Załącznik nr 3
do Zarządzenia Nr 4/2018
Dyrektora Instytutu Spawalnictwa
z dnia 12.09.2018 r.

Instrukcja postępowania
w sytuacji naruszenia systemu ochrony danych osobowych
w Instytucie Spawalnictwa

§ 1.

1. Instrukcja przeznaczona jest dla osób zatrudnionych przy przetwarzaniu danych osobowych w Instytucie i należy ją stosować w powiązaniu z „Polityką bezpieczeństwa w zakresie ochrony danych osobowych w Instytucie Spawalnictwa" oraz „Instrukcją zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Instytucie Spawalnictwa".
2. Instrukcja określa tryb postępowania w przypadku, gdy:
   1) zaistniało podejrzenie naruszenia ochrony danych osobowych w systemie informatycznym lub w zbiorze danych osobowych zebranych i przetwarzanych w innej formie,
   2) stwierdzono naruszenie ochrony danych osobowych w systemie informatycznym lub w zbiorze danych osobowych zebranych i przetwarzanych w innej formie,

§ 2.

1. ***Naruszenie ochrony danych osobowych*** oznacza naruszenie bezpieczeństwa prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesłanych lub w inny sposób przetwarzanych.
2. W przypadku podejrzenia naruszenia ochrony danych należy przeprowadzić postępowanie wyjaśniające.

§ 3.

1. Każdy użytkownik, w przypadku stwierdzenia lub podejrzenia naruszenia zabezpieczenia zbioru danych osobowych w systemie informatycznym, zobowiązany jest niezwłocznie poinformować o tym ASI, który przekazuje informację IOD. IOD współdziała z ASI przy usuwaniu skutków naruszenia.
2. W przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych przetwarzanych w inny sposób należy fakt ten zgłosić IOD.

§ 4.

1. LADO komórki organizacyjnej w której zostało zgłoszone podejrzenie naruszenia lub w której stwierdzono naruszenie, zobowiązany jest wygenerować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia oraz złożyć pisemne wyjaśnienie IOD.
2. IOD na podstawie wyjaśnień przystępuje do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby nieupoważnionej.
3. Po ustaleniu stanu faktycznego IOD sporządza notatkę służbową, z którą zapoznaje ADO.
4. W przypadku naruszenia ochrony danych osobowych, ADO bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie **72 godzin** po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne , by naruszenie to skutkowało ryzykiem naruszenia praw i wolności osób fizycznych. Zgłoszenie musi zawierać wszystkie elementy wymienione w art.33 ust.3 RODO
5. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je ADO.

6. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, ADO bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Zawiadomienie nie jest wymagane w przypadkach wymienionych w art. 34 ust.3 RODO
7. ADO dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

§ 5.

1. LADO w porozumieniu z IOD niezwłocznie podejmuje odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu do danych osobie nieupoważnionej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów jej ingerencji.
2. W przypadku stwierdzenia lub podejrzenia naruszenia zabezpieczenia zbioru danych osobowych w systemie informatycznym ASI niezwłocznie podejmuje odpowiednie działania polegające w szczególności na:
   1) fizycznym odłączeniu urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nieupoważnionej,
   2) wylogowaniu użytkownika podejrzanego o naruszenie zabezpieczenia zbioru danych,
   3) zmianie haseł oraz czasowym odebraniu prawa dostępu użytkownikowi, poprzez którego hasło uzyskano nielegalny dostęp do danych.

§ 6.

ASI powinien sprawdzić:

1) stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
2) zawartość zbioru danych osobowych,
3) sposób działania programu,

oraz wykluczyć możliwość obecności wirusów komputerowych.

§ 7.

Po dokonaniu powyższych czynności, ASI powinien przeprowadzić i przedstawić IOD szczegółową analizę stanu systemu informatycznego obejmującą identyfikację:

1) rodzaju zaistniałego zdarzenia,
2) metody uzyskania dostępu do danych przez osobę nieupoważnioną,
3) skali zniszczeń lub zagrożeń.

§ 8.

ASI lub inna upoważniona przez niego osoba powinna, w porozumieniu z LADO, niezwłocznie przywrócić normalny stan działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, niezbędne jest odtworzenie jej z ostatniej kopii awaryjnej z zachowaniem wszelkiej ostrożności, mającej na celu uniknięcie ponownego uzyskania dostępu tą samą drogą przez osobę nieupoważnioną.

§ 9.

Po przywróceniu prawidłowego stanu bazy danych osobowych, ASI lub inna upoważniona przez niego osoba powinna, w porozumieniu z LADO, przeprowadzić szczegółową analizę w celu określenia przyczyny naruszenia ochrony danych osobowych oraz przedsięwziąć

kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości. Wnioski z analizy ASI przekazuje IOD.

§ 10.

Jeżeli przyczyną zdarzenia był/o:

1) istotny błąd osoby zatrudnionej przy przetwarzaniu danych osobowych - należy przeprowadzić dodatkowe szkolenie wszystkich osób biorących udział w przetwarzaniu danych,
2) zaniedbanie ze strony osoby zatrudnionej przy przetwarzaniu danych osobowych - należy wyciągnąć konsekwencje służbowe,
3) uaktywnienie wirusa - należy w miarę możliwości ustalić źródło jego pochodzenia oraz wykonać dodatkowe testy i zabezpieczenia antywirusowe,
4) zły stan urządzenia lub sposób działania programu - należy niezwłocznie przeprowadzić kontrolne czynności serwisowo-programowe,
5) włamanie w celu pozyskania bazy danych osobowych - należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających w celu zapewnienia skutecznej ochrony bazy danych.

ZATWIERDZAM

DYREKTOR
dr inż. Adam Pietras