Instrukcja nr 2 do Polityki bezpieczeństwa danych w systemach informacyjnych.

Instrukcja

w sprawie ochrony danych w systemach informacyjnych (kartotekowych i informatycznych) Instytutu Matki i Dziecka.

§ 1 Niniejsza instrukcja przeznaczona jest dla osób gromadzących i przetwarzających dane, w tym dane osobowe zwykłe lub dane szczególnej w Instytucie (dalej dane osobowe) Matki i Dziecka z wykorzystaniem papierowego i elektronicznego nośnika informacji. Instrukcja wynika z wprowadzonej Polityki bezpieczeństwa danych w systemach informacyjnych, jest zgodna z dotychczasowymi regulacjami dotyczącymi trybu przetwarzania danych osobowych w systemach informacyjnych.

§ 2

Niniejsza instrukcja określa:

1. Zasady postępowania przy przetwarzaniu danych w tym danych osobowych.
2. Prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych.
3. Zabezpieczenie zbiorów danych osobowych.
4. Odpowiedzialność za naruszenie przepisów ustawy o ochronie danych osobowych i aktów wykonawczych.

§ 3

1. Dane w tym dane osobowe zwykłe mogą być przetwarzane w:
    a) systemach informatycznych;
    b) kartotekach, skorowidzach, księgach, wykazach, zestawieniach, raportach i innych zbiorach ewidencyjnych w tym medycznych;
    c) Przetwarzanie danych osobowych jest dopuszczalne tylko gdy spełniony jest, co najmniej jedna z przesłanek wymienionych w art. 6 (dane zwykłe) lub 9 (dane szczególnej kategorii) RODO.
2. Zaleca się szczególną ostrożność przy przetwarzaniu niezbędnych, do realizacji zadań Instytutu, danych szczególnej kategorii.

§ 4

1. Dostęp do dokumentów i systemów informatycznych zawierających dane osobowe mają wyłącznie pracownicy, którzy:
    a) posiadają pisemne upoważnienie;
    b) odbyli szkolenie z przepisów dotyczących ochrony danych osobowych;
2. Dane osobowe mogą być przetwarzane przez uprawnioną osobę w zakresie określonym w upoważnieniu do przetwarzania danych osobowych.
3. Wzór upoważnienia, o którym mowa w ust.1 określa załącznik nr 1 do Polityki bezpieczeństwa danych w systemach informacyjnych.
4. Pracownicy, którzy nie przetwarzają danych osobowych składają oświadczenie o zapoznaniu się z przepisami dotyczącymi ochrony danych oraz ich przestrzeganiu.
5. Ewidencję osób upoważnionych, które mają dostęp do danych osobowych oraz przeszkolonych bez upoważnienia do przetwarzania danych prowadzi Inspektor Ochrony Danych.

§ 5

Inspektor Ochrony Danych każdorazowo po udzieleniu pracownikowi upoważnienia dostępu do danych osobowych zapoznaje go z obowiązującymi przepisami w zakresie danych osobowych w tym o odpowiedzialności karnej za ich naruszenie. §6

Pracownicy posiadający upoważnienie dostępu do danych osobowych zobowiązani są do:

1. Rygorystycznego przestrzegania zasad i sposobu postępowania z dokumentami i systemami informatycznymi zawierającymi dane osobowe.
2. Zgłaszania bezpośrednim przełożonym wszystkich dostrzeżonych przypadków naruszenia zasad ochrony danych osobowych.

§ 7

Przekazywanie danych osobowych może być realizowane wyłącznie na zasadach określonych w RODO.

§ 8

Formą technicznego zabezpieczenia pomieszczeń i urządzeń, w których przetwarzane są dane, w tym dane osobowe, jest właściwe postępowanie z kluczami użytku bieżącego oraz zapasowymi. Wykaz osób upoważnionych do pobierania kluczy aktualizuje upoważniony pracownik Działu Administracyjnego, który jest także odpowiedzialny za organizowanie napraw oraz uzupełniania niezbędnych zamków i kluczy.
Klucze użytku bieżącego do pomieszczeń, w których przetwarzane są dane, a zwłaszcza dane osobowe po zakończeniu pracy podlegają zdaniu na portierni pracownikom ochrony (z wyłączeniem pracowników zatrudnionych w systemie czasu pracy równoważnej, którzy przekazują klucze w ramach przekazania obowiązków na stanowisku umieszczając informacje na ten temat w prowadzonych raportach).
Zasady użytkowania kluczy są następujące:

