INSTRUKCJA
ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM
SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH
W FIRMIE MKPUBLIKACJE

obowiązuje od 25 maja 2018 r.

SPIS TREŚCI

Rozdział 1
Postanowienia ogólne

§1

Stosownie do postanowień §3 i §5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 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), ustala się treść Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w firmie MKPUBLIKACJE, zwaną dalej Instrukcją.

§2

Instrukcja ma zastosowanie na obszarze wskazanym w Polityce bezpieczeństwa przetwarzania danych osobowych w firmie MKPUBLIKACJE (dalej Polityka bezpieczeństwa), w którym przetwarzane są dane osobowe w systemie informatycznym.

§3

Administrator danych osobowych za pośrednictwem Administratora Systemu Informatycznego sprawuje ogólną kontrolę i nadzór nad przestrzeganiem postanowień instrukcji, a w szczególności:

1) sporządza kopie bezpieczeństwa dla baz sieciowych;
2) pozbawia urządzenia i inne nośniki informacji przeznaczone do likwidacji zapisu danych lub – gdy nie jest to możliwe – uszkadza je trwale w sposób uniemożliwiający odczytanie danych;
3) nadzoruje usuwanie awarii sprzętu komputerowego w sposób zapewniający bezpieczeństwo przetwarzanych danych osobowych;
4) zabezpiecza zbiory danych osobowych wysyłanych poza obszar określony w Polityce bezpieczeństwa;
5) sprawuje nadzór nad fizycznym zabezpieczeniem pomieszczeń, w których przetwarzane są dane osobowe;
6) sprawuje nadzór nad czynnościami związanymi z ochroną przeciwwirusową, czynnościami serwisowymi dotyczącymi systemu informatycznego, w którym przetwarzane są dane osobowe;
7) nadzoruje obieg i przetwarzanie wydruków z systemu informatycznego zawierających dane osobowe;
8) podejmuje i nadzoruje wszelkie inne działania zmierzające do zapewnienia bezpieczeństwa przetwarzanych w systemie informatycznym danych osobowych.

§4

Ilekroć w Instrukcji jest mowa o:

1) **systemie informatycznym** – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
2) **zabezpieczeniu systemu informatycznego** – należy przez to rozumieć zastosowane środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, mające na celu w szczególności zabezpieczenie danych przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, zmianą, utratą uszkodzeniem lub zniszczeniem;
3) **zbiorze danych osobowych** – rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
4) **przetwarzaniu danych** – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
5) **usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
6) **administratorze danych osobowych (ADO)** – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, decydujące o celach i środkach przetwarzania danych osobowych;
7) **administratorze bezpieczeństwa informacji (ABI)** – rozumie się przez to osobę wyznaczoną przez administratora danych, nadzorującą przestrzeganie zasad ochrony danych osobowych, w

szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
8) **administratorze systemu informatycznego (ASI)** – należy przez to rozumieć osobę, o której mowa w rozdziale 2;
9) **użytkowniku** – rozumie się przez to upoważnionego przez administratora danych, wyznaczonego do przetwarzania danych osobowych pracownika;
10) **identyfikator użytkownika (login)** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
11) **hasło** – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
12) **uwierzytelnianie** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
13) **nośniki danych osobowych** – dyskietki, płyty CD lub DVD, pamięć flash, dyski twarde, taśmy magnetyczne lub inne urządzenia/materiały służące do przechowywania plików z danymi.

Rozdział 2
Administrator Systemu Informatycznego
§5

ASI wyznaczany jest przez ADO drogą pisemnego upoważnienia. W przypadku nie wyznaczenia ASI, jego funkcję pełni osoba pełniąca funkcję ADO. Wzór upoważnienia ASI stanowi załącznik nr 1 do niniejszego dokumentu. ASI jest również zobowiązany do podpisania oświadczenia, stanowiącego załącznik nr 4 i 5 do Polityki Bezpieczeństwa.

§6

ASI jest odpowiedzialny za przestrzeganie zasad bezpieczeństwa przetwarzania danych osobowych w zakresie systemu informatycznego służącego do tego celu. Do obowiązków ASI należy także kontrola przepływu informacji pomiędzy systemem informatycznym, a siecią publiczną oraz kontrola działań inicjowanych z sieci publicznej i systemu informatycznego. Obowiązkiem ASI jest również zabezpieczenie sprzętu komputerowego przed nieuprawnionym dostępem oraz przeprowadzanie analizy ryzyka uwzględniającej realne zagrożenia dla systemu informatycznego.

