

POLSKIE DRUŻYNY STRZELECKIE (PDS)



„ZATWIERDZAM”

Załącznik Nr 3 do Zarządzenia
Komendanta Naczelnego PDS
Nr 1/D z dnia 15.01.2020 r.

Do użytku wewnętrznego

Jacek Rudolfiniowski

INSTRUKCJA postępowania w sytuacji naruszenia Ochrony Danych Osobowych (ODO)

ROZPOCZĘTO: 15.01.2020 r.

ZAKOŃCZONO:

WARSZAWA

POLSKIE DRUŻYNY STRZELECKIE (PDS)

INSTRUKCJA postępowania w sytuacji naruszenia Ochrony Danych Osobowych (ODO)

Za naruszenie ochrony danych osobowych uznaje się przypadki, w których:

- stwierdzono naruszenie zabezpieczenia systemu teleinformatycznego;
- stan urządzenia, zawartość zbioru danych osobowych;
- ujawnione metody pracy;
- sposób działania programu lub jakość komunikacji w sieci teleinformatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.

Każdy pracownik Firmy (Stowarzyszenia, Spółki...), który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych w systemie teleinformatycznym Firmy (Stowarzyszenia, Spółki...) zobowiązany jest do niezwłocznego poinformowania o tym Administratora systemu, lokalnego Inspektora Danych Osobowych (IDO) lub w przypadku ich nieobecności Administratora Bezpieczeństwa Informacji (ABI).

Administrator bazy danych osobowych, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony tej bazy danych zobowiązany jest do niezwłocznego:

1. Zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnym wykryciu tego faktu.
2. Jeżeli zasoby systemu na to pozwalają, wygenerowania i wydrukowania wszystkich dokumentów i raportów, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i podpisania.
3. Przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń, metody dostępu osoby niepowołanej do danych, itp.
4. Podjęcia odpowiednich kroków w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych, w tym m.in.:
 - a) fizycznego odłączenia urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie niepowołanej;
 - b) wylogowania użytkownika podejrzanego o naruszenie ochrony danych;
 - c) zmianę HASŁA Administratora i użytkownika poprzez którego uzyskano nielegalny dostęp w celu uniknięcia ponownej próby uzyskania takiego dostępu.
5. Szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych.
6. Przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, odtworzenia jej z ostatniej KOPII awaryjnej z zachowaniem wszelkich środków ostrożności mających na celu uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną, tą samą drogą.

POLSKIE DRUŻYNY STRZELECKIE (PDS)

Po przywróceniu pierwotnego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę /audyt/ w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia. Należy przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

Jeżeli przyczyną zdarzenia była „Infekcja wirusem” należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne wykluczające powtórzenie się podobnego zdarzenia w przyszłości.

Jeżeli przyczyną zdarzenia był **BŁĄD** użytkownika systemu informatycznego, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych.

Jeżeli przyczyną zdarzenia było **ZANIEDBANIE** ze strony użytkownika systemu należy wyciągnąć konsekwencje dyscyplinarne wynikające z Kodeksu pracy oraz Ustawy o ochronie danych osobowych.

Administrator bazy danych osobowych, w której nastąpiło naruszenie ochrony danych osobowych, w porozumieniu z właściwym lokalnym Inspektorem Ochrony Danych Osobowych (I ODO) przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia i w terminie 7 dni od daty jego zaistnienia przekazuje lokalnemu Administratorowi danych oraz Administratorowi Bezpieczeństwa Informacji (ABI).

Opracowano na podstawie:

[Ustawa z 10 maja 2018 r. o ochronie danych osobowych \(Dz. U. z 2018 r. poz. 1000\)](#)

Warszawa; dnia 15. 01. 2020 r.

Wykonano w 1 Egz.

- do powielenia w ilości egzemplarzy – wg potrzeb.

POLSKIE DRUŻYNY STRZELECKIE (PDS)

ZAŁĄCZNIK Nr ...

WYKAZ osób zapoznanych z „INSTRUKCJĄ postępowania...”

L. p.	Nazwisko i Imię	Stanowisko	Data i podpis
1	2	3	4
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			
23.			
24.			

POLSKIE DRUŻYNY STRZELECKIE (PDS)

„INSTRUKCJA postępowania...

zawiera 5

(pięć) stron
(słownie)

ponumerowanych

Warszawa; 15.01.2020 r.
(Miejscowość i data)