a. Ewidencja osób uprawnionych do pobierania kluczy od konkretnych pomieszczeń znajduje się w portierni Instytutu Matki i Dziecka i stanowi podstawę do wydawania kluczy. Odpowiedzialny za jej aktualizację jest Kierownik Działu Administracyjnego.
b. Wydawanie i przyjmowanie kluczy upoważnionym osobom odbywa się po dokonaniu wpisu do książki poboru kluczy znajdującej się na portierni i potwierdzeniu pobrania poprzez złożenie podpisu.
c. Przed otwarciem pomieszczeń biurowych pracownik sprawdza wizualnie stan zabezpieczenia pomieszczenia.
d. Po otwarciu pomieszczeń biurowych, jeszcze przed przystąpieniem do pracy, pracownicy sprawdzają stan zastosowanych zabezpieczeń sprzętu biurowego, urządzeń, a także przechowywanej w tych pomieszczeniach dokumentacji.
e. W przypadku stwierdzenia zmian lub naruszenia stanu zabezpieczeń, o których mowa w ust. a, b i c pracownik, który to stwierdził, natychmiast powiadamia o tym kierownika jednostki lub komórki organizacyjnej.
f. Po zakończeniu pracy, pracownicy zobowiązani są do uporządkowania swoich stanowisk pracy (zasada czystego biurka) oraz wykonania czynności zabezpieczających, które polegają na:
    1.) zabezpieczeniu dokumentacji;
    2.) wyłączeniu systemów i urządzeń informatycznych;
    3.) wyłączeniu wszystkich urządzeń energetycznych zasilanych energią elektryczną;
    4.) zamknięciu okien i drzwi.
g. Klucze do pomieszczeń i znajdujących się tam urządzeń do przetwarzania danych podlegających szczególnej ochronie. Sposób ochrony określa Instrukcja ochrony obiektu Instytutu Matki i Dziecka sporządzona przez agencje ochrony po uzyskaniu akceptacji Dyrektora Instytutu.
h. Sposób postępowania z kluczami i zabezpieczenie pomieszczenia kancelarii niejawnej regulują odrębne przepisy.
i. W czasie pracy klucze należy przechowywać w miejscu niedostępnym dla osób postronnych (w szafkach, biurkach itp.).

4. Zabrania się pozostawiania kluczy w zamkach drzwi, sejfów itp. oraz wynoszenia kluczy od pomieszczeń i urządzeń poza siedzibę Instytutu Matki i Dziecka.

Poza kluczami użytku bieżącego wykorzystywane są także klucze zapasowe, których użytkowanie jest następujące:

a. Kluczy zapasowych używa się w przypadku ewakuacji sprzętu i wyposażenia spowodowanej atakiem terrorystycznym, klęską żywiołową lub na polecenie Administratora Danych, Inspektora Ochrony Danych lub jego Zastępcy.
b. Komplety kluczy znajdują się zabezpieczonych pojemnikach (woreczkach) w portierni Instytutu Matki i Dziecka.
c. Wydawanie zdeponowanych kluczy zapasowych odbywa się wyłącznie za zgodą osób wymienionych w ustępie a, lub osób zastępujących. W przypadku nieobecności pracownika odpowiedzialnego za pobranie kluczy, wydanie ich innej upoważnionej doraźnie osobie odnotowuje się w oddzielnym dokumencie. Otwarcia pomieszczenia (urządzenia np. szafy), dokonuje powołana komisja, która w protokole odnotowuje: imienny skład komisji, przyczynę, okoliczności i datę zdarzenia. Wzór protokołu otwarcia znajduje się w załączniku do niniejszej instrukcji.

