) kategorie danych osobowych przetwarzanych w zborach danych osobowych;
6) podstawa prawna przetwarzania danych osobowych;
7) źródło pozyskiwania danych osobowych;
8) planowany termin usunięcia kategorii danych osobowych;
9) nazwa współadministratora i dane kontaktowe;
10) nazwa podmiotu przetwarzającego dane osobowe i dane kontaktowe;
11) kategorie odbiorców danych osobowych;
12) nazwa systemu lub oprogramowania w którym przetwarzane są dane osobowe;
13) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa danych osobowych.

ROZDZIAŁ IX

Organizacja ochrony danych osobowych.

Administrator danych.

28. Administrator danych realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:

1) stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;

2) podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem, przede wszystkim, zmian w obowiązującym prawie, organizacji administratora danych oraz technik zabezpieczenia danych osobowych;

3) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi ich zadań i obowiązków, według wzoru stanowiącego ***załącznik nr 2 do polityki;***

4) wyznacza inspektora ochrony danych oraz administratora systemu, w tym określa zakres ich zadań i obowiązków;

5) zleca administratorowi systemu by zapewnił użytkownikom odpowiednie stanowiska pracy umożliwiające bezpieczne przetwarzanie danych osobowych;

6) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych;

7) wykonuje inne obowiązki określone w rozdziale IV rozporządzenia.

Inspektor ochrony danych.

29. Inspektor ochrony danych wykonuje zadania polegające na:

1) informowaniu administratora danych oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

2) monitorowaniu przestrzegania rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych osobowych oraz polityk administratora w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

3) udzielaniu na żądanie zaleceń co do oceny skutków dla ochrony danych osobowych oraz monitorowanie jej wykonania zgodnie z art. 35 rozporządzenia;

4) współpracy z organem nadzorczym;

5) pełnieniu funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 rozporządzenia, oraz w stosownych przypadkach prowadzenia konsultacji we wszelkich innych sprawach;

6) prowadzeniu szkoleń wstępnych dla osób upoważnianych do przetwarzania danych osobowych; wzór karty szkolenia wstępnego z zakresu ochrony danych osobowych stanowi ***załącznik nr 3 do polityki;***

7) inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

Administrator systemu.

30. Administrator systemu realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad funkcjonowaniem systemu informatycznego administratora danych, w tym w szczególności:

1) zarządza systemem informatycznym w którym przetwarzane są dane osobowe posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora;

2) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe;

3) na wniosek administratora danych, przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników zgodnie z zasadami określonymi w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;

4) nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;

5) sprawuje nadzór nad wdrożeniem i funkcjonowaniem stosownych środków technicznych w celu zapewnienia bezpieczeństwa danych osobowych;

6) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia zabezpieczeń systemu informatycznego;

7) podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego;

8) wyrejestrowuje użytkowników na polecenie administratora danych;

9) zmienia na poszczególnych stacjach roboczych hasła dostępu ujawniając je wyłącznie danemu użytkownikowi oraz, w razie potrzeby, administratorowi danych;

10) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego, informuje administratora danych oraz inspektora ochrony danych o naruszeniu i współdziała z nimi przy usuwaniu skutków naruszenia;

11) prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym;

12) sprawuje nadzór nad wykonywaniem napraw, konserwacji oraz likwidacji urządzeń komputerowych i nośników danych na których zapisane są dane osobowe;

13) wykonuje kopie zapasowe, dba o ich właściwe zabezpieczenie i przechowywanie oraz okresowo sprawdza je pod kątem ich dalszej przydatności do odtwarzania;

14) podejmuje działania służące zapewnieniu niezawodności zasilania komputerów,

innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

Kierownicy działów urzędu.

31. Kierownicy działów nadzorują i kontrolują przestrzeganie zasad ochrony danych osobowych przez pracowników zatrudnionych w podległym im dziale oraz przez podmioty zewnętrzne realizujące na rzecz urzędu/gminy zadania w zakresie spraw prowadzonych przez dział, jeżeli w celu realizacji tych zadań podmioty te przetwarzają dane osobowe powierzone im przez urząd, w tym w szczególności:

1) sprawują nadzór nad stosowaniem przez pracowników i podmioty zewnętrzne odpowiednich środków technicznych, fizycznych i organizacyjnych w zakresie ochrony danych osobowych;

2) zgłaszają inspektorowi ochrony danych wnioski i uwagi co do sposobu usprawnienia zabezpieczenia danych osobowych przetwarzanych w dziale;

3) kontrolują pracowników w zakresie należytego zabezpieczania szaf i biurek, w których gromadzone są dane osobowe; sprzątania biurek i innego umeblowania z dokumentów zawierających dane osobowe – poprzez ich odpowiednie zabezpieczenie w zamykanych na klucz szafach lub biurkach, lub zniszczenie - w przypadku braku przydatności do dalszego korzystania, w niszczarce;

4) przeciwdziałają dostępowi do zbiorów danych osobowych pracownikom i podmiotom zewnętrznym, którzy nie mają odpowiedniego upoważnienia do przetwarzania danych osobowych.

Pracownicy upoważnieni do przetwarzania danych osobowych.

32. Pracownicy upoważnieni do przetwarzania danych osobowych są zobowiązani przestrzegać zasad ochrony danych osobowych, w tym w szczególności:

1) mogą przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez administratora danych w upoważnieniu i tylko w celu wykonywania nałożonych na nich obowiązków; zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie; rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych;

2) muszą zachować tajemnicę danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania; przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u administratora danych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji;

3) zapoznają się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej polityki;

4) stosują określone przez administratora danych procedury oraz wytyczne mające na celu zgodne z prawem, w tym zwłaszcza adekwatne, przetwarzanie danych osobowych;

5) korzystają z systemu informatycznego w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład tego systemu;

6) zabezpieczają dane przed ich udostępnianiem osobom nieupoważnionym.

Pracownicy sprzątający po godzinach pracy urząd.

33. Pracownicy sprzątający po godzinach pracy urząd, realizują następujące zadania w zakresie ochrony danych osobowych:

1) sprawdzają czy szafy i biurka, w których gromadzone są zbiory danych osobowych, zamknięte są na klucz; w przypadku braku należytego zabezpieczenia, niezwłocznie zgłaszają ten fakt inspektorowi ochrony danych;

2) sprawdzają czy na szafkach i biurkach lub innych ogólnie dostępnych miejscach nie znajdują się pozostawione przez pracowników dokumenty, które mogą zawierać dane osobowe; w przypadku stwierdzenia, że doszło do pozostawienia dokumentów i ich nienależytego zabezpieczenia, zgłaszają ten fakt inspektorowi ochrony danych;

3) sprawdzają czy w koszach na śmieci nie pozostawiono zbędnych kserokopii, odpisów, projektów dokumentów i innych pism, które mogą zawierać informacje urzędowe, w tym dane osobowe; w przypadku znalezienia takich rzeczy usunięci ich z koszy na śmieci, zabezpieczenie i zgłoszenie tego faktu inspektorowi ochrony danych.

Pracownik prowadzący rejestr wniosków o udostępnienie danych osobowych.

34. Pracownik prowadzący rejestr wniosków o udostępnienie danych osobowych wpisuje do rejestru każdy wniosek o udostępnienie danych osobowych wpływający do urzędu oraz udzieloną na nią odpowiedź.

ROZDZIAŁ X

Infrastruktura przetwarzania danych osobowych.

Obszar przetwarzania danych osobowych.

35. Wykaz budynków i pomieszczeń wchodzących w skład obszaru w którym przetwarzane są dane osobowe, sporządza się według wzoru stanowiącego ***załącznik nr 4 do polityki.*** Wykaz sporządza i aktualizuje inspektor ochrony danych.

Zbiory danych.

36. Wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych w urzędzie, sporządza się według wzoru stanowiącego ***załącznik nr 5 do polityki.*** Wykaz sporządza i aktualizuje inspektor ochrony danych.

System informatyczny.

37. System informatyczny administratora danych obsługiwany jest przez serwer główny oraz jeden serwer zapasowy na którym gromadzone są kopie zapasowe zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania. W razie potrzeby administrator danych może podjąć decyzje o dodatkowym gromadzeniu kopii zapasowych zbiorów danych oraz programów i narzędzi programowych na serwerach zewnętrznych należących do podmiotów specjalizujących się w archiwizacji/przechowywaniu zbiorów danych osobowych, na podstawie odpowiedniej umowy.

Ewidencje.

38. W ramach struktury organizacyjnej administratora danych prowadzone są następujące ewidencje wchodzące w skład dokumentacji z zakresu ochrony danych osobowych:

1) inspektor ochrony danych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, według wzoru stanowiącego ***załącznik nr 6 do polityki;***

2) osoba zajmująca się obsługą sekretariatu prowadzi ewidencję wniosków o udostępnienie danych osobowych wpływających do urzędu;

3) administrator systemu prowadzi ewidencję:

a) serwerów, komputerów, nośników przenośnych oraz kluczy kryptograficznych, według wzoru stanowiącego ***załącznik nr 7 do polityki;***

b) oprogramowania komputerowego, według wzoru stanowiącego ***załącznik nr 7 do polityki.***

Sposób przepływu danych w systemie informatycznym.

39. Sposób przepływu danych w systemie informatycznym opisuje i aktualizuje administrator systemu, według ustalonego przez siebie i zaakceptowanego przez

Poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym.

40. Ze względu na fakt, że system informatyczny administratora danych połączony jest z siecią publiczną, należy zapewnić wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym.

Strategia zabezpieczenia danych osobowych (działania niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych).

Bezpieczeństwo osobowe

41. Administrator danych przeprowadza nabór na wolne stanowiska urzędnicze w drodze konkursu. Kandydaci na pracowników są dobierani z uwzględnieniem ich kompetencji merytorycznych, a także kwalifikacji moralnych. Zwraca się uwagę na takie cechy kandydata, jak uczciwość, odpowiedzialność i przewidywalność zachowań.

42. Ryzyko ze strony osób, które potencjalnie mogą w łatwiejszy sposób uzyskać dostęp do danych osobowych (np. osoby sprzątające pomieszczenia administratora danych), jest minimalizowane przez zobowiązywanie ich do zachowania tajemnicy na podstawie odrębnych, pisemnych oświadczeń oraz szkolenia.

Szkolenia w.zakresie ochrony danych osobowych

43. Inspektor ochrony danych organizuje następujące typy szkoleń:

1) szkoli się każdą osobę, która ma zostać upoważniona do przetwarzania danych osobowych;

2) szkolenia wewnętrzne wszystkich osób upoważnionych do przetwarzania danych osobowych przeprowadzane są w przypadku każdej zmiany zasad lub procedur ochrony danych osobowych;

3) przeprowadza się szkolenia dla osób innych niż upoważnione do przetwarzania danych,

jeśli pełnione przez nich funkcje wiążą się z zabezpieczeniem danych osobowych.

44. Tematyka szkoleń obejmuje między innymi:

1) przepisy i procedury dotyczące ochrony danych osobowych, sporządzania i przechowywania ich kopii, niszczenia wydruków i zapisów na nośnikach;

2) sposoby ochrony danych osobowych przed osobami postronnymi i procedury udostępniania danych osobom, których one dotyczą;

3) obowiązki osób upoważnionych do przetwarzania danych osobowych;

4) odpowiedzialność za naruszenie obowiązków z zakresu ochrony danych osobowych;

5) zasady i procedury określone w rozporządzeniu, innych przepisach Unii i prawa krajowego w zakresie ochrony danych osobowych oraz w wewnętrznych politykach i dokumentach z nią związanych.

Strefy bezpieczeństwa.

45. W siedzibie administratora danych wydzielono **strefę bezpieczeństwa klasy I**, do której dostęp zabezpieczony jest wewnętrznymi środkami kontroli, takimi jak odrębny system alarmowy wyodrębniony z systemu alarmowego zainstalowanego w pozostałych pomieszczeniach urzędu (rozwiązanie to obejmuje tylko pomieszczenia serwerowni). W skład tej strefy wchodzą:

1) pomieszczenia z serwerami, w których może przebywać wyłącznie administrator danych, administrator systemu i/lub inspektor ochrony danych; inne osoby upoważnione do przetwarzania danych osobowych tylko w ich towarzystwie, a osoby postronne w ogóle nie mają dostępu;

2) pomieszczenie w którym znajduje się kasa, w którym mogą przebywać wyłącznie upoważnieni do tego pracownicy urzędu, tj. pracownicy zajmujący się obsługą kasy i pracownicy ich zastępujący; inne osoby upoważnione do przetwarzania danych osobowych tylko w ich towarzystwie, a osoby postronne w ogóle nie mają dostępu.

46. W **strefie bezpieczeństwa klasy II** do danych osobowych mają dostęp wszystkie osoby upoważnione do przetwarzania danych osobowych zgodnie z zakresami upoważnień do ich przetwarzania, a osoby postronne mogą w niej przebywać tylko w obecności pracownika upoważnionego do przetwarzania danych osobowych. Strefa ta obejmuje wszystkie pozostałe pomieszczenia zaliczone do obszaru przetwarzania danych w siedzibie administratora danych.

Zabezpieczenie sprzętu.

47. Serwery (podstawowy i do gromadzenia kopii zapasowych) znajdują się w odrębnych pomieszczeniach zamykanych drzwiami z dwoma zamkami. Okna do pomieszczeń są okratowane oraz zainstalowany jest system alarmowy, wyodrębniony z systemu alarmowego zainstalowanego w pozostałych pomieszczeniach urzędu. W pomieszczeniach może przebywać wyłącznie administrator danych, administrator systemu i/lub inspektor ochrony danych, inne osoby upoważnione do przetwarzania danych osobowych tylko w ich towarzystwie, a osoby postronne w ogóle nie mają dostępu.

48. Administrator systemu instruuje użytkowników jak postępować aby zapewnić

prawidłową eksploatację systemu informatycznego.

49. Wszystkie urządzenia systemu informatycznego administratora danych są zasilane za pośrednictwem zasilaczy awaryjnych (UPS).

50. Okablowanie sieciowe zostało zaprojektowane w ten sposób, że dostęp do linii teletransmisyjnych jest możliwy tylko z pomieszczeń zamykanych na klucz. Ponadto kable sieciowe nie krzyżują się z okablowaniem zasilającym, co zapobiega interferencjom.

