

ZARZĄDZENIE NR 71/2018
WÓJTA GMINY ROGÓŹNO

z dnia 17 lipca 2018 r.

**w sprawie ustanowienia instrukcji zarządzania systemem informatycznym służącym
przetwarzaniu danych osobowych w Urzędzie Gminy Rogóźno**

Na podstawie art. 24 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) zarządza się, co następuje:

§ 1. Ustanawiam instrukcję zarządzania systemem informatycznym służącym przetwarzaniu danych osobowych w Urzędzie Gminy Rogóźno, która stanowi załącznik do niniejszego zarządzenia.

§ 2. 1. Zobowiązuję pracowników do zapoznania się z instrukcją zarządzania systemem informatycznym służącym przetwarzaniu danych osobowych w Urzędzie Gminy Rogóźno w terminie 7 dni od dnia wejścia w życie niniejszego zarządzenia.

2. Zobowiązuje pracowników do przestrzegania i stosowania zasad określonych w instrukcji zarządzania systemem informatycznym służącym przetwarzaniu danych osobowych w Urzędzie Gminy Rogóźno

§ 3. Wykonanie zarządzenia powierzam Inspektorowi Ochrony Danych

§ 4. Traci moc zarządzenie Nr 1/2016 Wójta Gminy Rogóźno z dnia 25 stycznia 2016 r. w sprawie ochrony danych osobowych w Urzędzie Gminy Rogóźno.

§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFOMATYCZNYM SŁUŻĄCYM PRZETWARZANIU DANYCH OSOBOWYCH W URZĘDZIE GMINY ROGÓŻNO

Rozdział 1. Wprowadzenie

§ 1. 1. Niniejsza instrukcja określa zasady eksploatacji i zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Urzędzie Gminy Rogóżno.

2. Zasady opisane w niniejszej instrukcji są zgodne z obowiązującymi przepisami prawnymi, w szczególności:

1) rozporządzeniem Parlamentu Europejskiego i Rady /UE/ 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE /Dz. Urz. UE.L nr 119, str.1/;

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

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

§ 2. 1. Podstawą do nadania uprawnień do przetwarzania danych osobowych w systemie informatycznym Urzędu jest upoważnienie do przetwarzania danych osobowych. Upoważnienie nadawane jest przez Administratora Danych Osobowych.

2. Upoważnienie nadawane jest na wniosek przełożonego danego pracownika, a w przypadku osoby nie będącej pracownikiem Urzędu- na wniosek pracownika koordynującego działania osoby, dla której upoważnienie jest wydawane.

3. Inspektor Ochrony Danych:

1) w przypadku gdy dana osoba otrzymuje po raz pierwszy upoważnienie do przetwarzania danych osobowych-informuje ja o obowiązkach związanych z zapewnieniem ochrony danych osobowych;

2) odbiera od tej osoby oświadczenie o zapoznaniu się z obowiązującymi zasadami ochrony danych osobowych.

4. Inspektor Ochrony Danych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych. Każda zmiana w zakresie informacji zawartych w ewidencji podlega niezwłocznemu odnotowaniu.

5. Uprawnienia dostępu do systemu informatycznego nadawane są na podstawie wniosku przełożonego pracownika, a w przypadku osoby nie będącej pracownikiem Urzędu- na wniosek pracownika koordynującego działania danej osoby. Wniosek kierowany jest do ADO i może być połączony z wnioskiem o nadanie upoważnienia do przetwarzania danych osobowych.

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

7. IOD informuje osobę 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 użytkownikowi i znane jest tylko użytkownikowi, który się nim posługuje.

11. Administrator Systemów Informatycznych przekazuje użytkownikowi identyfikator i hasło.

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

Rozdział 3.

Procedura odbierania uprawnień do przetwarzania danych w systemie informatycznym

§ 3. 1. 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. Administrator Danych Osobowych dokonuje, na podstawie informacji przekazanej przez IDO, odebrania lub zmiany zakresu upoważnienia, IDO zaś dokonuje odebrania lub zmiany zakresu uprawnień w systemie informatycznym. O powyższym IDO 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.

Rozdział 4.

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

§ 4. 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 ASI.

Rozdział 5.

Procedura rozpoczęcia, zawieszenia i zakończenia pracy przeznaczona dla użytkowników systemu

§ 5.1. 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 ASI.

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 niepodejrzanie 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 oraz zdaje klucz do sekretariatu.

Rozdział 6.

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

§ 6. 1. Za tworzenie i przechowywanie kopii zapasowych odpowiedzialny jest ASI.

2. Kopie zapasowe systemów przetwarzających dane osobowe są codziennie zapisywane na taśmy magnetyczne. 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. IOD 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.

Rozdział 7.

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

§ 7. 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 zamkniętych szafach i meblach biurowych. ASI 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 potwierdzone jest protokołem przechowywanym przez ASI.

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

1) zawarcia umowy;

2) zagwarantowania poufności danych przez usługodawcę;

3) umożliwienia prowadzenia nadzoru nad procesem niszczenia nośników przez ASI lub upoważnionego przez niego pracownika Urzędu;

4) udokumentowania faktu zniszczenia nośników protokołem.

Rozdział 8.

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

§ 8. 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 IOD;

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 ABI. 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.

Rozdział 9.

Odnoszenie informacji o udostępnieniu danych osobowych

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

2. Odnoszenie faktu udostępnienia danych następuje:

1) w przypadku [...] poprzez wprowadzenie przez użytkownika w polu [...] informacji o udostępnieniu danych,

2) w przypadku [...] poprzez wprowadzenie przez użytkownika w polu [...] informacji o udostępnieniu danych.

3. 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.

Rozdział 10.

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

§ 10. 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 potwierdzone 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 ASI.

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.