1. Procedura postępowania z incydentami ochrony danych osobowych

1. Osobami odpowiedzialnymi za bezpieczeństwo danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do pomieszczeń oraz systemów, w których przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń, są Administrator Danych, IOD oraz ASI (w odniesieniu do danych przetwarzanych w systemach informatycznych).
2. Za naruszenie ochrony danych osobowych uważa się 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, a w szczególności:
   2.1. nieuprawniony dostęp lub próbę dostępu do systemu lub pomieszczeń, w których następuje proces przetwarzania danych (widoczne uszkodzenia bądź naruszenia zabezpieczeń),
   2.2. naruszenie lub próbę naruszenia zbioru danych oraz integralności systemu,
   2.3. nieautoryzowane zniszczenie lub próbę zniszczenia danych zgromadzonych w zbiorach papierowych oraz systemie,
   2.4. zmianę lub utratę danych zapisanych na kopiach zapasowych lub archiwalnych dokonaną w sposób nieautoryzowany,
   2.5. nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu),
   2.6. inny stan systemu lub pomieszczeń niż pozostawiony przez użytkownika po zakończeniu lub po przerwie w pracy z systemem,
   2.7. podejrzenie o wycieku danych osobowych,
   2.8. zagubienie lub nieautoryzowane usunięcie danych osobowych,
   2.9. otrzymanie zgłoszenia, od osoby której dane dotyczą o niewłaściwym wykorzystaniu jej danych,
   2.10. podejrzenie, że do systemów lub pomieszczeń, gdzie są przetwarzane dane osobowe miały dostęp osoby nieuprawnione.
3. Naruszenia dotyczą zarówno danych osobowy przetwarzanych w formie elektronicznej, jak i papierowej.
4. Każdy pracownik jest zobowiązany do niezwłocznego (lecz nie później niż w ciągu godziny od zdarzenia) poinformowania IOD, a w przypadku danych osobowych przetwarzanych z użyciem systemu informatycznego służącego do przetwarzania danych osobowych również ASI, o każdym przypadku złamania zasad przetwarzania danych, a w szczególności o sytuacjach udostępnienia danych osobom nieuprawnionym.
5. Informacje o naruszeniu bezpieczeństwa danych osobowych należy przekazać w pierwszej kolejności osobiście lub telefonicznie, a przesłać na adres email wiadomość opisującą rodzaj naruszenia. Opis powinien zawierać co najmniej następujące informacje:
   5.1. data i miejsce zdarzenia,
   5.2. kategorie danych oraz przybliżoną liczbę osób, których dotyczy naruszenie,
   5.3. opis naruszenia,
   5.4. możliwe konsekwencje naruszenia danych,

5.5. informacje o ewentualnym podjęciu środków zaradczych.

6. Do czasu przybycia IOD lub ASI lub osoby upoważnionej przez wskazane podmioty, pracownik:

   6.1. zabezpiecza dostęp do miejsca lub urządzenia,

   6.2. wstrzymuje pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamia bez koniecznej potrzeby komputerów i innych urządzeń, które w związku z naruszeniem ochrony zostały wstrzymane,

   6.3. podejmuje, stosownie do zaistniałej sytuacji inne, niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.

7. Dokonywanie zmian w miejscu naruszenia ochrony bez uzyskania zgody IOD lub ASI jest możliwe tylko w sytuacji, jeżeli zachodzi konieczność ratowania osób lub mienia albo zapobieżenia grożącemu niebezpieczeństwu.

8. IOD lub ASI, który wykrył lub został poinformowany o nieprawidłowościach przy przetwarzaniu danych osobowych powinien niezwłocznie zidentyfikować problem, zabezpieczyć dane i przedsięwziąć wszelkie niezbędne kroki, aby uniknąć w przyszłości podobnych zdarzeń.

9. IOD lub ASI, po otrzymaniu zgłoszenia o naruszeniu:

   9.1. ocenia zaistniałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane osobowe, stan urządzeń i zbioru danych,

   9.2. podejmuje niezbędne działania mające na celu uniemożliwienie dalszego naruszenia zabezpieczenia systemu (odłączenie urządzeń, odłączenie wadliwych urządzeń, zmiana haseł, blokowanie dostępu do sieci telekomunikacyjnej, programów oraz zbiorów danych),

   9.3. zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia, jak również sprawdza zawartość zbioru danych osobowych,

   9.4. sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych,

   9.5. sprawdza sposób działania programu (w tym również obecność wirusów komputerowych);

   9.6. ustala charakter i rodzaj naruszenia oraz metody działania osób naruszających zabezpieczenie systemu,

   9.7. niezwłocznie zapewnia przywrócenie prawidłowego stanu działania systemu, a w przypadku uszkodzenia danych, odtwarza je z ostatnich kopii awaryjnych z zachowaniem należytych środków ostrożności,

   9.8. sprawdza jakość komunikacji w systemie informatycznym,

   9.9. dokonuje analizy stanu systemu wraz z oszacowaniem rozmiaru szkód powstałych wskutek naruszenia oraz poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych,

   9.10. spisuje relację osoby zatrudnionej przy przetwarzaniu danych, która dokonała powiadomienia,

   9.11. podejmuje decyzję o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych i w przypadkach uzasadnionych niezwłocznie powiadamia właściwą osobę podejmującą decyzję w imieniu Administratora Danych,

   9.12. sporządza raport zawierający w szczególności: dane personalne osoby, która stwierdziła naruszenie, datę i godzinę powiadomienia, opis podjętych czynności i ich uzasadnienie,

9.13. podejmuje czynności mające na celu minimalizację szkody.

