

Naruszenia- wytyczne

Dokument opisuje zasady postępowania w razie stwierdzenia lub podejrzenia naruszenia przetwarzania danych osobowych w rozumieniu RODO („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”).

Spis treści

1. Wstęp	1
2. Naruszenie ochrony danych osobowych.....	1
3. Postępowanie w razie podejrzenia naruszenia	2
4. Tabela form naruszenia	3
5. Zawiadomienie o naruszeniu.....	7
6. Postępowanie w razie stwierdzenia naruszenia.....	7
7. Odnotowywanie naruszeń.....	8
8. Postanowienia końcowe.....	8

1. Wstęp

1. Do przestrzegania zaleceń opisanych w niniejszym dokumencie zobowiązane są wszystkie osoby, współpracujące z ADO (niezależnie od stażu pracy, zajmowanego stanowiska lub podstawy współpracy).
2. W każdym przypadku stwierdzenia naruszenia ochrony danych osobowych należy również dokonać ustaleń, czy nie została naruszona ochrona tajemnicy przedsiębiorstwa lub innych prawnie chronionych dóbr ADO oraz rozmiarów ewentualnych szkód i ich skutków. Ustaleń tych dokonuje osoba wyznaczona przez ADO.

2. Naruszenie ochrony danych osobowych

1. Naruszenie może być skutkiem w szczególności:
 - 1) szkodliwego wpływu środowiska na przetwarzanie danych osobowych zarówno w systemie informatycznym jak i w pomieszczeniach, w których przetwarza się dane,
 - 2) zewnętrznych zdarzeń losowych,
 - 3) zamierzonych lub niezamierzonych czynności osób upoważnionych do przetwarzania danych osobowych,
 - 4) nieuprawnionych działań osób nieupoważnionych do dostępu do danych osobowych,
 - 5) działań przestępczych, w postaci m.in. napadu rabunkowego, kradzieży, włamania, oszustwa, podpalenia, sabotażu, zniszczenia mienia.
2. Za naruszenie ochrony danych osobowych uznaje się w szczególności sytuacje:
 - 1) naruszenia poufności danych osobowych (np. kradzież dokumentacji kadrowej),
 - 2) naruszenia dostępności danych osobowych (np. zablokowanie systemu IT ADO w związku z atakiem *ransomware*),
 - 3) naruszenia integralności danych osobowych (np. ingerencja osoby nieuprawnionej w dane osobowe znajdujące się w dokumentacji kadrowej).

3. Postępowanie w razie podejrzenia naruszenia

1. Każda osoba współpracująca z ADO, która w ramach obowiązków służbowych ma dostęp do danych osobowych, jest zobowiązana do zgłaszania sytuacji, które stanowią lub mogą stanowić naruszenie ochrony danych osobowych.
2. Osoba zatrudniona powinna dokonać zgłoszenia naruszenia niezwłocznie po zaobserwowaniu zdarzenia, które je stanowi lub może je stanowić. Jeśli niezwłoczne zgłoszenie nie jest możliwe, osoba zatrudniona powinna podjąć działania zmierzające do zgłoszenia naruszenia w terminie nie dłuższym niż 4h od czasu zaobserwowania zdarzenia mogącego stanowić naruszenie.
3. Często występujące przykłady naruszeń i zalecane w tej sytuacji sposoby postępowania wskazano w rozdziale 4.
4. Formularz zgłoszenia naruszenia stanowi **załącznik nr 2 do Polityki bezpieczeństwa**.

