Wyciąg z Polityki ochrony danych osobowych IT CONNECT Sp. z o.o.
Dokumentacja, rejestr, ocena, audyty

Dokumentacja ochrony danych osobowych

1) IT CONNECT Sp. z o.o. prowadzi dokumentację ochrony danych osobowych na którą składają się:
    a. opis obszaru przetwarzania danych osobowych zgodnie z pkt. 1
    b. opis zasobów danych osobowych zgodnie z pkt. 2
    c. ewidencje o których mowa w ppkt. 2)
    d. rejestr czynności przetwarzania
    e. dokumentacja audytów o której mowa w ppkt. 3)
    f. umowy z podmiotami przetwarzającymi
    g. umowy ze współadministratorami
2) w ramach dokumentacji ochrony danych osobowych prowadzone są następujące ewidencje:
    a. inspektor ochrony danych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych,
    b. Specjalista ds. kadr i Koordynator Projektów Rekrutacyjnych prowadzi ewidencję udostępnień danych osobowych,
    c. administrator systemu prowadzi ewidencję użytkowników systemu informatycznego, a także ewidencję komputerów przenośnych.
3) na dokumentację audytów, o których mowa w ppkt. 1 lit. d) składają się:
    a. dokumentacja sprawdzeń planowych
    b. dokumentacja sprawdzeń doraźnych

Rejestr czynności przetwarzania

1) IT CONNECT Sp. z o.o prowadzi rejestr czynności przetwarzania tak, by był on zgodny z wymogami art. 30 RODO. Przeprowadzając okresowy przegląd dokumentacji (…) dokonuje się oceny spełnienia powyższego wymogu.
2) IT CONNECT Sp. z o.o przekazuje rejestr czynności przetwarzania organowi nadzorczemu na jego żądanie.

Ocena skutków przetwarzania

1) Ocena skutków o której mowa w ppkt. 1) obejmuje:
    a. systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
    b. ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
    c. wskazanie środków zaplanowanych w celu zaradzenia ryzyku, ze szczególnym

wyróżnieniem tych opracowanych i wdrożonych

d. ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą

Audyty wewnętrzne

1) W celu zapewnienia przestrzegania przepisów o ochronie danych osobowych inspektor ochrony danych przeprowadza następujące audyty wewnętrzne:

   - sprawdzenie prawidłowości i aktualności dokumentacji z zakresu ochrony danych osobowych;

   - sprawdzenie przestrzegania zasad i procedur określonych w dokumentacji ochrony danych osobowych.

   - sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

2) Audyty wewnętrzne wskazane w ppkt. 1) są przeprowadzane okresowo zgodnie z planem sprawdzeń przygotowywanym przez inspektora ochrony danych osobowych (sprawdzenia planowe). Plan sprawdzeń obejmuje maksimum 1 rok. Jest on przekazywany administratorowi danych do wiadomości w terminie minimum 2 tygodni przed rozpoczęciem okresu, który plan obejmuje. Jeśli sprawdzenie planowe obejmuje kontrolę w konkretnej jednostce lub dziale to kierownik tej jednostki jest zawiadamiany o sprawdzeniu nie później niż na 7 dni przed rozpoczęciem sprawdzenia.

Niezależnie od działań wskazanych w ppkt. 1) inspektor ochrony danych nie rzadziej niż raz do roku przeprowadza audyt przestrzegania zasad i procedur ochrony danych osobowych w IT CONNECT.

NARUSZENIE OCHRONY DANYCH OSOBOWYCH

Postępowanie w przypadku stwierdzenia lub podejrzenia stwierdzenia naruszenia ochrony danych osobowych

1) Zasady postępowania w przypadku stwierdzenia naruszenia lub podejrzenia naruszenia bezpieczeństwa systemu informatycznego określa *Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w* IT CONNECT Sp. z o.o..

2) Każdy kto stwierdził inne niż określone w ppkt. 1) naruszenie ochrony danych osobowych lub podejrzewa takie naruszenie powinien niezwłocznie poinformować o tym inspektora procesów biznesowych. Jako inne niż określone w ppkt. 1) naruszenie rozumie się w szczególności brak realizacji lub niewłaściwą realizację wymogów określonych w części VI niniejszej *Polityki*.

3) Inspektor ochrony danych po otrzymaniu zawiadomienia, o którym mowa w ppkt. 2) przeprowadza niezwłocznie postępowanie wyjaśniające w celu ustalenia czy naruszenie ochrony danych osobowych miało miejsce (tzw. sprawdzenie doraźne).

4) Sprawdzenie doraźne może zostać wszczęte przez inspektora procesów biznesowych, także z własnej inicjatywy, gdy w inny sposób niż w skutek zawiadomienia poweźmie informację o naruszeniu lub możliwym naruszeniu ochrony danych osobowych.

5) W przypadku stwierdzenia naruszenia ochrony danych osobowych w trybie określonym w

ppkt. 3 lub 4) inspektor ochrony danych :

a. w porozumieniu z odpowiednim kierownikiem podejmuje niezwłoczne, możliwe do wprowadzenia na bieżąco, działania zapobiegające dalszemu naruszaniu ochrony danych osobowych,

b. w porozumieniu z odpowiednim kierownikiem stosuje niezwłoczne, możliwe do wprowadzenia na bieżąco, środki eliminujące lub zmniejszające ryzyko naruszenia praw lub wolności osoby, której dane dotyczą,

c. sporządza raport naruszenia ochrony danych osobowych, a następnie niezwłocznie przekazuje jego kopię administratorowi danych.

