Załącznik nr 1
do *Polityki Bezpieczeństwa Informacji*, stanowiącej załącznik do Zarządzenia Nr 61/0101/2020 Rektora AJP
z dnia 1 września 2020 r.

I N S T R U K C J A

zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

§ 1.
Wprowadzenie

1. Niniejszy dokument stanowi instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Akademii im. Jakuba z Paradyża, zwaną dalej Instrukcją i jest wypełnieniem obowiązku wynikającego z art. 24 ust. 1-2 rozporządzenia 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 (ogólne rozporządzenie o ochronie danych lub RODO).
2. Instrukcja określa sposób zarządzania systemem informatycznym, wykorzystywanym do przetwarzania danych osobowych, w celu zabezpieczenia danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
3. W Instrukcji zostały uregulowane procedury:
    1) nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemach informatycznych oraz wskazanie osób odpowiedzialnych za te czynności;
    2) rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
    3) tworzenia kopii zapasowych zbiorów danych oraz określenie pro gramów i narzędzi programowych służących do ich przetwarzania wraz z określeniem sposobu, miejsca i okresu ich przechowywania;
    4) wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych; a także
    5) metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
    6) sposoby zabezpieczenia systemu informatycznego przed działalnością oprogramowania szkodliwego oraz dostępem do nich osób nieupoważnionych.

§ 2.
Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem

1. Środki uwierzytelniania dostępu do systemu informatycznego służącego do przetwarzania danych osobowych to identyfikator użytkownika i hasło dostępu.
2. Każdy identyfikator użytkownika zabezpieczony jest hasłem.
3. ADO stosuje następujące zasady tworzenia hasła:
    1) hasło nie może składać się z żadnych danych personalnych (imienia, nazwiska, adresu zamieszkania użytkownika lub najbliższych osób) lub ich fragmentów,
    2) hasło musi składać się z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,
    3) hasło nie może składać się z identycznych znaków lub ciągu znaków z klawiatury,
    4) hasło nie może być jednakowe z identyfikatorem użytkownika,
    5) hasło musi być unikalne, tj. takie, które nie było poprzednio stosowane przez użytkownika.

4. Hasło, w trakcie wpisywania, nie może być wyświetlane na ekranie. Użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności.
5. Zaleca się zmienianie hasła nie rzadziej niż co 30 dni. Jeżeli zmiana hasła nie jest możliwa w wymaganym czasie, należy jej dokonać w najbliższym możliwym terminie.
6. W przypadku złamania poufności hasła, użytkownik zobowiązany jest niezwłocznie zmienić hasło i poinformować o tym fakcie ADO.
7. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego służącego do przetwarzania danych osobowych nie powinien być przydzielany innej osobie. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych osobowych, należy niezwłocznie zablokować w systemie informatycznym służącym do przetwarzania danych osobowych oraz unieważnić przypisane mu hasło.

§ 3.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu informatycznego służącego do przetwarzania danych

1. Przed rozpoczęciem przetwarzania danych osobowych użytkownik powinien sprawdzić, czy nie ma oznak fizycznego naruszenia zabezpieczeń. W przypadku wystąpienia jakichkolwiek nieprawidłowości, należy powiadomić Administratora Systemów Informatycznych.
2. Przystępując do pracy w systemie informatycznym służącym do przetwarzania danych osobowych, użytkownik jest zobowiązany wprowadzić swój identyfikator oraz hasło dostępu. Zabrania się wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem identyfikatora i hasła dostępu innego użytkownika.
3. W przypadku opuszczenia stanowiska pracy trwającego dłużej niż jedną godzinę, użytkownik musi wylogować się z systemu informatycznego służącego do przetwarzania danych osobowych lub danych istotnych.
4. Zakończenie pracy w systemie informatycznym służącym do przetwarzania danych osobowych następują poprzez wylogowanie się z tego systemu. Za wykonanie kopii danych odpowiedzialny jest Administrator Systemów Informatycznych. Użytkownik może wykonywać kopie tylko pod nadzorem Administratora Systemów Informatycznych.

§ 4.

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

1. Za sporządzanie kopii zapasowych zbiorów danych odpowiedzialny jest ASI systemu informatycznego służącego do przetwarzania danych osobowych.
2. Kopie zapasowe powinny być kontrolowane przez ASI, w szczególności pod kątem prawidłowości ich wykonania poprzez częściowe lub całkowite odtworzenie na wydzielonym sprzęcie komputerowym.
3. Nośniki informatyczne zawierające dane osobowe lub kopie systemów informatycznych służących do przetwarzania danych osobowych lub danych istotnych są przechowywane w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych.
4. W przypadku likwidacji nośników informatycznych zawierających dane osobowe lub kopie zapasowe systemów informatycznych służących do przetwarzania danych osobowych należy przed ich likwidacją usunąć dane osobowe lub uszkodzić je w sposób uniemożliwiający odczyt danych osobowych.

§ 5.

