WÓJT GMINY
PARCHOWO
woj. pomorskie

ZARZĄDZENIE Nr 10.2017
WÓJTA GMINY PARCHOWO
z dnia 27 stycznia 2017 r.

w sprawie ochrony danych osobowych w Urzędzie Gminy Parchowo

Na podstawie art. 36 ust. 1 i ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2016 r. poz. 922) i § 3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) oraz art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t. j. Dz. U. z 2016 r. poz. 446 ze zm.) zarządza się, co następuje:

§ 1. W Urzędzie Gminy Parchowo wprowadza się:
1) politykę bezpieczeństwa, stanowiącą załącznik nr 1 do zarządzenia;
2) instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, stanowiącą załącznik nr 2 do zarządzenia.

§ 2. Zobowiązuje się wszystkich pracowników Urzędu Gminy Parchowo do zapoznania się z niniejszym zarządzeniem i załącznikami do zarządzenia oraz do przestrzegania zasad zawartych w tych dokumentach. Oświadczenie o zapoznaniu się należy wpiąć do akt osobowych pracowników Urzędu Gminy Parchowo.

§ 3. Nadzór nad wykonaniem zarządzenia powierza się Sekretarzowi Gminy Parchowo.

§ 4. Traci moc zarządzenie Wójta Gminy Parchowo Nr 7/2009 z dnia 03 lutego 2009 r. w sprawie ochrony danych osobowych w Urzędzie Gminy Parchowo

§ 5. Zarządzenie wchodzi w życie od 1 lutego 2017 r.

WÓJT
Andrzej Dołębski

Karol Chabowski
ADWOKAT

Załącznik Nr 1 do zarządzenia Nr 10.2017
Wójta Gminy Parchowo
z dnia 27 stycznia 2017 r.

POLITYKA BEZPIECZEŃSTWA W URZĘDZIE GMINY PARCHOWO

Rozdział I
Postanowienia ogólne, definicje

§ 1.

1. Polityka Bezpieczeństwa w Urzędzie Gminy Parchowo jest zbiorem zasad i procedur obowiązujących przy przetwarzaniu i wykorzystywaniu danych osobowych we wszystkich zbiorach danych osobowych administrowanych przez Urząd Gminy Parchowo.
2. Podstawą do opracowania i wdrożenia dokumentu są:
   1) ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2016 r. poz. 922);
   2) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. Nr 100, poz. 1024).
3. Przetwarzanie danych osobowych w Urzędzie Gminy Parchowo jest dopuszczalne wyłącznie pod warunkiem przestrzegania ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych i wydanych na jej podstawie przepisów wykonawczych w tym niniejszej polityki i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, które powinny być spójne z polityką bezpieczeństwa informacji wymaganą przez ustawę o informatyzacji działalności podmiotów realizujących zadania publiczne.
4. Polityka Bezpieczeństwa ma zastosowanie do ochrony zbiorów danych osobowych przetwarzanych w Urzędzie Gminy Parchowo, w celu ich bezpiecznego wykorzystania oraz określa zasady korzystania z systemów informatycznych.

§ 2.

Określenia i skróty użyte w Polityce Bezpieczeństwa Informacji oznaczają:

1) OchrDanychU – ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz.U. z 2016 poz. 922);
2) Rozporządzenie – rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024);
3) Urząd – Urząd Gminy Parchowo;
4) Administrator Danych Osobowych – Wójta Gminy Parchowo, zwanego dalej „ADO";
5) Administrator Bezpieczeństwa Informacji – osobę powołaną przez Wójta Gminy Parchowo, wpisaną do prowadzonego przez Generalnego Inspektora Ochrony Danych Osobowych rejestru administratorów bezpieczeństwa informacji, zwaną dalej „ABI";

6) Administrator Systemów Informatycznych – osobę wyznaczoną przez Wójta Gminy Parchowo, zwaną dalej „ASI";
7) osoba upoważniona lub użytkownik systemu – osobę posiadającą upoważnienie wydane przez ADO lub uprawnioną przez niego osobę i dopuszczoną jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu, zwaną dalej „użytkownikiem";
8) osoby zatrudnione przy przetwarzaniu danych osobowych – wszystkie osoby, w tym użytkowników systemu informatycznego, mające dostęp do danych osobowych.

Rozdział II
Obszary przetwarzania danych osobowych

§ 3.

1. Obszar przetwarzania danych osobowych w Urzędzie obejmuje budynek, pomieszczenia i części pomieszczeń, w których przetwarzane są dane osobowe (miejsca, w których wykonuje się operacje na danych osobowych, tj. wpisuje, zmienia, kopiuje) oraz miejsca, gdzie przechowuje się nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające elektroniczne nośniki informacji, pomieszczenia, w których składowane są uszkodzone nośniki danych).
2. Obszar przetwarzania danych osobowych określony jest w „Wykazie pomieszczeń, w których przetwarzane są dane osobowe", stanowiącym załącznik nr 1 do Polityki Bezpieczeństwa Informacji. Wykaz ten zawiera następujące informacje:
   1) lokalizację budynku,
   2) numer pomieszczenia i jego przeznaczenie,
   3) wskazanie piętra budynku,
   4) określenie referatu użytkującego dane pomieszczenie,
   5) wskazanie liczby osób pracujących w pomieszczeniu: wskazanie stanowisk i liczby osób,
   6) określenie zabezpieczenia pomieszczenia.
3. Obszar przetwarzania danych oraz warunki ochrony tego obszaru określone zostały w załączniku nr 2 do Polityki Bezpieczeństwa Informacji „Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe".
4. Osoby odpowiedzialne na podstawie pracowniczych zakresów czynności za funkcjonowanie podległych sobie zbiorów danych mają obowiązek zgłoszenia zamiaru przetwarzania danych osobowych w nowoutworzonym zbiorze danych w formie wniosku do ABI. Wzór wniosku stanowi załącznik nr 14 do polityki bezpieczeństwa. ABI po otrzymaniu ww. wniosku odnotowuje w załączniku nr 3 do polityki bezpieczeństwa informacji nowoutworzony zbiór danych osobowych. ABI ocenia konieczność rejestracji zbioru danych w rejestrze publicznym GIODO i dokonuje jego rejestracji lub odnotowania w rejestrze zbiorów danych prowadzonych przez ABI.
5. Analogicznie osoby odpowiedzialne na podstawie pracowniczych zakresów czynności za funkcjonowanie podległych sobie zbiorów danych mają obowiązek zgłoszenia zaprzestania przetwarzania danych osobowych w istniejącym zbiorze danych w formie wniosku do ABI. Wzór wniosku stanowi załącznik nr 14 do polityki bezpieczeństwa. ASI po otrzymaniu ww. wniosku wykreśla z załącznika nr 3 do polityki bezpieczeństwa informacji zbiór danych osobowych, w którym zaprzestano przetwarzania danych osobowych. ABI ocenia konieczność wyrejestrowania zbioru danych w rejestrze publicznym GIODO i dokonuje jego wyrejestrowania lub wykreśla z rejestru zbiorów danych prowadzonych przez ABI.

§ 4.

1. Wykaz zbiorów danych przetwarzanych w Urzędzie określony został w załączniku nr 3 do Polityki Bezpieczeństwa Informacji – „Wykaz zasobów danych osobowych i systemów ich przetwarzania". Wykaz ten zawiera następujące informacje:
   1) nazwę zbioru danych,
   2) określenie systemu przetwarzania danych osobowych,
   3) lokalizację miejsca przetwarzania danych osobowych,
   4) stosowane przy przetwarzaniu danych osobowych oprogramowanie,
   5) precyzyjny zakres danych osobowych w systemie (pola i relacje pomiędzy nimi),
   6) określenie pól informacyjnych w systemie,
   7) określenie sposobu przepływu danych pomiędzy systemami,
   8) wskazanie możliwość wydruku zakresu przetwarzania danych osobowych.
2. Szczegółowe informacje dotyczące stosowanego sprzętu oraz oprogramowania danego systemu informatycznego są zawarte w instrukcjach zarządzania danym systemem. Działające systemy to programy ujęte w załączniku Nr 15 do Polityki Bezpieczeństwa Informacji pod nazwą "Ewidencja Oprogramowania". Ewidencja ma charakter przyrostowy i prowadzona jest przez ASI w formie pliku EXCEL oraz aktualnego wydruku przechowywanego wraz z niniejszą polityką.