6) Raport o którym mowa w ppkt. 5 lit. c) zawiera w szczególności:

a. opis okoliczności naruszenia ochrony danych osobowych;

b. opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazuje kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

c. opis możliwych konsekwencji naruszenia ochrony danych osobowych;

d. ocenę czy jest prawdopodobne, że naruszenie skutkowało ryzykiem lub wysokim ryzykiem naruszenia wolności lub praw osób fizycznych;

e. wskazanie zastosowanych lub proponowanych działań zaradczych, ze szczególnym uwzględnieniem takich, które zmierzają do zminimalizowania ewentualnych negatywnych skutków naruszenia.

7) Administrator danych osobowych po zapoznaniu się z raportem o którym mowa w ppkt. 6) podejmuje decyzje o dalszym trybie postępowania, a w szczególności:

a. jeśli to właściwe, zarządza podjęcie czynności zmierzających do usunięcia naruszenia i jego skutków oraz zapobieżeniu naruszeniom ochrony danych osobowych na przyszłość.

b. jeśli to możliwe, zarządza zastosowanie środków eliminujących lub zmniejszających prawdopodobieństwo ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,

c. jeśli jest to właściwe zawiadamia o naruszeniu właściwe organy, w tym zgłasza naruszenie organowi nadzorczemu oraz informuje o naruszeniu osoby, których naruszenie dotyczy. Do zgłasza naruszeni organowi nadzorczemu zgodnie z art. 33 ust. 1 RODO oraz zawiadamia o naruszeniu osób, których dane dotyczą zgodnie z art. 34 ust. 1 RODO stosuje się postanowienia pkt. 2 i 3 niniejszej części,.

Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu i zawiadomienie osoby, której dane dotyczą.

1) Jeśli administrator danych ustali, że jest prawdopodobne, że naruszenie ochrony danych osobowych stwierdzone w trybie określonym w pkt. 1 skutkowało ryzykiem naruszenia wolności lub praw osób fizycznych nakazuje inspektorowi ochrony danych osobowych przygotowanie projektu zgłoszenia naruszenia organowi nadzorczemu,

2) Zgłoszenie naruszenia wskazane w ppkt. 1) zawiera, w szczególności:

a. informacje zawarte w raporcie, zgodnie z pkt. 1 ppkt. 6),

b. wskazanie imienia i nazwiska oraz danych kontaktowych inspektora ochrony danych osobowych jako osoby właściwej do kontaktu w sprawie. W szczególnych przypadkach, po konsultacji z administratorem danych osobowych, do kontaktu w sprawie może być wskazana inna osoba niż inspektor ochrony danych .

3) Zgłoszenie naruszenia ochrony danych osobowych, o którym mowa w ppkt. 1-2) administrator danych zatwierdza i przekazuje organowi nadzorczemu bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.

4) Jeżeli dotrzymanie terminu wskazanego w ppkt. 3) jest niemożliwe administrator danych do zgłoszenia dołącza wyjaśnienie przyczyn opóźnienia. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić od razu, administrator danych udziela tych informacji sukcesywnie, bez zbędnej zwłoki.

Zawiadomienie osoby, której dane dotyczą.

1) Jeśli administrator danych ustali, że naruszenie ochrony danych osobowych stwierdzone w trybie określonym w pkt. 1 może powodować wysokie ryzyko naruszenia wolności lub praw osób fizycznych i nie da się zastosować środków eliminujących to wysokie ryzyko, nakazuje inspektorowi ochrony danych osobowych przygotowanie projektu zawiadomienia o naruszeniu dla wszystkich osób, których danych naruszenie dotyczy.

2) Zawiadomienie o którym mowa w ppkt. 1) powinno być napisane jasnym i prostym językiem oraz zawierać, w szczególności:

   a. opis charakteru naruszenia,

   b. opis możliwych konsekwencji naruszenia,

   c. wskazanie zastosowanych lub planowanych działań zaradczych, ze szczególnym uwzględnieniem takich, które mogą zminimalizować ewentualne negatywne skutki naruszenia,

   d. wskazanie imienia i nazwiska oraz danych kontaktowych inspektorowi ochrony danych osobowych, jako osoby właściwej do kontaktu w sprawie. W szczególnych przypadkach, po konsultacji z administratorem danych osobowych, do kontaktu w sprawie może być wskazana inna osoba niż inspektor ochrony danych .

3) Zawiadomienie o naruszeniu ochrony danych osobowych, o którym mowa w ppkt. 1-2) administrator danych zatwierdza i przekazuje niezwłocznie wszystkim osobom, których danych naruszenie dotyczy.

4) Jeżeli administrator danych oceni, że realizacja wymogów określonych w ppkt. 1-3) wymagałoby niewspółmiernie dużego wysiłku, w szczególności niewspółmiernie dużego wysiłku wymagałoby nawiązanie bezpośredniego, indywidualnego kontaktu z osobami, których danych naruszenie dotyczy, może podjąć decyzje o przekazaniu informacji zainteresowanym poprzez wydanie publicznego komunikatu lub o zastosowaniu innego podobnego środka, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Dokumentacja naruszenia ochrony danych osobowych.

1) Inspektor ochrony danych prowadzi dokumentację naruszenia danych osobowych.

2) W skład dokumentacji o której mowa w ppkt. 1) wchodzą:
    a. kopia raportu o którym mowa w pkt. 1 ppkt. 6,
    b. kopia zgłoszenia o którym mowa w pkt. 2
    c. kopie zawiadomień o których mowa w pkt. 3
    d. wszelkie inne dokumenty, w tym notatki służbowe, pliki, zdjęcia i inne dowody zebrane w trakcie przeprowadzania czynności wyjaśniających pozwalające ustalić okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.
3) Dokumentacja naruszenia ochrony danych osobowych pozostaje do wglądu organu nadzorczego.