UNIWERSYTET
ŁÓDZKI

Zalecenia dotyczące postępowania w przypadku naruszenia ochrony danych osobowych w Uniwersytecie Łódzkim lub ryzyka takiego naruszenia

§ 1

Naruszenie ochrony danych osobowych, zgodnie z art. 4 pkt 12 RODO tj. 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) (Dz. Urz. UE L 119, s.1), oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych (utrata poufności, integralności lub dostępności).

Naruszenie ochrony danych osobowych może dotyczyć danych osobowych przetwarzanych w różnych formach np. elektronicznej lub papierowej oraz może wynikać z rozmyślnego lub przypadkowego działania człowieka lub z przyczyn niezależnych od człowieka[1].

Naruszeniem ochrony danych osobowych może być, w szczególności:

a) kradzież, zagubienie lub pozostawienie w niezabezpieczonej lokalizacji nośnika zawierającego dane osobowe (np. dysku twardego, pendrive, płyty CD, DVD, karty pamięci, dokumentu papierowego),
b) utracenie danych osobowych spowodowane np. awarią, nieprawidłowym działaniem lub błędną obsługą systemu informatycznego, omyłkowym zniszczeniem papierowej dokumentacji, utraceniem danych w wyniku zdarzeń losowych np. pożaru, zalania,
c) błędne wprowadzenie lub zmodyfikowanie danych osobowych (np. wprowadzenie do systemu błędnych danych),

[1] PN-ISO/IEC 27002, PN-ISO/IEC 27005

tel.: 42 635 42 14
ul. Narutowicza 68, 90-136 Łódź
e-mail: iod@uni.lodz.pl
www.uni.lodz.pl

d) przekazanie danych osobowych osobom nieuprawnionym (np. wysłanie błędnie zaadresowanego listu/maila, przekazanie dokumentacji nieuprawnionej osobie, ustne ujawnienie danych osobowych nieuprawnionej osobie),

e) niezamierzona publikacja danych (np. niezamierzone opublikowanie danych osobowych na portalu internetowym, udostępnienie nieprawidłowo zanonimizowanego dokumentu),

f) nieuprawnione uzyskanie dostępu do danych osobowych (np. wynikające z błędnie przydzielonych praw dostępu w systemie informatycznym, nieprawidłowo ustawionego monitora umożliwiającego wgląd w dane osobom postronnym, przełamaniem zabezpieczeń chroniących dostęp do danych),

g) działanie szkodliwego oprogramowania ingerującego w poufność, integralność i dostępność danych osobowych.

§ 2

Każdy pracownik w przypadku stwierdzenia naruszenia ochrony danych osobowych lub podejrzenia[2], że mogło zaistnieć takie naruszenie, zobowiązany jest niezwłocznie[3]:

1. jeżeli sytuacja to umożliwia, samodzielnie powziąć czynności mające na celu wyeliminowanie lub ograniczenie zaistniałego zagrożenia dla danych osobowych tak, aby zminimalizowane zostało ryzyko naruszenia praw i wolności osób, których dane dotyczą[4].

1. zawiadomić o zaistniałym zdarzeniu:

   a) bezpośredniego przełożonego lub

   b) Inspektora Ochrony Danych w UŁ (IOD w UŁ).

Przełożony zgłasza zaistniałe zdarzenie IOD w UŁ.

§ 3

Pracownik, który stwierdził naruszenie ochrony danych osobowych lub takie ryzyko zobowiązany jest niezwłocznie:

[2]W związku z trudnością dokonania, w wielu możliwych przypadkach, przez osobę szybkiej i jednoznacznej oceny czy dane zdarzenie stanowi naruszenie ochrony danych osobowych, mając na uwadze bezpieczeństwo danych osobowych, zaleca się wstępnie zakwalifikować to zdarzenie jako naruszenie ochrony danych osobowych i stosować się do dalszych wytycznych niniejszej instrukcji.

[3]Niezwłoczność działania wynika m. in. z nałożonego na administratora obowiązku, o którym mowa w art. 33 ust. 1 RODO.