4. Tabela form naruszenia

Lp.	Forma naruszenia	Przykład naruszenia	Zalecany sposób postępowania
1	Dokonywanie nieuprawnionej instalacji systemów, programów lub aplikacji.	Samodzielne zainstalowanie pobranej z internetu aplikacji do rozpakowywania plików ZIP.	1. Należy zawiadomić IT o zdarzeniu i postępować zgodnie z jego wskazówkami. 2. W razie stwierdzenia przez IT, że zdarzenie może stanowić naruszenie ochrony danych osobowych, należy wypełnić dokument „Naruszenia - formularz” i wysłać go na adres ADO.
2	Dokonywanie nieuprawnionych zmian w ustawieniach systemów, programów lub aplikacji, wykorzystywanych do przetwarzania danych osobowych.	Wyłączenie w systemie wymogu, zgodnie z którym hasło użytkownika nie może być takie samo jak jednego z pięciu z wcześniej używanych haseł.	1. Należy zawiadomić IT o zdarzeniu i postępować zgodnie z jego wskazówkami. 2. W razie stwierdzenia przez IT, że zdarzenie może stanowić naruszenie ochrony danych osobowych, należy wypełnić dokument „Naruszenia - formularz” i wysłać go na adres ADO.
3	Pobranie załącznika lub kliknięcie w link, umieszczony w treści wiadomości, gdy istnieją uzasadnione wątpliwości co do tożsamości rzeczywistego nadawcy.	Pobranie załącznika z poczty elektronicznej, opisanego jako faktura, od kontrahenta, z którym ADO nie współpracuje od lat. Kliknięcie na otrzymany w SMS-ie link, opisany jako prowadzący do aktualizacji programu antywirusowego.	1. Należy zawiadomić IT o zdarzeniu i postępować zgodnie z jego wskazówkami. 2. W razie stwierdzenia przez IT, że zdarzenie może stanowić naruszenie ochrony danych osobowych, należy wypełnić dokument „Naruszenia - formularz” i wysłać go na adres ADO.
4	Pozbywanie się zbędnych dokumentów papierowych, zawierających dane osobowe, w sposób niezapewniający, że do danych nie będą mieć dostępu osoby nieupoważnione.	Wyrzucanie błędnie wypisanych umów do kosza na śmieci.	1. Należy podjąć próbę odzyskania niewłaściwie usuniętych dokumentów, a następnie ich prawidłowego zniszczenia. 2. Należy wypełnić dokument „Naruszenia - formularz” i wysłać go na adres ADO.
5	Pozbywanie się zbędnych nośników lub sprzętów, zawierających dane osobowe, w sposób niezapewniający, że do danych nie będą mieć dostępu osoby nieupoważnione.	Przekazywanie niepotrzebnych już pendrive’ów członkom rodziny lub znajomym.	1. Należy podjąć próbę odzyskania nośników lub sprzętów, a następnie ich prawidłowego zniszczenia lub usunięcia znajdujących się na nich danych. 2. Należy wypełnić dokument „Naruszenia - formularz” i wysłać go na adres ADO.
6	Pozostawienie dokumentów zawierających dane osobowe w miejscu, do którego mają niekontrolowany dostęp osoby nieupoważnione.	Kładzenie dokumentów tekstem do góry na tacce przy przezroczystym oknie, wychodzącym na chodnik.	1. Należy przenieść dokumenty w miejsce, do którego nie będą miały dostępu osoby nieupoważnione. 2. Należy podjąć działania mające na celu ustalenie, czy osoby nieupoważnione uzyskały dostęp do danych osobowych. 3. Należy wypełnić dokument „Naruszenia - formularz” i wysłać go na adres ADO.
7	Pozostawienie kluczy do pomieszczeń, gdzie na stałe są przetwarzane dane osobowe, w miejscu, do którego mają niekontrolowany dostęp osoby nieupoważnione.	Zostawianie klucza do sekretariatu w zamku po godzinach pracy.	1. Należy przenieść klucze w miejsce, do którego nie będą miały dostępu osoby nieupoważnione. 2. Należy podjąć działania mające na celu ustalenie, czy osoby