§ 5.

Przetwarzanie danych osobowych odbywa się na serwerze i na stacjach roboczych użytkowników.

§ 6.

1. W ramach procesów przetwarzania danych ma miejsce przepływ danych pomiędzy różnymi systemami informatycznymi. Informacje na temat przepływu danych pomiędzy różnymi systemami informatycznymi znajdują się w „Wykazie zasobów danych osobowych i systemów ich przetwarzania, o którym mowa w § 4 ust. 1".
2. Szczegółowe informacje dotyczące przepływu danych osobowych pomiędzy danymi systemami informatycznymi znajdują się w instrukcjach zarządzania danym systemem.

§ 7.

W systemie informatycznym obowiązują zabezpieczenia na poziomie podstawowym. Szczegółowe omówienie środków zabezpieczenia technicznego i organizacyjnego znajduje się w „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy w Parchowie", stanowiącej załącznik nr 2 do Zarządzenia Wójta Gminy Parchowo z dnia 27 stycznia 2017 r.

Rozdział III
Zarządzanie przetwarzaniem danych osobowych oraz czuwanie nad ich bezpieczeństwem

§ 8.

1. ADO powołuje zarządzającego oprogramowaniem, który przeprowadza okresową inwentaryzację oprogramowania oraz ustanawia zasady i procedury ciągłego utrzymania oprogramowania.
2. ADO powołuje Administratora Systemów Informatycznych (ASI).

§ 9.

W celu realizacji powierzonych zadań ABI w Urzędzie ma prawo:

1) kontrolować komórki organizacyjne Urzędu w zakresie właściwego zabezpieczenia systemów informatycznych oraz pomieszczeń, w których przetwarzane są dane osobowe;
2) wydawać polecenia kierownikom komórek organizacyjnych Urzędu w zakresie bezpieczeństwa danych osobowych;
3) informować ADO o przypadkach naruszenia bezpieczeństwa danych osobowych;
4) żądać od wszystkich pracowników Urzędu wyjaśnień w sytuacjach naruszenia bezpieczeństwa danych osobowych.

§ 10.

1. Wójt Gminy Parchowo wyznacza właścicieli zasobów danych osobowych.
2. Rolę właścicieli zasobów danych osobowych pełnią kierownicy referatów odpowiedzialni za dany zasób danych osobowych.
3. Do obowiązków właścicieli zasobów danych osobowych należy w szczególności:
   1) zarządzanie zasobem danych osobowych w ramach zadań realizowanych przez kierowane referaty;
   2) występowanie z wnioskiem do ADO o nadanie upoważnień dotyczących dostępu do zasobu danych osobowych podległym pracownikom zgodnie z załącznikiem nr 13 do polityki bezpieczeństwa informacji;
   3) zgłaszanie do ABI zamiaru utworzenia zbioru danych osobowych oraz informacji dotyczących zmian w zakresie i sposobach przetwarzania tego zbioru;
   4) udostępnianie danych osobowych innemu podmiotowi lub osobie, której dane dotyczą;
   5) przestrzeganie obowiązków dotyczących obszaru przetwarzania, wykazu osób upoważnionych do przetwarzania danych osobowych, zastosowania zabezpieczeń zbiorów;
   6) prowadzenie ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w kierowanym referacie, z uwzględnieniem zakresu odpowiedzialności za ochronę tych danych w stopniu odpowiednim do zadań wykonywanych przez te osoby przy przetwarzaniu danych osobowych i przekazywanie ABI aktualnej ewidencji tych osób wraz z priorytetami im przydzielonymi;
   7) zapoznawanie pracowników mających dostęp do danych osobowych z przepisami dotyczącymi ochrony danych osobowych.

§ 11.

1. Administrator Systemu Informatycznego odpowiada za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych Urzędu.
2. Do obowiązków ASI w zakresie ochrony danych osobowych należy w szczególności:
   1) zapewnienie bezawaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych osobowych w Urzędzie;
   2) nadzór nad naprawami, konserwacją i likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;
   3) nadzór nad przeglądami, konserwacją, uaktualnianiem systemów służących do przetwarzania danych osobowych;
   4) podejmowanie natychmiastowych działań zabezpieczających stan systemu informatycznego w Urzędzie w przypadku otrzymania informacji o naruszeniu zabezpieczeń informatycznych;
   5) nadzór nad przesyłaniem danych osobowych drogą teletransmisji;

6) nadzór nad przestrzeganiem zasad bezpieczeństwa w przypadku udostępniania danych osobowych innym podmiotom drogą teletransmisji danych;
7) przeciwdziałanie dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe;
8) podejmowanie działań w przypadku naruszeń w systemie zabezpieczeń;
9) nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych;
10) podejmowanie działań w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego.

Rozdział IV
Gromadzenie danych osobowych

§ 12.

Dane osobowe przetwarzane w Urzędzie mogą być uzyskiwane bezpośrednio od osób, których te dane dotyczą lub z innych źródeł, w granicach dozwolonych przepisami prawa.

§ 13.

1. Zebrane dane osobowe mogą być wykorzystane wyłącznie do celów dla jakich były, są lub będą zbierane i przetwarzane. Po wykorzystaniu dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą.
2. W przypadku konieczności udostępnienia dokumentów i danych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych osobowych.

§ 14.

Jeżeli dane osobowe są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem OchrDanychU albo są zbędne do realizacji celu, dla którego zostały zebrane, ADO jest zobowiązany do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

Rozdział V
Przetwarzanie danych osobowych

§ 15.

1. Właściciel zasobów danych osobowych obowiązany jest zgłaszać ABI zamiar utworzenia nowego zbioru danych osobowych.
2. ABI przygotowuje projekt zgłoszenia zbioru danych osobowych do rejestracji GIODO, jeżeli takie zgłoszenie jest ustawowo wymagane, na podstawie obowiązującego wzoru zgłoszenia.
3. ASI, w uzgodnieniu z ABI, określa warunki techniczne dotyczące zabezpieczeń w systemie informatycznym, o których mowa w części E i F zgłoszenia zbioru danych osobowych do rejestracji GIODO.
4. ABI sprawdza warunki techniczne dotyczące zabezpieczeń w systemie informatycznym opisane w części E i F zgłoszenia zbioru danych osobowych do rejestracji GIODO; w przypadku niewystarczającego poziomu zabezpieczeń występuje z wnioskiem do ASI o podniesienie poziomu zabezpieczeń.
5. Przygotowany przez ABI projekt zgłoszenia zbioru danych osobowych do rejestracji GIODO parafują właściciel zasobów danych osobowych oraz ASI.
6. Parafowany wniosek ABI przedstawia do akceptacji Sekretarza Gminy.

7. Sekretarz Gminy przedkłada wniosek o rejestrację zbioru danych osobowych ADO i zgłasza go do GIODO.
8. Właściciel zasobów danych osobowych zgłasza – w terminie 5 dni – zmiany dotyczące przetwarzania danych w zarejestrowanym zbiorze danych osobowych do ABI.
9. ASI zgłasza – w terminie 5 dni – zmiany dotyczące sposobu przetwarzania danych osobowych oraz ich zabezpieczeń w systemie informatycznym.
10. ABI przygotowuje aktualizację zgłoszenia zbioru danych osobowych do GIODO w terminie 30 dni od dnia dokonania zmiany w zbiorze, na podstawie obowiązującego wzoru. Przepisy ust. 2 – 7 stosuje się odpowiednio.

Rozdział VI
Obowiązek informacyjny

§ 16.

