Załącznik nr 2 do Zarządzenia nr 7/2018 Dyrektora SP nr 15 z Oddz. Int. w Kielcach

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

w Szkole Podstawowej nr 31
Z Oddziałami Integracyjnymi
w Kielcach

1. Przedmiot instrukcji

Przedmiotem instrukcji jest określenie sposobu zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji określonych w rozporządzeniu 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) oraz Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i ich swobodnego przepływu oraz uchylenia dyrektywy 95/46/WE /Dz. Urz. UE.L nr 119, str. 1/, oraz Ustawą Polską z dnia 10 maja 2018 r. o ochronie danych osobowych.

Instrukcja zawiera ogólne informacje o systemie informatycznym i zbiorach danych osobowych, które przy ich użyciu są przetwarzane, a także opisuje zastosowane rozwiązania techniczne, jak również procedury eksploatacji i zasady użytkowania, jakie zastosowano w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych.

2. Definicje

Zbiór danych osobowych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
Administrator danych osobowych (ADO) - organ, jednostka organizacyjna lub podmiot, decydujące o celach i środkach przetwarzania danych osobowych.
Inspektor ochrony danych (IOD) - osoba wyznaczona przez administratora danych osobowych, odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w jednostce ADO.
Administrator systemu informatycznego (ASI) - osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego do przetwarzania danych osobowych**.**
System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
Ustawa - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i ich swobodnego przepływu oraz uchylenia dyrektywy 95/46/WE /Dz. Urz. UE.L nr 119, str. 1/, oraz Ustawa Polska z dnia 10 maja 2018 r. o ochronie danych osobowych;
Rozporządzenie - rozporządzenie 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. z 2004 r. Nr 100, poz. 1024).
Odbiorca danych - każdy, komu udostępnia się dane osobowe, z wyłączeniem: osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, administratora mającego siedzibę w państwie trzecim, podmiotu, któremu powierzono przetwarzanie danych,

organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

3. Nadawanie uprawnień do przetwarzania danych osobowych.

a) Procedura zarządzania uprawnieniami użytkowników

Procedura opisuje zasady przyznawania, modyfikacji i usuwania uprawnień użytkowników do przetwarzania zbiorów w systemie informatycznym lub w wersji papierowej.

1. Przyznanie, modyfikacja lub cofnięcie upoważnień do przetwarzania danych osobowych w systemie informatycznym lub w zbiorze papierowym realizowane jest przez ADO przy udziale IOD.
   (Załącznik 1 - Zlecenie nadania, modyfikacji uprawnień użytkownika)
2. Przed nadaniem upoważnienia przez ADO, IOD zobowiązany jest do sprawdzenia, czy osoba upoważniona:
   - odbyła szkolenie z zakresu przestrzegania zasad bezpieczeństwa danych osobowych lub została zapoznana z Polityką bezpieczeństwa informacji i Instrukcją zarządzania systemem informatycznym lub z Regulaminem ochrony danych osobowych,
   - podpisała oświadczenie o zachowaniu poufności,
   - będzie przetwarzać dane osobowe w zakresie i celu określonym w upoważnieniu.
3. ADO przy udziale IOD zobowiązany jest do bieżącej aktualizacji upoważnień, a także ich zakresu.
4. Po akceptacji upoważnienia, IOD przekazuje go Informatykowi (ASI) celem nadania identyfikatora oraz uprawnień użytkownika w systemie informatycznym i aplikacjach.
   (Załącznik 2 - Upoważnienie do przetwarzania danych)
5. Każdy użytkownik musi posiadać swój własny indywidualny identyfikator (login).
6. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielany innej osobie.
7. ASI zobowiązany jest po realizacji zlecenia przekazać uzupełniony formularz Upoważnienia do ADO i IOD.
8. IOD odpowiada za przechowywanie i aktualizację wszystkich upoważnień.
9. ADO i IOD opowiada za prowadzenie rejestru osób upoważnionych do przetwarzania danych osobowych.
   (Załącznik 3 - Ewidencja osób upoważnionych do przetwarzania danych)

b) Procedura zarządzania uprawnieniami administratorów

1. ASI powoływany jest przez ADO, jeżeli ASI nie został powołany jego wszystkie obowiązki zostają podzielone pomiędzy ADO i IOD.
   (Załącznik 4 - Powołanie ASI)
2. ASI, jeżeli to możliwe, zobowiązany jest do pracy na koncie nieuprzywilejowanym. Użycie tzw. konta administracyjnego dopuszczalne jest jedynie w sytuacjach awaryjnych lub podczas poważnych zmian wprowadzanych w administrowanym systemie.

c) Procedura dostępu podmiotów zewnętrznych

Procedura opisuje zasady zapewnienia bezpiecznego przetwarzania danych osobowych przez podmioty zewnętrzne, gdy cel i zakres tego przetwarzania określa ADO.