10. IOD po identyfikacji problemu dokonuje klasyfikacji naruszenia. Naruszenie klasyfikowane jest jako:

10.1. nieskutkujące ryzykiem naruszenia praw lub wolności osób fizycznych,

10.2. skutkujące ryzykiem naruszenia praw lub wolności osób fizycznych.

11. Naruszenie kwalifikuje się jako skutkujące ryzykiem naruszenia praw lub wolności osób fizycznych w szczególności, jeżeli konsekwencją naruszenia bezpieczeństwa danych osobowych jest utrata kontroli nad danymi osobowymi lub ograniczenie praw osób, których dane dotyczą, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne.

11. Jeżeli naruszenie zostanie zakwalifikowane jako nieskutkujące ryzykiem naruszenia praw lub wolności osób fizycznych, IOD:

11.1. bada przebieg sprawy,

11.2. sporządza Protokół z czynności sprawdzających.

12. Jeżeli naruszenie zostanie zakwalifikowane jako skutkujące ryzykiem naruszenia praw lub wolności osób fizycznych, IOD:

12.1. bada przebieg sprawy,

12.2. sporządza Protokół z czynności sprawdzających,

12.3. przygotowuje zgłoszenie naruszenia do Prezesa Urzędu Ochrony Danych Osobowych.

13. Przygotowane przez IDO zgłoszenie naruszenia, Administrator Danych przekazuje do Prezesa Urzędu Ochrony Danych Osobowych niezwłocznie, lecz nie później niż w ciągu 72 godzin po stwierdzeniu naruszenia. Do zgłoszenia przekazanego po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

14. Administrator Danych informuje Prezesa Urzędu Ochrony Danych Osobowych o zaistniałym naruszeniu, poprzez podanie następujących informacji:

14.1. opisu charakteru naruszenia ochrony danych osobowych, w tym jeżeli to możliwe wskazania kategorii i przybliżonej liczby osób, których dane dotyczą, oraz kategorii i przybliżonej liczby wpisów danych osobowych, których dotyczy naruszenie,

14.2. imienia i nazwiska oraz danych kontaktowych IOD lub oznaczenia innego punktu kontaktowego, od którego można uzyskać więcej informacji na temat naruszenia,

14.3. opisu możliwych konsekwencji naruszenia ochrony danych osobowych,

14.4. opisu środków zastosowanych lub proponowanych przez Administratora Danych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środków w celu zminimalizowania ewentualnych negatywnych skutków naruszenia.

15. Administrator Danych lub IOD (na podstawie upoważnienia Administratora Danych) w celu wyjaśnienia sprawy, w zależności od potrzeby prowadzi korespondencję z Prezesem Urzędu Ochrony Danych Osobowych udzielając wszelkich niezbędnych informacji.

16. W miarę możliwości Administrator Danych lub IOD (na podstawie upoważnienia Administratora Danych) informuje osobę, której dane zostały naruszone o rodzaju zagrożenia, a w szczególności przedstawia opis

charakteru naruszenia, podjęte działania w celu ograniczenia zagrożenia oraz wydaje zalecenia co do minimalizacji potencjalnych niekorzystnych skutków.

17. Zawiadomienie, o którym mowa w pkt 16 powyżej, nie jest wymagane, w następujących przypadkach:

17.1. Administrator Danych wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,

17.2. Administrator Danych zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,

17.3. 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.

18. Jeżeli naruszenie danych osobowych ma znamiona przestępstwa wówczas Administrator Danych lub IOD (na podstawie upoważnienia Administratora Danych) informuje odpowiednie organy ścigania.

19. W celu minimalizacji strat oraz w ramach zastosowania środków zaradczych przed następnymi naruszeniami Administrator Danych:

19.1. jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu, uaktywnienie się wirusa komputerowego - niezwłocznie przeprowadza, w stosownym zakresie, przeglądy oraz konserwacje urządzeń i programów, ustala źródło pochodzenia wirusa oraz wdraża skuteczniejsze zabezpieczenia antywirusowe,

19.2. jeżeli przyczyną zdarzenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych - przeprowadza dodatkowe kursy i szkolenia osób biorących udział przy przetwarzaniu danych, a wobec osób winnych zaniedbań wnioskuje o ich ukaranie w trybie przewidzianym odrębnymi przepisami,

19.3. zleca IOD przeprowadzenie dodatkowych szkoleń uzupełniających dotyczących zasad ochrony danych osobowych.

20. W stosunku do osoby, która zaniedbuje obowiązki związane z ochroną danych osobowych mogą zostać wyciągnięte konsekwencje dyscyplinarne przewidziane Kodeksem Pracy oraz wewnętrznymi regulacjami obowiązującymi w strukturze Administratora Danych.