1. Kierownicy komórek organizacyjnych Urzędu, w których są zbieranie i przetwarzane dane osobowe, są odpowiedzialni za poinformowanie osób, których dane osobowe przetwarzają, o:
   1) adresie siedziby urzędu, pod którym dane są zbierane i przetwarzane;
   2) celu zbierania danych;
   3) dobrowolności lub obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej;
   4) prawie wglądu do treści swoich danych oraz możliwości ich poprawiania.
2. W przypadku zbierania danych osobowych nie bezpośrednio od osoby, której one dotyczą, osobę tę należy dodatkowo poinformować o źródle danych oraz o uprawnieniach wynikających z art. 32 ust. 1 pkt 7 i 8 OchrDanychU.
3. Wzór formularza stosowanego dla spełnienia obowiązków, o których mowa w ust. 1 i ust. 2, stanowi załącznik nr 4 do Polityki Bezpieczeństwa.

§ 17.

1. Materiały dotyczące innej niż ustawowa działalności Urzędu mogą być wysyłane tylko do tych osób, które wcześniej wyraziły zgodę na piśmie na przetwarzanie ich danych osobowych w tym celu.
2. Kandydaci do pracy w Urzędzie w procesie rekrutacji są zobowiązani podpisać pisemną zgodę na przetwarzanie ich danych osobowych.
3. Dokumenty złożone w celu określonym w ust. 2 są przechowywane w komórce organizacyjnej, która przetwarza te dane i są włączane do akt osobowych pracownika.
4. Wzór formularza stosowanego dla spełnienia obowiązków wymienionych w ust. 2, stanowi załącznik 5 do Polityki Bezpieczeństwa Informacji.

Rozdział VII
Udostępnianie danych osobowych

§ 18.

1. ADO udostępnia dane osobowe przetwarzane we własnych zbiorach tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
2. Dane osobowe mogą być udostępniane w następujących przypadkach:
   1) na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów;
   2) na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych;
   3) na podstawie wniosku osoby, której dane dotyczą.
3. Wniosek o udostępnienie danych osobowych powinien zawierać informacje umożliwiające

wyszukanie żądanych danych osobowych w zbiorze oraz wskazywać ich zakres i przeznaczenie. Wzór wniosku stanowi załącznik nr 6 do Polityki Bezpieczeństwa.

4. Udostępniając dane osobowe, należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
5. W przypadku żądania udzielenia informacji na temat przetwarzanych danych osobowych na pisemny wniosek pochodzący od osoby, której dane dotyczą, odpowiedź na wniosek następuje w terminie 30 dni od daty jego otrzymania.
6. Wniosek o udostępnienie przekazywany jest do właściciela zasobów danych osobowych, który podejmuje decyzję o udostępnieniu, i informuje o tym ABI.
7. ABI akceptuje decyzję o udostępnieniu i przekazuje ją do właściciela zasobów danych osobowych.
8. Właściciel zasobów danych osobowych jest odpowiedzialny za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku.

§ 19.

Odmowa udostępnienia danych osobowych następuje wówczas, gdy spowodowałoby to istotne naruszenia dóbr osobistych osób, których dane dotyczą, lub innych osób oraz jeżeli dane osobowe nie mają istotnego związku ze wskazanymi we wniosku motywami działania wnioskodawcy.

Rozdział VIII
Ochrona przetwarzania danych osobowych

§ 20.

1. Do przetwarzania danych mogą być dopuszczeni pracownicy Urzędu posiadający upoważnienie nadane przez ADO. Wzór upoważnienia określa załącznik nr 7 do Polityki Bezpieczeństwa.
2. Upoważnienie do przetwarzania danych osobowych wydawane jest w dwóch egzemplarzach. Jeden egzemplarz przechowywany jest w aktach personalnych pracownika a drugi w dokumentacji prowadzonej przez ABI.
2. ABI prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych. Wzór ewidencji stanowi załącznik nr 8 do Polityki Bezpieczeństwa.

§ 21.

ADO zobowiązany jest do zbierania, ewidencjonowania i przechowywania:

1) oświadczeń osób przetwarzających dane osobowe o zachowaniu w tajemnicy danych, z którymi mają styczność, oraz środkach bezpieczeństwa stosowanych przy przetwarzaniu danych osobowych; wzór formularza oświadczenia stanowi załącznik nr 10 do Polityki Bezpieczeństwa;
2) oświadczeń osób zatrudnianych na podstawie umowy zlecenia, umowy o dzieło lub innej umowy cywilnej o zachowaniu tajemnicy; wzór formularza oświadczenia stanowi załącznik nr 9 do Polityki Bezpieczeństwa;
3) porozumień zawartych z osobami zatrudnionymi przy przetwarzaniu danych osobowych w zakresie wykorzystania oddanego im do dyspozycji sprzętu informatycznego, oprogramowania oraz zasobów sieci informatycznej; wzór formularza porozumienia stanowi załącznik nr 9 do Polityki Bezpieczeństwa.

§ 22.

1. Powierzenie przetwarzania danych osobowych odbywa się zgodnie z art. 31 OchrDanychU na podstawie umowy zawartej na piśmie pomiędzy ADO a danym podmiotem, któremu zleca się czynności związane z przetwarzaniem danych osobowych.

2. Właściciel zasobów danych osobowych informuje ABI o zamiarze powierzenia danych osobowych do przetwarzania.
3. ABI przygotowuje projekt umowy powierzenia danych osobowych innemu podmiotowi.
4. W projekcie umowy należy wyspecyfikować zakres czynności związanych z przetwarzaniem powierzonych danych osobowych, zakres danych oraz wymagania dotyczące ochrony danych.
5. Każda osoba delegowana do wykonywania zadań na rzecz Urzędu, związanych z powierzeniem przetwarzania danych osobowych, obowiązana jest podpisać oświadczenie o zachowaniu w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia.
6. Projekt umowy parafują:
   1) ABI,
   2) właściciel zasobów danych osobowych,
   3) ASI – jeżeli zlecenie czynności dotyczyć będzie przetwarzania danych w systemie informatycznym,
   4) radca prawny.
7. Zaparafowany projekt umowy jest przedkładany przez ABI do akceptacji i podpisu ADO. Wzór umowy powierzenia przetwarzania danych osobowych stanowi załącznik nr 11 do Polityki Bezpieczeństwa Informacji.

§ 23.

1. Podmiot przetwarzający dane osobowe jest zobowiązany do zastosowania środków organizacyjnych i technicznych, zabezpieczających zbiór przed dostępem osób nieupoważnionych na zasadach określonych w przepisach o ochronie danych osobowych.
2. Podmiot, o którym mowa w ust. 1, jest zobowiązany przetwarzać dane osobowe wyłącznie w zakresie określonym w umowie.
3. Podmiot przetwarzający dane osobowe ponosi odpowiedzialność za ochronę przetwarzanych danych osobowych.

Rozdział IX
Postępowanie w przypadkach naruszenia bezpieczeństwa ochrony danych osobowych

§ 24.

Przepisy niniejszego rozdziału stosuje się w przypadku:
1) stwierdzenia naruszenia zabezpieczenia systemu informatycznego w obszarze danych osobowych;
2) podejrzenia naruszenia bezpieczeństwa danych osobowych ze względu na stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci komputerowej.

§ 25.

Zasady postępowania przypadku naruszenia bezpieczeństwa danych osobowych obowiązują wszystkie osoby biorące udział w procesie przetwarzania danych osobowych.

§ 26.

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

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

§ 27.

1. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie powiadomić o tym fakcie bezpośredniego przełożonego lub ABI (ewentualnie osobę przez niego upoważnioną), a następnie postępować stosownie do podjętej przez niego decyzji.
2. Zgłoszenie naruszenia ochrony danych osobowych powinno zawierać:
   1) opisanie działania wskazującego na naruszenie ochrony danych osobowych;
   2) określenie sytuacji i czasu, w jakim stwierdzono naruszenie ochrony danych osobowych;
   3) wskazanie istotnych informacji mogących wskazywać na przyczynę naruszenia;
   4) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

§ 28.

