Załącznik nr 2 do Zarządzenia nr 41/2018 z dnia 25.05.2018
Wójta Gminy Trzyciąż w sprawie wprowadzenia Dokumentacji sposobu przetwarzania danych osobowych.

Instrukcja zarządzania systemem informatycznym

Data wydania:	25.05.2018 r.	Wydanie:	1
Dokument spełnia wymagania:	• Ustawa z dnia 29.08.1997 o ochronie danych osobowych (Dz.U. z 2016 r. poz.922), • Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004 r. sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych, organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 r. 100 poz. 1024), • ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)		

Trzyciąż, 2018

Spis treści:

1. Postanowienia ogólne

1. Niniejsza Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej Instrukcją, przyjęta została w celu wykazania, że dane osobowe w systemach informatycznych Urzędu Gminy Trzyciąż przetwarzane są w sposób zgodny z przepisami prawa mającymi zastosowanie do takiej czynności, zgodnie z zasadą art. 5 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 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 (dalej RODO).
2.Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy w Trzyciążu, określa zasady, tryb postępowania i zalecenia Administratora Danych, które muszą być stosowane przez osoby przez niego upoważnione do przetwarzania danych osobowych w systemach informatycznych.
3. Instrukcja została opracowana zgodnie z wymogami § 5 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).
4. Podstawowymi celami zabezpieczeń systemów informatycznych służących do przetwarzania danych osobowych, jest zapewnienie jak najwyższego poziomu bezpieczeństwa przetwarzanych danych osobowych w systemach informatycznych.
5. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania w systemach, charakteru poufnego wraz z zachowaniem ich integralności i rozliczalności.
6. Inspektor Ochrony Danych powinien posiadać stosowne uprawnienia w nadzorowanych systemach informatycznych, gwarantujące skuteczne wykonywanie zadań z zakresu nadzoru wszędzie tam, gdzie jest to możliwe. Nie oznacza to automatycznego prawa dostępu do danych osobowych przetwarzanych w tych systemach.

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

Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych (wzór upoważnienia stanowi załącznik do niniejszej instrukcji). Wydanie upoważnienia oraz rejestracja Użytkownika systemu informatycznego przetwarzającego dane osobowe

następuje na wniosek przełożonego użytkownika lub koordynatora zadania, na rzecz którego będą wykonywane czynności związane z przetwarzaniem danych osobowych. W formie ustnej lub pisemnej składa on wniosek do Inspektora Ochrony Danych odpowiedniego dla zakresu danych o wydanie upoważnienia do przetwarzania danych osobowych. Wniosek ten powinien zawierać:

• imię i nazwisko pracownika, któremu upoważnienie zostanie nadane,
• zakres upoważnienia do przetwarzania danych osobowych,
• datę, z jaką upoważnienie ma być nadane,
• okres ważności upoważnienia (w zależności od stosunku pracy na podanym stanowisku).

Upoważnienie zostaje przekazane pracownikowi za potwierdzeniem odbioru, a także dołączone do akt osobowych pracownika oraz do ewidencji prowadzonej przez IOD.

Konto i hasło do systemu informatycznego przetwarzającego dane osobowe są przydzielane użytkownikowi tylko w przypadku, gdy posiada on pisemne upoważnienie do przetwarzania danych osobowych wydane przez administratora danych osobowych lub osobę przez niego uprawnioną. Za przydzielenie i wygenerowanie identyfikatora i hasła użytkownikowi, który pierwszy raz będzie korzystał z systemu informatycznego, odpowiada administrator odpowiedniego systemu informatycznego. Wyrejestrowanie użytkownika z systemu informatycznego może nastąpić na wniosek administratora danych osobowych, przełożonego użytkownika.

Pisemny wniosek o wyrejestrowanie użytkownika systemu należy złożyć do Administratora systemu informatycznego. Wyrejestrowanie użytkownika z systemu realizuje administrator odpowiedniego systemu informatycznego.

Inspektor Ochrony Danych jest zobowiązany do prowadzenia ewidencji pracowników upoważnionych do przetwarzania danych osobowych w Urzędzie Gminy w Trzyciążu. Zgodnie z art. 39 ust. 1 ustawy taka ewidencja zawiera:

• imię i nazwisko osoby upoważnionej,
• datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,

3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.

Przed rozpoczęciem pracy, w trakcie rozpoczynania pracy z systemem informatycznym oraz w trakcie pracy każdy pracownik obowiązany jest do zwrócenia bacznej uwagi, czy nie wystąpiły symptomy mogące świadczyć o naruszeniu zasad ochrony danych osobowych. Szczegółowy opis takich symptomów oraz sposób postępowania w przypadku ich wykrycia został opisany w dokumencie „Polityka bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Trzyciążu" punkt 6.