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

1. Nie należy przechowywać zbędnych nośników informacji zawierających dane osobowe oraz kopii zapasowych, a także wydruków i innych dokumentów zawierających dane osobowe. Po upływie

okresu ich użyteczności lub przechowywania, dane osobowe powinny zostać skasowane lub zniszczone tak, aby nie było możliwe ich odczytanie.

2. Elektroniczne nośniki informacji zawierające dane osobowe oraz kopie zapasowe nie mogą być wynoszone poza pomieszczenia stanowiące obszar przetwarzania danych osobowych, określony w PBI.
3. Elektroniczne nośniki informacji zawierające dane osobowe oraz kopie zapasowe, a także wydruki i inne dokumenty zawierające dane osobowe przechowywane są w zamykanych szafach w pomieszczeniach stanowiących obszar przetwarzania danych osobowych, określony w PBI w sposób zabezpieczający je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem i zniszczeniem.
4. W przypadku uszkodzenia lub zużycia nośnika informacji zwierających dane osobowe lub dane istotne należy go fizycznie zniszczyć tak, aby nie było możliwe odczytanie danych.

§ 6.

Sposób zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych

1. Do ochrony przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych stosowane jest oprogramowanie antywirusowe.
2. Każdy zbiór wczytywany do komputera, w tym także wiadomość e-mail, musi być przetestowany programem antywirusowym.
3. Na każdym stanowisku wyposażonym w dostęp do sieci Internet musi być zainstalowanie oprogramowanie antywirusowe. Niedopuszczalne jest stosowanie dostępu do sieci Internet bez aktywnej ochrony antywirusowej oraz zabezpieczenia przed dostępem szkodliwego oprogramowania.
4. Aktualizacje oprogramowania antywirusowego powinno odbywać się nie rzadziej niż raz w miesiącu.

§ 7.

Sposób zapewnienia odnotowania informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia

1. W systemie informatycznym służącym do przetwarzania danych osobowych odnotowywane są informacje o odbiorcach danych, a w szczególności imię i nazwisko lub nazwa odbiorcy, data udostępnienia oraz zakres udostępnienia.
2. W przypadku, gdy w systemie informatycznym służącym do przetwarzania danych osobowych nie jest możliwe odnotowywanie takich informacji, ADO odnotowuje je w rejestrze odbiorców danych osobowych.
3. W rejestrze odnotowywane są imię i nazwisko lub nazwa odbiorcy, data udostępnienia oraz zakres udostępnienia. Rejestr prowadzony w formie elektronicznej będzie przekazywany w formie wydruku z systemu informatycznego na każdorazowe żądanie IODO.

§ 8.

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

1. Przeglądy i konserwacje sprzętu komputerowego oraz nośników informacji służących do przetwarzania danych osobowych, przeprowadzane są w pomieszczeniach stanowiących obszar przetwarzania danych osobowych, określony w PBI przez firmy zewnętrzne na podstawie zawartych umów. W umowie musi znajdować się zapis o powierzeniu danych osobowych.

2. W przypadku przekazywania do naprawy sprzętu komputerowego z zainstalowanym systemem informatycznym służącym do przetwarzania danych osobowych lub nośnikiem informacji służących do przetwarzania danych osobowych, powinien on zostać pozbawiony danych osobowych przez fizyczne wymontowanie dysku lub skasowanie danych lub naprawa powinna zostać przeprowadzona w obecności ADO.
3. Przeglądy techniczne wykonywane muszą być nie rzadziej niż raz w roku.
4. Nadzór nad przeprowadzaniem przeglądów technicznych, konserwacji i napraw sprzętu komputerowego, na którym zainstalowano system informatyczny służący do przetwarzania danych osobowych, systemu informatycznego służącego do przetwarzania danych osobowych oraz nośników informacji służących do przetwarzania danych osobowych pełni ASI.
5. Zabronione jest wykonywanie przeglądów i konserwacji systemów informatycznych służących do przetwarzania danych osobowych oraz nośników informacji służących do przetwarzania danych osobowych samodzielnie przez pracownika lub współpracownika ADO.

§ 9.

Pozostałe zasady ochrony systemu informatycznego służącego do przetwarzania danych osobowych

1. ADO ma prawo do kontroli stanu zabezpieczeń oraz przestrzegania zasad ochrony danych osobowych w dowolnym terminie.
2. Należy instalować zalecane przez producentów oprogramowania poprawki i uaktualnienia systemu informatycznego służącego do przetwarzania danych osobowych celem wyeliminowania błędów w działaniu lub poprawienia wydajności działania.
3. Dopuszcza się użytkowanie sprzętu informatycznego poza z siedzibą Akademii im. Jakuba z Paradyża zachowaniem szczególnej dbałości o powierzony sprzęt i dane ze szczególnym uwzględnieniem zabezpieczenia przed utratą danych oraz sprzętu.
4. Użytkownicy (za wyjątkiem osób upoważnionych) nie posiadają statusu administratora jednostki komputerowej.

Rektor AJP: *prof. dr hab. Elżbieta Skorupska-Raczyńska*