1. Administrator Bezpieczeństwa Informacji podejmuje działania mające na celu:
   1) minimalizację negatywnych skutków zdarzenia;
   2) wyjaśnienie okoliczności zdarzenia;
   3) zabezpieczenie dowodów zdarzenia,
   4) umożliwienie dalszego bezpiecznego przetwarzania danych.
2. Dla realizacji celów określonych w ust. 1 ABI ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, w szczególności:
   1) żądania wyjaśnień od pracowników;
   2) korzystania z pomocy konsultantów;
   3) nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.

§ 29.

Odmowa udzielenia wyjaśnień lub współpracy z ABI traktowana będzie jako naruszenie obowiązków pracowniczych.

§ 30.

ABI po opanowaniu sytuacji nadzwyczajnej opracowuje raport końcowy, w którym przedstawia przyczyny i skutki zdarzenia oraz wnioski, w tym kadrowe, ograniczające możliwość wystąpienia zdarzenia w przyszłości; wzór raportu końcowego stanowi załącznik nr 12 do Polityki Bezpieczeństwa Informacji.

Załącznik nr 1 do Polityki Bezpieczeństwa

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

Wykaz pomieszczeń Urzędu Gminy w Parchowie, w których przetwarzane są dane osobowe

	Lokalizacja Adres i numer budynku	Numer i przeznaczenie pomieszczenia*	Piętro	Nazwa referatu użytkującego pomieszczenie	Osoby pracujące w pomieszczeniu**	Zabezpieczenie pomieszczenia***
1.	2.	3.	4.	5.	6.	7.

*Należy podać numer pomieszczenia i jego przeznaczenie np. pokój biurowy, archiwum, kancelaria, serwerownia, biuro przepustek.
** Należy podać same stanowiska i liczbę osób bez imion i nazwisk.
*** Należy podać sposób zabezpieczenia pomieszczenia np. drzwi zamykane na klucz, kraty w oknach, pomieszczenie monitorowane, kontrola dostępu itp.

Załącznik nr 2 do Polityki Bezpieczeństwa

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

Zasady ochrony pomieszczeń, w których przetwarzane są dane osobowe

§ 1. Ochrona pomieszczeń

1. Sekretarz Gminy oraz kierownicy referatów Urzędu Gminy w Parchowie odpowiadają za należyte zabezpieczenie fizyczne zasobów danych osobowych w podległych komórkach.
2. ABI zobowiązany jest przeprowadzać bezpośrednią kontrolę stanu zabezpieczeń fizycznych zbiorów danych osobowych oraz zgłaszać Sekretarzowi Gminy uwagi lub propozycje kontroli.
3. Obszarem, w którym przetwarzane są dane osobowe, jest siedziba Urzędu Gminy w Parchowie, ul. Krótka 2, 77-124 Parchowo
4. ABI jest odpowiedzialny za prowadzenie i uaktualnianie wykazu pomieszczeń, w których przetwarzane są dane osobowe.
5. Przebywanie osób nieuprawnionych do dostępu do danych osobowych w pomieszczeniach, o których mowa w pkt 4, jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych lub za zgodą właściciela zasobów danych osobowych.
6. Osoby upoważnione do przetwarzania danych osobowych zobowiązane są do przestrzegania zasad dotyczących wprowadzania osób trzecich do obszaru przetwarzania danych osobowych, o którym mowa w ust. 3. Ruch osób z zewnątrz w wymienionym obszarze powinien odbywać się pod kontrolą osób upoważnionych.
7. Sekretarz Gminy może zezwolić na przebywanie w pomieszczeniach, o których mowa w pkt 4, osobom sprzątającym te pomieszczenia poza godzinami pracy Urzędu bez konieczności obecności osoby dopuszczonej do przetwarzania danych. Osoby sprzątające podpisują oświadczenie o zachowaniu poufności.
8. Budynki lub pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane na czas nieobecności w nich osób upoważnionych do przetwarzania danych osobowych, w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.
9. Pomieszczenia, w których przetwarzane są dane osobowe wrażliwe, oraz pomieszczenia serwerowni i archiwów powinny podlegać ochronie poprzez zastosowanie:

1) systemu kontroli dostępu,

2) wzmocnienia drzwi i okien,

3) systemu sygnalizacji alarmu i włamania.

10. Właściciel zasobów danych osobowych zabezpiecza obszar przetwarzania danych zgodnie z pkt. 8–10.

11. Budynek i pomieszczenia Urzędu Gminy w Parchowie posiadają następujące zabezpieczenia:

1) drzwi zewnętrzne (3szt.) zaopatrzone są w podwójne zamki patentowe;
2) dostęp (klucze) do drzwi głównych wejściowych posiadają: Wójt Gminy i wskazani pracownicy gospodarczy;
3) dostęp (klucze) do drzwi bocznych posiadają wskazani pracownicy gospodarczy;
4) klucze w tym zapasowe do wszystkich drzwi znajdują się Biurze Obsługi Interesanta Urzędu w szafie zamkniętej na klucz;
5) wszystkie okna budynku na poziomie parteru zabezpieczone są kratami lub roletami zawnętrznymi;
6) okna do pomieszczeń podlegających specjalnej ochronie (Kancelaria Materiałów Niejawnych, Ewidencja Ludności, Serwerownia) zabezpieczone są kratami;
7) drzwi do pomieszczeń biurowych posiadają zamki patentowe. Klucze do pomieszczeń biurowych są zabezpieczone w metalowej skrzynce zamykanej na zamek, pracownicy rano je odbierają i zdają po zakończeniu pracy odnotowując ten fakt w rejestrze pobranych kluczy;
8) dokumenty z danymi osobowymi przechowywane są w szafach na akta wyposażonych w zamki patentowe;
9) system sygnalizacji alarmu i włamania, do którego szyfr posiadają: Wójt Gminy i wskazani pracownicy, jest podłączony do jednostek Agencji Ochrony;

§ 2. Ochrona danych osobowych przetwarzanych poza obszarem przetwarzania

1. W przypadku przetwarzania danych osobowych na urządzeniach przenośnych lub dokumentach papierowych poza obszarem wymienionym w § 1 pkt 3 należy bezwzględnie chronić te dane przed dostępem do nich osób nieupoważnionych.

2. Zasady ochrony komputerów przenośnych, na których przetwarzane są dane osobowe, określa ASI w „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy w Parchowie".

§ 3. Monitorowanie ochrony zasobów danych osobowych

1. Właściciele zasobów danych osobowych i Sekretarz Gminy przekazują (w formie elektronicznej) ABI:
   1) aktualny wykaz zasobów danych osobowych przetwarzanych w danej komórce organizacyjnej,
   2) wykaz osób upoważnionych do przetwarzania określonego zasobu danych osobowych,
   3) wykaz pomieszczeń, w których przetwarzany jest poszczególny zasób danych osobowych w podległej komórce organizacyjnej i ich zabezpieczeń.
2. Pracownik właściwy w sprawach kadrowych na bieżąco informuje ABI o:
   1) ustaniu zatrudnienia osoby w Urzędzie;
   2) przeniesieniu pracownika do innego referatu Urzędu, celem kontroli jego uprawnień do dostępu do danych osobowych.
3. ASI przekazuje ABI:
   1) aktualny wykaz systemów teleinformatycznych, w których przetwarzane są dane osobowe;
   2) informacje o programach zastosowanych do przetwarzania danych osobowych;
   3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
   4) sposób przepływu danych pomiędzy poszczególnymi systemami.
4. ABI ustala szczegółowe zakresy informacji oraz formę i tryb ich przekazywania.
5. Każda zmiana informacji w zakresie ujętym w pkt 1–3 wymaga bieżącej aktualizacji przez osoby wskazane w wymienionych punktach.
6. Na podstawie przekazywanych informacji ABI prowadzi aktualny wykaz zasobów danych osobowych przetwarzanych w Urzędzie.

