Załącznik
do Zarządzenia Nr 12/2015
Dyrektora Instytutu Spawalnictwa
z dnia 01.12.2015 r.

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

§ 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 w Gliwicach" oraz „Instrukcją zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Instytucie Spawalnictwa w Gliwicach".
2. Instrukcja określa tryb postępowania w przypadku, gdy:
   - stwierdzono naruszenie zabezpieczenia systemu informatycznego lub naruszenie zabezpieczenia zbioru danych osobowych zebranych i przetwarzanych w innej formie,
   - stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych.

§ 2.

1. Dane osobowe zostają ujawnione, gdy stają się znane osobom nieuprawnionym w całości lub w części pozwalającej na określenie tożsamości osoby, której dane dotyczą.
2. W stosunku do danych osobowych, które zostały zagubione lub pozostawione bez nadzoru poza obszarem bezpieczeństwa, należy przeprowadzić postępowanie wyjaśniające, czy dane te należy uznać za ujawnione.

§ 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 ABI. ABI współdziała z ASI przy usuwaniu skutków naruszenia.
2. W przypadku stwierdzenia naruszenia ochrony danych osobowych przetwarzanych w inny sposób należy fakt ten zgłosić ABI.

§ 4.

ABI lub ASI (stosownie do rodzaju naruszenia) po uzyskaniu informacji o naruszeniu ochrony danych osobowych, powinien w pierwszej kolejności:

1) zapisać wszelkie informacje związane z danym zdarzeniem, a w szczególności dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych i czas samodzielnego wykrycia tego faktu,
2) wygenerować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia,
3) przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby nieupoważnionej.

§ 5.

1. ASI lub ABI (stosownie do rodzaju naruszenia) niezwłocznie podejmują 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 ABI 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, w porozumieniu z LADO, powinna 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 ABI.

§ 10.

Jeżeli przyczyną zdarzenia był/o:

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

§ 11.

ABI przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia, który w terminie nie przekraczającym 14 dni od daty zaistnienia zdarzenia, przekazuje ADO.

ZATWIERDZAM

DYREKTOR

dr inż. Adam Pietras