51. Bieżąca konserwacja i drobne naprawy sprzętu wykorzystywanego do przetwarzania danych osobowych prowadzone są tylko przez administratora systemu. Natomiast poważne naprawy wykonywane przez podmioty zewnętrzny realizowane są po zawarciu z tymi podmiotami odpowiednich umów, których celem jest należyte zabezpieczenie i ochrona danych osobowych w trakcie wykonywania ww. napraw.

52. Administrator systemu dopuszcza konserwowanie i naprawę sprzętu poza siedzibą administratora danych jedynie po trwałym usunięciu danych osobowych. Zużyty sprzęt służący do przetwarzania danych osobowych może być zbywany dopiero po trwałym usunięciu danych, a urządzenia uszkodzone mogą być przekazywane w celu utylizacji (jeśli trwałe usunięcie danych wymagałoby nadmiernych nakładów ze strony administratora) właściwym podmiotom, z którymi zawiera się odpowiednie umowy.

53. Wszystkie awarie, działania konserwacyjne i naprawy systemu informatycznego są opisywane w stosownych protokołach, podpisywanych przez osoby w tych działaniach uczestniczące, a także przez administratora systemu.

Zabezpieczenia we własnym zakresie.

54. Niezwykle ważne dla bezpieczeństwa danych osobowych jest bezwzględne przestrzeganie przez każdą osobę upoważnioną do przetwarzania danych osobowych i użytkownika następujących zasad:

1) ustawiania ekranów komputerowych tak, by osoby niepowołane nie mogły oglądać ich zawartości, a zwłaszcza nie naprzeciwko wejścia do pomieszczenia;

2) niepozostawiania bez kontroli dokumentów, nośników danych i sprzętu w hotelach i innych miejscach publicznych oraz w samochodach;

3) dbania o prawidłową wentylację komputerów (nie można zasłaniać kratek wentylatorów meblami, zasłonami lub stawiać komputerów tuż przy ścianie);

4) niepodłączania do listew podtrzymujących napięcie przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejniki, czajniki, wentylatory);

5) pilnego strzeżenia akt, płyt, pamięci przenośnych i komputerów przenośnych;

6) kasowania po wykorzystaniu danych na dyskach przenośnych;

7) nieużywania powtórnie dokumentów zadrukowanych jednostronnie;

8) niezapisywania hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku i pozostawianie ich w łatwo dostępnych miejscach;

9) powstrzymywania się przez osoby upoważnione do przetwarzania danych osobowych od samodzielnej ingerencji w oprogramowanie i konfigurację powierzonego

sprzętu (szczególnie komputerów przenośnych), nawet gdy z pozoru mogłoby to usprawnić pracę lub podnieść poziom bezpieczeństwa danych;

10) przestrzegania przez osoby upoważnione do przetwarzania danych osobowych swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń administratora systemu i inspektora ochrony danych;

11) opuszczania stanowiska pracy dopiero po aktywizowaniu wygaszacza ekranu lub po zablokowaniu stacji roboczej w inny sposób;

12) kopiowania tylko jednostkowych danych (pojedynczych plików); obowiązuje zakaz robienia kopii całych zbiorów danych lub takich ich części, które nie są konieczne do wykonywania obowiązków przez pracownika; jednostkowe dane mogą być kopiowane na nośniki magnetyczne, optyczne i inne po ich zaszyfrowaniu i przechowywane w zamkniętych na klucz szafach; po ustaniu przydatności tych kopii dane należy trwale skasować lub fizycznie zniszczyć nośniki, na których są przechowywane;

13) udostępniania danych osobowych pocztą elektroniczną tylko w postaci zaszyfrowanej;

14) niewynoszenia na jakichkolwiek nośnikach całych zbiorów danych oraz szerokich z nich wypisów, nawet w postaci zaszyfrowanej;

15) wykonywania kopii roboczych danych, na których się właśnie pracuje, tak często, aby zapobiec ich utracie;

16) kończenia pracy na stacji roboczej po wprowadzeniu danych przetwarzanych tego dnia w odpowiednie obszary serwera, a następnie prawidłowym wylogowaniu się użytkownika i wyłączeniu komputera oraz odcięciu napięcia w UPS i listwie;

17) niszczenia w niszczarce lub chowania do szaf lub biurek zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;

18) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych;

19) zachowania w tajemnicy danych osobowych, w tym także wobec najbliższych;

20) chowania do zamykanych na klucz szaf lub biurek wszelkich akt zawierających dane osobowe przed opuszczeniem miejsca pracy, po zakończeniu dnia pracy;

21) należytym zabezpieczaniu kluczy do szaf i biurek;

22) zamykania okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych;

23) zamykania okien w razie opuszczenia pomieszczenia, w tym zwłaszcza po zakończeniu dnia pracy;

24) zamykania drzwi do biur na klucz po zakończeniu pracy w danym dniu i złożenia klucza w sekretariacie lub przekazanie sprzątaczce;

25) zabronione jest przebywanie w obszarze przetwarzania danych osobowych po

godzinach pracy urzędu bez zgody bezpośredniego przełożonego pracownika.

Postępowanie z nośnikami i ich bezpieczeństwo.

55. Osoby upoważnione do przetwarzania danych osobowych powinny pamiętać, że:

1) dane z nośników przenośnych niebędących kopiami zapasowymi po wprowadzeniu do systemu informatycznego administratora danych powinny być trwale usuwane z tych nośników przez fizyczne zniszczenie (np. płyty CD-ROM) lub usunięcie danych programem trwale usuwającym pliki; jeśli istnieje uzasadniona konieczność, dane pojedynczych osób (a nie całe zbiory czy szerokie wypisy ze zbiorów) mogą być przechowywane na specjalnie oznaczonych nośnikach; nośniki te muszą być przechowywane w zamkniętych na klucz szafach, nieudostępnianych osobom postronnym; po ustaniu przydatności tych danych nośniki powinny być trwale kasowane lub niszczone; w zależności od sytuacji należy stosować szyfrowanie danych.

2) uszkodzone nośniki przed ich wyrzuceniem należy zniszczyć fizycznie w niszczarce służącej do niszczenia nośników;

3) zabrania się powtórnego używania do sporządzania brudnopisów pism jednostronnie zadrukowanych, jeśli zawierają one dane chronione; zaleca się natomiast dwustronne drukowanie brudnopisów pism i sporządzanie dwustronnych dokumentów;

4) po wykorzystaniu wydruki zawierające dane osobowe należy codziennie przed zakończeniem pracy zniszczyć w niszczarce. O ile to możliwe, nie należy przechowywać takich wydruków w czasie dnia na biurku ani też wynosić poza siedzibę administratora danych.

Wymiana danych i ich bezpieczeństwo.

56. Bezpieczeństwo danych, a w szczególności ich integralność i dostępność, w dużym stopniu zależy od zdyscyplinowanego, codziennego umieszczania danych w wyznaczonych zasobach serwera. Pozwala to – przynajmniej w pewnym stopniu – uniknąć wielokrotnego wprowadzania tych samych danych do systemu informatycznego administratora danych.

57. Inne wymogi bezpieczeństwa systemowego są określane w instrukcjach obsługi producentów sprzętu i używanych programów, wskazówkach administratora systemu oraz w instrukcji.

58. Przed atakami z sieci zewnętrznej wszystkie komputery administratora danych (w tym także przenośne) chronione są środkami dobranymi przez administratora systemu w porozumieniu z inspektorem ochrony danych.

59. Ważne jest, by użytkownicy zwracali uwagę na to, czy urządzenie, na którym pracują, domaga się aktualizacji tych zabezpieczeń. O wszystkich takich przypadkach należy informować administratora systemu oraz umożliwić mu monitorowanie oraz aktualizację środków (urządzeń, programów) bezpieczeństwa.

60. Administrator systemu w porozumieniu z inspektorem ochrony danych dobiera elektroniczne środki ochrony przed atakami z sieci stosownie do pojawiania się nowych

zagrożeń (nowe wirusy, robaki, trojany, inne możliwości wdarcia się do systemu), a także stosownie do rozbudowy systemu informatycznego administratora danych i powiększania bazy danych. Jednocześnie należy zwracać uwagę, czy rozwijający się system zabezpieczeń sam nie wywołuje nowych zagrożeń.

Kontrola dostępu do systemu.

61. Poszczególnym osobom upoważnionym do przetwarzania danych osobowych przydziela się konta opatrzone niepowtarzalnym identyfikatorem, umożliwiające dostęp do danych osobowych, zgodnie z zakresem upoważnienia do ich przetwarzania.

62. Administrator systemu po uprzednim przedłożeniu mu upoważnienia do przetwarzania danych osobowych, przydziela pracownikowi upoważnionemu do przetwarzania danych osobowych konto w systemie informatycznym, dostępne po wprowadzeniu prawidłowego identyfikatora i uwierzytelnieniu hasłem. System wymusza zmianę hasła przy pierwszym logowaniu.

63. W razie potrzeby, po uzyskaniu uprzedniej akceptacji inspektora ochrony danych, administrator systemu może przydzielić konto opatrzone identyfikatorem osobie upoważnionej do przetwarzania danych osobowych, nieposiadającej statusu pracownika.

64. Pierwsze hasło wymagane do uwierzytelnienia się w systemie informatycznym przydzielane jest przez administratora systemu.

65. Do zagwarantowania poufności i integralności danych osobowych konieczne jest przestrzeganie przez użytkowników swoich uprawnień w systemie, tj. właściwego korzystania z baz danych, używania tylko własnego identyfikatora i hasła oraz stosowania się do zaleceń administratora systemu i inspektora ochrony danych.

Kontrola dostępu do sieci.

66. System informatyczny posiada połączenie z Internetem. Dostęp do niego jest jednak ograniczony.

67. Administrator danych wykorzystuje centralną zaporę sieciową w celu separacji lokalnej sieci od sieci publicznej.

68. Operacje za pośrednictwem rachunku bankowego administratora danych może wykonywać wyłącznie pracownik upoważniony do tego przez administratora danych, po uwierzytelnieniu się zgodnie z procedurami określonymi przez bank obsługujący rachunek.

Komputery przenośne i praca na odległość.

69. Urządzenia przenośne oraz nośniki danych wynoszone z siedziby administratora danych nie powinny być pozostawiane bez nadzoru w miejscach publicznych. Komputery przenośne należy przewozić w służbowych torbach; stosowanie własnych toreb na laptopy nie jest dopuszczalne.

70. Nie należy pozostawiać bez kontroli dokumentów, nośników danych i sprzętu w hotelach i innych miejscach publicznych ani też w samochodach.

71. Informacje przechowywane na urządzeniach przenośnych lub komputerowych nośnikach danych należy chronić przed uszkodzeniami fizycznymi; w przypadku działania silnego pola elektromagnetycznego należy przestrzegać zaleceń producentów

dotyczących ochrony sprzętu.

72. Wykorzystywanie komputerów przenośnych administratora danych w miejscach publicznych jest dozwolone, o ile otoczenie, w którym znajduje się użytkownik, stwarza warunki minimalizujące ryzyko zapoznania się z danymi przez osoby nieupoważnione. W konsekwencji korzystanie z komputera przenośnego będzie z reguły niedozwolone w restauracjach czy środkach komunikacji publicznej.

73. W domu niedozwolone jest udostępnianie domownikom komputera przenośnego należącego do administratora danych. Użytkownik powinien zachować w tajemnicy wobec domowników identyfikator i hasło, których podanie jest konieczne do rozpoczęcia pracy na komputerze przenośnym administratora danych.

Monitorowanie dostępu do systemu i jego użycia.

74. System informatyczny administratora danych dzięki funkcjonalności polegającej na monitorowaniu użycia stacji roboczych śledzi, kto, kiedy i jakie programy uruchamia na poszczególnych stacjach roboczych.

75. Administrator systemu przeprowadza synchronizację zegarów stacji roboczych z serwerem, ograniczając dopuszczalność zmian w ustawieniach zegarów. Jakiekolwiek zmiany ustawień zegarów mogą być dokonywane jedynie przez administratora systemu z konta o uprawnieniach administracyjnych.

Przeglądy okresowe zapobiegające naruszeniom obowiązku szczególnej staranności administratora danych.

76. Inspektor ochrony danych przeprowadza raz w roku przegląd przetwarzanych danych osobowych pod kątem celowości ich dalszego przetwarzania. Osoby upoważnione do przetwarzania danych osobowych, w tym zwłaszcza kierownicy poszczególnych działów, są obowiązani współpracować z inspektorem ochrony danych w tym zakresie i wskazywać mu dane osobowe, które powinny zostać usunięte ze względu na zrealizowanie celu przetwarzania danych osobowych lub brak ich adekwatności do realizowanego celu.

77. Inspektor ochrony danych może zarządzić przeprowadzenie dodatkowego przeglądu w wyżej określonym zakresie w razie zmian w obowiązującym prawie, ograniczających dopuszczalny zakres przetwarzanych danych osobowych. Dodatkowy przegląd jest możliwy także w sytuacji zmian organizacyjnych u administratora danych.

78. Z przebiegu usuwania danych osobowych należy sporządzić protokół.

ROZDZIAŁ XI

Udostępnianie danych osobowych.

79. Administrator danych udostępnia dane osobowe tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa lub innym osobom lub podmiotom na podstawie zawartej umowy powierzenia przetwarzania danych osobowych z uwzględnieniem obowiązujących przepisów prawa.

80. Dane osobowe udostępnia się na pisemny wniosek chyba że, odrębne przepisy prawa stanowią inaczej.

81. Wniosek powinien zawierać informacje, umożliwiające wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie. Wniosek należy uzasadnić.

82. Wniosek jest rozpatrywany przez upoważnionego pracownika urzędu.

83. Ewidencja wniosków o udostępnienie danych osobowych prowadzona jest w sekretariacie urzędu. Wzór ewidencji wniosków o udostępnienie danych osobowych stanowi ***załącznik nr 8 do polityki.***

84. Decyzję w sprawie udostępniania lub odmowy udostępnienia danych osobowych podejmuje upoważniony pracownik.

85. Upoważniony pracownik może odmówić udostępnienia danych osobowych, jeżeli udostępnienie jest niezgodne z prawem lub spowodowałoby naruszenie dóbr osobistych osób, których dane dotyczą lub osób trzecich.