Załącznik nr 3 do Polityki Bezpieczeństwa

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

...../.....

Wykaz zasobów danych osobowych i systemów ich przetwarzania

Lp.	Nazwa zbioru/zasobu danych osobowych	System przetwarzania /nazwa systemu	Lokalizacja miejsca przetwarzania	Zastosowane oprogramowanie	Pełny zakres danych osobowych w systemie*	Pola informacyjne w systemie**	Sposób przepływu danych pomiędzy systemami	Możliwość wydruku zakresu przetwarzanych danych osobowych
1.								
2.								

* Należy podać zakres upoważnienia związany z czynnościami przy przetwarzaniu danych osobowych: zbieranie danych, wprowadzanie danych pracowniczych, odczyt, zapis, modyfikacja, drukowanie, usuwanie/niszczenie.

** Należy podać identyfikator (id, login) dla każdego systemu, do którego dana osoba ma dostęp.

Załącznik nr 4 do Polityki Bezpieczeństwa

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

...../.....

OŚWIADCZENIE

Ja niżej podpisany(a) ..... oświadczam, iż zostałem(am) poinformowana przez pracownika Urzędu Gminy ..... o:

1) adresie siedziby urzędu, pod którym dane są zbierane i przetwarzane;
2) celu zbierania danych, dobrowolności lub obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej;
3) prawie wglądu do treści swoich danych oraz możliwości ich poprawiania;
4) możliwości wniesienia żądania zaprzestania przetwarzania moich danych osobowych;
5) możliwości wniesienia sprzeciwu.

....
(Miejsce złożenia oświadczenia) (Data złożenia oświadczenia) (Numer PESEL)

.....
(Podpis osoby składającej)

Załącznik nr 5 do Polityki Bezpieczeństwa

.....
(pieczęć nagłówkowa urzędu)

.....
(miejscowość, data)

Adresat:

.....

.....

.....

W związku z art. 24 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922) uprzejmie Pana/Panią informuję, iż administratorem danych osobowych zawartych w przekazanych przez Pana/Panią dokumentach aplikacyjnych jest Urząd Gminy ..... (*wskazać dokładny adres*).

Pana/Pani dane osobowe będą przetwarzane w celu przeprowadzenia procesu rekrutacyjnego oraz wybrania pracownika i zawarcia umowy o pracę. Dane osobowe nie będą udostępnianie innym podmiotom. Posiada Pan/Pani prawo dostępu do treści swoich danych oraz ich poprawiania. Zebrane dane osobowe zostały przez Panią/Pana podane dobrowolnie.

.....
(podpis ADO)

Załącznik nr 6 do Polityki Bezpieczeństwa

……..……., dnia .....

……./.....

WNIOSEK O UDOSTĘPNIENIE DANYCH OSOBOWYCH

1. Wniosek do:

1) ……..……
……;
2) ……..……
……..
(dokładna nazwa administratora danych)

2. Wnioskodawca ……..
……..……
……..
……..……
……..
(nazwa firmy, adres, NIP, REGON, dane do korespondencji)

3. Podstawa prawna upoważniająca wnioskodawcę do przetwarzania danych osobowych jako odbiorcy danych, zgodnie z art. 7 ust. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2014 r. poz. 1182 ze zm.);

1) ……..……
……;
2) ……..……
……;
3) ……..……
……;
4) ……..……
……..

4. Cel przetwarzania danych:

1) ……..……
……;
2) ……..……
……;
3) ……..……
……..

5. Nazwa zbioru, z którego mają być udostępnione dane osobowe lub informacje umożliwiające zidentyfikowanie dokumentów, w których występowały dane osobowe (*np. sygnatura akt, rok złożonych dokumentów, symbol wydziału itp.*):

1) ……..……
……;
2) ……..……
……;

3) .....
.....

6. Zakres wymaganych danych, jakie mają być udostępnione:

1) .....
.....;
2) .....
.....;
3) .....
.....;
4) .....
.....

7. Inne informacje umożliwiające wyszukiwanie danych w zbiorze:

1) .....
.....;
2) .....
.....;
3) .....
.....

8. Forma doręczenia udostępnianych danych osobowych:

1) .....
.....;
2) .....
.....;
3) .....
.....

9. Lista załączników do wniosku:

1) .....;
2) .....;
3) .....

Załącznik nr 7 do Polityki Bezpieczeństwa

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

...../.....

Pan/Pani .....
zatrudniony/a w Urzędzie Gminy
w .....
na stanowisku .....

UPOWAŻNIENIE

do przetwarzania danych osobowych

I. Upoważniam Panią/Pana .....
(imię i nazwisko)
zatrudnioną/zatrudnionego w .....
(nazwa komórki organizacyjnej)
do przetwarzania danych osobowych, w celach związanych z wykonywaniem obowiązków na stanowisku: .....
(zajmowane stanowisko)
oraz do obsługi systemu informatycznego i urządzeń wchodzących w jego skład.
Niniejsze upoważnienie obejmuje przetwarzanie danych osobowych w formie tradycyjnej (kartoteki, ewidencje, rejestry, spisy itp.*) i elektronicznej, wg wykazu zbiorów podanych w pkt. II.

II. Upoważniam Panią/Pana do przetwarzania danych osobowych zawartych w następujących zbiorach: (proszę wpisać zgodnie z wykazem obowiązujących nazw zbiorów danych osobowych przetwarzanych w jednostkach organizacyjnych urzędu oraz podać nr identyfikujący zbiór – zgodnie z załącznikiem 3 do Polityki Bezpieczeństwa Informacji)

1.....
2.....
3.....
4.....
5.....

Otrzymuje:

.....

Załącznik nr 8 do Polityki Bezpieczeństwa

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

...../.....

Ewidencja osób upoważnionych do przetwarzania danych osobowych w Urzędzie Gminy Parchowo

Lp.	Imię i nazwisko	Data zapoznania z dokumentem	Stanowisko/funkcja	Typ umowy/porozumienia				Zakres rzeczowy uprawnienia	Ramy czasowe	
				Pracownik	Współpracownik	Wolontariusz	Praktyka/Staż		od ...[1]	do ...[2]
1										
2										

[1] Data zatrudnienia lub nawiązania współpracy z daną osobą.

[2] Następny dzień roboczy po ustaniu zatrudnienia danej osoby lub zakończeniu z nią współpracy – wynika to z faktu, iż ostatniego dnia zatrudnienia/współpracy dana osoba może jeszcze musieć przetwarzać dane osobowe, wykonując swoje obowiązki stanowiskowe.

Załącznik nr 9 do Polityki Bezpieczeństwa

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

...../.....

Porozumienie zawierane pomiędzy Wójtem Gminy w Parchowie. a pracownikiem zatrudnionym przy przetwarzaniu danych osobowych, w sprawie wykorzystania oddanego do dyspozycji sprzętu informatycznego, oprogramowania oraz zasobów sieci informatycznej

§ 1

Wójt Gminy w Parchowie, zwany dalej „Wójtem", oraz ..... (*wskazać imię i nazwisko pracownika*), zwany dalej „pracownikiem", zawierają na czas trwania zatrudnienia pracownika w Urzędzie Gminy w Parchowie porozumienie w sprawie wykorzystania sprzętu informatycznego, oprogramowania i zasobów sieci informatycznej.