Załącznik nr 3 do Polityki bezpieczeństwa (Naruszenia – wytyczne)

			nieupoważnione uzyskały dostęp do danych osobowych. 3. Należy wypełnić dokument „Naruszenia - formularz” i wysłać go na adres ADO.
8	Pozostawienie kluczy do szafek, szaf lub szuflad, gdzie na stałe są przechowywane dokumenty, nośniki lub sprzęty zawierające dane osobowe, w miejscu, do którego mają niekontrolowany dostęp osoby nieupoważnione.	Zostawianie klucza do szafy pancernej w zamku poza godzinami pracy.	1. Należy przenieść klucze w miejsce, do którego nie będą miały dostępu osoby nieupoważnione. 2. Należy podjąć działania mające na celu ustalenie, czy osoby nieupoważnione uzyskały dostęp do danych osobowych. 3. Należy wypełnić dokument „Naruszenia - formularz” i wysłać go na adres ADO.
9	Pozostawienie nośników zawierających dane osobowe w miejscu, do którego mają niekontrolowany dostęp osoby nieupoważnione.	Pozostawienie przenośnego dysku z kopią zapasową bazy danych na publicznie dostępnym korytarzu.	1. Należy przenieść nośniki w miejsce, do którego nie będą miały dostępu osoby nieupoważnione. 2. Należy podjąć działania mające na celu ustalenie, czy osoby nieupoważnione uzyskały dostęp do danych osobowych. 3. Należy wypełnić dokument „Naruszenia - formularz” i wysłać go na adres ADO.
10	Pozostawienie osoby nieupoważnionej w obszarze przetwarzania danych osobowych lub umożliwienie jej takiego dostępu.	Pozostawianie kuriera w sekretariacie bez nadzoru osoby upoważnionej.	1. Należy ocenić, czy w wyniku zdarzenia osoba nieupoważniona mogła poznać zabezpieczenia lub uzyskać dostęp do danych osobowych. 2. W razie stwierdzenia, że w wyniku zdarzenia mogło dojść do naruszenia ochrony danych osobowych, należy wypełnić dokument „Naruszenia - formularz” i wysłać go na adres ADO.
11	Pozostawienie sprzętu, zawierającego dane osobowe (lub z pomocą którego możliwy jest dostęp do danych osobowych) w miejscu, do którego mają niekontrolowany dostęp osoby nieupoważnione.	Pozostawienie niezaszyfrowanego dysku przenośnego na ladzie recepcji budynku, do której mają swobodny dostęp osoby nieupoważnione.	1. Należy przenieść sprzęt w miejsce, do którego nie będą miały dostępu osoby nieupoważnione. 2. Należy podjąć działania mające na celu ustalenie, czy osoby nieupoważnione uzyskały dostęp do danych osobowych. 3. Należy wypełnić dokument „Naruszenia - formularz” i wysłać go na adres ADO.
12	Przekazanie danych osobowych bez stosownej umowy (lub innego instrumentu prawnego) w sytuacji, gdy zawarcie takiej umowy jest wymagane.	Przekazanie danych osobowych pracownikom firmie prowadzącej szkolenie BHP bez zawarcia umowy powierzenia przetwarzania danych osobowych.	Należy zawiadomić ADO o zdarzeniu i postępować zgodnie z jego wskazówkami.
13	Stwierdzenie błędu w działaniu systemu, aplikacji, programu lub sprzętu.	Wyświetlenie przez system płac informacji o usunięciu bazy danych pracowników.	1. Należy zawiadomić IT o zdarzeniu i postępować zgodnie z jego wskazówkami.