ROZDZIAŁ XII
Powierzenie przetwarzania danych osobowych.

86. Administrator danych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej.

87. Podmiot, o którym mowa w pkt 86, jest zobowiązany do zastosowania środków organizacyjnych i technicznych zabezpieczających dane osobowe przed nieuprawnionym dostępem na zasadach określonych w rozporządzeniu i innych przepisach o ochronie danych osobowych. Przykładowy wzór umowy o powierzeniu przetwarzania danych osobowych, którego ostateczna treść zostanie uzgodniona pomiędzy administratorem danych a podmiotem przetwarzającym dane, stanowi ***załącznik nr 9 do polityki.***

ROZDZIAŁ XIII
Audyt bezpieczeństwa informacji.

88. Celem audytu bezpieczeństwa informacji jest wykonanie obowiązków wynikających z rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, zwanym dalej KRI.

89. Do przeprowadzenia audytu upoważnia się zespół składający się z minimum 2 osób, w tym jedną z tych osób powinien być inspektor ochrony danych.

90. Dopuszcza się wybór innych osób, instytucji lub firm do przeprowadzenia audytu; kryteriami jakimi należy się kierować przy wyborze innych osób/instytucji/firm prowadzących audyt są: odpowiednie kwalifikacje, doświadczenie, znajomość metodyki audytu w zakresie bezpieczeństwa informacji, a także niezależność od obszaru audytowanego.

ROZDZIAŁ XIV
Analiza ryzyka.

91. Ogólny poziom ryzyka naruszenia bezpieczeństwa danych osobowych w systemach nieinformatycznych szacuje się na poziomie niskim. Zastosowane techniczne i organizacyjne środki ochrony są adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych osobowych, jednak możliwe jest wystąpienie nowych zagrożeń lub zwiększenie poziomu danej kategorii. Stosowane zabezpieczenia należy na bieżąco monitorować.

92. Uwzględniając kategorie przetwarzanych danych osobowych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka, dla systemów informatycznych stosuje się wysoki poziom bezpieczeństwa. Inspektor ochrony danych przeprowadza okresową analizę ryzyka dla poszczególnych systemów i na tej podstawie przedstawia administratorowi danych propozycje dotyczące zastosowania środków technicznych i organizacyjnych, celem zapewnienia właściwej ochrony przetwarzanym danych.

ROZDZIAŁ XV
Ocena ryzyka i przeglądy.

93. Uwzględniając kategorie przetwarzanych danych osobowych oraz zagrożenia zidentyfikowane w wyniku przeprowadzonej analizy ryzyka, stosuje się wysoki poziom bezpieczeństwa.

94. Przegląd stanu ochrony danych osobowych jest przeprowadzany przynajmniej raz w roku.

95. Przegląd przeprowadza inspektor ochrony danych, upoważniony pracownik urzędu lub uprawniony podmiot zewnętrzny na podstawie umowy zawartej z administratorem danych.

96. Przegląd obejmuje wszystkie obszary działalności i elementy infrastruktury, w których wymagane jest przestrzeganie zasad przetwarzania danych osobowych, w szczególności systemy informatyczne, zabezpieczenia fizyczne oraz organizacyjne.

97. Dokonujący przeglądu przygotowuje plan przeglądu z uwzględnieniem jego zakresu oraz niezbędnych zasobów, takich jak czas i ilość osób dokonujących czynności.

98. Przegląd jest protokołowany.

99. Dokonujący przeglądu opracowuje wyniki przeprowadzonego przeglądu, które następnie przekazuje w formie raportu z przeglądu administratorowi danych.

100. Na podstawie raportu z przeglądu administrator danych inicjuje działania zapobiegawcze lub kontrolujące.

ROZDZIAŁ XVI
Postanowienia końcowe.

101. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana

jest zapoznać się, przed dopuszczeniem jej do przetwarzania danych osobowych, z powszechnie obowiązującymi przepisami prawa i procedurami wewnętrznymi w zakresie ochrony danych osobowych oraz złożyć oświadczenie potwierdzające znajomość ich treści i zobowiązanie do przestrzegania ich postanowień, według wzoru stanowiącego ***załącznik nr 10 do polityki.***

102. Osoby, o których mowa w pkt 101, zobowiązane są zachować w tajemnicy dane osobowe do których będą miały dostęp oraz sposoby ich zabezpieczenia. W tym celu podpisują oświadczenie, według wzoru stanowiącego ***załącznik nr 10 do polityki.***

Załącznik nr 1 do polityki bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno, przyjętej zarządzeniem nr 83/2018 Wójta Gminy Zbójno z dnia 10 grudnia 2018 r.

....., dnia .....

.....
(Imię i nazwisko kandydata)

.....
(Adres zamieszkania kandydata)

Oświadczenie kandydata do pracy o wyrażeniu zgody na udostępnienie danych osobowych w procesie rekrutacyjnym w Urzędzie Gminy Zbójno

Niniejszym oświadczam, że wyrażam zgodę na przetwarzanie moich danych osobowych przez Urząd Gminy Zbójno w celach rekrutacyjnych, zgodnie z art. 6 ust. 1 lit. 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. Urz. UE. L2016. 119.1)

.....
(Podpis kandydata)

Załącznik nr 2 do polityki bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno, przyjętej zarządzeniem nr 83/2018 Wójta Gminy Zbójno z dnia 10 grudnia 2018 r.

UPOWAŻNIENIE nr ....
do przetwarzania danych osobowych w Urzędzie Gminy Zbójno

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. Urz. UE L 2016 Nr 119), upoważniam:

Panią/Pana .....

zatrudnioną/ego na stanowisku .....

do dostępu i przetwarzania danych osobowych gromadzonych w Urzędzie Gminy Zbójno w zakresie niezbędnym do realizacji zadań i wykonywania obowiązków wynikających z aktualnego zakresu obowiązków, czynności, uprawnień i odpowiedzialności oraz posiadanych upoważnień i pełnomocnictw.

Upoważnienie wydaje się na czas .....

.....
(Data i podpis administratora danych)

Przyjmuje upoważnienie; zapoznałem się z jego treścią, która jest dla mnie zrozumiała i zobowiązuje się z niego korzystać zgodnie z prawem.

.....
(Data i podpis upoważnionego)

Pouczenie

Osoba upoważniona do przetwarzania danych osobowych jest obowiązana zachować w tajemnicy dane osobowe oraz sposoby ich zabezpieczenia, w tym także po ustaniu zatrudnienia, stosunku umownego lub cofnięciu upoważnienia.

WO

Załącznik nr 3 do polityki bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno, przyjętej zarządzeniem nr 83/2018 Wójta Gminy Zbójno z dnia 10 grudnia 2018 r.

Karta szkolenia wstępnego z zakresu ochrony danych osobowych przetwarzanych w Urzędzie Gminy Zbójno

Imię i nazwisko osoby odbywającej szkolenie: .....
Stanowisko: .....
Instruktaż przeprowadzony: ..... (data) ..... (imię i nazwisko przeprowadzającego instruktaż)
W ramach szkolenia poruszone zostały następujące tematy i zagadnienia:
Zgodnie z polityką bezpieczeństwa danych osobowych i instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Zbójno wymaga się tego, aby: 1) dostęp do danych osobowych miały osoby posiadające upoważnienie do przetwarzania danych; 2) każdy z pracowników powinien zachować szczególną ostrożność przy przenoszeniu danych; 3) dane były chronione przed dostępem do nich osób nieupoważnionych; 4) pomieszczenia, w których są przetwarzane dane osobowe, powinny być zamykane na klucz; 5) dostęp do kluczy posiadają tylko upoważnieni pracownicy; 6) dostęp do pomieszczeń możliwy jest tylko i wyłącznie w godzinach pracy; w sytuacji, gdy jest wymagany poza godzinami pracy – możliwy jest tylko na podstawie zezwolenia administratora danych lub inspektora ochrony danych; 7) dostęp do pomieszczeń, w których są przetwarzane dane osobowe, mogą mieć tylko upoważnieni pracownicy; 8) w przypadku pomieszczeń, do których dostęp mają również osoby nieupoważnione, mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności; 9) szafy, w których przechowywane są dane, powinny być zamykane na klucz; 10) klucze do tych szaf posiadają tylko upoważnieni pracownicy; 11) szafy z danymi powinny być otwarte tylko na czas potrzebny na dostęp do danych, a następnie powinny być zamykane; 12) dane w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny do

wykonania czynności służbowych, a następnie muszą być chowane do szaf;

13) dostęp do komputerów, na których są przetwarzane dane, mają tylko upoważnieni pracownicy;

14) monitory komputerów, na których przetwarzane są dane, są tak ustawione, aby osoby nieupoważnione nie miały wglądu w dane;

15) w razie potrzeby wyniesienia komputera przenośnego (np. typu notebook) zawierającego dane osobowe lub inne informacje chronione, komputer taki musi być odpowiednio dodatkowo zabezpieczony, a dane zaszyfrowane;

16) nie należy udostępniać osobom nieupoważnionym tych komputerów;

17) w razie potrzeby przeniesienia danych osobowych pomiędzy komputerami należy zrobić to z zachowaniem szczególnej ostrożności;

18) nośniki użyte do tego należy wyczyścić (skasować nieodwracalnie), aby nie zostały na nich dane osobowe;

19) jeśli nie ma możliwości skasowania danych z nośnika (np. płyta cd-rom), należy go zniszczyć fizycznie;

20) w przypadku wykorzystania do przenoszenia dysków, dane należy kasować z tych dysków;

21) niezabezpieczonych danych osobowych nie należy przesyłać drogą elektroniczną;

22) sieć komputerowa powinna być zabezpieczona przed wszelkim dostępem z zewnątrz;

23) błędne lub nieaktualne wydruki i wersje papierowe zawierające dane osobowe lub inne informacje chronione niszczone są za pomocą niszczarki lub w inny mechaniczny sposób uniemożliwiający powtórne ich odtworzenie;

24) używania tylko zabezpieczonej szyfrowaniem poczty elektronicznej;

25) używania na stanowisku pracy tylko autoryzowanych przez administratora systemów informatycznych i/lub inspektora ochrony danych dysków/pamięci przenośnych/płyt cd/dvd itp. i innych urządzeń pod rygorem odpowiedzialności dyscyplinarnej;

26) używania w trakcie pracy na urządzeniach przenośnych szyfrowania plików zawierających dane osobowe lub inne ważne dane organizacji, które mogą stanowić informację chronioną i nie powinny być dostępne dla osób postronnych;

27. Zastosowanie się do poleceń wydawanych przez inspektora ochrony danych w zakresie dotyczącym ochrony danych i bezpieczeństwa informacji.

28. Nie należy udzielać informacji z danymi osobowymi telefonicznie – zakaz dotyczy każdej organizacji – takie dane podajemy tylko na wniosek, chyba że dotyczą ochrony zdrowia lub życia i mamy możliwość weryfikacji osoby, która próbuje takie dane uzyskać (służby, straże, kuratorzy, rodzice biologiczni itd.) lub prawo nakazuje/umożliwia żeby takie dane udostępnić.

Za prawidłowy nadzór przetwarzania danych oraz zapewnienie im odpowiedniej ochrony odpowiada każdy pracownik na swoim stanowisku pracy, zgodnie z obowiązkami pracowniczymi oraz procedurami i instrukcjami.

Za nieprzestrzeganie procedur bezpieczeństwa i naruszenie ochrony danych grozi odpowiedzialność finansowa, odszkodowawcza, dyscyplinarna, a w skrajnych przypadkach nawet karna.

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia bezpieczeństwa danych osobowych to głównie:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.;

2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy;

3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru;

4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów, lub inny komunikat o podobnym znaczeniu;

5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;

6) nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych;

7) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);

8) nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie;

9) ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń;

10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony informacji – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu itp.;

11) ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. bocznej furtki itp.;

12) podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub skopiowano dane;

13) rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych itp.).Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych, tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie

niezabezpieczonej itp.

Zostałem/am poinformowany/a, że szczegółowy i pełny wykaz przypadków naruszeń ochrony danych oraz instrukcja postępowania w sytuacji naruszenia ochrony danych znajduje się w polityce bezpieczeństwa danych osobowych i zobowiązuję się z nimi niezwłocznie zapoznać oraz postępować w sposób określony w tej procedurze.

Uwagi:

.....

Ponadto na podstawie §20 ust. 2 pkt 6. Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, oświadczam, że zostałem/am poinstruowany/a i poinformowany/a o:

a) zagrożeniach bezpieczeństwa informacji,

b) skutkach naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialności prawnej,

c) stosowaniu środków zapewniających bezpieczeństwo informacji, w tym urządzeń i oprogramowania minimalizującego ryzyko błędów ludzkich.

Przeczytałem/am powyższy instruktaż, w pełni go zrozumiałem/am i go akceptuję. Zobowiązuję się go przestrzegać, co potwierdzam własnoręcznym podpisem*.

.....

(Data i podpis osoby, której udzielono instruktażu)

.....

(Data i podpis udzielającego instruktażu)

** Podpis jest potwierdzeniem odbycia szkolenia i zapoznania się z przepisami oraz zasadami przetwarzania i ochrony danych osobowych. Podpisaną kartę przechowuje kadrowa i inspektor ochrony danych.*

Załącznik nr 4 do polityki bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno, przyjętej zarządzeniem nr 83/2018 Wójta Gminy Zbójno z dnia 10 grudnia 2018 r.

Wykaz budynków i pomieszczeń wchodzących w skład obszaru przetwarzania danych osobowych

Adres	Pomieszczenia

Załącznik nr 5 do polityki bezpieczeństwa danych osobo h przetwarzanych w Urzędzie Gminy Zbójno, przy j zarządzeniem nr 83/2018 Wójta Gminy Zbójno z dnia 10 grudnia 2018 r.

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Lp.	Nazwa zbioru danych/operacji przetwarzania danych osobowych	Nazwa programu/aplikacji w którym przetwarzane są dane osobowe	Sposób gromadzenia	Miejsce przetwarzania danych osobowych	Uwagi
1.					
...					

Załącznik nr 6 do polityki bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno, przyjętej zarządzeniem nr 83/2018 Wójta Gminy Zbójno z dnia 10 grudnia 2018 r.