§ 2

Wójt zobowiązuje się do:

1) zaznajomienia pracownika z obowiązującymi przy realizacji powierzonych mu zadań i obowiązków przepisami prawa i regulacjami wewnętrznymi, w szczególności związanymi z przetwarzaniem danych osobowych, przy wykorzystaniu sprzętu informatycznego, oprogramowania i zasobów sieci informatycznej;
2) zapewnienia pracownikowi niezbędnego sprzętu informatycznego, w tym komputera, drukarki i urządzeń, umożliwiających komunikację dla prawidłowego i terminowego wykonywania zadań i obowiązków;
3) zapewnienia pracownikowi legalnego oprogramowania wspierającego realizację powierzonych mu zadań i obowiązków;
4) braku konsekwencji służbowych w przypadku niewywiązania się pracownika z zadań i obowiązków spowodowanego niedziałaniem lub wadliwym działaniem sprzętu informatycznego, oprogramowania lub udostępnionych zasobów, chyba że działanie takie będzie wynikiem działania pracownika;
5) akceptowania wykorzystywania w miejscu pracy przez pracownika powierzonego mu sprzętu informatycznego, oprogramowania i zasobów sieciowych dla celów służących

samokształceniu, w tym szczególnie podnoszenia kwalifikacji związanych z wykonywanymi zadaniami i pełnionymi obowiązkami, pod warunkiem wcześniejszego prawidłowego i terminowego wykonania powierzonych mu zadań i obowiązków.

§ 3

Pracownik zobowiązuje się do:

1) przestrzegania obowiązujących przepisów prawa i regulacji wewnętrznych w zakresie wykorzystania sprzętu informatycznego, oprogramowania i zasobów sieci informatycznej podczas wykonywania swoich zadań i obowiązków, w tym w szczególności podczas przetwarzania danych osobowych;
2) wykorzystywania powierzonego mu sprzętu informatycznego, oprogramowania i zasobów sieciowych wyłącznie dla realizacji powierzonych mu zadań i obowiązków lub dla celów służących samokształceniu, w tym szczególnie podnoszenia kwalifikacji związanych z pełnionymi obowiązkami;
3) dbania o powierzony mu sprzęt informatyczny, oprogramowanie i zasoby sieciowe;
4) powstrzymania się od działań mogących mieć wpływ na bezpieczeństwo danych, w tym w szczególności od dokonywania jakichkolwiek zmian w konfiguracji powierzonego mu sprzętu informatycznego, od instalowania lub odinstalowania oprogramowania na powierzonym mu sprzęcie informatycznym oraz od wykorzystywania sprzętu lub oprogramowania do celów prywatnych, niezwiązanych w żaden sposób z wykonywanymi zadaniami i obowiązkami lub samokształceniem.

§ 4

Wójt informuje, a pracownik przyjmuje do wiadomości, że praca sieci informatycznej, sprzętu informatycznego, łączy teleinformatycznych i telekomunikacyjnych, działanie oprogramowania, przepływ danych i informacji oraz działania wszystkich pracowników związane z tymi elementami podlegają stałemu monitoringowi w celu zapewnienia bezpieczeństwa danych.

....

(podpis Wójta) *(podpis pracownika)*

Załącznik nr 10 do Polityki Bezpieczeństwa

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

...../.....

OŚWIADCZENIE

Ja niżej podpisany(a) ..... oświadczam, iż zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał(a) dostęp w związku z wykonywaniem:

Rodzaj zadań	Właściwe zaznaczyć
Zadań i obowiązków wynikających z umowy o pracę zarówno w trakcie wykonywania umowy, jak i po jej rozwiązaniu	
Zadań wynikających z umowy cywilnoprawnej zarówno w trakcie wykonywania umowy, jak i po jej wygaśnięciu	
Zadań wynikających z umowy praktyki zarówno w trakcie wykonywania umowy, jak i po jej wygaśnięciu	

*Właściwe zaznaczyć.

Zobowiązuję się przestrzegać regulaminów, instrukcji i procedur obowiązujących w Urzędzie Gminy w Parchowie dotyczących ochrony danych osobowych, w szczególności oświadczam, że bez upoważnienia służbowego nie będę wykorzystywał(a) danych osobowych ze zbiorów Urzędu Gminy w Parchowie

Oświadczam, że zostałem(am) poinformowany(a) o obowiązujących w Urzędzie Gminy w Parchowie zasadach dotyczących przetwarzania danych osobowych określonych w Polityce Bezpieczeństwa Informacji.

Oświadczam, że zostałem(am) zapoznany(a) z przepisami o ochronie danych osobowych oraz o grożącej, stosownie do przepisów rozdziału 8 ustawy o ochronie danych osobowych, odpowiedzialności karnej.

.....	.....	.....
(*miejsce złożenia oświadczenia*)	(*data złożenia oświadczenia*)	(*numer PESEL*)

.....

(*podpis osoby składającej oświadczenie*)

Załącznik nr 11 do Polityki Bezpieczeństwa

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

...../.....

Umowa powierzenia przetwarzania danych osobowych

Umowa Nr .....

Zawarta w dniu ..... r. w ..... pomiędzy:

..... z siedzibą w .....
przy ul. ....., wpisaną do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla ..... w .....,
..... Wydział Gospodarczy Krajowego Rejestru Sądowego, pod numerem KRS.....
....., NIP ....., wysokość kapitału zakładowego ..... zł,
reprezentowaną przez:
....., zwaną dalej **Zleceniodawcą,**
a
..... z siedzibą w ..... przy ul. ....., wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego przez Sąd Rejonowy dla ..... –
..... w .....,Wydział Krajowego Rejestru Sądowego pod numerem KRS:
....., o kapitale zakładowym w wysokości ..... złotych
NIP: ..... Regon: .....

reprezentowaną przez:
....., zwaną dalej **Wykonawcą**,
zwanymi łącznie „Stronami" o następującej treści:

§ 1.

1. W związku z realizacją umowy nr ..... z dnia ..... r. o ..... Zleceniodawca powierza Wykonawcy trybie art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2014 r. poz. 1182 ze zm.), zwanej dalej „ustawą", przetwarzanie danych osobowych.
2. Zleceniodawca oświadcza, że jest administratorem danych osobowych, które powierza.
3. Powierzone dane zawierają informacje o osobach fizycznych/pracownikach pracodawców lub pracodawcach będących osobami fizycznymi.
4. Zleceniodawca powierza Wykonawcy przetwarzanie danych osobowych w zakresie określonym w § 2.

§ 2.

1. Wykonawca będzie przetwarzał, powierzone na podstawie niniejszej Umowy, następujące kategorie danych osobowych/zbiory danych osobowych:
   1) imię i nazwisko,
   2) numer ewidencyjny PESEL,
   3) seria i numer dowodu osobistego,

4) .....

2. Powierzone przez Zleceniodawcę dane osobowe będą przetwarzane przez Wykonawcę wyłącznie w celu wykonywania przez Wykonawcę na rzecz Zleceniodawcy usług szczegółowo opisanych w umowie, o której mowa w § 1 ust. 1, i w sposób zgodny z niniejszą Umową.

§ 3.

1. Wykonawca zobowiązuje się, przy przetwarzaniu danych osobowych, o których mowa w § 2 ust. 1, do ich zabezpieczenia poprzez podjęcie środków technicznych i organizacyjnych, o których mowa w art. 36–39a ustawy.
2. Wykonawca oświadcza, że zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informacyjne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024):
   1) prowadzi dokumentację opisującą sposób przetwarzania danych osobowych,
   2) znajdujące się w jego posiadaniu urządzenia i systemy informatyczne służące do przetwarzania danych osobowych zapewniają poziom bezpieczeństwa określony, jako wysoki,
   3) stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy, zmianą, utratą, uszkodzeniem lub zniszczeniem, w zakresie, za który odpowiada Wykonawca.
3. Wykonawca zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, ustawą oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
4. Wykonawca zobowiązuje się niezwłocznie zawiadomić Zleceniodawcę o:
   1) każdym prawnie umocowanym żądaniu udostępnienia danych osobowych właściwemu organowi państwa, chyba że zakaz zawiadomienia wynika z przepisów prawa, a szczególności przepisów postępowania karnego, gdy zakaz ma na celu zapewnienie poufności wszczętego dochodzenia;
   2) każdym nieupoważnionym dostępie do danych osobowych;
   3) każdym żądaniu otrzymanym od osoby, której dane przetwarza, powstrzymując się jednocześnie od odpowiedzi na żądanie.
5. Zleceniodawca ma prawo do kontroli sposobu wykonywania niniejszej Umowy poprzez przeprowadzenie zapowiedzianych na 7 dni kalendarzowych wcześniej doraźnych kontroli dotyczących przetwarzania danych osobowych przez Wykonawcę oraz żądania składania przez niego pisemnych wyjaśnień.
6. Na zakończenie kontroli, o których mowa w ust. 8, przedstawiciel Zleceniodawcy sporządza protokół w 2 egzemplarzach, który podpisują przedstawiciele obu stron. Wykonawca może wnieść zastrzeżenia do protokołu w ciągu 5 dni roboczych od daty jego podpisania przez strony.
7. Wykonawca zobowiązuje się dostosować do zaleceń pokontrolnych mających na celu usunięcie uchybień i poprawę bezpieczeństwa przetwarzania danych osobowych.