			2. W razie stwierdzenia przez IT, że zdarzenie może stanowić naruszenie ochrony danych osobowych, należy wypełnić dokument „Naruszenia - formularz” i wysłać go na adres ADO.
14	Stwierdzenie braku możliwości uzyskania dostępu do wcześniej dostępnych systemów, programów, aplikacji, sprzętów lub sieci.	Brak możliwości uzyskania dostępu do listy kontrahentów przez osobę, która takiego dostępu potrzebuje w ramach obowiązków służbowych i miała wcześniej nadany taki dostęp.	1. Należy zawiadomić IT o zdarzeniu i postępować zgodnie z jego wskazówkami. 2. W razie stwierdzenia przez IT, że zdarzenie może stanowić naruszenie ochrony danych osobowych, należy wypełnić dokument „Naruszenia - formularz” i wysłać go na adres ADO.
15	Stwierdzenie zmiany dostępnych uprawnień w systemach, programach lub aplikacjach.	Możliwość aktualizacji oprogramowania w systemie operacyjnym Windows mimo niewykonywania pracy na koncie administratora.	1. Należy zawiadomić IT o zdarzeniu i postępować zgodnie z jego wskazówkami. 2. W razie stwierdzenia przez IT, że zdarzenie może stanowić naruszenie ochrony danych osobowych, należy wypełnić dokument „Naruszenia - formularz” i wysłać go na adres ADO.
16	Stwierdzenie, że interfejs systemu, programu lub aplikacji wykorzystywanej do przetwarzania danych osobowych odbiega od dotychczasowego.	Wyświetlanie w dostępnym przez internet systemie CRM komunikatu ALL YOUR BASE ARE BELONG TO US.	1. Należy zawiadomić IT o zdarzeniu i postępować zgodnie z jego wskazówkami. 2. W razie stwierdzenia przez IT, że zdarzenie może stanowić naruszenie ochrony danych osobowych, należy wypełnić dokument „Naruszenia - formularz” i wysłać go na adres ADO.
17	Ślady świadczące o włamaniu lub próbie włamania do pomieszczeń, gdzie na stałe przetwarzane są dane osobowe.	Stłuczone okno w sekretariacie.	1. Należy dokonać sprawdzenia, czy doszło do włamania lub innego przestępstwa i podjąć adekwatne środki (np. wezwać policję). 2. Należy ocenić, czy w wyniku zdarzenia osoba nieupoważniona mogła poznać zabezpieczenia lub uzyskać dostęp do danych osobowych. W miarę możliwości należy dokonać także odpowiedniej zmiany zabezpieczeń lub przenieść dokumenty, nośniki lub sprzęty w inne, bezpieczne miejsce. 3. W razie stwierdzenia, że w wyniku zdarzenia mogło dojść do naruszenia ochrony danych osobowych, należy wypełnić dokument „Naruszenia - formularz” i wysłać go na adres ADO.
18	Ślady świadczące o włamaniu lub próbie włamania do szafek, szaf lub szuflad, gdzie przechowywana jest dokumentacja papierowa, nośniki lub sprzęty zawierające dane osobowe.	Wyłamany zamek w szafce, gdzie są przechowywane umowy z kontrahentami.	1. Należy dokonać sprawdzenia, czy doszło do włamania lub innego przestępstwa i podjąć adekwatne środki (np. wezwać policję). 2. Należy ocenić, czy w wyniku zdarzenia osoba nieupoważniona mogła poznać zabezpieczenia lub uzyskać dostęp do danych osobowych. W miarę możliwości należy dokonać także odpowiedniej zmiany zabezpieczeń lub przenieść

