POLITYKA OCHRONY DANYCH OSOBOWYCH

W SYTUACJI NARUSZENIA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

W FUNDACJI RAZEM-CS

1. Niniejsza Polityka określa zasady dotyczące postępowania w przypadku wystąpienia zdarzeń w obszarze bezpieczeństwa przetwarzanych danych osobowych.
2. Przedstawione zasady w zakresie naruszeń bezpieczeństwa dotyczą danych osobowych przetwarzanych:
    a. W sposób tradycyjny
    b. W systemach informatycznych
3. Niniejsza Polityka określa tryb postępowania w przypadku, gdy:
    a. Stwierdzono naruszenie zabezpieczeń danych osobowych przetwarzanych w formie papierowej lub w systemie informatycznym
    b. Zawartość zbioru danych osobowych, stan sprzętu komputerowego, ujawnione metody pracy, sposób działania systemu mogą wskazywać na naruszenie zabezpieczeń danych osobowych
    c. Inne okoliczności mogą świadczyć o nieuprawnionym dostępie do danych osobowych.
4. Naruszeniami ochrony danych osobowych w systemie informatycznym są zdarzenia skutkujące częściową utratą funkcjonalności zasobów lub możliwości korzystania z zasobów, którymi m.in. mogą być:
    a. Wszelkiego rodzaju różnice w funkcjonowaniu systemu (np. Komunikaty informujące o błędach, brak dostępu do funkcji systemu, nieprawidłowości w wykonywanych operacjach)
    b. Stan stacji roboczej (np. brak zasilania, problemy z uruchomieniem)
    c. Różnice w zawartości zbioru danych osobowych (np. brak lub nadmiar danych)
    d. Inne zakłócenia pracy systemu
5. Każda osoba zatrudniona w Fundacji RAZEM-CS w Zamościu, stażysta, praktykant, który stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych powinien niezwłocznie poinformować o tym fakcie bezpośrednio przełożonego lub osobę zarządzającą systemem komputerowym i oprogramowaniem bądź Administratora Danych Osobowych.
6. Po otrzymaniu zgłoszenia zdarzenia dotyczącego zagrożenia bezpieczeństwa danych osobowych, niezwłocznie należy:
    a. Zapisać wszelkie informacje związane z danym zdarzeniem a szczególnie dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych

b. Wygenerować i wydrukować jeżeli zdarzenie dotyczy naruszenia zabezpieczenia danych w systemie informatycznym wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia, a następnie opatrzeć je datą i podpisem
c. Przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej
d. Podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu do danych osobie niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów jej ingerencji. W przypadku zdarzeń związanych z systemem teleinformatycznym, a w szczególności należy:
    i. Fizycznie odłączyć urządzenia i segmenty sieci, które mogły umożliwić dostęp do danych osobowych osobie niepowołanej
    ii. Wylogować użytkownika podejrzanego o naruszenie ochrony danych osobowych
    iii. Zmienić hasło na koncie użytkownika przez którego uzyskano nielegalny dostęp do danych osobowych w celu uniknięcia ponownej próby uzyskania takiego dostępu

7. jeżeli nieautoryzowane działania wystąpiły w systemie informatycznym służącym do przetwarzania danych osobowych Osoba zarządzająca sprzętem komputerowym i oprogramowaniem powinna podjąć działania zabezpieczające system teleinformatyczny (np. zablokowanie dostępu do serwerów)
8. Po wyeliminowaniu bezpośredniego zagrożenia należy przeprowadzić przegląd stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych.
9. Niezwłocznie należy przywrócić prawidłowy stan działania systemu.
10. Jeżeli nastąpiło uszkodzenie zawartości zbioru danych należy odtworzyć ją z kopii zapasowej z zachowaniem wszelkich środków ostrożności, mających na celu uniknięcie ponownego uzyskania dostępu tą samą drogą przez osobę niepowołaną.
11. Po przywróceniu prawidłowego stanu zawartości zbioru danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyny naruszania ochrony danych osobowych oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości:

a. Jeżeli przyczyną zdarzenia było zaniedbanie ze strony zatrudnionej osoby przy przetwarzaniu danych osobowych, należy wyegzekwować konsekwencje uregulowane przepisami o ochronie danych osobowych
b. Jeżeli przyczyną zdarzenia był błąd osoby zatrudnionej przy przetwarzaniu danych osobowych, należy przeprowadzić dodatkowe szkolenie osób biorących udział przy przetwarzaniu danych
c. Jeśli przyczyną zdarzenia było uaktywnienie wirusa, należy ustalić źródło jego pochodzenia oraz wykonać odpowiednie zabezpieczenia antywirusowe
d. Jeśli przyczyną zdarzenia było włamanie w celu pozyskania danych osobowych, należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających w celu zapewnienia skuteczniejszej ochrony danych
e. Jeśli przyczyną zdarzenia było uszkodzenie sprzętu lub awaria systemu informatycznego, należy przeprowadzić kontrolę przeglądów oraz konserwacji sprzętu, urządzeń i systemów
f. Jeśli przyczyną zdarzenia był zły stan urządzenia lub awarii sytemu informatycznego, wówczas należy niezwłocznie podjąć kontrolę czynności serwisowych/naprawczych.

12. Administrator Danych Osobowych lub osoba zarządzająca sprzętem komputerowym i oprogramowaniem przygotowuje szczegółowy raport dotyczący przyczyn, okoliczności i wniosków z zaistniałego naruszenia ochrony danych osobowych (dołączając ewentualnie kopie dowodów dokumentujących to zdarzenie).