§ 10

1. Urządzenia i systemy informatyczne służące do przetwarzania danych, a zwłaszcza danych osobowych zabezpiecza się poprzez:
    a) urządzenia sprzętowe takie jak routery i przełączniki sieciowe, które umożliwiają nadzór i kontrolę ruchu w sieci komputerowej;
    b) specjalistyczne oprogramowanie antywirusowe, antyspamowe;
    c) konieczność uwierzytelnienia użytkowników, przy pomocy osobistych loginów i haseł.
2. Urządzenia (sprzęt komputerowy) i systemy informatyczne służące do przetwarzania danych, a zwłaszcza danych osobowych lub danych medycznych oraz inne oprogramowanie winny być ustawiane, instalowane i konfigurowane przez upoważnione do tego osoby.
3. Zabrania się instalacji oprogramowania na urządzeniach przez osoby do tego nieupoważnione.
4. Urządzenia, na których przetwarzane są dane, a zwłaszcza dane osobowe lub dane medyczne powinny być tak ustawione w pomieszczeniu, aby osoby postronne wchodzące do pomieszczenia oraz osoby znajdujące się poza pomieszczeniem, ale mogące w sposób techniczny lub fizyczny zobaczyć wnętrze pomieszczenia, nie miały możliwości zobaczenia treści danych znajdujących się na monitorze urządzenia.
5. Systemy informatyczne i urządzenia, na których te systemy pracują, powinny umożliwiać uwierzytelnienie użytkowników eliminując w ten sposób możliwość przetwarzania danych, a zwłaszcza danych osobowych, które nie zostały upoważnione i uwierzytelnione.
6. Każde odejście od pracującego urządzenia i systemu informatycznego wymaga zabezpieczenia przed dostępem osób trzecich. W tym celu systemy informatyczne i urządzenia zabezpiecza się poprzez blokady programowe systemu lub urządzenia, wyłączenie systemu, wyłączenie urządzenia.
7. Zabrania się pozostawiania uruchomionych urządzeń (sprzętu komputerowego) i systemów informatycznych bez nadzoru osoby przetwarzającej dane, a zwłaszcza dane osobowe lub dane medyczne, która została na nich uwierzytelniona.
8. Każda osoba przetwarzająca dane, a zwłaszcza dane osobowe w systemie informatycznym musi posiadać swój własny identyfikator i hasło, którym uwierzytelnia/identyfikuje się w systemie. Jeżeli system nie posiada takiego zabezpieczenia, należy wprowadzić zabezpieczenia dostępu do systemu operacyjnego urządzenia oraz samego urządzenia.

9. Zabrania się wszelakiego zapisywania haseł oraz udostępniania i przekazywania haseł innym uprawnionym i nieuprawnionym osobom.
10. Szczegółowe zasady postępowania z systemami informatycznymi zawarte są w „Instrukcji zarządzania systemami informatycznymi w Instytucie Matki i Dziecka" będącej integralną częścią Polityki bezpieczeństwa danych w systemach informacyjnych.

§ 11

Na czas remontu pomieszczeń, naprawy urządzeń i sprzętu oraz w czasie innych okoliczności zakłócających normalny tok pracy, Kierownik jednostki lub komórki organizacyjnej jest zobowiązany do spowodowania należytego zabezpieczenia (wnioskowania o zabezpieczenie przez wyspecjalizowane komórki i pracowników) dokumentów i systemów informatycznych zawierających dane w tym dane osobowe lub dane medyczne.

§ 12

Kierownik jednostki lub komórki organizacyjnej, w których przetwarzane są dane w tym dane osobowe lub dane medyczne, zobowiązany jest do egzekwowania od podległych pracowników, aby po zakończeniu pracy należycie zabezpieczali dokumenty i systemy informatyczne zawierające dane, a zwłaszcza dane osobowe lub dane medyczne. § 13

Pracownik, który został upoważniony do dostępu do danych osobowych w przypadku przejścia na inne stanowisko pracy lub rozwiązania stosunku zobowiązany jest do rozliczenia się z dokumentów zawierających dane osobowe oraz identyfikatorów i haseł do systemów informatycznych.

§ 14

Inspektor Ochrony Danych w szczególnie uzasadnionych przypadkach może wyrazić zgodę na przechowywanie dokumentów zawierających dane osobowe poza pomieszczeniami do tego wyznaczonymi, pod warunkiem zagwarantowania ich właściwego zabezpieczenia. § 15

1. Przesyłki zawierające dane osobowe, dane medyczne są wysyłane jako polecone ze zwrotnym potwierdzeniem odbioru oraz zabezpieczone w sposób uniemożliwiający zapoznanie się z ich treścią przez osoby nieupoważnione.
2. Przy postępowaniu z dokumentami zawierającymi dane w tym dane osobowe zastosowanie ma „Instrukcja kancelaryjna dla Instytutu Matki i Dziecka w Warszawie", „Instrukcja w sprawie organizacji i zakresie działania archiwum zakładowego" oraz inne zarządzenia i instrukcje regulujące działalność Instytutu Matki i Dziecka.
3. Dokumentacja zawierająca dane osobowe, może być udostępniana zgodnie z obowiązującymi przepisami prawa w sposób uniemożliwiający zapoznanie się z ich treścią przez osoby nieuprawnione.
4. Przekazywanie dokumentu zawierającego dane osobowe, pomiędzy uprawnionymi jednostkami, komórkami organizacyjnymi lub pracownikami Instytutu, powinno odbywać się w zakresie niezbędnym do wykonywania obowiązków służbowych, z zachowaniem zasad obiegu dokumentów w Instytucie Matki i Dziecka. Sposób przekazania dokumentu powinien uniemożliwić ewentualne nieuprawnione zapoznanie się z jego treścią, kradzież, zgubienie lub zniszczenie.