1. ADO i IOD prowadzi rejestr podmiotów zewnętrznych, którym ADO udostępnia dane osobowe oraz podmiotów, którym powierzono przetwarzanie danych osobowych w formie usługi zewnętrznej (outsourcing).
   (Załącznik 5 - Rejestr podmiotów zewnętrznych)
2. ADO powierza do przetwarzania dane osobowe, będące w jego obszarze fizycznym i pod jego pełną kontrolą, podmiotom zewnętrznym w oparciu o umowę powierzenia danych lub umowę poufności. W tej sytuacji podmiot zewnętrzny zobowiązany jest do zachowania poufności powierzonych mu danych i przetwarzania ich zgodnie z celem umowy, wyłącznie w miejscu lub systemie wskazanym przez ADO.
   (Załącznik 6 - Umowa o poufności)
3. ADO powierza dane osobowe do przetwarzania w formie usługi zewnętrznej (outsourcing) podmiotom zewnętrznym w oparciu o umowę powierzenia przetwarzania danych osobowych. W tej sytuacji podmiot zewnętrzny zobowiązany jest do przetwarzania danych zgodnie z zakresem i celem określonym w umowie powierzenia przetwarzania danych osobowych, a także zobowiązany jest do stosowania zabezpieczeń określonych w rozporządzeniu 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).
   (Załącznik 7 – Umowa powierzenia)

4. Metody i środki uwierzytelniania

a) Zasady przydzielania oraz postępowania z hasłami

1. ASI przekazuje użytkownikowi w formie ustnej lub pisemnej tzw. hasło startowe do systemu.
2. Użytkownik w trakcie pierwszego logowania do systemu zobowiązany jest do niezwłocznej zmiany tego hasła.
3. Hasło nie może być powszechnie używanym słowem. W szczególności nie należy używać żadnych popularnych słów, imion, nazw, albo prostych kombinacji klawiszy, zwłaszcza takich, które mogą, w sposób łatwy, być skojarzone z użytkownikiem.
4. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
5. Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.

b) Hasła użytkowników - dostęp do sieci / terminali / serwerów usług

1. Hasło dostępu musi składać się z co najmniej ośmiu znaków.
2. Hasło musi składać się z dużych i małych liter oraz z cyfr lub znaków specjalnych.

3. Zmiana hasła odbywa się nie rzadziej niż co 30 dni.

c) Hasła użytkowników - aplikacje przetwarzające dane osobowe

1. Hasło do programu musi składać się co z najmniej z ośmiu znaków.
2. Hasło musi składać się z dużych i małych liter oraz z cyfr lub znaków specjalnych.
3. Zmiana hasła odbywa się nie rzadziej niż co 30 dni.

d) Hasła administratorów - systemy informatyczne

1. Hasła administratora muszą składać się z co najmniej dwunastu znaków.
2. Hasła muszą składać się z dużych i małych liter oraz z cyfr lub znaków specjalnych.
3. Hasła powinno być znane tylko ASI.
4. ASI powinien prowadzić metrykę haseł.
   (Załącznik 8 – Metryka haseł)
5. Metryka haseł przechowywana jest w miejscu, specjalnie zabezpieczonym do którego dostęp mają wyłącznie ASI oraz ADO. Miejsce przechowywania metryki haseł - gabinet dyrektora szkoły, szafa zamykana na klucz.
6. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.
7. W sytuacjach awaryjnych hasła mogą być przekazane decyzją ADO osobie zastępującej administratora systemu.
8. Po każdorazowym wystąpieniu sytuacji awaryjnej, ASI zobowiązany jest do zmiany tych haseł.

5. Procedura rozpoczęcia, zawieszenia i zakończenia pracy

Procedura opisuje zasady zabezpieczenia danych osobowych przed nieuprawnionym dostępem w sytuacji, gdy użytkownik rozpoczyna, zawiesza lub kończy pracę.