8. Wykonawca zobowiązuje się odpowiedzieć niezwłocznie i właściwie na każde pytanie Zleceniodawcy dotyczące przetwarzania powierzonych mu na podstawie Umowy danych osobowych.

§ 4.

1. Wykonawca jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z Umową, a w szczególności za udostępnienie osobom nieupoważnionym.
2. W przypadku naruszenia przepisów ustawy lub niniejszej Umowy z przyczyn leżących po stronie Wykonawcy, w następstwie czego Zleceniodawca, jako administrator danych osobowych, zostanie zobowiązany do wypłaty odszkodowania lub zostanie ukarany karą grzywny, Wykonawca zobowiązuje się pokryć Zleceniodawcy poniesione z tego tytułu straty i koszty.

§ 5.

Niniejsza Umowa powierzenia zostaje zawarta na czas określony od dnia ..... do dnia .....

§ 6.

Zleceniodawca ma prawo rozwiązać niniejszą Umowę bez zachowania terminu wypowiedzenia, gdy Wykonawca:

1) wykorzystał dane osobowe w sposób niezgodny z niniejszą Umową,
2) powierzył przetwarzanie danych osobowych podwykonawcom bez zgody Zleceniodawcy,
3) nie zaprzestanie niewłaściwego przetwarzania danych osobowych,
4) zawiadomi o swojej niezdolności do dalszego wykonywania niniejszej Umowy, a w szczególności o niespełnianiu wymagań określonych w § 3.

§ 7.

Wykonawca, w przypadku wygaśnięcia niniejszej Umowy niezwłocznie, ale nie później niż w terminie 5 dni kalendarzowych, zobowiązuje się zwrócić lub usunąć wszelkie dane osobowe, których przetwarzanie zostało mu powierzone, w tym skutecznie usunąć je również z nośników elektronicznych pozostających w jego dyspozycji i potwierdzić powyższe przekazanym Zleceniodawcy protokołem.

§ 8.

Wszelkie zmiany niniejszej Umowy wymagają formy pisemnej pod rygorem nieważności.

§ 9.

W sprawach nieuregulowanych w niniejszej Umowie mają zastosowanie przepisy Kodeksu Cywilnego oraz ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

§ 10.

Spory wynikłe z tytułu Umowy będzie rozstrzygał Sąd właściwy dla miejsca siedziby Zleceniodawcy.

§ 11.

Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

.....
(podpis Zleceniodawcy)

.....
(podpis Wykonawcy)

Załącznik nr 12 do Polityki Bezpieczeństwa

……., dnia .....

……./.....

RAPORT
z naruszenia bezpieczeństwa zasad ochrony danych osobowych
w Urzędzie Gminy w Parchowie

1. Data: …… Godzina: ……

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

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

3. Lokalizacja zdarzenia:

……
……
……..
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:
……
……
……
……
……

5. Przyczyny wystąpienia zdarzenia:
……
……
……
……
……
6. Podjęte działania:
……
……
……
……
……7. Skutki zdarzenia:
……
……

.....
.....
.....
.....
.....
.....

7. Postępowanie wyjaśniające:

.....
.....
.....
.....
.....

.....
(data, podpis ABI)

Załącznik nr 13 do Polityki Bezpieczeństwa Informacji

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

...../.....

Wniosek

o nadanie/cofnięcie uprawnień do przetwarzania danych osobowych

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922) wnoszę o nadanie/cofnięcie uprawnień dla

Pani/Pana

.....

Zajmującego stanowisko

.....

do przetwarzania danych osobowych zawartych w następujących zbiorach: **(proszę wpisać zgodnie z wykazem obowiązujących nazw zbiorów danych osobowych przetwarzanych w jednostkach organizacyjnych urzędu oraz podać nr identyfikujący zbiór – zgodnie z załącznikiem 3 do Polityki Bezpieczeństwa Informacji)**

.....

.....

.....

na okres od ..... **do** .....

.....

(data i podpis wnioskującego do Administratora Danych Osobowych)

Wyrażam zgodę / nie wyrażam zgody* (skreślić niepotrzebne)

.....

(data i podpis Administratora Danych Osobowych)

Załącznik nr 14 do Polityki Bezpieczeństwa Informacji

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

...../.....

Wniosek

o umieszczenie w wykazie zbiorów danych / wykreślenie z wykazu zbiorów danych

Na podstawie § 4 rozporządzenia z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (t.j. Dz.U. z 2004 r. Nr 100, poz. 1024)

wnoszę o umieszczenie w wykazie zbiorów danych / wykreślenie z wykazu zbiorów danych * (skreślić niepotrzebne)

poniższego zbioru danych osobowych

Lp.	Nazwa zbioru/zasobu danych osobowych	System przetwarzania /nazwa systemu	Lokalizacja miejsca przetwarzania	Zastosowane oprogramowanie	Pełny zakres danych osobowych w systemie*	Sposób przepływu danych pomiędzy systemami	Możliwość wydruku zakresu przetwarzanych danych osobowych

.....

(data i podpis wnioskującego do Administratora Bezpieczeństwa Informacji)

* Należy podać zakres upoważnienia związany z czynnościami przy przetwarzaniu danych osobowych: zbieranie danych, wprowadzanie danych pracowniczych, odczyt, zapis, modyfikacja, drukowanie, usuwanie/niszczenie.

Załącznik nr 2 do zarządzenia Nr 10.2017
Wójta Gminy Parchowo
z dnia 27 stycznia 2017 r.

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

§ 1.
Wprowadzenie

1. Niniejsza instrukcja określa zasady eksploatacji i zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Parchowo.
2. Zasady opisane w niniejszym dokumencie są zgodne z obowiązującymi wymaganiami prawnymi, w szczególności:
   1) ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2016 r. poz. 922), zwaną dalej „OchrDanychU",
   2) rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024), zwanym dalej „DokPrzetwR".
3. W instrukcji stosuje się następujące skróty:
   1) ABI – Administrator Bezpieczeństwa Informacji, realizujący czynności określone w art. 36a OchrDanychU;
   2) ASI – Administrator Systemu Informatycznego, odpowiedzialny za administrację systemami informatycznymi Urzędu.

§ 2.
Procedura nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

1. Podstawą do nadania uprawnień do przetwarzania danych osobowych w systemie informatycznym Urzędu jest upoważnienie do przetwarzania danych osobowych. Upoważnienie wydawane jest przez Administratora Danych Osobowych.
2. 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.
3. Administrator Bezpieczeństwa Informacji:
   1) w przypadku gdy dana osoba otrzymuje po raz pierwszy upoważnienie do przetwarzania danych osobowych informuje ją o obowiązkach związanych z zapewnieniem ochrony danych osobowych;
   2) odbiera od powyższej osoby podpis pod upoważnieniem do przetwarzania danych osobowych i oświadczeniem o zapoznaniu się z obowiązującymi zasadami ochrony danych osobowych.
4. ABI prowadzi, w imieniu i z upoważnienia Administratora Danych Osobowych, ewidencję osób upoważnionych do przetwarzania danych osobowych. Każda zmiana

w zakresie informacji zawartych w ewidencji podlega niezwłocznemu odnotowaniu przez ABI.