§ 16

1. Dokumenty zawierające dane osobowe są archiwizowane lub we właściwym czasie niszczone komisyjnie w warunkach gwarantujących zabezpieczenie danych osobowych, w sposób uniemożliwiający ich odtworzenie, na podstawie decyzji Administratora Danych.
2. Niszczenie dokumentów (materiałów, nośników) zawierających dane osobowe odbywa się zgodnie z normą DIN 66399 opracowaną przez Standards Committee for Information Technology and Applications (NIA), która zastąpiła normę DIN 32757-1:995-01, która miała zastosowanie wyłącznie do sposobu niszczenia nośników papierowych.
3. W przypadku dokumentów papierowych niszczenie odbywa się z wykorzystaniem, niszczarek o poziomie bezpieczeństwa, co najmniej P-2 (były DIN-2, szerokość paska papieru nie większa

niż 6 mm, długość paska nielimitowana, powierzchnia ogółem nie większa niż 800mm^2). Materiały zniszczone w ten sposób mogą być przekazywane do utylizacji.

4. Wskazane jest sukcesywne wprowadzanie niszczarek o poziomie bezpieczeństwa P-3 (była norma DIN 3, szerokość ścinka nie większa niż 2mm, powierzchnia ścinka nie większa niż 320 mm^2) do niszczenia nośników zawierających szczególnie wrażliwe i poufne (w rozumieniu ustawy o ochronie danych osobowych i tajemnic zawodowych)
5. Niedopuszczalne jest przekazywanie materiałów na nośnikach papierowych zawierających dane osobowe, dane medyczne do utylizacji bez ich uprzedniego zniszczenia w wyżej opisany sposób.
6. W przypadku dokumentów umieszczonych na elektronicznych nośnikach informacji ich niszczenie polega na usunięciu dokumentu z nośnika, (jeżeli nośnik na to pozwala i umożliwia dalszą pracę z nośnikiem), a w innych przypadkach na fizycznym lub magnetycznym zniszczeniu nośnika przez upoważnione osoby z Działu Informatyki zgodnie z wyżej wymienionymi normami.
7. Niedopuszczalne jest przekazywanie urządzeń (komputerów) zawierających dyski twarde oraz innych magnetycznych nośników informacji, na których przetwarzane były dane, dane osobowe, dane medyczne do odsprzedania lub utylizacji bez ich uprzedniego zniszczenia w wyżej opisany sposób.

§ 17

Wykazy i spisy zdawczo-odbiorcze dokumentów zawierających dane osobowe przekazywane są do Archiwum Zakładowego gdzie przechowuje się także protokoły zniszczenia dokumentów.

Załącznik nr 1
do Instrukcji w sprawie ochrony danych w systemach informacyjnych (kartotekowych i informatycznych) Instytutu Matki i Dziecka.

PROTOKÓŁU OTWARCIA POMIESZCZENIA (wzór)

„WYRAŻAM ZGODĘ NA OTWARCIE POMIESZCZENIA/POMIESZCZEŃ/SZAFY/SEJFU

Warszawa, dnia ….……..……

Egz. Nr .....

PROTOKÓŁ

wydania kluczy zapasowych oraz komisyjnego otwarcia/zamknięcia pomieszczenia/szafy/sejfu* pod nieobecność wykonawcy

Na polecenie ……..w dniu ……..… komisja w składzie:

1. …… 2.
…… 3.
……

pobrała klucze zapasowe i dokonała nimi otwarcia pomieszczenia/szafy/sejfu* będącego w dyspozycji ……,

(opis pomieszczenia/szafy/sejfu)

opieczętowanego pieczęcią numerową/plombą nr ……*
i pobrano ……
……..
Powyższe ……...
…….. wydano ……
……. - …….

(imię i nazwisko osoby pobierającej) (czytelny podpis)

Po dokonaniu w/w czynności pomieszczenie/szafa/sejf* zostały zamknięte i zaplombowane pieczęcią numerową ……...
Klucze przekazano ……

Podpisy członków komisji:

1. .....
2. .....
3. .....

*niepotrzebne skreślić