1. Użytkownik rozpoczynając pracę w systemie informatycznym przetwarzającym dane osobowe podaje swój unikalny identyfikator użytkownika oraz swoje hasło.
2. W przypadku zablokowania się przez użytkownika, podczas próby logowania się do systemu, użytkownik ten zobowiązany jest do niezwłocznego powiadomienia o tym fakcie ASI, w celu odblokowania swojego konta.
3. Użytkownik podczas pracy w systemie przetwarzającym dane osobowe zobowiązany jest uniemożliwić osobom nieuprawnionym wgląd w te dane np.: wyświetlane na monitorze komputerowym.
4. W przypadku stwierdzenia przez użytkownika podejrzenia naruszenia bezpieczeństwa systemu, użytkownik zobowiązany jest do niezwłocznego powiadomienia o tym fakcie ASI.
5. Przed czasowym opuszczeniem stanowiska pracy użytkownik zobowiązany jest do zablokowania systemu operacyjnego poprzez uruchomienie blokady lub wygaszacza ekranu, wymagającego ponowne wprowadzenie hasła lub wylogowania się z niego.
6. Z chwilą zakończenia pracy użytkownik zobowiązany jest do:
   - wylogowania się z systemu przetwarzającego dane osobowe,
   - wylogowanie się z systemu operacyjnego lub wyłączenia komputera,
   - zabezpieczenia stanowiska pracy, a w szczególności dokumentacji oraz wszelkiego rodzaju nośników przechowujących dane osobowe.

6. Tworzenie kopii zapasowych oraz sposób, miejsce i okres ich przechowywania

1. Zbiory danych w systemie informatycznym są zabezpieczone przed utratą lub uszkodzeniem za pomocą:
   - urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej,
   - sporządzania kopii zapasowych zbiorów danych (kopie pełne).
2. Za tworzenie kopii bezpieczeństwa Systemu Informatycznego odpowiedzialny jest Administrator Systemu Informatycznego lub osoba wyznaczona przez niego,
3. Pełne kopie zapasowe zbiorów danych są tworzone co najmniej raz na kwartał, kopie przyrostowe w razie potrzeby wykonywane są częściej,
4. W szczególnych przypadkach – przed aktualizacją lub zmianą w systemie należy bezwarunkowo wykonać pełną kopię zapasową systemu,
5. Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu. Za przeprowadzanie tej procedury odpowiedzialny jest Administrator Systemu Informatycznego lub inna wyznaczona przez niego osoba,
6. W przypadku komputerów stacjonarnych i przenośnych nie będących własnością zespołu, użytkownik systemu ma obowiązek sporządzania kopii zapasowych jak również ochrony nośników informacji. Wymaga się od użytkownika stosowania zasad dotyczących ochrony danych osobowych przed dostępem osób nieuprawnionych.

7. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji

Procedura użytkowania elektronicznych nośników informacji zawierających dane osobowe

Procedura opisuje zasady użytkowania i zabezpieczania komputerowych nośników informacji.

1. Obowiązkiem ASI jest prowadzenie ewidencji wszelkich nośników komputerowych służących do przechowywania danych osobowych.
   (Załącznik 9 – Ewidencja nośników komputerowych)
2. Nośniki danych należy przechowywać w sposób uniemożliwiający dostęp do nich osób nieuprawnionych oraz zabezpieczający je przed zagrożeniami typu: pożar, zalanie, kradzież, skopiowanie, zniszczenie itp...
3. Zabrania się bez zgody ADO wynoszenia na zewnątrz nośników zawierających dane osobowe.
4. W przypadku wyrażenia zgody przez ADO na wyniesienie, dane osobowe znajdujące się na wynoszonych nośnikach należy bezwzględnie zabezpieczyć poprzez ich zaszyfrowanie.
5. W przypadku przekazywania sprzętu komputerowego poza obszar organizacji, należy pozbawić go wszelkich zamontowanych w nim nośników zawierających dane osobowe, w szczególności dysków twardych lub wymazać je specjalistycznym oprogramowanie uniemożliwiających ich ponowne odczytanie.
6. Użytkownicy zobowiązani są do usuwania danych osobowych z nośników, jeżeli ustał już cel ich przetwarzania. Wyjątkiem są dane osobowe, które należy przechowywać z powodu odrębnych przepisów prawa.