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Nr upoważnienia	Imię i nazwisko osoby upoważnionej	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia	Identyfikator w systemie informatycznym
1.					

Załącznik nr 7 do polityki bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno, przyjętej zarządzeniem nr 83/2018 Wójta Gminy Zbójno z dnia 10 grudnia 2018 r.

Ewidencja oprogramowania komputerowego

Lp.	Nazwa oprogramowania i jego ilość	Dostawca oprogramowania	Przeznaczenie oprogramowania	Okres obowiązywania licencji

Ewidencja serwerów, komputerów, nośników przenośnych i kluczy kryptograficznych

Lp.	Nazwa urządzenia	Numer fabryczny/seria urządzenia	Przeznaczenie urządzenia	Użytkownik

Załącznik nr 8 do polityki bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno, przyjętej zarządzeniem nr 83/2018 Wójta Gminy Zbójno z dnia 10 grudnia 2018 r.

Ewidencja wniosków o udostępnienie danych osobowych

Lp.	Data wpływu	Nazwa wnioskodawcy	Treść żądania wnioskodawcy	Pracownik odbierający wniosek	Pracownik udzielający odpowiedzi	Data udzielenia odpowiedzi	Znak sprawy

Umowa powierzenia przetwarzania danych osobowych

zawarta dnia ..... pomiędzy:

(zwana dalej „Umową")

Gminą Zbójno, Zbójno 35A, 87-645 Zbójno, reprezentowaną przez:

.....

zwaną w dalszej części umowy **„Administratorem danych" lub „Administratorem"**

a

.....

reprezentowana przez:

.....

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

Powierzenie przetwarzania danych osobowych

§1.1. Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 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 (zwanego w dalszej części „Rozporządzeniem") dane osobowe do przetwarzania, na zasadach
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.

3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

Zakres i cel przetwarzania danych

§2.1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie umowy dane (**należy podać rodzaj danych*) ..... *np. dane zwykłe oraz dane szczególnych kategorii* ..... *(*należy podać kategorię osób, których dane dotyczą) np. pracowników administratora, klientów administratora itd. w postaci* ..... *np. imion i nazwisk, adresu zamieszkania, nr PESEL itd.*

2. Powierzone przez Administratora danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu ..... (**należy podać cel przetwarzania danych przez podmiot przetwarzający) np. realizacji umowy z dnia ..... nr ..... w zakresie prowadzenia kadr.*

Obowiązki podmiotu przetwarzającego

§3.1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.

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 w celu realizacji niniejszej umowy.

4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.

5. Podmiot przetwarzający po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa/ zwraca Administratorowi wszelkie dane osobowe (*należy wybrać czy podmiot przetwarzający ma usunąć czy zwrócić dane*) oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.

6. 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.

7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi w ciągu ..... (**można wskazać np. w ciągu 24 h*).

Prawo kontroli

§4.1. Administrator danych zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.

2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego i z minimum ..... *(*należy wpisać z ilu dniowym wyprzedzeniem Administrator informuje o kontroli*) jego uprzedzeniem.

3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora danych nie dłuższym niż 7 dni (**administrator termin może określić dowolnie*).

4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

Dalsze powierzenie danych do przetwarzania

§5.1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora danych.

2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora danych chyba, że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.

3. Podwykonawca, o którym mowa w §3 ust. 2 Umowy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.

4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za nie wywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

Odpowiedzialność Podmiotu przetwarzającego

§6.1. 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 Generalnego Inspektora Ochrony Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora danych.

Czas obowiązywania umowy

§7.1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas *nieokreślony/określony* od ..... do ..... .*

2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem ..... * okresu wypowiedzenia.

Rozwiązanie umowy

§8. Administrator danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym gdy Podmiot przetwarzający:

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

2) przetwarza dane osobowe w sposób niezgodny z umową;

3) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora danych;

Zasady zachowania poufności

§9.1. 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.

Postanowienia końcowe

§10.1. 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 Administratora danych (**lub Podmiotu przetwarzającego w zależności od postanowień stron*).

....

(Administrator danych) (Podmiot przetwarzający)

Załącznik nr 10 do polityki bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno, przyjętej zarządzeniem nr 83/2018 Wójta Gminy Zbójno z dnia 10 grudnia 2018 r.

.....

(Miejscowość i data)

.....

(Imię i nazwisko składającego oświadczenie)

.....

(Stanowisko, funkcja, zatrudnienie)

Oświadczenie
o przestrzeganiu zasad i przepisów ochrony danych osobowych i o zachowaniu tajemnicy danych osobowych

Oświadczam, że zostałem zapoznany z:

1) powszechnie obowiązującymi przepisami o ochronie danych osobowych;
2) obowiązującymi u administratora danych wewnętrznymi procedurami, instrukcjami itp. w zakresie ochrony danych osobowych;
3) zasadami przetwarzania i ochrony danych osobowych opisanymi w polityce bezpieczeństwa danych osobowych przetwarzanych w Urzędzie Gminy Zbójno.

Jednocześnie oświadczam, że zobowiązuję się przestrzegać zasad i przepisów z zakresu ochrony danych osobowych oraz informacji prawem chronionych podczas wykonywania obowiązków służbowych, w tym zobowiązuję się do:

1) dołożenia wszelkich starań przy wykonywaniu powierzonych mi obowiązków w celu ochrony danych osobowych i informacji prawem chronionych;
2) przetwarzania danych osobowych zgodnie z obowiązującymi w tym zakresie przepisami prawa i regulacjami wewnętrznymi administratora danych;
3) zabezpieczenia przetwarzanych danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa, nieuprawnioną zmianą lub zniszczeniem, utratą, uszkodzeniem;
4) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, również po ustaniu zatrudnienia.

.....

(Podpis osoby składającej oświadczenie)

Załącznik nr 2 do zarządzenia nr 83/2018 Wójta Gminy Zbójno z dnia 10 grudnia 2018 r. w sprawie wprowadzenia dokumentacji przetwarzania danych osobowych w Urzędzie Gminy Zbójno.

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Zbójno

Wprowadzenie

1. Niniejsza instrukcja określa zasady eksploatacji i zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Zbójno, zwanym dalej urzędem.

2. Zasady opisane w niniejszym dokumencie są zgodne z obowiązującymi wymaganiami prawnymi, w szczególności:

1) Rozporządzeniem Parlamentu Europejskiego i Rady (2016/679) z 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 (Dz.Urz. UE L 2016, Nr 119, s. 1), tzw. RODO;

2) ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000).

3. W instrukcji stosuje się następujące skróty:

1) urząd – Urząd Gminy Zbójno;

1) IOD - Inspektor Ochrony Danych, pracownik urzędu wyznaczony przez Administratora Danych do wykonywania obowiązków IOD określonych w RODO;

2) AS - Administrator Systemu, pracownik urzędu odpowiedzialny za administrację systemami informatycznymi urzędu;

3) AD - Administrator Danych, którym jest Wójt Gminy Zbójno.

Procedura nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

4. Podstawą do nadania uprawnień do przetwarzania danych osobowych w systemie informatycznym urzędu jest upoważnienie do przetwarzania danych osobowych. Upoważnienie wydawane jest przez AD.

5. Upoważnienie wydawane jest na wniosek przełożonego danego pracownika, a w przypadku osoby nie będącej pracownikiem urzędu – na wniosek pracownika urzędu koordynującego działania osoby, dla której upoważnienie jest wydawane.

6. Inspektor Ochrony Danych:

1) w przypadku gdy dana osoba otrzymuje po raz pierwszy upoważnienie do przetwarzania danych osobowych – przeprowadza wstępne szkolenie w zakresie zasad ochrony danych osobowych;

2) odbiera od powyższej osoby podpis pod:

- upoważnieniem do przetwarzania danych osobowych,
- oświadczeniem o zapoznaniu się z obowiązującymi zasadami ochrony danych osobowych,
- zobowiązaniem się do zachowania w tajemnicy danych osobowych.

7. IOD prowadzi, w imieniu i z upoważnienia AD ewidencję osób upoważnionych do przetwarzania danych osobowych. Każda zmiana w zakresie informacji zawartych w ewidencji podlega niezwłocznemu odnotowaniu przez IOD.

8. Uprawnienia dostępu do systemu informatycznego nadawane są na podstawie wniosku przełożonego danego pracownika, a w przypadku osoby niebędącej pracownikiem urzędu – na wniosek pracownika urzędu koordynującego działania danej osoby.

9. Za nadanie uprawnień w systemie informatycznym odpowiada AS. Uprawnienia nie mogą być nadane w przypadku, jeżeli dana osoba nie posiada upoważnienia do przetwarzania danych osobowych w wymaganym zakresie.

10. AS informuje osobę wnioskującą o fakcie nadania lub odmowy nadania uprawnień.

11. W przypadku nadawania użytkownikowi uprawnień do danego systemu informatycznego po raz pierwszy, AS dokonuje nadania użytkownikowi identyfikatora, wygenerowania hasła oraz wpisania identyfikatora do ewidencji osób upoważnionych do przetwarzania danych osobowych.

12. Identyfikator użytkownika w systemie informatycznym musi być unikalny dla użytkownika. Nie może być to identyfikator, który w przeszłości był już stosowany w systemie informatycznym. Sprawdzenie unikalności identyfikatora odbywa się na podstawie ewidencji osób upoważnionych do przetwarzania danych osobowych.

13. Hasło użytkownika jest przydzielane indywidualnie każdemu z użytkowników i znane jest tylko użytkownikowi, który się nim posługuje.

14. AS przekazuje użytkownikowi identyfikator i hasło.

15. Użytkownik jest zobowiązany do zmiany hasła przy pierwszym dostępie do systemu informatycznego.

Procedura odbierania uprawnień do przetwarzania danych w systemie informatycznym

16. W przypadku konieczności odebrania lub zmiany zakresu upoważnienia – w związku ze zmianą zakresu obowiązków służbowych pracownika lub zakończeniem pracy – jego przełożony wnioskuje do IOD o wykonanie powyższej czynności. AD dokonuje, na podstawie informacji przekazanej przez IOD, odebrania lub zmiany zakresu upoważnienia, AS zaś dokonuje odebrania lub zmiany zakresu uprawnień w systemie informatycznym.

17. W przypadku konieczności odebrania lub zmiany zakresu upoważnienia dla osób nie będących pracownikami urzędu o wykonanie powyższej czynności wnioskuje pracownik urzędu koordynujący działania danej osoby.

Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

18. Użytkownicy systemu informatycznego przetwarzającego dane osobowe wykorzystują w procesie uwierzytelnienia identyfikatory i hasła.

19. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi i nie podlega zmianie.

20. Nowe hasło jest przekazywane użytkownikowi przez AS.

21. Po zalogowaniu do systemu z wykorzystaniem otrzymanego hasła użytkownik jest zobowiązany do dokonania jego natychmiastowej zmiany, nawet jeżeli system informatyczny nie wymusza takiego działania.

22. Hasła dostępu do systemu informatycznego muszą spełniać poniższe warunki:

1) posiadać długość co najmniej 8 znaków;
2) zawierać litery małe i duże;
3) zawierać cyfry lub znaki specjalne.

23. Hasło jest zmieniane przez użytkownika nie rzadziej niż co 30 dni lub niezwłocznie w przypadku podejrzenia, iż mogły z nim się zapoznać nieuprawnione osoby.

24. Hasło powinno różnić się od poprzednio używanych.

25. Użytkownik zobowiązany jest do:

1) nieujawniania hasła innym osobom, w tym innym użytkownikom;
2) zachowania hasła w tajemnicy, również po jego wygaśnięciu;
3) niezapisywania hasła;
4) postępowania z hasłami w sposób uniemożliwiający dostęp do nich osobom trzecim;
5) przestrzegania zasad dotyczących jakości i częstości zmian hasła;
6) wprowadzania hasła do systemu w sposób minimalizujący podejrzenie go przez innych użytkowników systemu.

26. W przypadku zapomnienia hasła użytkownik powinien zwrócić się do AS o wygenerowanie nowego hasła.

27. W przypadku podejrzenia zapoznania się z hasłem przez osobę nieuprawnioną użytkownik jest zobowiązany do natychmiastowej zmiany hasła oraz powiadomienia o zaistniałym fakcie AS.

Procedura rozpoczęcia, zawieszenia i zakończenia pracy przeznaczona dla użytkowników systemu

28. Rozpoczynając pracę w systemie informatycznym przetwarzającym dane osobowe, użytkownik:

1) uruchamia komputer;
2) wprowadza niezbędne do pracy identyfikatory i hasła;

3) hasła są wprowadzane w sposób minimalizujący ryzyko podejrzenia ich przez osoby trzecie;

4) w przypadku problemów z rozpoczęciem pracy, spowodowanych odrzuceniem przez system wprowadzonego identyfikatora i hasła, natychmiast kontaktuje się z AD;

5) w przypadku niestandardowego zachowania aplikacji przetwarzającej dane osobowe pracownik natychmiast powiadamia o zaistniałym fakcie AD.

29. Zawieszając pracę w systemie informatycznym (w tym odchodząc od stanowiska pracy), użytkownik blokuje stację roboczą. Kontynuacja pracy może nastąpić po odblokowaniu stacji roboczej i po wprowadzeniu hasła, w sposób gwarantujący jego niepodejrzenie przez osoby trzecie.

30. Opuszczając pomieszczenie, w którym przetwarzane są dane osobowe, pracownik zobowiązany jest do zamknięcia pomieszczenia na klucz, jeżeli w pomieszczeniu tym nie przebywa inna osoba upoważniona do przebywania w tym pomieszczeniu. Zabronione jest pozostawianie bez nadzoru w pomieszczeniach, w których przetwarzane są dane osobowe, osób nieupoważnionych.

31. Kończąc pracę w systemie informatycznym pracownik wylogowuje się ze wszystkich aplikacji, z których korzystał, wyłącza stację roboczą i zabezpiecza nośniki danych. W przypadku gdy pracownik jest ostatnią osobą opuszczającą pomieszczenie, sprawdza zamknięcie okien, zamyka na klucz drzwi do pomieszczenia oraz zdaje klucz w sekretariacie.

Procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

32. Za tworzenie i zabezpieczanie kopii zapasowych odpowiedzialny jest AS.

33. Kopie zapasowe systemów przetwarzających dane osobowe (serwer główny, stacje robocze) są codziennie zapisywane na serwer zapasowy.

34. AS odpowiedzialny jest za realizację działań odtworzeniowych w przypadku konieczności podjęcia takich działań w związku z awarią systemu informatycznego urzędu. Po odtworzeniu systemu informatycznego AS odpowiedzialny jest za przeprowadzenie testów poprawności działania systemu przed jego oddaniem do użytkowania.

35. AS przeprowadza weryfikację możliwości odtworzenia danych zapisanych na serwerze zapasowym. Weryfikacja taka powinna być przeprowadzana nie rzadziej niż raz na pół roku.

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

36. Dane osobowe przechowywane są w postaci elektronicznej na:

1) nośnikach elektronicznych wbudowanych w sprzęt informatyczny lub stanowiących element tego systemu;

2) przenośnych nośnikach elektronicznych;

3) serwerach – głównym i zapasowym.

37. Dane przechowywane są 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 urzędzie, a w przypadku nośników optycznych stosuje się niszczenie w niszczarkach umożliwiających niszczenie tego typu nośników.

38. Dane osobowe w systemie informatycznym przechowywane są przez czas wymagany do spełnienia celu, dla którego są one przetwarzane. Po jego upływie dane podlegają skasowaniu lub anonimizacji.

39. Przenośne elektroniczne nośniki informacji zawierające dane osobowe są przechowywane przez pracowników w sposób minimalizujący ryzyko ich uszkodzenia lub zniszczenia, w szczególności w zamykanych szafach i meblach biurowych. Przenośne elektroniczne nośniki informacji powinny być zaszyfrowane przy użyciu narzędzi zaakceptowanych do użycia w urzędzie.

40. W przypadku wycofania sprzętu komputerowego z użycia dane osobowe na nim zapisane są kasowane przy użyciu dedykowanego oprogramowania do bezpiecznego usuwania danych zaakceptowanego do użycia w urzędzie. W przypadku braku możliwości programowego usunięcia danych dysk podlega fizycznemu zniszczeniu. Za zniszczenie danych odpowiada AS. Zniszczenie nośnika potwierdzane jest protokołem przechowywanym przez AS.

41. Dopuszcza się powierzenie niszczenia nośników danych wyspecjalizowanym podmiotom zewnętrznym, pod warunkiem:

1) zawarcia umowy, o której mowa w art. 31 uodo;
2) zagwarantowania poufności danych przez usługodawcę;
3) umożliwienia prowadzenia nadzoru nad procesem niszczenia nośników przez AS lub upoważnionego przez niego pracownika urzędu;
4) udokumentowania faktu zniszczenia nośników protokołem.

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem działania jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

42. W celu zabezpieczenia systemu informatycznego przed działaniem niebezpiecznego oprogramowania zabrania się:

1) uruchamiania jakiegokolwiek oprogramowania, które nie zostało zatwierdzone do użytku w urzędzie;
2) samowolnego korzystania z nośników przenośnych;
3) otwierania poczty elektronicznej, której tytuł nie sugeruje związku z pełnionymi obowiązkami służbowymi; w przypadkach wątpliwych należy skonsultować się z AS;
4) korzystania z Internetu w celach nie związanych z pełnionymi obowiązkami służbowymi;

5) podłączania komputerów do sieci zewnętrznych za pośrednictwem modemów.

43. W przypadku zauważenia objawów mogących wskazywać na obecność niebezpiecznego oprogramowania użytkownik jest zobowiązany powiadomić AS. Do objawów powyższych można zaliczyć:

1) istotne spowolnienie działania systemu informatycznego;
2) nietypowe działanie aplikacji;
3) nietypowe komunikaty;
4) utratę danych lub modyfikację danych.

44. System informatyczny jest zabezpieczony przed działaniem niebezpiecznego oprogramowania poprzez:

1) oprogramowanie antywirusowe;
2) zaporę sieciową;
3) aktualizację oprogramowania systemowego;
4) konfigurację oprogramowania minimalizującą ryzyko naruszenia bezpieczeństwa.

45. AS jest odpowiedzialny za nadzór nad działaniem powyższych zabezpieczeń, a w szczególności za:

1) weryfikację aktualności sygnatur systemu antywirusowego i podejmowanie ewentualnych działań korekcyjnych;
2) weryfikację logów systemu antywirusowego i podejmowanie działań korekcyjnych;
3) przegląd logów zapory sieciowej oraz podejmowanie działań mających na celu zablokowanie ataków sieciowych;
4) weryfikację poprawności aktualizacji oprogramowania systemowego.

Odnotowanie informacji o udostępnieniu danych osobowych

46. Urząd udostępnia dane osobowe jedynie w przypadkach prawnie dopuszczalnych. W przypadku udostępnienia danych fakt ten należy odnotować w sposób ustalony przez AD.

Procedura wykonywania przeglądu i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

47. Przegląd i konserwacja sprzętu informatycznego realizowany jest przez upoważnionych pracowników urzędu oraz przez podmioty zewnętrzne.

48. Prace serwisowe wykonywane na terenie urzędu przez podmioty zewnętrzne podlegają bezpośredniemu nadzorowi AS.

49. Przekazanie sprzętu informatycznego do naprawy poza teren urzędu jest dopuszczalne, jeżeli spełnione zostaną poniższe warunki:

1) sprzęt przekazywany jest bez nośników zawierających dane osobowe, zaś fakt usunięcia nośników danych lub stwierdzenia braku nośników danych jest potwierdzany protokołem;

2) przekazanie sprzętu potwierdzane jest protokołem, pozwalającym na jednoznaczne wskazanie osoby przekazującej i osoby odbierającej sprzęt.

50. Protokoły, o których mowa w punkcie 2, lub ich kopie przechowywane są przez AS.

51. Wszelkie prace serwisowe wykonywane przez podmioty zewnętrzne wymagają sporządzenia protokołu serwisowego, zawierającego co najmniej poniższe informacje:

1) wskazanie osoby przeprowadzającej prace serwisowe oraz podmiotu, którego osoba ta jest pracownikiem;

2) wskazanie osoby nadzorującej przebieg prac serwisowych (dotyczy sytuacji, gdy prace realizowane są w siedzibie Urzędu);

3) przedmiot prac serwisowych (w szczególności identyfikator sprzętu w przypadku prac serwisowych dotyczących sprzętu);

4) zakres prac serwisowych i ich wynik;

5) czas przeprowadzania prac serwisowych.

Załącznik nr 3 do zarządzenia nr 83/2018 Wójta Gminy Zbójno z dnia 10 grudnia 2018 r. w sprawie wprowadzenia dokumentacji przetwarzania danych osobowych w Urzędzie Gminy Zbójno.

Instrukcja postępowania w przypadku zagrożenia bezpieczeństwa danych osobowych oraz instrukcja postępowania w przypadku incydentów bezpieczeństwa danych osobowych w Urzędzie Gminy Zbójno

W przypadku stwierdzenia naruszenia zasad ochrony danych osobowych lub ich zagrożenia, każdy pracownik jest zobowiązany poinformować o tym fakcie administratora danych i/lub inspektora ochrony danych i/lub bezpośredniego przełożonego. Inspektor ochrony danych i/lub bezpośredni przełożony pracownika są zobowiązany powiadomić o tym fakcie administratora danych.

I. Instrukcja postępowania w przypadku zagrożenia bezpieczeństwa danych osobowych

1. Zagrożeniem bezpieczeństwa danych osobowych jest sytuacja, w której występuje zagrożenie zaistnienia incydentu. Przykładowy katalog zagrożeń:

1) nieprzestrzeganie polityki bezpieczeństwa informacji w Urzędzie Gminy Zbójno przez osoby przetwarzające dane, np. niezamykanie pomieszczeń, szaf, biurek, brak stosowania zasad ochrony haseł;

2) niewłaściwe zabezpieczenie fizyczne dokumentów, urządzeń i/lub pomieszczeń;

3) niewłaściwe zabezpieczenie oprogramowania lub sprzętu IT przed wyciekiem, kradzieżą i/lub utratą danych osobowych.

2. Postępowanie administratora danych i/lub inspektora ochrony danych i/lub bezpośredniego przełożonego w przypadku stwierdzenia wystąpienia zagrożenia:

1) ustalenie zakresu i przyczyn zagrożenia oraz jego ewentualnych skutków;

2) w miarę możliwości przywrócenie stanu zgodnego z zasadami ochrony danych osobowych;

3) w razie konieczności zainicjowanie działań dyscyplinarnych;

4) zarekomendowanie działań zapobiegawczych w kierunku wyeliminowania podobnych zagrożeń w przyszłości;

5) udokumentowanie prowadzonego postępowania w formie raportu z naruszeń ochrony danych osobowych, którego wzór stanowi ***załącznik nr 1*** do niniejszej instrukcji oraz wpisanie go do rejestru naruszeń ochrony danych osobowych, którego wzór stanowi ***załącznik nr 2*** do niniejszej instrukcji.

3. Postępowanie pracownika w przypadku stwierdzenia wystąpienia zagrożenia do czasu przybycia administratora danych i/lub inspektora ochrony danych i/lub bezpośredniego przełożonego pracownika:

1) powstrzymanie się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów;

2) zabezpieczenie elementów systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osób nieupoważnionych;

3) podjęcie, stosownie do zaistniałej sytuacji, wszelkich niezbędnych działań celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.

II. Instrukcja postępowania w przypadku incydentów bezpieczeństwa danych osobowych

1. Incydentem jest sytuacja naruszenia bezpieczeństwa informacji ze względu na dostępność, integralność i poufność. Incydenty powinny być wykrywane, rejestrowane i monitorowane w celu zapobieżenia ich ponownemu wystąpieniu. Przykładowy katalog incydentów:

1) losowe zdarzenie wewnętrzne, np. awaria komputera, serwera, twardego dysku, błąd użytkownika, informatyka, zgubienie danych;

2) losowe zdarzenie zewnętrzne, np. klęski żywiołowe, zalanie, awaria zasilania, pożar;

3) incydent umyślny, np. wyciek informacji, ujawnienie danych nieupoważnionym osobom, świadome zniszczenie danych, działanie wirusów komputerowych, włamanie do pomieszczeń lub systemu informatycznego (wewnętrzne i zewnętrzne).

2. Postępowanie administratora danych i/lub inspektora ochrony danych i/lub bezpośredniego przełożonego w przypadku stwierdzenia wystąpienia incydentu:

1) ustalenie czasu zdarzenia będącego incydentem;

2) ustalenie zakresu incydentu;

3) określenie przyczyn, skutków oraz szacowanie zaistniałych szkód;

4) zabezpieczenie dowodów;

5) ustalenie osób odpowiedzialnych za naruszenie;

6) usunięcie skutków incydentu;

7) ograniczenie szkód wywołanych incydentem;

8) zainicjowanie działań dyscyplinarnych;

9) zarekomendowanie działań zapobiegawczych w kierunku wyeliminowania podobnych zagrożeń w przyszłości;

10) udokumentowanie prowadzonego postępowania w formie raportu z naruszeń ochrony danych osobowych, którego wzór stanowi ***załącznik nr 1*** do niniejszej instrukcji oraz wpisanie go do rejestru naruszeń ochrony danych osobowych, którego wzór stanowi ***załącznik nr 2*** do niniejszej instrukcji.

3. Inspektor ochrony danych gromadzi raporty z naruszeń ochrony danych osobowych oraz prowadzi rejestr naruszeń ochrony danych osobowych.

4. Przykładowy katalog naruszeń bezpieczeństwa danych osobowych stanowi ***załącznik nr 3*** do niniejszej instrukcji

5. W celu realizacji zadań określonych w powyższych instrukcjach administrator danych, inspektor ochrony danych i bezpośredni przełożony pracownika mają prawo do podejmowania wszelkich działań dopuszczonych przez prawo, a w szczególności:

1) żądania wyjaśnień od pracowników;
2) korzystania z pomocy konsultantów;
3) nakazania przerwania pracy, zwłaszcza w zakresie przetwarzanych danych osobowych.

6. Polecenie administratora danych, inspektora ochrony danych i bezpośredniego przełożonego pracownika wydawane w czasie realizacji zadań wynikających z niniejszych instrukcji są priorytetowe i winny być wykonywane przed innymi. Odmowa udzielenia wyjaśnień lub współpracy traktowana będzie jako ciężkie naruszenie obowiązków pracowniczych.

7. Administrator danych i/lub inspektor ochrony danych, zgodnie z rozporządzeniem, podejmuje decyzję czy należy zgłosić naruszenie do Prezesa Urzędu Ochrony Danych Osobowych i poinformować o naruszeniu osobę, której danych osobowych dotyczy naruszenie. W tym celu korzysta się z listy kontrolnej pn. „jak postąpić w przypadku naruszenia ochrony danych osobowych", której wzór stanowi ***załącznik nr 4*** do instrukcji.

8. Zgłoszenie naruszenia ochrony danych osobowych do Prezesa Urzędu Ochrony Danych Osobowych stanowi ***załącznik nr 5*** do instrukcji.

Załącznik nr 1 do instrukcji postępowania w przypadku zagrożenia bezpieczeństwa danych osobowych oraz instrukcji postępowania w przypadku incydentów bezpieczeństwa danych osobowych w Urzędzie Gminy Zbójno przyjętych zarządzeniem nr 83/2018 Wójta Gminy Zbójno z dnia 10 grudnia 2018 r.

Raport z naruszenia ochrony danych osobowych

1. Data ..... Godzina .....

2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem (imię, nazwisko, stanowisko służbowe):

.....

3. Lokalizacja zdarzenia (nr pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):

.....

4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:

.....

5. Podjęte działania:

.....

6. Wstępna ocena przyczyn wystąpienia naruszenia:

.....

7. Postępowanie wyjaśniające i naprawcze:

.....

.....

Podpis pracownika

.....

Data i podpis administratora danych /inspektora ochrony danych/bezpośredniego przełożonego

Załącznik nr 2 do instrukcji postępowania w przypadku zagrożenia bezpieczeństwa danych osobowych oraz instrukcji postępowania w przypadku incydentów bezpieczeństwa danych osobowych w Urzędzie Gminy Zbójno przyjętych zarządzeniem nr 83/2018 Wójta Gminy Zbójno z dnia 10 grudnia 2018 r.

