PROCEDURA POSTĘPOWANIA
W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH
W
SPÓŁCE ZARGOOD INTERNATIONAL SP. Z O.O. SP. K. Z SIEDZIBĄ W KRAKOWIE
KRS: 0000513116, NIP: 6751503331, REGON: 123138170

Opracowana na podstawie:
Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej jako: „RODO").

§ 1.
Postanowienia ogólne:

1. Niniejsza Procedura Postępowania w Sytuacji Naruszenia Ochrony Danych Osobowych (dalej, jako **PROCEDURA**) zawiera opis procedur wykrywania oraz klasyfikowania naruszeń ochrony danych osobowych, a także reguluje procedury postępowania w razie zaistnienia takich naruszeń.
2. Niniejsza PROCEDURA obejmuje obszar siedziby Spółki Zargood International Sp. z o.o. Sp. k. z siedzibą w Krakowie, zwanej dalej również **SPÓŁKĄ**, tj. pomieszczenia zajmowane przez SPÓŁKĘ przy Al. Pokoju 78 w Krakowie.
3. Budynki lub pomieszczenia, w których przetwarzane są dane, powinny być zamykane na czas nieobecności użytkowników, w sposób uniemożliwiający do nich dostęp osób trzecich.
4. Przebywanie osób nieuprawnionych wewnątrz obszaru, w którym są przetwarzane dane jest możliwe tylko w obecności użytkownika i za zgodą przełożonego.
5. Do stosowania niniejszej PROCEDURY obowiązani są wszyscy pracownicy oraz współpracownicy SPÓŁKI upoważnieni do przetwarzania danych osobowych, na podstawie pisemnego upoważnienia, jak i podmioty, którym SPÓŁKA, jako Administrator danych osobowych powierzyła przetwarzanie danych osobowych na podstawie odrębnej umowy.

§ 2.

Celem PROCEDURY jest ustalenie jednolitych zasad postępowania w przypadku, gdy:

- Stwierdzone zostało naruszenie lub istnieje podejrzenie naruszenia ochrony danych osobowych, zgromadzonych w systemach informatycznych lub na innych nośnikach informacji, w tym nośnikach papierowych.
- Stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zasad ochrony danych.

§ 3.

1. Codzienną kontrolę w zakresie ochrony danych osobowych sprawuje użytkownik.
2. Nadzór nad przestrzeganiem zasad ochrony danych osobowych w SPÓLCE sprawuje przełożony.

§ 4.

1. Naruszenie ochrony danych osobowych może być spowodowane:

a. niewłaściwym oddziaływaniem czynników zewnętrznych, takich jak: temperatura otoczenia, wilgotność, pole elektromagnetyczne, wirusy komputerowe, skutki powodzi, pożaru, itp.;
b. niekontrolowanym działaniem osób trzecich, powodującym zakłócenia systemu podczas włamania, niewłaściwym działaniem zespołów serwisowych, przetwarzaniem danych osobowych bez uprawnień, tworzeniem w zbiorach użytkownika nieautoryzowanych kont dostępu;
c. umyślnym lub nieumyślnym działaniem, a także zaniechaniem działania użytkowników przetwarzających dane osobowe.

2. Za naruszenie ochrony danych osobowych uważa się w szczególności:
   a. brak możliwości fizycznego dostępu do danych np. zagubiony klucz do pomieszczenia lub mebli biurowych, w których przechowywane są dokumenty, zniszczona szafa z dokumentami, brak nośników informacji, zalane pomieszczenie, brak sprzętu komputerowego, itp.;
   b. brak dostępu do zawartości zbioru danych – zbiór istnieje, lecz nie można go otworzyć;
   c. zmienioną zawartość zbioru, niepoprawną treść, postać, różnicę w danych, itp.;
   d. próbę lub fakt nieuprawnionego dostępu do zbioru danych lub pomieszczenia, w którym jest przetwarzany np. zmiana ułożenia kolejności dokumentów, otwarte drzwi lub meble biurowe, nietypowe ustawienie sprzętu lub pojawienie się nowych dokumentów;
   e. różnicę funkcjonowania systemu, a w szczególności wyświetlania komunikatów i informacji o błędach oraz nieprawidłowościach w wykonywaniu operacji;
   f. zniszczenie lub próby zniszczenia, w sposób nieautoryzowany danych ze zbioru lub danych systemowych;
   g. zmianę lub utratę danych zapisanych na kopiach awaryjnych lub zapisach archiwalnych;
   h. nieskuteczne niszczenie nośników informacji zawierających dane osobowe (płyty, pen drive, nośniki optyczne, wydruki papierowe), umożliwiające ponowny ich odczyt przez osoby nieuprawnione;
   i. próba nielegalnego logowania się do systemu lub włamania do systemu;
   j. zmienione oprogramowanie systemu, stwierdzone przez użytkownika po przerwie w przetwarzaniu danych.
3. Niniejszą PROCEDURĘ stosuje się także w przypadku stwierdzenia, że stan pomieszczeń i szaf, bądź mebli biurowych, w których przechowuje się dokumentację lub zawartości tej dokumentacji wzbudzają podejrzenie, że dostęp do nich mogły mieć osoby trzecie.

§ 5.