7. Likwidacja uszkodzonych lub przestarzałych nośników mogących zawierać dane osobowe, w szczególności dysków twardych, odbywa się poprzez komisyjne ich niszczenie (fizyczne) uniemożliwiające późniejszy odczyt z nich danych, a następnie przekazywanie ich do utylizacji.
(Załącznik 10 – Protokół zniszczenia nośników komputerowych)

8. Sposób zabezpieczenia systemu informatycznego

Procedura zabezpieczania systemu informatycznego przetwarzającego dane osobowe

Procedura opisuje zasady użytkowania i zabezpieczania systemu informatycznego przed ingerencją wirusów komputerowych oraz innego szkodliwego oprogramowania.

1. Obowiązkiem ASI jest zarządzanie oprogramowaniem służącym do ochrony antywirusowej dla systemu informatycznego, w szczególności dla stacji roboczych wchodzących w jego skład.
2. Obowiązkiem ASI jest konfiguracja oraz nadzór nad oprogramowaniem oraz sprzętem sieciowym służącym do zarządzania i monitorowania ruchem sieciowym, w szczególności na styku sieci wewnętrznej z siecią Internet.
3. Obowiązkiem ASI jest konfiguracja bezprzewodowych punktów dostępowych pod kątem bezwzględnego zabezpieczenia ich standardem szyfrowania WPA lub nowszym.
4. Każda stacja robocza przetwarzająca dane osobowe powinna bezwzględnie posiadać zainstalowany i uruchomiony program antywirusowy oraz zaporę sieciową, w tym posiadać licencję pozwalającą na ich użytkowanie.
5. Program antywirusowy powinien zapewniać:
    - automatyczną ochronę systemu operacyjnego, systemu plików, a także poczty elektronicznej,
    - automatycznie aktualizować swoją bazę definicji wirusów,
6. W przypadku zidentyfikowania przez oprogramowanie antywirusowe sytuacji zagrożenia, należy bezzwłocznie powiadomić o tym fakcie ASI.
7. Użytkownicy, korzystający z komputerów przenośnych na których przetwarzane są dane osobowe, w szczególności tych wynoszonych poza obszar organizacji zobowiązani są do przestrzegania zasad bezpieczeństwa dotyczących tych urządzeń.
(Załącznik 11 – Regulamin użytkowania komputerów przenośnych)

9. Sposób realizacji wymogów określonych w rozporządzeniu

Zgodnie z rozporządzeniem, system informatyczny wykorzystywany do przetwarzania danych osobowych powinien posiadać funkcjonalności umożliwiające odnotowanie informacji o udostępnieniach danych odbiorcom, zawierające informacje komu, kiedy i w jakim zakresie dane osobowe zostały udostępnione.

Procedura związana z udostępnieniem danych osobowych

1. Dane osobowe udostępnia się na pisemny wniosek odbiorcy danych ze wskazaniem przez niego podstawy prawnej zapewniającej legalne ich przetwarzanie.
2. Zgody na udostępnienie danych może udzielać ASI w porozumieniu z ADO.
3. Odnotowanie faktu udostępnienia danych powinno nastąpić:
    - obowiązkowo w systemie informatycznym przetwarzającym te dane,

- opcjonalnie w postaci ewidencji udostępnień danych.
  (Załącznik 12 – Ewidencja udostępnień danych)

4. ADO odpowiada za udostępnienie danych zgodnie z ich przeznaczeniem.
5. W przypadku żądania osoby, której dane są przetwarzane, należy przygotować raport w formie wydruku z systemu informatycznego zawierający informacje o udostępnieniach danych tej osoby, ewentualnie wyciąg, jeżeli jest prowadzony, z rejestru papierowego.

10. Procedury wykonywania przeglądów i konserwacji systemów informatycznych

Celem procedury jest zapewnienie bezawaryjnego i prawidłowego funkcjonowania systemu informatycznego przetwarzającego dane osobowe.