Rejestr naruszeń ochrony danych osobowych w Urzędzie Gminy Zbójno

Rejestr naruszeń ochrony danych osobowych					
Rodzaj naruszenia	Obowiązek zgłoszenia organowi nadzorczemu	Obowiązek zawiadomienia osoby, której dane dotyczą	Okoliczności naruszenia	Skutki naruszenia	Podjęte działania zaradcze
1.					
2.					
…					

Załącznik nr 3 do instrukcji postępowania w przypadku zagrożenia bezpieczeństwa danych osobowych oraz instrukcji postępowania w przypadku incydentów bezpieczeństwa danych osobowych w Urzędzie Gminy Zbójno przyjętych zarządzeniem nr 83/2018 Wójta Gminy Zbójno z dnia 10 grudnia 2018 r.

Przykładowy katalog naruszeń ochrony danych osobowych

NR (KOD) NARUSZEŃ	FORMY NARUSZEŃ	SPOSÓB POSTĘPOWANIA
A	**Forma naruszeń ochrony danych osobowych przez pracownika zatrudnionego przy przetwarzaniu danych osobowych**	
A.1	**w zakresie wiedzy:**	
A.1.1	Ujawnianie sposobu działania aplikacji i systemu zabezpieczeń osobom niepowołanym	Natychmiast przerwać rozmowę lub inna czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić Inspektora Ochrony Danych.
A.1.2.	Ujawnienie informacji o sprzęcie i pozostałej infrastrukturze informatycznej	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić Inspektora Ochrony Danych.
A.1.3.	Dopuszczenie i stwarzanie warunków, aby ktokolwiek taką wiedzę mógł pozyskać Np. z obserwacji lub dokumentacji	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić
A.2.	**w zakresie sprzętu i oprogramowania:**	
A.2.1.	Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.	Niezwłocznie zakończyć działanie aplikacji. Sporządzić raport.
A.2.2.	Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. Pouczyć osobę, która dopuściła do takiej sytuacji. Sporządzić raport.
A.2.3.	Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych i sieci ZSD	Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie. Niezwłocznie powiadomić Inspektora Ochrony Danych. Sporządzić raport.
A.2.4.	Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych przez osoby nie będące pracownikami ZSD.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić, jakie czynności zostały przez osoby nieuprawnione wykonane. Przerwać działające programy. Niezwłocznie powiadomić Inspektora Ochrony Danych. Sporządzić raport.
A.2.5.	Samodzielne instalowanie jakiegokolwiek oprogramowania.	Pouczyć osobę popełniającą wymienioną czynność, aby jej zaniechała. Sporządzić raport.
A.2.6.	Modyfikowanie parametrów systemu i aplikacji.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Sporządzić raport.
A.2.7.	Odczytywanie dyskietek i innych nośników przed sprawdzeniem ich programem antywirusowym.	Pouczyć osobę popełniającą wymienioną czynność, aby zaczęła stosować się do wymogów bezpieczeństwa pracy. Wezwać służby informatyczne w celu wykonania kontroli antywirusowej. Sporządzić raport.
A.3.	**w zakresie dokumentów i obrazów zawierających dane osobowe:**	
A.3.1.	Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru	Zabezpieczyć dokumenty. Sporządzić raport.

A.3.2.	Przechowywanie dokumentów zabezpieczonych w niedostatecznym stopniu przed dostępem osób niepowołanych.	Powiadomić przełożonych. Spowodować poprawienie Zabezpieczeń. Sporządzić raport.
A.3.3.	Wyrzucanie dokumentów nieprawidłowo zniszczonych – możliwość odczytania danych.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić przełożonych. Sporządzić raport.
A.3.4.	Dopuszczenie do kopiowania dokumentów i utraty kontroli nad kopią.	Zaprzestanie kopiowania. Odzyskać i zabezpieczyć wykonane kopię. Powiadomić przełożonych. Sporządzić raport.
A.3.5.	Dopuszczenie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. Jeżeli ujawnione zostały ważne dane – sporządzić raport.
A.3.6.	Sporządzanie kopii danych na nośnikach danych w sytuacjach nie przewidzianych procedurą.	Spowodować zaprzestanie kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić Inspektora Ochrony Danych. Sporządzić raport.
A.3.7.	Utrata kontroli nad kopią danych osobowych	Podjąć próbę odzyskania kopii. Powiadomić Inspektora Ochrony Danych. Sporządzić raport.
A.4.	**w zakresie pomieszczeń i infrastruktury służących do przetwarzania danych osobowych:**	
A.4.1.	Opuszczanie i pozostawienie bez dozoru nie zamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwo danych osobowych.	Zabezpieczyć (zamknąć) pomieszczenie. Powiadom przełożonych. Sporządzić raport.
A.4.2.	Wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym.	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich tożsamość. Powiadomić przełożonych i Inspektora Ochrony Danych. Sporządzić raport.
A.4.3.	Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakiekolwiek urządzenia do sieci komputerowej ZSD, demontowały elementy obudów gniazd i torów kablowych lub dokonywały jakichkolwiek manipulacji.	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i Inspektora Ochrony Danych. Sporządzić raport.
A.5.	**w zakresie pomieszczeń, w których znajdują się centralne komputery i urządzenia sieci.**	
A.5.1.	Dopuszczanie lub ignorowanie faktu, że osoby spoza służb informatycznych i telekomunikacyjnych dokonują jakichkolwiek manipulacji przy urządzeniach lub okablowaniu sieci komputerowej w miejscach publicznych (korytarze, itp.)	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i Inspektora Ochrony Danych. Sporządzić raport.
A.5.2.	Dopuszczanie do znalezienia się w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej osób spoza służb informatycznych i telekomunikacyjnych lub ignorowanie takiego faktu.	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania i opuszczenia chronionych pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i Inspektora Ochrony Danych. Sporządzić raport.

B	**Zjawiska świadczące o możliwości naruszenia ochrony danych osobowych.**	
B.1	Ślady manipulacji przy układach sieci komputerowej lub komputerach	Powiadomić niezwłocznie Inspektora Ochrony Danych oraz służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.2	Obecność nowych kabli o nieznanym przeznaczeniu i pochodzeniu.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.3	Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służących do przetwarzania danych osobowych.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.4	Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.5	Obecność nowych programów w komputerze lub inne zmiany konfiguracji oprogramowania	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
B.6	Slajdy włamań do pomieszczeń, w których przetwarzane są dane osobowe	Postępować zgodnie z właściwymi przepisami. Powiadomić niezwłocznie Inspektora Ochrony Danych. Sporządzić raport.
C	**Formy naruszenia ochrony danych osobowych przez obsługę informatyczną w kontaktach z użytkownikiem.**	
C.1	Próba uzyskania hasła uprawniającego do dostępu do danych osobowych w ramach pomocy technicznej.	Powiadomić inspektora bezpieczeństwa informacji. Sporządzić raport.
C. 2	Prośba nieuzasadnionego przeglądania (modyfikowania) w ramach pomocy technicznej danych osobowych za pomocą aplikacji w bazie danych identyfikatorem i hasłem użytkownika.	Powiadomić inspektora bezpieczeństwa informacji. Sporządzić raport.
D.	**Formy naruszenia dostępu do systemu komputerowego przez Inspektora Ochrony Danych.**	
D.1	Próba uzyskania hasła dostępu do systemu komputerowego.	Powiadomić administratora systemu informatycznego. Sporządzić raport.

Załącznik nr 4 do instrukcji postępowania w przypadku zagrożenia bezpieczeństwa danych osobowych oraz instrukcji postępowania w przypadku incydentów bezpieczeństwa danych osobowych w Urzędzie Gminy Zbójno przyjętych zarządzeniem nr 83/2018 Wójta Gminy Zbójno z dnia 10 grudnia 2018 r.

Jak postąpić w przypadku naruszenia ochrony danych osobowych

Krok 1. **Czy doszło do naruszenia?**	
Wykryłeś zdarzenie zagrażające bezpieczeństwu lub zostałeś o nim powiadomiony. Ustal, czy doszło do naruszenia danych osobowych.	☐
Krok 2. **Czy naruszenie stanowi ryzyko dla praw i wolności osób fizycznych?**	
Stwierdziłeś, że doszło do naruszenia danych osobowych. Oceń, czy naruszenie może narazić prawa i wolności osób fizycznych na ryzyko.	☐
Krok 3. **Kiedy nie musisz powiadamiać organu nadzorczego?**	
Jeśli stwierdziłeś, że naruszenie nie może narazić praw i wolności osób fizycznych na ryzyko, nie musisz powiadamiać organu nadzorczego (w Polsce Prezes Urzędu Ochrony Danych Osobowych – zgodnie z projektem ustawy o ochronie danych osobowych z 12 września 2017 r.) ani osób fizycznych, których dane dotyczą.	☐
Krok 4. **Kiedy musisz powiadomić organ nadzorczy?**	
Jeśli stwierdziłeś, że naruszenie może narazić prawa i wolności osób fizycznych na ryzyko, powiadom o tym organ nadzorczy (w Polsce Prezes Urzędu Ochrony Danych Osobowych – zgodnie z projektem ustawy o ochronie danych osobowych z 12 września 2017 r.).	☐
Jeżeli naruszenie wpływa na osoby fizyczne w więcej niż jednym państwie członkowskim, powiadom o nim wszystkie właściwe organy nadzorcze.	☐
Krok 5. **Kiedy nie musisz powiadamiać osoby fizycznej?**	
Jeżeli stwierdziłeś, że naruszenie nie może narazić praw i wolności osób fizycznych na wysokie ryzyko, nie musisz powiadamiać o nim osób fizycznych, których danych dotyczy naruszenie.	☐
Krok 6. **Kiedy musisz powiadamiać osobę fizyczną?**	
Jeżeli stwierdziłeś, że naruszenie może narazić prawa i wolności osób fizycznych na wysokie ryzyko, musisz powiadomić o nim osoby fizyczne, których danych dotyczy naruszenie.	☐

Przekaż poszkodowanym osobom informacje o krokach, jakie mogą podjąć, aby ochronić się przed konsekwencjami naruszenia ochrony danych osobowych.	☐
Krok 7. **Czy udokumentować naruszenie?**	
Udokumentuj naruszenie ochrony danych, do którego doszło w Twoim podmiocie.	☐
Zachowaj dokumentację naruszeń ochrony danych osobowych w odpowiednim rejestrze.	☐

Zał. nr 5

Zgłoszenie naruszenia ochrony danych osobowych

1. Dane wnioskodawcy

A. Podaj typ zgłoszenia

Wskaż czy zgłaszasz naruszenie ochrony danych osobowych mające charakter jednorazowego zdarzenia (np. zgubienie, kradzież nośnika danych, przypadkowe wysłanie danych osobie nieuprawnionej), czy przygotowujesz wstępne zgłoszenie, które uzupełnisz później, lub czy uzupełniasz lub zmieniasz wcześniejsze zgłoszenie.

- (•) Zgłoszenie kompletne/jednorazowe
- ( ) Zgłoszenie wstępne
- ( ) Zgłoszenie uzupełniające/zmieniające

Podaj datę poprzedniego zgłoszenia (opcjonalnie – jeśli zgłoszenie jest uzupełniające/zmieniające)

Kliknij tutaj, aby wprowadzić datę.

2. Podmiot zgłaszający

A. Dane administratora danych

Pełna nazwa administratora	Kliknij tutaj, aby wprowadzić tekst.
REGON – jeśli został podany (opcjonalnie)	Kliknij tutaj, aby wprowadzić tekst.
Sektor (opcjonalnie)	Dla sektora publicznego: Wybierz element. / Dla sektora prywatnego: Wybierz element.

B. Adres siedziby administratora danych

Państwo	Kliknij tutaj, aby wprowadzić tekst.	Miejscowość	Kliknij tutaj, aby wprowadzić tekst.
Województwo	Kliknij tutaj, aby wprowadzić tekst.	Ulica	Kliknij tutaj, aby wprowadzić tekst.
Powiat	Kliknij tutaj, aby wprowadzić tekst.	Kod pocztowy	Kliknij tutaj, aby wprowadzić tekst.
Gmina	Kliknij tutaj, aby wprowadzić tekst.	Numer domu	Podaj numer / Numer lokalu: Podaj numer

C. Osoby uprawnione do reprezentowania administratora

1.	Imię i nazwisko: Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.

(Aby dopisać kolejne osoby, należy po kliknięciu na powyższe pole kliknąć przycisk [+], który pojawi się po prawej stronie)

D. Pełnomocnik

☐ Wniosek wypełniany przez pełnomocnika (opcjonalnie)

Pełnomocnictwo udzielone w formie elektronicznej oraz dowód uiszczenia opłaty skarbowej należy załączyć podczas składania wniosku przez portal biznes.gov.pl.
Pełnomocnictwo opatrzone kwalifikowanym podpisem elektronicznym osoby udzielającej pełnomocnictwa.

E. Inspektor ochrony danych

Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.
Numer telefonu	Kliknij tutaj, aby wprowadzić tekst.
Adres e-mail	Kliknij tutaj, aby wprowadzić tekst.

☐ Inspektor nie został wyznaczony

Jeśli inspektor nie został wyznaczony podaj dane innego punktu kontaktowego, od którego można uzyskać więcej informacji o naruszeniu.

Kliknij tutaj, aby wprowadzić tekst.

F. Inne podmioty uczestniczące w przetwarzaniu danych, których dotyczy naruszenie (opcjonalnie)

Podaj nazwy podmiotów, dane kontaktowe i wyjaśnij ich rolę w procesie przetwarzania, którego dotyczy naruszenie

Kliknij tutaj, aby wprowadzić tekst.

3. Czas naruszenia

A. Wykrycie naruszenia i powiadomienie organu nadzorczego

Data stwierdzenia naruszenia
Wskaż kiedy dowiedziałeś/aś się o naruszeniu.
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Kliknij tutaj, aby wprowadzić datę.

Sposób stwierdzenia naruszenia
Np. zgłoszenie osoby której dane dotyczą czy cykliczny przegląd logów systemowych zgodnie z wdrożoną polityką bezpieczeństwa

Kliknij tutaj, aby wprowadzić tekst.