			dokumenty, nośniki lub sprzęty w inne, bezpieczne miejsce. 3. W razie stwierdzenia, że w wyniku zdarzenia mogło dojść do naruszenia ochrony danych osobowych, należy wypełnić dokument „Naruszenia - formularz” i wysłać go na adres ADO.
19	Udostępnienie danych osobowych osobie, której tożsamości nie zweryfikowano.	Przekazanie informacji o stanie zadłużenia jakieś osoby osobie, która zadzwoniła w tej sprawie do ADO i nie przedstawiła się.	1. Należy podjąć działania mające na celu ustalenie tożsamości osoby, która weszła w posiadanie danych osobowych oraz - w zależności od sytuacji - odzyskanie danych osobowych lub zobowiązanie osoby, która weszła w posiadanie danych do zachowania tych danych w tajemnicy. 2. Należy wypełnić dokument „Naruszenia - formularz” i wysłać go na adres ADO.
20	Ujawnienie informacji o zabezpieczeniach fizycznych osobom nieupoważnionym.	Przekazanie osobie podającej się za bezpośredniego przełożonego hasła dostępu do systemu płac.	1. Należy w miarę możliwości jak najszybciej uniemożliwić osobie nieupoważnionej dostęp do zabezpieczeń i podjąć inne adekwatne działania (np. wezwanie policji). 2. Należy ocenić, czy w wyniku zdarzenia osoba nieupoważniona mogła poznać zabezpieczenia lub uzyskać dostęp do danych osobowych. W miarę możliwości należy dokonać także odpowiedniej zmiany zabezpieczeń (np. przez zmianę hasła do systemu). 3. W razie stwierdzenia, że w wyniku zdarzenia mogło dojść do naruszenia ochrony danych osobowych, należy wypełnić dokument „Naruszenia - formularz” i wysłać go na adres ADO.
21	Umożliwienie osobom nieupoważnionym dostępu do zabezpieczeń.	Umożliwienie osobie podającej się za serwisanta wejścia na teren serwerowni.	1. Należy w miarę możliwości jak najszybciej uniemożliwić osobie nieupoważnionej dostęp do zabezpieczeń i podjąć inne adekwatne działania (np. wezwanie policji). 2. Należy ocenić, czy w wyniku zdarzenia osoba nieupoważniona mogła poznać zabezpieczenia lub uzyskać dostęp do danych osobowych. W miarę możliwości należy dokonać także odpowiedniej zmiany zabezpieczeń (np. przez zmianę kodu do systemu alarmowego). 3. W razie stwierdzenia, że w wyniku zdarzenia mogło dojść do naruszenia ochrony danych osobowych, należy wypełnić dokument „Naruszenia - formularz” i wysłać go na adres ADO.

22	Umożliwienie uzyskania przez osoby nieupoważnione dostępu do informacji o zabezpieczeniach.	Prowadzenie głośnej rozmowy na temat zasad uzbrajania i rozbrajania systemu alarmowego w obecności osób nieupoważnionych.	1. Należy ocenić, czy w wyniku zdarzenia osoba nieupoważniona mogła poznać zabezpieczenia lub uzyskać dostęp do danych osobowych. W miarę możliwości należy dokonać także odpowiedniej zmiany zabezpieczeń (np. przez zmianę kodu do systemu alarmowego) 2. W razie stwierdzenia, że w wyniku zdarzenia mogło dojść do naruszenia ochrony danych osobowych, należy wypełnić dokument „Naruszenia - formularz” i wysłać go na adres ADO.
		Umieszczenie hasła dostępu do systemu na karteczce przyklejonej do monitora komputera na recepcji, widocznej przez osoby rozmawiające z pracownikiem recepcji.	
24	Utrata kontroli nad dokumentacją papierową, zawierającą dane osobowe.	Kradzież teczek z dokumentacją, zostawioną w zaparkowanym aucie.	1. Należy podjąć próbę odzyskiwania dokumentów i podjąć inne adekwatne działania (np. zgłoszenie sprawy na policję). 2. Należy wypełnić dokument „Naruszenia - formularz” i wysłać go na adres ADO.
25	Utrata kontroli nad nośnikiem lub sprzętem, zawierającymi dane osobowe.	Zgubienie w autobusie pendrive’a.	1. Należy podjąć próbę odzyskiwania nośnika lub sprzętu i podjąć inne adekwatne działania (np. zgłoszenie sprawy na policję). 2. Należy wypełnić dokument „Naruszenia - formularz” i wysłać go na adres ADO.
26	Wykorzystywanie nośników danych, które nie pochodzą z zaufanego źródła.	Odczyt danych z płyty CD umieszczonej w komputerze bez wcześniejszego jej przeskanowania programem antywirusowym.	1. Należy zaprzestać tego działania. 2. Należy zgłosić sprawę IT w celu sprawdzenia przez niego, czy nie doszło do nieuprawnionych zmian w komputerze, systemie lub sieci. 3. W razie stwierdzenia przez IT, że zdarzenie może stanowić naruszenie ochrony danych osobowych, należy wypełnić dokument „Naruszenia - formularz” i wysłać go na adres ADO.