5. Uprawnienia dostępu do systemu informatycznego nadawane są na podstawie wniosku przełożonego danego pracownika, a w przypadku osoby nie będącej pracownikiem Urzędu na wniosek pracownika Urzędu koordynującego działania danej osoby. Wniosek niniejszy kierowany jest do ABI i może być połączony z wnioskiem o nadanie upoważnienia do przetwarzania danych osobowych.
6. Za nadanie uprawnień w systemie informatycznym odpowiada ASI. Uprawnienia nie mogą być nadane w przypadku, jeżeli dana osoba nie posiada upoważnienia do przetwarzania danych osobowych w wymaganym zakresie.
7. ABI informuje osobę wnioskującą o fakcie nadania lub odmowy nadania uprawnień.
8. W przypadku nadawania użytkownikowi uprawnień do danego systemu informatycznego po raz pierwszy, ASI dokonuje nadania użytkownikowi identyfikatora, wygenerowania hasła oraz wpisania identyfikatora do ewidencji osób upoważnionych do przetwarzania danych osobowych.
9. 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.
10. Hasło użytkownika jest przydzielane indywidualnie każdemu z użytkowników i znane jest tylko użytkownikowi, który się nim posługuje.
11. ASI przekazuje użytkownikowi identyfikator i hasło.
12. Użytkownik jest zobowiązany do zmiany hasła przy pierwszym dostępie do systemu informatycznego.

§ 3.
Procedura odbierania uprawnień do przetwarzania danych w systemie informatycznym

1. W przypadku konieczności odebrania lub zmiany zakresu upoważnienia – w związku ze zmianą zakresu obowiązków służbowych pracownika lub zakończeniem pracy – jego przełożony wnioskuje do ABI o wykonanie powyższej czynności. Administrator Danych Osobowych dokonuje, na podstawie informacji przekazanej przez ABI, odebrania lub zmiany zakresu upoważnienia, ASI zaś dokonuje odebrania lub zmiany zakresu uprawnień w systemie informatycznym. O powyższym ASI informuje osobę wnioskującą.
2. 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.

§ 4.
Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Użytkownicy systemu informatycznego przetwarzającego dane osobowe wykorzystują w procesie uwierzytelnienia identyfikatory i hasła.
2. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi i nie podlega zmianie.
3. Nowe hasło jest przekazywane użytkownikowi przez ASI.
4. Po zalogowaniu do systemu z wykorzystaniem otrzymanego hasła użytkownik jest zobowiązany do dokonania jego natychmiastowej zmiany, nawet, jeżeli system informatyczny nie wymusza takiego działania.
5. 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.

6. Hasło jest zmieniane przez użytkownika nie rzadziej niż co 30 dni lub niezwłocznie w przypadku podejrzenia, iż mogły z nim się zapoznać nieuprawnione osoby. Hasło powinno różnić się od poprzednio używanych.
7. 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.
8. W przypadku zapomnienia hasła użytkownik powinien zwrócić się do ASI o wygenerowanie nowego hasła.
9. W przypadku podejrzenia zapoznania się z hasłem przez osobę nieuprawnioną użytkownik jest zobowiązany do natychmiastowej zmiany hasła oraz powiadomienia o zaistniałym fakcie ABI.

§ 5.
Procedura rozpoczęcia, zawieszenia i zakończenia pracy przeznaczona dla użytkowników systemu

1. 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 ASI,
   5) w przypadku niestandardowego zachowania aplikacji przetwarzającej dane osobowe pracownik natychmiast powiadamia o zaistniałym fakcie ABI.
2. Zawieszając pracę w systemie informatycznym (w tym odchodząc od stanowiska pracy), użytkownik blokuje stację roboczą. Kontynuacja pracy może nastąpić po odblokowaniu stacji roboczej po wprowadzeniu hasła, w sposób gwarantujący jego niepodejrzenie przez osoby trzecie.
3. 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.
4. 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.

§ 6.
Procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

1. Za tworzenie i przechowywanie kopii zapasowych odpowiedzialny jest ASI.
2. Kopie zapasowe systemów przetwarzających dane osobowe są codziennie zapisywane na taśmy magnetyczne lub na innym nośniku. Zapis odbywa się w godzinach 16–20.
3. Nośniki kopii zapasowych oznaczane są w sposób umożliwiający określenie daty utworzenia kopii oraz nazwy systemu.
4. Nośniki z kopiami zapasowymi przechowywane są w sejfie.
5. Utworzone kopie zapasowe podlegają weryfikacji ze względu na sprawdzenie możliwości odczytu danych.
6. ASI odpowiada za prowadzenie ewidencji wykonania kopii zapasowych.
7. ABI określa czas przechowywania poszczególnych kopii zapasowych, w zależności od celu przetwarzania danych zapisanych na kopiach zapasowych.
8. ASI odpowiedzialny jest za realizację działań odtworzeniowych w przypadku konieczności podjęcia takich działań w związku z awarią systemu informatycznego Urzędu. Po odtworzeniu systemu informatycznego ASI odpowiedzialny jest za przeprowadzenie testów poprawności działania systemu przed jego oddaniem do użytkowania.
9. ASI przeprowadza weryfikację możliwości odtworzenia danych zapisanych na kopiach zapasowych. Weryfikacja taka powinna być przeprowadzana nie rzadziej niż raz na pół roku.

§ 7.
Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz nośników kopii zapasowych

1. Dane osobowe przechowywane są w postaci elektronicznej na:
   1) nośnikach elektronicznych wbudowanych w sprzęt informatyczny lub stanowiących element tego systemu,
   2) przenośnych nośnikach elektronicznych.
2. 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.
3. 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.
4. 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. ABI wyznacza pomieszczenia, w których mogą być przechowywane takie nośniki.
5. 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 ASI. Zniszczenie nośnika potwierdzane jest protokołem przechowywanym przez ABI.

6. Dopuszcza się powierzenie niszczenia nośników danych wyspecjalizowanym podmiotom zewnętrznym, pod warunkiem:
   1) zawarcia umowy, o której mowa w art. 31 OchrDanychU,
   2) zagwarantowania poufności danych przez usługodawcę,
   3) umożliwienia prowadzenia nadzoru nad procesem niszczenia nośników przez ABI lub upoważnionego przez niego pracownika Urzędu,
   4) udokumentowania faktu zniszczenia nośników protokołem.

§ 8.
Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem działania jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

1. 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 ASI;
   4) korzystania z Internetu w celach nie związanych z pełnionymi obowiązkami służbowymi;
   5) podłączania komputerów do sieci zewnętrznych za pośrednictwem modemów.
2. W przypadku zauważenia objawów mogących wskazywać na obecność niebezpiecznego oprogramowania użytkownik jest zobowiązany powiadomić ASI. Do objawów powyższych można zaliczyć:
   1) istotne spowolnienie działania systemu informatycznego,
   2) nietypowe działanie aplikacji,
   3) nietypowe komunikaty,
   4) utratę danych lub modyfikację danych.
3. 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.
4. ASI 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.

§ 9.
Odnotowanie informacji o udostępnieniu danych osobowych

1. Urząd udostępnia dane osobowe jedynie w przypadkach prawnie dopuszczalnych.

2. Przy odnotowywaniu przez użytkownika informacji o udostępnieniu danych, użytkownik wprowadza zapis „Dane osobowe w zakresie ››zakres‹‹ udostępniono ››odbiorca‹‹ w dniu ››data‹‹", wprowadzając zamiast zapisów w nawiasach klamrowych odpowiednie informacje.

§ 10.
Procedura wykonywania przeglądu i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

1. Przegląd i konserwacja sprzętu informatycznego realizowany jest przez upoważnionych pracowników Urzędu oraz przez podmioty zewnętrzne.
2. Prace serwisowe wykonywane na terenie Urzędu przez podmioty zewnętrzne podlegają bezpośredniemu nadzorowi ASI.
3. Przekazanie sprzętu teleinformatycznego 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.
4. Protokoły, o których mowa w punkcie 3, lub ich kopie przechowywane są przez ABI.
5. 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.