Rozdział 3
Zakres przedmiotowy instrukcji
§7

Niniejsza Instrukcja zawiera w szczególności:
1) sposób przydziału haseł dla użytkowników i częstotliwości ich zmiany oraz wskazania osób odpowiedzialnych za te czynności;
2) sposób rejestrowania i wyrejestrowywania użytkowników oraz wskazania osób odpowiedzialnych za te czynności;
3) procedury rozpoczęcia, zawieszenia i zakończenia pracy;
4) metody i częstotliwość tworzenia kopii awaryjnych;
5) metodę i częstotliwość sprawdzania obecności wirusów komputerowych oraz metodę ich usuwania;
6) sposób i czas przechowywania nośników informacji, w tym kopii informatycznych i wydruków;
7) sposób dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych;
8) sposób postępowania w zakresie komunikacji w sieci komputerowej.

§8

Działaniem Instrukcji objęci są:
1) administrator danych osobowych;
2) administrator bezpieczeństwa informacji;
3) administrator systemu informatycznego;
4) osoby zatrudnione przy przetwarzaniu danych osobowych.

Rozdział 4
Nadawanie uprawnień do przetwarzania danych oraz ich rejestrowanie w systemie informatycznym

§9

1) Użytkownikiem systemu informatycznego może być jedynie osoba posiadająca odpowiednie upoważnienie i zarejestrowana w rejestrze użytkowników.
2) Rejestr użytkowników systemu prowadzi administrator danych osobowych lub administrator bezpieczeństwa informacji.
3) Każdy zarejestrowany użytkownik korzysta z przydzielonego mu konta użytkownika, opatrzonego identyfikatorem i hasłem dostępu.
4) Użytkownik zamierzający przetwarzać dane osobowe, po uzyskaniu upoważnienia stanowiącego załącznik nr 3 do Polityki Bezpieczeństwa, oraz podpisaniu oświadczenia stanowiącego załącznik nr 4 i 5 do Polityki Bezpieczeństwa, składa ustnie wniosek do ASI o nadanie identyfikatora i hasła w celu umożliwienia wykonywania przetwarzania danych osobowych w systemie informatycznym, ASI zobowiązany jest niezwłocznie przydzielić użytkownikowi identyfikator i hasło. Podanie użytkownikowi hasła nie może nastąpić w sposób umożliwiający zapoznanie się z nim osobom trzecim.
5) Nadawanie identyfikatorów i przydzielanie haseł:
   a) w celu jednoznacznego określenia użytkowników przyjmuje się następującą metodologię nadawania nazw kont: pierwsza litera imienia + nazwisko (nie używając polskich znaków i wielkich liter);
   b) hasło składa się z co najmniej 8 znaków; zalecane jest, aby zawierało małe i wielkie litery oraz cyfry i znaki specjalne;
   c) zmiana hasła powinna być wykonywana nie rzadziej niż co 30 dni. W systemie informatycznym zapewnia się automatyczne wymuszanie zmiany hasła,
   d) identyfikator użytkownika powinien być inny dla każdego użytkownika, a po jego wyrejestrowaniu z systemu informatycznego, nie powinien być przydzielany innej osobie;
   e) identyfikatory użytkowników ujawnione są w wykazie osób upoważnionych do przetwarzaniu danych osobowych;
   f) hasła pozostają tajne, każdy użytkownik jest zobowiązany do zachowania w tajemnicy swego hasła, także po jego zmianie;
   g) obowiązek ten rozciąga się także na okres po upływie ważności hasła;
   h) hasło, co do którego zaistniało choćby podejrzenie ujawnienia powinno być niezwłocznie zmienione przez użytkownika;
   i) utrata upoważnienia do przetwarzania danych osobowych, powoduje natychmiastowe usunięcie z grona użytkowników systemu informatycznego.

§10

W przypadku wygaśnięcia przesłanek uprawniających użytkownika do przetwarzania danych osobowych, w szczególności cofnięcia upoważnienia, stanowiącego załącznik nr 3 do Polityki Bezpieczeństwa, ASI zobowiązany jest do dopełnienia czynności uniemożliwiających ponowne wykorzystanie identyfikatora użytkownika, którego uprawnienia wygasły.

§11

1) Indywidualny zakres czynności osoby upoważnionej przy przetwarzaniu danych osobowych powinien określać zakres odpowiedzialności tej osoby za ochronę tych danych przed:
   a) niepowołanym dostępem;
   b) nieuzasadnioną modyfikacją lub zniszczeniem;
   c) nielegalnym ujawnieniem;
   d) pozyskaniem – w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu danych osobowych.
2) Jeżeli istnieje taka możliwość, ekrany monitorów, na których możliwy jest dostęp do danych osobowych, powinny być automatycznie wyłączane po upływie ustalonego czasu nieaktywności użytkownika.
3) Monitory komputerów powinny być tak ustawione, aby uniemożliwić osobom postronnym wgląd do danych osobowych.