Za naruszenie zasad ochrony danych osobowych uważa się w szczególności:

1. nieupoważniony dostęp, modyfikację, kopiowanie lub zniszczenie/usunięcie danych osobowych, zarówno w systemie informatycznym, jak i na nośnikach papierowych i elektronicznych,
2. udostępnianie danych osobowych nieuprawnionym podmiotom lub osobom,
3. nieautoryzowany dostęp do danych przez połączenie sieciowe,
4. nieautoryzowany dostęp do pomieszczeń, w których przetwarza się dane osobowe,
5. niedopełnienie obowiązku ochrony danych osobowych przez umożliwienie dostępu do danych (np. pozostawienie kopii danych, niezablokowanie dostępu do systemu, brak nadzoru nad serwisantami i innymi osobami nieuprawnionymi przebywającymi w pomieszczeniach gdzie przetwarza się dane osobowe,
6. wykrycie niezabezpieczonego kanału dystrybucji danych osobowych,
7. nielegalne bądź nieświadome ujawnienie danych osobowych,

8. pozyskiwanie danych osobowych z nielegalnych źródeł,
9. przetwarzanie danych osobowych niezgodne z uprawnionym celem i zakresem,
10. stwierdzenie obecności wirusów komputerowych lub innych programów godzących w integralność systemu informatycznego,
11. ujawnienie indywidualnych haseł dostępu do danych osobowych w systemie,
12. przesyłanie danych osobowych przez Internet bez zabezpieczenia,
13. przesyłanie dokumentów papierowych i nośników elektronicznych z danymi bez zabezpieczenia,
14. wykonanie nieuprawnionych kopii danych osobowych,
15. naruszenie bezpieczeństwa kopii danych osobowych,
16. kradzież nośników zawierających dane osobowe lub oprogramowanie,
17. kradzież sprzętu służącego do przetwarzania danych osobowych,
18. utratę danych osobowych w systemie informatycznym, na kopiach bezpieczeństwa i na innych nośnikach,
19. brak aktualnych kopii bezpieczeństwa danych osobowych lub brak odpowiednich nośników do sporządzania kopii,
20. niewłaściwe niszczenie nośników z danymi osobowymi pozwalające na ich odczyt,
21. naruszenie zasad ochrony fizycznej pomieszczeń, w których przetwarza się dane osobowe,
22. dopuszczenie do przetwarzania danych osobowych pracowników bez odpowiednich upoważnień,
23. nie przeszkolenie pracowników w zakresie bezpieczeństwa danych osobowych,
24. inne sytuacje wskazujące lub potwierdzające naruszenie bezpieczeństwa danych osobowych w SPÓŁCE.

§ 6.

O możliwości zaistnienia przypadku naruszenia zasad ochrony danych osobowych mogą świadczyć m.in.:

1. nadmierne, w stosunku do wykonywanych zadań (zakres upoważnienia), uprawnienia użytkownika do zasobów systemu,
2. niestabilna praca systemu, w którym przetwarza się dane osobowe,
3. korzystanie z zasobów systemu poza godzinami pracy (bez zgody przełożonego),
4. nowe „podejrzane" konta użytkowników,
5. wysoka aktywność kont, które długo pozostawały niewykorzystane,
6. zanotowanie w krótkim czasie dużej liczby nieudanych prób logowania (zakładamy jednakże, że system jest tak skonfigurowany, iż po trzech próbach podania błędnego hasła wymaga interwencji administratora),
7. anomalie w pracy systemu lub programu (świadczące np. o obecności wirusa),
8. naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach, w których przetwarza się dane osobowe (wyłamane lub zacinające się zamki, naruszone plomby, niedomykające się okna itp.),

§ 7.

Osoba, która podejrzewa lub stwierdzi naruszenie zasad ochrony danych osobowych ma obowiązek niezwłocznie (bezpośrednio lub telefonicznie):

1. powiadomić o zaistniałym zdarzeniu swojego przełożonego,
2. określić (opisać) symptomy świadczące o możliwości naruszenia lub naruszeniu zasad ochrony danych,

3. określić sytuację i czas w jakim je zauważono,
4. podać wszelkie istotne informacje mogące pomóc w ustaleniu przyczyny naruszenia zasad ochrony danych osobowych,
5. nie podejmować dalszej pracy w systemie informatycznym bez decyzji przełożonego.

§ 8.

Przełożony ocenia sytuację i podejmuje odpowiednie do potrzeb działania, a w szczególności:

1. dokonuje rozpoznania zdarzenia,
2. ocenia wagę problemu,
3. ocenia możliwość wystąpienia strat w zasobach informacyjnych i systemowych w przypadku dalszego działania systemu,
4. lokalizuje źródło problemu (przeprowadza analizę posiadanych danych).

§ 9.

W przypadku stwierdzenia, że podejrzenie nie świadczy o naruszeniu zasad ochrony danych, przełożony po przeanalizowaniu sytuacji i wyeliminowaniu możliwości wystąpienia ich w przyszłości, podejmuje decyzję o dalszej pracy systemu.

§ 10.

Każda interwencja przełożonego kończy się niezwłoczną analizą postępowania i sporządzeniem raportu.

§ 11.

Każda informacja o naruszeniu ochrony danych i jego okolicznościach, kierowana poza SPÓLKĘ, może być przekazana wyłącznie przez administratora danych osobowych lub wyznaczoną przez niego osobę.

§ 12.

Każda osoba dopuszczona do przetwarzania danych osobowych obowiązana jest zapoznać się z niniejszą PROCEDURĄ oraz złożyć stosowne oświadczenie dotyczące znajomości wymienionych regulacji.

§ 13.

1. Osoba upoważniona do przetwarzania danych osobowych za naruszenie obowiązków, wynikających z niniejszej PROCEDURY i przepisów o ochronie danych osobowych ponosi odpowiedzialność:
   a. przewidzianą w Regulaminie Pracy oraz Kodeksie Pracy (Dz. U. z 1974 r. Nr 24, poz. 141 ze zm.) za ciężkie naruszenie podstawowych obowiązków pracowniczych, gdy naruszenia dopuścił się pracownik;
   b. przewidzianą za istotne naruszenie innego stosunku prawnego, na podstawie którego została upoważniona do przetwarzania danych osobowych, w przypadku innej osoby niż pracownik.