[4]Brak samodzielnej, szybkiej i skutecznej reakcji spowodować może eskalację naruszenia praw i wolności osób których dane dotyczą. Przykładowo, w sytuacji znalezienia leżącego na ziemi elektronicznego nośnika lub dokumentacji papierowej należy nośnik/dokumentację niezwłocznie zabezpieczyć przed dostępem osób trzecich (tzn. podnieść, nie analizować zawartej w niej treści, zabezpieczyć w bezpiecznym miejscu a następnie dokonać czynności zgłoszenia incydentu, o którym mowa w dalszej części niniejszej instrukcji).

tel.: 42 635 42 14
ul. Narutowicza 68, 90-136 Łódź
e-mail: iod@uni.lodz.pl
www.uni.lodz.pl

1. jeżeli jest to możliwe, zabezpieczyć wszelkie dane osobowe przed czynnikiem zagrażającym ich bezpieczeństwu;
2. szczegółowo, pisemnie, udokumentować[5] okoliczności naruszenia danych osobowych lub takiego ryzyka w formie notatki służbowej, w tym opisać charakter zdarzenia, jeżeli to możliwe wskazać kategorię, zakres danych i liczbę osób, których dotyczy lub może dotyczyć naruszenie, miejsce i czas zdarzenia, opisać środki zastosowane lub proponowane w celu zapobiegnięcia dalszemu naruszaniu ochrony danych osobowych oraz wskazać możliwe konsekwencje wynikające z naruszenia i podjęte działania zaradcze.

§ 4

Po otrzymaniu zgłoszenia i notatki służbowej w sprawie naruszenia ochrony danych osobowych lub takiego ryzyka, IOD UŁ analizuje w jakim stopniu zdarzenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych tj. może powodować powstanie uszczerbku fizycznego lub szkody majątkowej lub niemajątkowej u osób fizycznych (np. utratę kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminację, kradzież lub sfałszowanie tożsamości, stratę finansową, nieuprawnione odwrócenie pseudonimizacji[6], naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne). IOD UŁ sporządza raport z naruszenia ochrony danych osobowych, stanowiący załącznik nr 6 do Polityki Ochrony Danych Osobowych w UŁ.

§ 5

Jeżeli z analizy, o której mowa w § 4 wynika, że jest prawdopodobne, że naruszenie ochrony danych osobowych będzie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, wówczas nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, IOD UŁ lub inna upoważniona osoba zawiadamia Administratora o konieczności zgłaszenia naruszenie ochrony danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych. Do zgłoszenia przekazanego po upływie 72 godzin należy dołączyć wyjaśnienie przyczyn opóźnienia[7].

[5] art. 33 ust. 5 RODO.

[6] Zgodnie z art. 4 pkt 5 RODO "pseudonimizacja" - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

[7] art. 33 ust. 1 RODO.

tel.: 42 635 42 14
ul. Narutowicza 68, 90-136 Łódź
e-mail: iod@uni.lodz.pl
www.uni.lodz.pl

§ 6

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych IOD UŁ lub inna upoważniona osoba:

1. bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu, tak aby umożliwić tej osobie podjęcie niezbędnych działań zapobiegawczych (wzór zawiadomienia stanowi załącznik do niniejszej instrukcji). Informacja taka powinna zawierać opis charakteru naruszenia ochrony danych osobowych oraz zalecenia dla danej osoby fizycznej co do minimalizacji potencjalnych niekorzystnych skutków;
2. zawiadomienie, o którym mowa w pkt 1 nie jest obowiązkowe, jeżeli wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

§ 7

Po każdym naruszeniu ochrony danych osobowych IOD UŁ we współpracy z jednostką organizacyjną, w której doszło do naruszenia, zobowiązany jest dokonać przeglądu środków techniczno-organizacyjnych zaimplementowanych w środowisku, w którym wystąpiło naruszenie, celem ustalenia co należy zmienić, aby zmniejszyć prawdopodobieństwo wystąpienia podobnego naruszenia w przyszłości.

§ 8

IOD UŁ prowadzi rejestr naruszeń ochrony danych osobowych w Uniwersytecie Łódzkim.

tel.: 42 635 42 14
ul. Narutowicza 68, 90-136 Łódź
e-mail: iod@uni.lodz.pl