Data powiadomienia przez podmiot przetwarzający
(opcjonalnie)
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Kliknij tutaj, aby wprowadzić tekst.

Powody opóźnienia powiadomienia organu nadzorczego o naruszeniu
Pole obowiązkowe jeśli czas od momentu stwierdzenia naruszenia do czasu wypełniania formularza jest dłuższy niż 72h

Kliknij tutaj, aby wprowadzić tekst.

B. Czas naruszenia

Data i czas zaistnienia/rozpoczęcia naruszenia
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Kliknij tutaj, aby wprowadzić tekst.

☐ Trwające naruszenie
Zaznacz to pole, jeśli naruszenie trwa nadal w momencie zgłaszania.

Data i czas zakończenia naruszenia
(opcjonalnie)
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Kliknij tutaj, aby wprowadzić tekst.

C. Komentarz do czasu naruszenia (opcjonalnie)

Możesz podać więcej szczegółów dotyczących czasu naruszenia i uzasadnić dlaczego nie są znane dokładne terminy zaistnienia naruszenia.

Kliknij tutaj, aby wprowadzić tekst.

4. Charakter naruszenia

A. Charakter

☐ Naruszenie poufności danych

Nieuprawnione lub przypadkowe ujawnienie bądź udostępnienie danych

☐ Naruszenie integralności danych

Wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania

☐ Naruszenie dostępności danych

Brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez osobę do tego uprawnioną

B. Na czym polegało naruszenie?

☐ Zgubienie lub kradzież nośnika/urządzenia

☐ Dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji

☐ Korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy

☐ Nieuprawnione uzyskanie dostępu do informacji

☐ Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń

☐ Złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność danych

☐ Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing)

☐ Nieprawidłowa anonimizacja danych osobowych w dokumencie

☐ Nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora

☐ Niezamierzona publikacja

☐ Dane osobowe wysłane do niewłaściwego odbiorcy

☐ Ujawnienie danych niewłaściwej osoby

☐ Ustne ujawnienie danych osobowych

Opisz na czym polegało naruszenie.

Kliknij tutaj, aby wprowadzić tekst.

C. Dzieci

☐ Naruszenie dotyczy przetwarzania danych w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.

(opcjonalnie)

D. Przyczyna naruszenia

☐ Wewnętrzne działanie niezamierzone

☐ Wewnętrzne działanie zamierzone

☐ Zewnętrzne działanie niezamierzone

☐ Zewnętrzne działanie zamierzone

Inne przyczyny (w tym nieznane)

Kliknij tutaj, aby wprowadzić tekst.

4.1. Kategorie danych osobowych

UWAGA: W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.

A. Kategorie danych

Szczegółowy opis kategorii danych, których dotyczy naruszenie

Wymień jakie dane uległy naruszeniu: np. w przypadku sklepu internetowego profil użytkownika, w skład którego wchodzą: nazwa użytkownika, imię, nazwisko, hasło (zapisane otwartym tekstem lub hashowane), adres e-mail, oraz historia transakcji - kwota, data i nazwa kupionego produktu.

Kliknij tutaj, aby wprowadzić tekst.

B. Dane podstawowe

☐ Dane identyfikacyjne

np. imię, nazwisko, nr dowodu osobistego, adres IP

☐ Krajowy numer identyfikacyjny

np. PESEL, SSN

☐ Dane kontaktowe

np. e-mail, numer telefonu, adres korespondencyjny

☐ Dane ekonomiczne i finansowe

np. historie transakcji, faktury, dane o rachunkach bankowych, wnioski o wsparcie finansowe

☐ Oficjalne dokumenty

np. akty notarialne, dowody osobiste, prawa jazdy, karty pobytu, legitymacje

☐ Dane lokalizacyjne

np. GPS, dane o przemieszczaniu, miejsce zamieszkania

☐ Inne

Opisz poniżej kategorie danych:

Kliknij tutaj, aby wprowadzić tekst.

C. Dane szczególnej kategorii

☐ Dane o pochodzeniu rasowym lub etnicznym

☐ Dane o poglądach politycznych

☐ Dane o przekonaniach religijnych lub światopoglądowych

☐ Dane o przynależności do związków zawodowych

☐ Dane dotyczące seksualności lub orientacji seksualnej

☐ Dane dotyczące zdrowia

☐ Dane genetyczne

☐ Dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej

D. Dane, o których mowa w art. 10 RODO

☐ Dane dotyczące wyroków skazujących

☐ Dane dotyczące czynów zabronionych

☐ Inne

Opisz poniżej kategorie danych:

Kliknij tutaj, aby wprowadzić tekst.

E. Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie

Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie

Nie dotyczy to liczby osób. Jednej osobie można przypisać kilka wpisów (np. jednej osobie można przypisać kilka wykonanych transakcji)

Kliknij tutaj, aby wprowadzić tekst.

4.2. Kategorie osób

UWAGA: W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.

A. Kategorie osób, których dane dotyczą

☐ Pracownicy

☐ Użytkownicy

☐ Subskrybenci

☐ Studenci

☐ Uczniowie

☐ Służby mundurowe (np. wojsko, policja)

☐ Klienci (obecni i potencjalni)

☐ Klienci podmiotów publicznych

☐ Pacjenci

☐ Dzieci

☐ Osoby o szczególnych potrzebach (np. osoby starsze, niepełnosprawne itp.)

Szczegółowy opis kategorii osób, których dotyczy naruszenie.

Opisz np. kogo i w jakim przedziale czasowym dotyczy naruszenie

Kliknij tutaj, aby wprowadzić tekst.

B. Liczba osób, których mogło dotyczyć naruszenie

Przybliżona liczba osób, których mogło dotyczyć naruszenie: Kliknij tutaj, aby wprowadzić tekst.

5. Środki bezpieczeństwa zastosowane przed naruszeniem

A. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa stosowanych przez administratora przed naruszeniem (opcjonalnie)

Kliknij tutaj, aby wprowadzić tekst.

6. Możliwe konsekwencje

A. Uszczerbek fizyczny, majątkowy, niemajątkowy lub inne znaczące konsekwencje dla osoby, której dane dotyczą

- ☐ Utrata kontroli nad własnymi danymi osobowymi
- ☐ Ograniczenie możliwości realizowania praw z art. 15-22 RODO
- ☐ Ograniczenie możliwości realizowania praw
- ☐ Dyskryminacja
- ☐ Kradzież lub sfałszowanie tożsamości
- ☐ Strata finansowa
- ☐ Naruszenie dobrego imienia
- ☐ Utrata poufności danych osobowych chronionych tajemnicą zawodową
- ☐ Nieuprawnione odwrócenie pseudonimizacji
- ☐ Inne

Opisz poniżej inne skutki naruszenia prawa do ochrony danych osoby, której dane dotyczą:

Kliknij tutaj, aby wprowadzić tekst.

B. Ryzyko naruszenia praw i wolności osób fizycznych

- ○ Niskie
- ◉ Średnie
- ○ Wysokie

7. Środki zaradcze

A. Komunikacja z osobami, których dane dotyczą

Czy osoby, których dane dotyczą, zostały powiadomione o naruszeniu?

◉ Tak	○ Nie, ale zostaną powiadomione	○ Nie, nie zostaną powiadomione	○ Nie oceniłem jeszcze

Czy indywidualnie?

○ Tak

○ Nie, gdyż indywidualne powiadomienie każdej osoby, której dane dotyczą wymagałoby niewspółmiernie dużego wysiłku. W związku z tym został wydany publiczny komunikat lub zastosowano podobny środek, za pomocą którego osoby, których dane dotyczą, zostały poinformowane w równie skuteczny sposób.

Wskaż datę kiedy osoby, których dane dotyczą, zostały powiadomione o naruszeniu

Kliknij tutaj, aby wprowadzić datę.

Wskaż datę kiedy zamierzasz powiadomić osoby, których dane dotyczą, o naruszeniu

Kliknij tutaj, aby wprowadzić datę.

☐ Nie znam jeszcze daty kiedy zamierzam powiadomić osoby, których dane dotyczą

Liczba zawiadomionych osób, których dane dotyczą

Kliknij tutaj, aby wprowadzić tekst.

Środki komunikacji wykorzystane do zawiadomienia osoby, której dane dotyczą

Kliknij tutaj, aby wprowadzić tekst.

Treść zawiadomienia

Kliknij tutaj, aby wprowadzić tekst.

Powód niezawiadomienia osób, których dane dotyczą:

○ Przed naruszeniem wdrożono odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, anonimizacja czy pseudonimizacja uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych

○ Po naruszeniu zastosowano środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą.

Opis tych środków

Kliknij tutaj, aby wprowadzić tekst.

Jeśli jeszcze nie oceniłeś, czy zamierzasz zawiadomić podmioty danych, pamiętaj, że po podjęciu takiej decyzji będziesz musiał złożyć zgłoszenie uzupełniające.

B. Środki w celu zaradzenia naruszeniu ochrony danych osobowych

Opisz dodatkowe środki (poza poinformowaniem osób) zastosowane lub proponowane w celu zminimalizowania ewentualnych negatywnych skutków naruszenia i jego ponownego wystąpienia.

Kliknij tutaj, aby wprowadzić tekst.

C. Transgraniczne przetwarzanie i inne powiadomienia

Naruszenie zostało lub zostanie zgłoszone innemu organowi nadzorczemu UE (opcjonalnie)

☐ Austria	☐ Belgia	☐ Bułgaria	☐ Chorwacja
☐ Cypr	☐ Czechy	☐ Dania	☐ Estonia
☐ Finlandia	☐ Francja	☐ Grecja	☐ Hiszpania
☐ Holandia	☐ Irlandia	☐ Litwa	☐ Luksemburg
☐ Łotwa	☐ Malta	☐ Niemcy	☐ Portugalia
☐ Rumunia	☐ Słowacja	☐ Słowenia	☐ Szwecja
☐ Węgry	☐ Wielka Brytania	☐ Włochy	

Naruszenie zostało lub zostanie zgłoszone innemu organowi nadzorczemu spoza UE (opcjonalnie)

Wymień inne organy nadzorcze spoza UE, którym naruszenie zostało lub zostanie zgłoszone

Kliknij tutaj, aby wprowadzić tekst.

Naruszenie zostało lub zostanie zgłoszone innemu organowi nadzorczemu UE z powodu innych zobowiązań prawnych (opcjonalnie)

Np. obowiązek zgłoszenia incydentu wynikający z ustawy o krajowym systemie cyberbezpieczeństwa. Wymień inne organy, którym naruszenie zostało lub zostanie zgłoszone z powodu innych zobowiązań prawnych.

Kliknij tutaj, aby wprowadzić tekst.

Informacja:

Administrator danych osobowych.
Administratorem Państwa danych osobowych będzie Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO) z siedzibą w Warszawie, przy ul. Stawki 2.

Można się z nami kontaktować w następujący sposób:
a) listownie: ul. Stawki 2, 00-193 Warszawa
b) przez elektroniczną skrzynkę podawczą dostępną na stronie https://www.uodo.gov.pl/pl/p/kontakt
c) telefonicznie: (22) 531 03 00

Inspektor ochrony danych.
Możecie się Państwo kontaktować również z wyznaczonym przez Prezesa UODO inspektorem ochrony danych pod adresem email IOD@uodo.gov.pl

Cele i podstawy przetwarzania.
Będziemy przetwarzać Państwa dane osobowe zawarte w formularzu w celu przyjmowania zgłoszeń o naruszeniu ochrony danych osobowych zgodnie z art. 33 ust 1 , 3 i 4 RODO, podejmowania działań określonych w art. 34 ust. 4 oraz art. 58 ust. 2 RODO[1], a także prowadzenia przez organ wewnętrznego rejestru naruszeń na podstawie art. 57 ust. 1 lit. u RODO. Następnie Państwa dane będziemy przetwarzać w celu wypełnienia obowiązku archiwizacji dokumentów wynikającego z ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

Odbiorcy danych osobowych.
Odbiorcami Państwa danych osobowych będą Minister Cyfryzacji w związku z zamieszczeniem formularza wniosku na platformie E-PUAP oraz Wojewoda Podlaski w związku z korzystaniem przez Prezesa UODO z systemu elektronicznego zarządzania dokumentacją (EZD PUW).

Okres przechowywania danych.
Będziemy przechowywać Państwa dane przez czas realizacji uprawnień Prezesa UODO wskazanych w art. 34 ust. 4 i art. 58 ust. 2 RODO, a następnie - zgodnie z obowiązującą w Urzędzie Prezesa UODO Instrukcją kancelaryjną oraz przepisami o archiwizacji dokumentów - przez okres 10 lat od końca roku, w którym zgłoszono naruszenie ochrony danych, lub - w przypadku skierowania wystąpienia lub wydania decyzji administracyjnej – wieczyście.

Prawa osób, których dane dotyczą.
Zgodnie z RODO przysługuje Państwu:
a) prawo dostępu do swoich danych oraz otrzymania ich kopii;
b) prawo do sprostowania (poprawiania) swoich danych;
c) prawo do usunięcia danych osobowych, w sytuacji, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa lub w ramach sprawowania władzy publicznej;
d) prawo do ograniczenia przetwarzania danych;
e) prawo do wniesienia skargi do Prezesa UODO (na adres Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00 - 193 Warszawa)

Informacja o wymogu podania danych.
Podanie przez Państwa danych osobowych w niniejszym formularzu jest obowiązkiem wynikającym z art. 33 ust. 3 RODO oraz z art. 63 § 2-3a ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego.

---

[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 (RODO) oraz podjętych działań.

Załącznik nr 4 do zarządzenia nr 83/2018 Wójta Gminy Zbójno z dnia 10 grudnia 2018 r. w sprawie wprowadzenia dokumentacji przetwarzania danych osobowych w Urzędzie Gminy Zbójno.

Procedura zarządzania oprogramowaniem w Urzędzie Gminy Zbójno

Wstęp

Urząd Gminy Zbójno zna wagę legalnego i etycznego użytkowania oprogramowania. Ten dokument jest drogowskazem dla naszych pracowników jak upewnić się, że nasz urząd używa oprogramowanie zarówno legalnie jak i w sposób etyczny. Wszystkie zasoby oprogramowania są wykorzystywane w celach publicznych i niekomercyjnych i nie są używane przez pracowników we własnych celach.