Rozdział 5
Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym

§12

1) Przed rozpoczęciem pracy w systemie informatycznym użytkownik zobowiązany jest do:
   a) zalogowania się do systemu z wykorzystaniem zastrzeżonych tylko dla siebie: identyfikatora i hasła w sposób uniemożliwiający ich ujawnienie osobom postronnym – hasło nie może zawierać mniej niż 8 znaków, osoba je tworząca obowiązana jest uczynić to w taki sposób, aby utrudnić jego ewentualne odczytanie, poprzez wprowadzenie do hasła: znaków szczególnych, cyfr, dużych liter itd.;
   b) sprawdzenia prawidłowości funkcjonowania sprzętu komputerowego i systemów, na swoim stanowisku pracy;
   c) w razie stwierdzenia nieprawidłowości, do powiadomienia o tym fakcie bezpośredniego przełożonego oraz ASI;
   d) w razie stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub stanu wskazującego na istnienie takiej możliwości, do podjęcia odpowiednich kroków stosownie do zasad postępowania w sytuacji naruszenia zabezpieczenia danych osobowych.
2) Przerywając przetwarzanie danych użytkownik powinien co najmniej: aktywować wygaszasz ekranu lub w inny sposób zablokować możliwość korzystania ze swego konta użytkownika przez inne osoby. Zalecane jest w takich przypadkach:
   a) skorzystanie z mechanizmu czasowej blokady dostępu do komputera poprzez uruchomienie wygaszacza ekranu z hasłem (hasło powinno być zbieżne z hasłem logowania do systemu);
   b) zakończenie pracy w systemie informatycznym – wylogowanie się z systemu.
3) Po zakończeniu przetwarzania danych osobowych w danym dniu, osoba upoważniona zobowiązana jest do:
   a) zakończenia pracy w systemie informatycznym;
   b) wylogowania się z systemu informatycznego;
   c) wyłączenia sprzętu komputerowego oraz zamknięcia szaf, w których przechowuje się nośniki, na których utrwalone są dane osobowe;
   d) zamknięcia pomieszczeń.
4) Nośniki informacji oraz wydruki z danymi osobowymi, które nie są przeznaczone do udostępnienia, przechowuje się w warunkach uniemożliwiających dostęp do nich osobom niepowołanym.

Rozdział 6
Kopie bezpieczeństwa
§13

1) Kopie bezpieczeństwa powinny być wykonywane codziennie (od poniedziałku do piątku).
2) Kopie bezpieczeństwa powinny być zapisywane na zewnętrznych nośnikach – nie mogą być przechowywane na tym samym dysku / komputerze, na którym istnieje oryginalna kopia danych.
3) Kopie bezpieczeństwa powinny być przechowywane w sejfie lub w przypadku braku takiej możliwości w zamkniętych szafach, znajdujących się w pomieszczeniach, które również są zamykane na klucz lub chmurze obliczeniowej w postaci zaszyfrowanej.
4) Kopie bezpieczeństwa nie powinny być przechowywane w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.
5) Osobą odpowiedzialną za tworzenie kopii zapasowych jest ASI.
6) Tworzone kopie bezpieczeństwa powinny być opisane w sposób pozwalający na określenie ich zawartości.
7) Kopie bezpieczeństwa należy okresowo sprawdzać pod kątem ich dalszej przydatności do odtworzenia danych w przypadku awarii systemu oraz bezzwłocznie usuwać po ustaniu ich użyteczności.
8) Kopie bezpieczeństwa, które uległy uszkodzeniu lub stały się niepotrzebne pozbawia się zapisu danych w sposób uniemożliwiający ich odtworzenie.
9) Jeżeli pozbawienie zapisu nie jest możliwe, kopie są niszczone w sposób uniemożliwiający odczytanie bądź odtworzenie danych zawartych na nośniku kopii.

§14

Urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, powinny być zabezpieczone przed utratą tych danych wskutek awarii zasilania lub zakłóceń w sieci zasilającej. Zabezpieczenie to powinno być tak skonstruowane, by umożliwiało zapisanie danych we wszystkich uruchomionych aplikacjach i wykonanie kopii bezpieczeństwa.

