Załącznik nr 8

Przykładowe zdarzenia naruszające bezpieczeństwo danych osobowych lub grożące takim naruszeniem

1. Zdarzenia naruszające bezpieczeństwo danych osobowych lub grożące takim naruszeniem dzielą się na:
   1) zagrożenia losowe zewnętrzne (np. takie jak pożar, powódź, brak zasilania), które mogą prowadzić do utraty integralności danych, zniszczenia i uszkodzenia infrastruktury technicznej systemu oraz zakłócenia ciągłości jego pracy;
   2) zagrożenia losowe wewnętrzne (np. takie jak pomyłki pracowników, awarie sprzętowe, błędy oprogramowania), które mogą prowadzić do zniszczenia danych, zakłócić ciągłość pracy systemu, powodować naruszenie poufności danych, integralności danych oraz ich prawidłowości,
   3) zagrożenia zamierzone, świadome i celowe, które polegać mogą na nieuprawnionym dostępie do systemu z jego wnętrza, nieuprawnionym przekazie danych, pogorszeniu jakości sprzętu i oprogramowania, bezpośrednim zagrożeniu materialnych składników systemu.
2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia ochrony danych osobowych, w tym zabezpieczenia Systemu Informatycznego, w którym przetwarzane są dane osobowe, to w szczególności:
   1) sytuacje losowe, nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu (np. takie jak pożar, zalanie pomieszczeń, katastrofa budowlana);
   2) rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji, w tym danych osobowych (np. takie jak prace na danych osobowych w celach prywatnych, nie zamknięcie pomieszczenia, w którym znajduje się komputer albo element wyposażenia do przechowywania danych osobowych);
   3) niewłaściwe parametry środowiska, w którym pracuje sprzęt komputerowy np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych);
   4) awaria sprzętu lub oprogramowania albo urządzenia lub elementu wyposażenia do przechowywania danych osobowych, które wyraźnie wskazują na umyślne działanie

w kierunku naruszenia zabezpieczeń lub ochrony danych, a także niewłaściwe działanie serwisu;

5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;
6) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
7) próba modyfikacji lub modyfikacja danych albo zmiana w strukturze danych bez odpowiedniego upoważnienia;
8) niedopuszczalna manipulacja danymi osobowymi w Systemie Informatycznym;
9) ujawnienie osobom nieupoważnionym danych osobowych lub procedury przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń;
10) odstępstwa od założonego rytmu pracy wskazujące na złamanie lub zaniechanie ochrony danych osobowych, w tym praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywych nieautoryzowanych próbach logowania;
11) istnienie nieautoryzowanych kont dostępu do danych osobowych.

3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc i urządzeń (np. szaf, regałów i sejfów) służących do przechowywania danych osobowych na papierowych nośnikach, wydrukach, lub innych elektronicznych nośnikach zewnętrznych tych danych.

Podstawowe zastosowane sposoby zabezpieczeń zapobiegające naruszeniom bezpieczeństwo danych osobowych, które wynikają z analizy ryzyka:

1. Podstawowym sposobem zabezpieczenia danych przetwarzanych w Systemie Informatycznym Administratora i dostępu do nich jest system definiowania loginów i haseł osób upoważnionych do przetwarzania danych osobowych. Są to zabezpieczenia programowe (logiczne) wmontowane w eksploatowane systemy uniemożliwiające dostęp do systemu osobom nieupoważnionym.
2. Zalogowanie się do Systemu Informatycznego Administratora wymaga podania loginu i hasła. Każdy pracownik samodzielnie ustala i zmienia hasło systemowe.
3. Wyłącznie Administrator Systemu Informatycznego ma dostęp do wszystkich loginów stosowanych przez upoważnionych pracowników.
4. Hasła systemowe powinny być zmieniane nie rzadziej, niż co 30 dni.

5. Na każdym komputerze pracującym w Systemie Informatycznym Administratora, który posiada dostęp do sieci Internetu, jest zainstalowany odpowiedni program antywirusowy.
6. Wydruki zawierające dane osobowe powinny znajdować się w miejscu, które uniemożliwia dostęp osobom nieuprawnionym.
7. Podstawowym sposobem zabezpieczenia danych przetwarzanych w formie tradycyjnej, tj. na papierowych nośnikach danyc, jest ograniczenie dostępu do niej za pomocą elementów **zabezpieczeń fizycznych** (ograniczenie dostępu do pomieszczeń i szaf lub innego wyposażenia biurowego, w których przechowywane są te dokumenty) **oraz organizacyjnych** (nadawanie, weryfikowanie i kontrolowanie dostępu do tych danych przez upoważnionych pracowników).
8. Przed rozpoczęciem pracy użytkownik Systemu Informatycznego Administratora ma obowiązek sprawdzić, czy stan urządzenia (komputer lub pomieszczenia i urządzenia do przechowywania danych na papierowych nośnikach) nie wskazuje na naruszenie lub próbę naruszenia danych osobowych.
9. Użytkownicy Systemu Informatycznego Administratora mogą zakończyć pracę po wylogowaniu się z systemu. Osoby te są obowiązane do wylogowania się z systemu także w przypadku czasowego opuszczenia stanowiska pracy. Dopuszcza się blokowanie stanowiska komputerowego.
10. W przypadku wykrycia korzystania z danych osobowych przez osoby nieuprawnione lub naruszenia zabezpieczeń dostępu do systemu, każdy, kto stwierdził powyższe naruszenie, zgodnie z obowiązującymi u Administratora zasadami jest zobowiązany powiadomić swojego przełożonego o tym fakcie.
11. Dane osobowe przetwarzane w Systemie Informatycznym Administratora zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.
12. Za wykonywanie kopii zapasowych, umożliwiających odtworzenie sprawności systemu, odpowiada Administrator Systemu Informatycznego. Są one przechowywane na serwerze oraz na nośnikach zewnętrznych, które są przechowywane w wyznaczonym do tego miejscu w Strefie I.
13. Z nośników magnetycznych kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności w taki sposób, aby nie można było odtworzyć ich zawartości.