Ilekroć w dalszej części procedury mowa jest o:

1) administratorze danych, należy przez to rozumieć Wójta Gminy Zbójno;
2) administratorze systemu, należy przez to rozumieć osobę zatrudnioną na stanowisku informatyka zarządzająca systemem informatycznym w Urzędzie Gminy Zbójno.

Rozdział I

Zasady użytkowania oprogramowania

Polityka ogólna

Urząd Gminy Zbójno posiada licencjonowane egzemplarze programów komputerowych różnych producentów oprogramowania. Licencjonowane i zarejestrowane egzemplarze programów zostały zainstalowane na komputerach oraz w sytuacji, gdzie jest to niezbędne i legalne - sporządzono odpowiednie kopie zapasowe oprogramowania zgodnie z warunkami umów licencyjnych. Bez pisemnej zgody producenta oprogramowania nie wolno wykonywać żadnych dodatkowych kopii programów ani też ich dokumentacji, chyba że pozwala na to licencja.

Oprogramowanie z innych źródeł

Urząd Gminy Zbójno dostarczy kopie legalnie nabytego oprogramowania, aby w sposób zgodny z prawem terminowo i w odpowiednich ilościach zapewnić oprogramowanie dla wszystkich komputerów. Używanie oprogramowania pochodzącego z jakiegokolwiek innego źródła może stanowić zagrożenie dla bezpieczeństwa Urzędu Gminy Zbójno oraz grozić może wszczęciem postępowania prawnego – używanie takiego oprogramowania jest ściśle zabronione.

Dodatkowe kopie

W niektórych przypadkach umowa licencyjna pozwala na sporządzenie dodatkowej kopii określonego programu, przeznaczonej do użytkowania na komputerze przenośnym lub komputerze domowym wykorzystywanym do celów służbowych. Pracownicy nie mogą wykonywać dodatkowych kopii oprogramowania lub dokumentacji bez zgody administratora systemu. Jeżeli takie działanie jest legalne, zezwolenie na te instalacje

będzie udzielane jedynie w przypadku, gdy to oprogramowanie jest niezbędne do wykonywania pracy.

Nieautoryzowane kopie

Nieautoryzowane kopiowanie chronionego prawem autorskim oprogramowania i dokumentacji jest sprzeczne z prawem i niezgodne z ustalonymi normami postępowania pracowników Urzędu Gminy Zbójno. Pracownicy wykonujący, kupujący lub używający nielegalnych kopii programów komputerowych lub dokumentacji podlegają natychmiastowemu postępowaniu dyscyplinarnemu, włącznie z natychmiastowym wypowiedzeniem umowy o pracę.

Wewnętrzna kontrola

Urząd Gminy Zbójno zastrzega sobie prawo do ochrony swojej reputacji i swoich inwestycji w programy komputerowe poprzez ustanowienie wewnętrznych mechanizmów kontroli zapobiegających wykonywaniu lub użytkowaniu nielegalnych kopii oprogramowania. Mechanizmy te obejmują częste, regularne kontrole sposobu wykorzystywania oprogramowania, zapowiedziane i niezapowiedziane przeglądy zawartości służbowych komputerów umożliwiające stwierdzenie zgodności zainstalowanego oprogramowania z umowami licencyjnymi, usuwanie wszelkich programów zainstalowanych na służbowych komputerach, dla których nie da się stwierdzić ważności licencji lub przedstawić jej dowodu, a także podjęcie postępowania dyscyplinarnego – łącznie ze zwolnieniem z pracy – w stosunku do pracowników naruszających postanowienia niniejszych zasad użytkowania oprogramowania.

Rozdział II
Procedury

Procedura 1 - centralizacja i zatwierdzanie zamówień na oprogramowanie.

1. Wszyscy pracownicy zapotrzebowanie na nowe oprogramowanie zgłaszają osobom odpowiedzialnym za zamówienia, którymi są:

1) wójt gminy;

2) sekretarz gminy;

2. Plany zakupowe zatwierdzane są przez wójta gminy lub sekretarza gminy.

3. Wyznaczony pracownik merytoryczny przygotowuje postępowanie o zamówienie publiczne zgodnie z ustawą prawo zamówień publicznych lub regulaminem wewnętrznym dotyczącym zakupów poniżej 30 000 euro.

Procedura 2 - spis wszystkich posiadanych licencji oraz zainstalowanego oprogramowania.

1. Osobą odpowiedzialną za pilnowanie, aby liczba zainstalowanego oprogramowania na stacjach roboczych i serwerach była zgodna z liczbą posiadanych licencji jest administrator systemu.

2. Obowiązki administratora systemu w zakresie zarządzania oprogramowaniem:

1) przynajmniej raz na 24 m-ce wykonać inwentaryzację oprogramowania we własnym zakresie lub zlecić to firmie do tego uprawnionej, z przeprowadzonej inwentaryzacji wykonać raport;

2) zainstalować nowe oprogramowanie na komputerach lub u użytkowników dla których było przewidziane i uaktualnić spis posiadanych licencji;

3) pilnować aby nowo zakupione oprogramowanie było zainstalowane i użytkowane zgodnie z zasadami jego licencjonowania;

4) jeżeli po wykonaniu inwentaryzacji okaże się, że brakuje licencji należy je bezzwłocznie uzupełnić lub odinstalować brakujące oprogramowanie.

Procedura 3 - przechowywanie oryginalnych dokumentów licencyjnych.

1. Wszystkie licencje i dokumenty licencyjne (karty rejestracyjne, nośniki, COA, EULA instrukcje, pudełka itp.) dla każdego używanego oprogramowania muszą znajdować się w szafie zamkniętej na klucz lub w zamkniętym sejfie i mają do nich dostęp tylko upoważnione osoby.

2. W teczkach poszczególnych komputerów znajdują się licencje oraz niezbędne dowody licencji OEM lub innej.

3. Dopuszcza się prowadzenie inwentaryzacji sprzętu i oprogramowania w wersji elektronicznej przy użyciu oprogramowania komputerowego.

4. Licencje gromadzi, przechowuje i je zabezpiecza w teczkach, o których mowa w pkt 2, administrator systemu.

Procedura 4 - instalowanie oprogramowania ściąganego z Internetu.

1. Ogólna zasada: instalowanie oprogramowania ściąganego z Internetu przez użytkowników jest zabronione.

2. Wyjątki: instalowanie oprogramowania ściąganego z Internetu przez użytkowników jest dozwolone pod warunkiem, że jest niezbędne do wykonywania pracy, będzie używane zgodnie z umową licencyjną i zostanie to sprawdzone przez administratora systemu i przez niego zaakceptowane, po uprzednim poinformowaniu o tym administratora danych.

Procedura 5 - używanie prywatnego oprogramowania w firmie.

1. Ogólna zasada: samowolne instalowanie oprogramowania prywatnego przez użytkowników jest zabronione.

2. Wyjątki: instalowanie prywatnego oprogramowania w urzędzie jest dozwolone pod warunkiem, że jest niezbędne do wykonywania pracy, będzie używane zgodnie z umową licencyjną i zostanie to sprawdzone przez administratora systemu i przez niego zaakceptowane, po uprzednim poinformowaniu o tym administratora danych.

Załącznik nr 5 do zarządzenia nr 83/2018 Wójta Gminy Zbójno z dnia 10 grudnia 2018 r. w sprawie wprowadzenia dokumentacji przetwarzania danych osobowych w Urzędzie Gminy Zbójno.

Procedura privacy by design i privacy by default w Urzędzie Gminy Zbójno

1. Zasada privacy by design.

Zasada privacy by design to zasada uwzględniania ochrony danych osobowych w fazie projektowania. Uregulowana zastała w art. 25 ust. 1 RODO.[1]

Uwzględniając:

1) stan wiedzy technicznej;
2) koszt wdrażania;
3) charakter, zakres, kontekst i cele przetwarzania danych;
4) ryzyko naruszenia praw lub wolności osób fizycznych (o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia) wynikające z przetwarzania

- administrator danych (zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania) wdraża odpowiednie środki techniczne i organizacyjne (takie jak pseudonimizacja), zaprojektowane w celu:

1) skutecznej realizacji zasad ochrony danych osobowych;
2) nadania przetwarzaniu niezbędnych zabezpieczeń

- tak, by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą.

2. Zasada privacy by default.

Zasada privacy by default uregulowana została w art. 25 ust. 2 RODO.

Administrator danych wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania.

Obowiązek ten odnosi się do:

1) ilości zbieranych danych osobowych;
2) zakresu ich przetwarzania;
3) okresu ich przechowywania;
4) ich dostępności.

W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

3. Administrator danych stosuje ochronę prywatności przy prowadzeniu wszelkich projektów i działań, tak w sferze publicznej, jak i prywatnej.

4. W Urzędzie Gminy Zbójno stosuje się:

[1] 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.

1) podejście proaktywne, niereaktywne i zaradcze, nie naprawcze;
2) prywatność jako ustawienie domyślne (privacy by default);
3) prywatność włączoną w projekt;
4) pełną funkcjonalność rozumianą jako osiąganie sumy dodatniej, a nie sumy zerowej;
5) ochronę prywatności od początku do końca cyklu życia informacji;
6) transparentność i przejrzystość oraz poszanowanie dla prywatności użytkowników.

5. Administrator danych przed rozpoczęciem przetwarzania danych osobowych wdraża odpowiednie środki techniczne oraz organizacyjne zapewniające ochronę danych osób fizycznych.

6. W Urzędzie Gminy Zbójno stosuje się środki techniczne i organizacyjne takie jak:
1) psuedonimizacja - oznacza przetworzenie danych osobowych w taki sposób, aby 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;
2) minimalizacja (minimising) – strategia polegająca na tym, że ilość zbieranych danych jest ograniczona do niezbędnego minimum;
3) ukrywanie (hiding) – dane, a także zależności między nimi, nie są „na widoku" dla osób mających dostęp do danych (należy poczynić dodatkowe działania w celu uzyskania dostępu);
4) separowanie (separating) – przetwarzanie danych odbywa się w stosunku do danych rozdzielonych, rozproszonych w poszczególnych zbiorach;
5) agregowanie (aggregating) – dane są przetwarzane w możliwie najwyższym stopniu zagregowania i z możliwie jak najmniejszą liczbą szczegółów (przy jakiej są nadal użyteczne);

7. Przetwarza się wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania.

8. Obowiązkiem administratora danych jest zadbanie o jak najlepszą ochronę danych osobowych w fazie projektowania (privacy by design).

9. Podstawowym celem powyższej zasady jest ,,wbudowanie,, zasad ochrony prywatności w taki sposób, aby od samego początku jego istnienia ochrona prywatności stanowiła jego część składową.

10. Mając na uwadze powyższą zasadę uwzględniając nowy projekt, nową usługę, w którym występuje przetwarzanie danych należy wdrożyć odpowiednie środki techniczne takie jak szyfrowanie danych oraz pseudonimizacja danych jak również minimalizację zbieranych danych.

11. Uwzględnia się ocenę skutków przetwarzania w każdym nowym projekcie.

12. Na etapie wdrażania nowego projektu, nowego procesu przetwarzania danych należy uwzględnić obecność inspektora ochrony danych na każdym etapie tworzenia projektu, procesu.

13. Ustawienie prywatności w każdej usłudze, każdym produkcie będą nakierowane na maksymalną ochronę użytkownika zgodnie z zasadą ,,privacy by default" (domyślna ochrona danych). Oznacza to zapewnienie ustawień zapewniających ochronę danych jako pierwotnych ustawień systemu informatycznego czy oprogramowania.

14. Powyższa zasada zakłada ochronę prywatności, jako domyślne ustawienie każdego programu (systemu), usługi, a zmiana takiego ustawienia powinna następować jedynie na wyraźne żądanie użytkownika programu, usługi. Użytkownicy, którzy chcą zrezygnować z części swojej prywatności powinni podjąć aktywne działania w tym kierunku, a nie być poddanymi ingerującym w ich prywatność decyzjom twórców systemu, usługi.

Załącznik nr 6 do zarządzenia nr 83/2018 Wójta Gminy Zbójno z dnia 10 grudnia 2018 r. w sprawie wprowadzenia dokumentacji przetwarzania danych osobowych w Urzędzie Gminy Zbójno.

Regulamin użytkowania komputerów przenośnych Urzędu Gminy Zbójno

1. Pracownicy upoważnieni do przetwarzania danych osobowych i pracujący na komputerach przenośnych muszą zapoznać się z Regulaminem użytkowania komputera przenośnego oraz pisemnego zobowiązania się do jego przestrzegania.

2. Dane osobowe lub danych poufne muszą zostać zaszyfrowane na dysku i zabezpieczone co najmniej 8-znakowym hasłem (duże, małe litery i cyfry).

3. Komputery przenośne są wykorzystywane do prac służbowych. W przypadku konieczności korzystania z komputera przenośnego w innym celu wszystkie dane osobowe muszą być zabezpieczone hasłem.

4. W przypadku kradzieży/zgubienia lub naruszenia ochrony danych osobowych osoba upoważniona zobowiązana jest zgłosić zdarzenie/problem inspektorowi ochrony danych.

5. Osoba upoważniona zobowiązana jest do zabezpieczenia komputera przenośnego w czasie transportu, a przede wszystkim:

1) zaleca się przenoszenie komputera przenośnego w przeznaczonej do tego teczce lub aktówce;

2) zabrania się pozostawiania komputera przenośnego w samochodzie podczas nieobecności osoby upoważnionej.

6. Gdy komputer przenośny jest pozostawiony w miejscu dostępnym dla osób nieupoważnionych, konieczne jest zabezpieczenie hasłem. Dotyczy to przede wszystkim zabezpieczenia komputera przenośnego na stanowisku pracy, podczas przedstawiania prezentacji, szkolenia.

7. Użytkownik komputera przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze. Nośniki z takimi kopiami powinny być przechowywane w miejscu zabezpieczonym przed dostępem osób nieupoważnionych.

8. Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, osoba upoważniona zobowiązana jest do chronienia wyświetlanych danych osobowych na monitorze przed wglądem osób nieupoważnionych.

Zapoznałam/em się z treścią regulaminu użytkowania komputerów przenośnych Urzędu Gminy Zbójno i zobowiązuje się do przestrzegania zasad w nim zawartych.

.....

(Podpis użytkownika)