5. Zawiadomienie o naruszeniu

- ADO (lub inna osoba wskazana w rozdziale 4) niezwłocznie po otrzymaniu zgłoszenia ws. naruszenia prowadzi postępowanie, mające na celu ustalenie:
 - czy doszło do naruszenia ochrony danych osobowych,
 - jakie działania należy podjąć w celu zakończenia lub zminimalizowania skutków naruszenia,
 - jakie działania należy podjąć zgodnie z przepisami prawa (np. zgłoszenie sprawy na policję lub zawiadomienie o naruszeniu Prezesa Urzędu Ochrony Danych Osobowych),
 - jakie działania należy podjąć dla uniknięcia podobnej sytuacji w przyszłości.
- ADO dokumentuje prowadzone przez siebie postępowanie.

6. Postępowanie w razie stwierdzenia naruszenia

- Na podstawie ustaleń, dokonanych w sposób opisany w rozdziale 5 powyżej, ADO podejmuje decyzję w sprawie:
 - działań, jakie należy podjąć zgodnie z przepisami prawa w razie stwierdzenia naruszeń,

- 2) działań mających na celu uniknięcie podobnego naruszenia w przyszłości.
2. W razie stwierdzenia, że naruszenie ochrony danych:
 - 1) nie powoduje ryzyka naruszenia praw lub wolności osób, których dane dotyczą - informacje nt. naruszenia odnotowuje się w rejestrze naruszeń,
 - 2) powoduje ryzyko naruszenia praw lub wolności osób, których dane dotyczą - naruszenie zgłasza się do Prezesa Urzędu Ochrony Danych Osobowych i odnotowuje w rejestrze naruszeń ADO,
 - 3) powoduje wysokie praw lub wolności osób, których dane dotyczą - o naruszeniu niezwłocznie informuje się osoby, których dane dotyczą, a ponadto naruszenie zgłasza się do Prezesa Urzędu Ochrony Danych Osobowych i odnotowuje w rejestrze naruszeń ADO.
3. W razie stwierdzenia, że naruszenie dotyczy danych osobowych, wobec których ADO ma status podmiotu przetwarzającego lub współadministratora, zgłoszenia dokonuje się właściwemu administratorowi danych osobowych (w sposób i w terminie wskazanym w umowie, będącej podstawą powierzenia przetwarzania lub współadministratowania danymi osobowymi).
4. Zgłoszenie naruszenia do Prezesa Urzędu Ochrony Danych Osobowych odbywa się zgodnie z procedurą opublikowaną na stronie Prezesa Urzędu Ochrony Danych Osobowych.
5. Informowanie osób, których dane dotyczą, o naruszeniu dokonuje się zgodnie z art. 34 RODO.
6. ADO może upoważnić wybrane przez siebie osoby do podejmowania działań, o których mowa w tym rozdziale.

7. Odnotowywanie naruszeń

1. ADO dokumentuje naruszenia poprzez gromadzenie wypełnionych formularzy zgłoszenia naruszeń.
2. Nie rzadziej niż jeden raz w roku ADO analizuje formularze, o których mowa w ust. 1 powyżej, w celu:
 - 1) oceny skuteczności środków technicznych i organizacyjnych zabezpieczenia danych osobowych;
 - 2) zidentyfikowania powtarzających się naruszeń;
 - 3) zaplanowania, w zależności od wyników oceny, działań zmierzających do poprawy środków organizacyjnych i technicznych zabezpieczenia danych osobowych.

8. Postanowienia końcowe

Niezgłoszenie naruszenia (podejrzenia naruszenia) ochrony danych osobowych lub zgłoszenie go z opóźnieniem może rodzić dla osoby odpowiedzialnej odpowiedzialność dyscyplinarną lub karną.