Każdy użytkownik, który ma dostęp do systemów informatycznych, posiada osobiste konto i hasło. Użytkownik hasła:

- zobowiązany jest uwierzytelniać się w systemie informatycznym wyłącznie na podstawie własnego konta i hasła.
- odpowiedzialny jest za wykorzystywanie swojego konta i hasła oraz za wszystkie czynności wykonane przy użyciu swojego konta i hasła.

- w żadnym wypadku nie może ujawniać swojego hasła, włącznie ze służbami informatycznymi zewnętrznymi czy współpracownikami.

W przypadku bezczynności użytkownika na stacji roboczej przez okres dłuższy niż 30 minut automatycznie włączana jest opcja wygaszania ekranu. Wygaszenie ekranu powinno być zaopatrzone w hasło po wznowieniu pracy na danej stacji roboczej. Hasło powinno składać się z co najmniej 8 znaków, powinno zawierać małe i wielkie litery oraz cyfry lub znaki specjalne oraz być zmieniane nie rzadziej niż co 30 dni. Zmianę użytkownika stacji roboczej każdorazowo musi poprzedzać wylogowanie się poprzedniego użytkownika. Niedopuszczalne jest, aby dwóch lub większa ilość Użytkowników wykorzystywała wspólnie jedno konto użytkownika. W przypadku, gdy przerwa w pracy na stacji roboczej trwa dłużej niż 60 minut Użytkownik obowiązany jest wylogować się z aplikacji i systemu stacji roboczej, na której pracuje oraz sprawdzić czy nie zostały pozostawione bez zamknięcia nośniki informacji zawierające dane osobowe. W pomieszczeniach, w których przetwarzane są dane i w których jednocześnie mogą przebywać osoby postronne, monitory stanowisk dostępu do danych powinny być ustawione w taki sposób, Żeby uniemożliwić tym osobom wgląd w dane. Zakończenie pracy użytkownika w systemie informatycznym obejmuje wylogowanie się użytkownika z aplikacji oraz zamknięciem systemu operacyjnego.

4. procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

W systemie wykonywane winny być kopie zapasowe, a ich nośniki przechowywane w bezpiecznym miejscu.
Kopie zapasowe winny być wykonywane z wykorzystaniem nośników zewnętrznych (płyty CD, przenośne dyski z opcją szyfrowania). Kopie powinny być wykonywane w częstotliwości nie rzadziej niż raz na 30 dni, łącznie z używanym do ich przetwarzania systemem informatycznym.
Procedura wykonywania kopii powinna być określona uprzednim ustalonym z pracownikami merytorycznymi harmonogramem wykonywania kopii zapasowych dla poszczególnych danych oraz metodą sporządzania kopii (przyrostowa, całościowa).
Przechowywanie nośników powinno trwać nie dłużej niż 3 miesiące od wykonania ostatniej kopii zapasowej. Stare nośniki zawierające kopie danych osobowych, należy przeznaczyć do likwidacji, pozbawić zapisu tych danych lub wykonać zerowanie trwałe w przypadku kopii umieszczonych na szyfrowanym przenośnym dysku twardym.

5. sposób, miejsce i okres przechowywania:
a) elektronicznych nośników informacji zawierających dane osobowe,
- Dane osobowe w postaci elektronicznej przetwarzane w systemie informatyczny, zapisane na dyskietkach, taśmach magnetycznych czy dyskach twardych nie są wynoszone poza siedzibę Urzędu.
- wymienne elektroniczne nośniki informacji są przechowywane w pokojach stanowiących obszar przetwarzania danych osobowych, określony w Polityce bezpieczeństwa przetwarzania danych osobowych.
- po zakończeniu pracy przez użytkowników systemu, wymienne elektroniczne nośniki informacji przechowywane są w zamykanych szafach biurowych lub kasetkach.

- w przypadku uszkodzenia lub zużycia nośnika zawierającego dane osobowe należy go fizycznie zniszczyć.
- dyski twarde z danymi osobowymi należy zniszczyć zgodnie z obowiązującymi w Urzędzie przepisami dotyczącymi gospodarki środkami trwałymi oraz wartościami niematerialnymi.

b) kopii zapasowych, o których mowa w pkt. 4,

- taśmy magnetyczne i optyczne z kopiami zapasowymi zbiorów danych osobowych łącznie z używanym do ich przetwarzania systemem informatycznym są przechowywane przez wyznaczonego pracownika i odpowiednio zabezpieczone.
- po okresie obowiązującego okresu przechowywania kopie podlegają likwidacji poprzez ich fizyczne zniszczenie, wraz z kierownikiem komórki organizacyjnej Urzędu gminy w Trzyciążu.

c) Wydruki

- wszelkie wydruki, zawierające dane osobowe, należy przechowywać w miejscu uniemożliwiającym ich odczyt przez osoby nieuprawnione, w zamkniętych szafach lub pomieszczeniach.
- wydruki, zawierające dane osobowe, po upływie czasu ich przydatności należy zniszczyć w stopniu uniemożliwiającym ich odczytanie np. przez pocięcie w niszczarce dokumentów.
- dane osobowe zapisane w formie papierowej innej niż wydruki z systemu informatycznego (pisma, ankiety itp.) są przechowywane na podobnych zasadach co wydruki.

6. sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, o którym mowa w pkt III ppkt 1 załącznika do rozporządzenia,

1. Ochrona antywirusowa
- za ochronę antywirusową odpowiada wyznaczony pracownik,
- ochrona antywirusowa jest realizowana przez oprogramowanie antywirusowe instalowane na serwerach i stacjach roboczych użytkowników.
- oprogramowanie antywirusowe jest uaktualniane automatycznie, co najmniej raz na 2 dni.
- dane zawarte na nośnikach zewnętrznych (np. dyskietki, płyty CD, nośnika magnetycznego – pendrive, przenośny dysk twardy) muszą być każdorazowo sprawdzone przez użytkownika danej stacji roboczej poprzez program antywirusowy przed wprowadzeniem do systemu.
- w przypadku poczty elektronicznej oprogramowanie antywirusowe zabezpiecza operator serwera na którym znajduje się poczta zewnętrzna Urzędu.

2. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej

Wyznaczony pracownik jest odpowiedzialny za aktywowanie i poprawne konfigurowanie specjalistycznego sprzętu i oprogramowania monitorującego wymianę danych na styku:

a) sieci lokalnej i sieci rozległej,

b) stanowiska komputerowego użytkownika systemu i pozostałych urządzeń wchodzących w skład sieci lokalnej.

7. sposób realizacji wymogów, o których mowa w § 7 ust. 1 pkt 4 rozporządzenia,

Zasady powierzenia przetwarzania danych osobowych określa pkt 4.7 Polityki bezpieczeństwa przetwarzania danych osobowych w Urzędzie Gminy w Trzyciążu.

8. procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

O przeprowadzanych przeglądach, konserwacjach i naprawach systemu w każdym przypadku informowany jest użytkownik danej stacji roboczej, który powinien być przy nich obecny.

Przeglądy i konserwacja urządzeń:
1) przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonym przez producenta sprzętu,
2) nieprawidłowości ujawnione w trakcie tych działań powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić IOD.
3) za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada wyznaczony pracownik.

Przegląd programów i narzędzi programowych przeprowadzany jest w następujących przypadkach:
a) zmiany wersji oprogramowania serwera plików;
b) zmiany wersji oprogramowania stanowiska komputerowego użytkownika systemu;
c) zmiany systemu operacyjnego serwera plików;
d) zmiany systemu operacyjnego stanowiska komputerowego użytkownika systemu;
e) wykonania zmian w projekcie systemu spowodowanych koniecznością naprawy, konserwacji lub modyfikacji systemu.

Przegląd przeprowadza projektant systemu w obecności wyznaczonego pracownika.
W przypadku stwierdzenia uszkodzenia urządzenia, dyski i inne informatyczne nośniki danych zawierające dane osobowe przed ich przekazaniem do naprawy innemu podmiotowi pozbawiane są zawartości.
W przypadku likwidacji urządzenia, dyski i inne informatyczne nośniki danych zawierające dane osobowe są niszczone w sposób uniemożliwiający odczytanie danych.
Naprawa wymienionych urządzeń zawierających dane osobowe, jeżeli nie można danych usunąć, wykonywana jest pod nadzorem IOD.

9. Postanowienia końcowe
Zabrania się:
a) samodzielnego instalowania oprogramowania, zarówno licencjonowanego jak i nielegalnego oraz darmowego oraz jego używanie;
b) samodzielnego naprawiania uszkodzeń mechanicznych, związanych ze złym funkcjonowaniem zestawu komputerowego;
c) montażu i demontażu urządzeń komputerowych;
d) podłączania dodatkowych urządzeń elektrycznych do listwy zasilającej komputer, bez uzgodnienia z administratorem sieci.
1. Każdy pracownik zatrudniony przy przetwarzaniu danych osobowych w systemie, zobowiązany jest zapoznać się z niniejszą Instrukcją i stosować jej przepisy na swoim stanowisku pracy.
2. W obszarach w których nie przetwarza się danych osobowych w systemach informatycznych przepisy niniejszej Instrukcji stosuje się odpowiednio.

W sprawach nieuregulowanych niniejszą Instrukcją mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 poz. 922), 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 /Dz. Urz. UE.L nr 119, str. 1/ (zwanym dalej RODO) i rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku 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).

Wszelkie zmiany Instrukcji mogą być wprowadzane tylko na podstawie zarządzeń Administratora Danych Osobowych.