

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

§ 1

Za przestrzeganie w Powiatowym Centrum Pomocy Rodzinie w Tucholi zapisów „instrukcji” odpowiedzialny jest Administrator danych.

§2

W związku z tym, że w Powiatowym Centrum Pomocy Rodzinie w Tucholi przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną, oraz uwzględniając kategorie przetwarzanych danych i zagrożenia wprowadza się poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym na poziomie **wysokim**.

§3

1. Obszar, w który są przetwarzane dane, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. Przebywanie osób nieuprawnionych w obszarze, w którym są przetwarzane dane, jest dopuszczalne za zgodą Administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
2. W systemie informatycznym służącym do przetwarzania danych osobowych, przetwarzać dane mogą wyłącznie osoby posiadające aktualne upoważnienie nadane przez Administratora danych. Użytkownik przetwarzający dane po otrzymaniu upoważnienia oraz loginu i hasła jest zobowiązany niezwłocznie dokonać zmiany hasła oraz zachować je w tajemnicy. Użytkownik jest zobowiązany do zmiany hasła nie rzadziej niż co 30 dni. Hasło nadane przez użytkownika musi składać się z co najmniej z 6 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
3. Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby: w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator oraz aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.
4. System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:
 - 1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

- poprzez zainstalowanie programu antywirusowego,
- poprzez zainstalowanie firewall (zapora sieciowa),
- poprzez zabezpieczenie sieci radiowej odpowiedniej mocy uwierzytelnieniem.

2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez zastosowanie zasilacza awaryjnego ups.

5. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.

- 1) W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się ono co najmniej z 6 znaków, zawiera małe i wielkie litery oraz cyfry i znaki specjalne.
- 2) Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie wszystkich danych osobowych muszą być tworzone nie rzadziej niż raz na tydzień

6. Kopie zapasowe:

- 1) Przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w pomieszczeniu zamkniętym nr 010 zaopatrzonym w system alarmowy i monitoring.
- 2) Usuwa się niezwłocznie po ustaniu ich użyteczności.

7. Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych w tym stosuje hasła dostępu do komputera przenośnego.

8. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

- 1) Likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
- 2) Przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
- 3) Naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.

§4

1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym — z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie — system ten zapewnia odnotowanie:

- 1) daty pierwszego wprowadzenia danych do systemu;

- 2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba.
2. Odnotowanie informacji, o których mowa w ust. 1 pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.
4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt 4, mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

§5

Po zakończeniu pracy w systemie informatycznym użytkownik ma obowiązek wylogować się z systemu. W przypadku braku czynności ze strony użytkownika w systemie informatycznym przez 10 min, system samoczynnie wyloguje użytkownika przetwarzającego dane osobowe.

§6

W sprawach nieuregulowanych w niniejszej „instrukcji” mają zastosowanie przepisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 7 kwietnia 2016 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).

