

**Tabela form naruszeń ochrony danych osobowych**

Nr (kod) naruszeń	Formy naruszeń	Sposób postępowania
<b>A</b>	<b>Forma naruszenia ochrony danych osobowych przez pracownika zatrudnionego przy przetwarzaniu danych</b>	
<b>A.1</b>	<b>W zakresie wiedzy:</b>	
A.1.1	Ujawnianie sposobu działania aplikacji i systemu jej zabezpieczeń osobom niepowołanym.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji.
A.1.2	Ujawnianie informacji o sprzęcie i infrastrukturze informatycznej.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji.
<b>A.2</b>	<b>W zakresie sprzętu i oprogramowania</b>	
A.2.1	Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.	Niezwłocznie zakończyć działanie aplikacji. Dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji..
A.2.2	Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiegokolwiek inne osoby niż osoba, której identyfikator został przydzielony.	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. Pouczyć osobę, która dopuściła do takiej sytuacji. Dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji.
A.2.3	Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych i sieci.	Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie. Dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji.
A.2.4	Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych przez osoby nie będące pracownikami, bądź nieupoważnione osoby.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić jakie czynności zostały przez osoby nieuprawnione wykonane. Przerwać działające programy. Dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji.
A.2.5	Samodzielne instalowanie jakiegokolwiek oprogramowania.	Pouczyć osobę popełniającą wymienioną czynność, aby jej zaniechała. Wezwać służby informatyczne w celu odinstalowania programów. Dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji.
A.2.6	Modyfikowanie parametrów systemu i aplikacji.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji.
A.2.7	Odczytywanie nośników przed sprawdzeniem ich programem antywirusowym.	Pouczyć osobę popełniającą wymienioną czynność, aby zaczęła stosować się do wymogów bezpieczeństwa pracy. Dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji.
<b>A.3</b>	<b>W zakresie dokumentów i obrazów zawierających dane osobowe.</b>	
A.3.1	Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru.	Zabezpieczyć dokumenty. Dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji.
A.3.2	Przechowywanie dokumentów zabezpieczonych w niedostatecznym stopniu przed dostępem osób niepowołanych.	Powiadomić przełożonych. Dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji.
A.3.3	Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić przełożonych. Dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji.

A.3.4	Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią.	Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić przełożonych. Dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji.
A.3.5	Dopuszczanie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. Jeżeli ujawnione zostały ważne dane - dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji.
A.3.6	Sporządzanie kopii danych na nośnikach danych w sytuacjach nie przewidzianych procedurą.	Spowodować zaprzestanie kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji.
A.3.7	Utrata kontroli nad kopią danych osobowych.	Podjąć próbę odzyskania kopii. Powiadomić administratora bezpieczeństwa informacji. Dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji.
<b>A.4</b>	<b>W zakresie pomieszczeń i infrastruktury służących do przetwarzania danych osobowych</b>	
A.4.1	Opuszczanie i pozostawianie bez dozoru nie zamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych.	Zabezpieczyć (zamknąć) pomieszczenie. Dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji.
A.4.2	Wpuszczanie do pomieszczeń osób nieznanymi i dopuszczanie do ich kontaktu ze sprzętem komputerowym.	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich tożsamość. Dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji.
A.4.3	Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakiegokolwiek urządzenia do sieci komputerowej, demontowały elementy obudów gniazd i torów kablowych lub dokonywały jakiegokolwiek manipulacji.	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania. Postarać się ustalić ich tożsamość. Dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji.
<b>A.5</b>	<b>W zakresie pomieszczeń w których znajdują się komputery centralne i urządzenia sieci.</b>	
A.5.1	Dopuszczenie lub ignorowanie faktu, że osoby spoza służb informatycznych i telekomunikacyjnych dokonują jakiegokolwiek manipulacji przy urządzeniach lub okablowaniu sieci komputerowej w miejscach publicznych (hole, korytarze, itp.).	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania i ew. opuszczenia pomieszczeń. Postarać się ustalić ich tożsamość. Dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji.
A.5.2	Dopuszczanie do znalezienia się w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej osób spoza służb informatycznych i telekomunikacyjnych lub ignorowania takiego faktu.	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania i opuszczenia chronionych pomieszczeń. Postarać się ustalić ich tożsamość. Dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji.
<b>B</b>	<b>Zjawiska świadczące o możliwości naruszenia ochrony danych osobowych.</b>	
B.1	Ślady manipulacji przy urządzeniach lub przewodach sieci komputerowej albo komputerach.	Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji.
B.2	Obecność nowych kabli o nieznanym przeznaczeniu i pochodzeniu.	Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji.

B.3	Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych.	Dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji.
B.4	Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych.	Dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji.
B.5	Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania.	Dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji.
B.6	Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe.	Postępować zgodnie z właściwymi przepisami. Dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji.
<b>C</b>	<b>Formy naruszenia ochrony danych osobowych przez obsługę informatyczną w kontaktach z użytkownikiem</b>	
C.1	Próba uzyskania hasła uprawniającego do dostępu do danych osobowych w ramach pomocy technicznej.	Dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji.
C.2	Próba nieuzasadnionego przeglądania lub modyfikowania danych osobowych w ramach pomocy technicznej.	Dokonać powiadomienia zgodnie z zapisami § 2 Instrukcji.