1. Obowiązkiem ASI jest nadzór za bezawaryjną pracę systemu informatycznego, w tym: serwerów i ich usług, baz danych, stacji roboczych, czy aplikacji służących do przetwarzania danych osobowych.
2. Przegląd i konserwacja systemu informatycznego powinna odbywać się zgodnie z zaleceniami określonymi przez producenta tego oprogramowania lub zgodnie z określonym przez ASI harmonogramem.
3. W przypadku zlecenia prac konserwacyjno-naprawczych sprzętu komputerowego lub uaktualnienia systemu informatycznego, wykonywane przez podmiot zewnętrzny, czynności te powinny wykonywane być na zasadach określonych w umowie z tymi podmiotami, ze szczególnym uwzględnieniem klauzul dotyczących ochrony przetwarzania danych osobowych.
4. W przypadku prac wykonywanych doraźnie przez osoby nie posiadające upoważnień do przetwarzania danych odbywających się w fizycznym obszarze ADO, prace takie powinny być wykonywane pod nadzorem ASI lub osób do tego upoważnionych.
5. Wszelkie aktualizacje oprogramowania powinny być wykonywane zgodne z zaleceniami producenta tego oprogramowania za zgodą ASI.

11. Zasady korzystania z Internetu i poczty elektronicznej

a) Procedura korzystania z Internetu

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
2. Użytkownik ponosi pełną odpowiedzialność za szkody spowodowane w skutek nieuprawnionego instalowania oprogramowania ściągniętego z Internetu.
3. Wszelkie zmiany zainstalowanego oprogramowania w systemie operacyjnym stacji roboczej wymagają zgody ASI i są wykonywane pod jego nadzorem.
4. Zabronione jest korzystanie ze stron o charakterze przestępczym, hackerskim, pornograficznym, lub innych łamiącym prawo.
5. Należy korzystać z przeglądarek internetowych z wyłączonymi opcjami autouzupełniania formularzy i zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanych połączeń poprzez przeglądarkę internetową, należy zwracać szczególną uwagę na to czy pojawiła się odpowiednia ikonka (kłódki) oraz czy adres strony rozpoczyna się frazą „https”.

b) Procedura korzystania z poczty elektronicznej

1. Przesyłanie wiadomości zawierających tzw. dane wrażliwie wewnątrz instytucji, bądź wszelkich danych osobowych poza nią, należy bezwzględnie zabezpieczać je przez:
    - korzystanie z protokołów szyfrowania wiadomości typu: PGP, S/MIME,
    - używanie formatów plików umożliwiających zakładanie na nie hasła typu: PDF, DOC, XLS,
    - wykorzystywanie programów do archiwizacji / kompresji plików umożliwiających zakładanie hasła typu: ZIP, RAR.
2. W przypadku wykorzystywania metod szyfrowania zabezpieczonych hasłem, należy stosować minimum osiem znaków, w tym duże, małe litery i cyfry lub znaki specjalne, a hasło przesłać odrębnym kanałem komunikacji typu: telefon, SMS.
3. Należy zwracać szczególną uwagę na poprawność wprowadzanych adresów odbiorców.
4. Nie należy otwierać załączników lub łączy internetowych typu „hyperlink" dołączonych do wiadomości nadesłanych przez nieznanych nadawców oraz zwrócić szczególną ostrożność w przypadku podejrzanych załączników lub linków nadanych przez znanych nam nadawców.
5. Należy okresowo kasować niepotrzebne wiadomości, ponieważ mogą znajdować się w nich dane osobowe, do których przetwarzania nie jesteśmy już upoważnieni.
6. W przypadku korzystania z tzw. wysyłki seryjnej (wysyłania wiadomości do wielu adresatów jednocześnie), należy stosować metodę ukrywania adresatów wiadomości korzystają z funkcji "Ukryte do Wiadomości" (UDW, BCC).

12. Wykaz załączników

Załącznik 1 - Zlecenie nadania, modyfikacji uprawnień użytkownika
Załącznik 2 - Upoważnienie do przetwarzania danych
Załącznik 3 - Ewidencja osób upoważnionych do przetwarzania danych
Załącznik 4 - Powołanie ASI
Załącznik 5 - Rejestr podmiotów zewnętrznych
Załącznik 6 - Umowa o poufności
Załącznik 7 – Umowa powierzenia
Załącznik 8 – Metryka haseł
Załącznik 9 – Ewidencja nośników komputerowych
Załącznik 10 – Protokół zniszczenia nośników komputerowych
Załącznik 11 – Regulamin użytkowania komputerów przenośnych
Załącznik 12 – Ewidencja udostępnień danych

Administrator Systemu Informatycznego **Administrator Danych Osobowych**

....
Podpis Podpis