Rozdział 7
Sposób i czas przechowywania oraz zasady likwidacji nośników informacji
§15

1) Wydruki komputerowe z systemu, zawierające dane osobowe są sporządzane jedynie dla celów operacyjnych.
2) Wydruk komputerowy z systemu, zawierający dane osobowe, po odpowiednim opisaniu i oznaczeniu, podlega zasadom ochrony danych osobowych przetwarzanych metodami tradycyjnymi.
3) Wydruki ze zbiorów danych osobowych tworzone i używane do celów roboczych, (operacyjnych) przechowywane są w zamykanych szafach.
4) Nośniki magnetyczne, optyczne i inne nośniki informatyczne, zawierające dane osobowe, przechowywane są w odpowiednich, przeznaczonych do tego zamykanych szafach.
5) Likwidacja wydruków z systemu, zawierających dane osobowe odbywa się za pomocą niszczarki do dokumentów lub w inny sposób, trwale uniemożliwiający odczytanie danych.
6) Z urządzeń, dysków lub innych nośników informatycznych, które zostały przeznaczone do przekazania innemu podmiotowi, usuwa się zapisane na ich dane.

Rozdział 8
Ochrona antywirusowa
§16

1) Ochrona antywirusowa jest realizowana poprzez zainstalowanie odpowiedniego oprogramowania antywirusowego.
2) W przypadku wykrycia wirusa komputerowego, użytkownik systemu zobowiązany jest do natychmiastowego poinformowania o tym fakcie ASI.
3) System informatyczny podlega regularnej (co najmniej raz w tygodniu), kontroli pod kątem obecności wirusów komputerowych.
4) Wykryte zagrożenia usuwa się niezwłocznie z systemu informatycznego.
5) Przed przystąpieniem do unieszkodliwienia wirusa, należy zabezpieczyć dane zawarte w systemie przed ich utratą.
6) Osobą odpowiedzialną za powyższe działania jest ASI.

Rozdział 9
Konserwacja i naprawa systemu przetwarzającego dane osobowe
§17

Stosuje się następujące procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych:

1) ASI raz na 3 miesiące wykonuje generalny przegląd systemu informatycznego, polegający na ustaleniu poprawności działania tych jego elementów, które są niezbędne do zapewnienia realizacji funkcji wynikających z niniejszej Instrukcji;
2) w przypadku stwierdzenia przez ASI nieprawidłowości w działaniu elementów systemu podejmuje on niezwłocznie czynności zmierzające do przywrócenia ich prawidłowego działania;
3) jeżeli do przywrócenia prawidłowego działania systemu niezbędna jest pomoc podmiotu zewnętrznego, wszelkie czynności na sprzęcie komputerowym dokonywane w obszarze przetwarzania danych osobowych, powinny odbywać się w obecności ASI lub w sytuacji wyjątkowej – osoby przez niego wyznaczonej.

§18

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 ASI.

Rozdział 10
Sposoby postępowania w zakresie komunikacji w sieci komputerowej
§19

1) Wszelkie pliki zawierające kopie danych osobowych zawartych w systemie, wysyłanych poza system, muszą być zabezpieczone hasłem;
2) W miarę możliwości, dane osobowe zawarte na serwerze sieciowym nie mogą być przechowywane na stacjach roboczych. Należy dane te umieszczać na dysku sieciowym;
3) Nieuzasadnione kopiowanie danych z serwera na stacje robocze bądź na nośniki informatyczne jest zabronione.

Rozdział 11
Zasady korzystania z komputerów przenośnych
§20

1) Osoba użytkująca przenośny komputer, służący do przetwarzania danych osobowych, obowiązana jest zachować szczególną ostrożność podczas transportu i przechowywania tego komputera poza obszarem, przeznaczonym do przetwarzania danych osobowych wskazanym w Polityce bezpieczeństwa.
2) W celu zapobieżenia dostępowi do tych danych osobie niepowołanej, należy:
   a) zabezpieczyć dostęp do komputera hasłem (w przypadku systemu operacyjnego Windows – w sposób który umożliwia to oprogramowanie);
   b) nie zezwalać na używanie komputera osobom nieupoważnionym do dostępu do danych osobowych;
   c) zabezpieczyć aplikacje przetwarzające dane osobowe hasłem.

Rozdział 12
Postanowienia końcowe
§21

W sprawach nieunormowanych stosuje się przepisy ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 poz. 1182 ze zm.) oraz przepisy rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 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).

MK PUBLIKACJE
Marek Kaniewski
09-407 Płock, ul. Powstańców Styczniowych 2A/50
tel. +48 664 600 900
NIP: 888-136-85-88 REGON: 911319334

…… *Płock, 25.05.2018 r.* ……
Miejscowość, data, podpis
Administratora Danych Osobowych

MK PUBLIKACJE
Marek Kaniewski
09-407 Płock, ul. Powstańców Styczniowych 2A/50
tel. +48 664 600 900
NIP: 888-136-85-88 REGON: 911319334

…… *Płock, 25.05.2018 r.* ……
Miejscowość, data, podpis
Administratora Bezpieczeństwa Informacji