

INSTRUKCJA POSTĘPOWANIA W SYTUACJI STWIERDZENIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Celem określenia możliwych naruszeń w zakresie ochrony danych osobowych oraz opisanie procedur postępowania w przypadku ich wystąpienia, w szczególności prowadzących do należytego wyjaśnienia okoliczności naruszenia i jego udokumentowania, jak również celem ograniczenia występowania podobnych naruszeń w przyszłości, przyjmuje się niniejszą Instrukcję i zobowiązuje się pracowników i zleceniobiorców firmy „Instytut Dietetyki i Promocji Zdrowia Katarzyna Kaszyca” do jej bezwzględnego stosowania.

1. Pojęcia użyte w Instrukcji oznaczają:

- 1) Rozporządzenie - Rozporządzenie 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, zwane „Rozporządzeniem” lub „RODO”
- 2) Administrator - Katarzyna Kaszyca prowadząca działalność gospodarczą pod firmą „Instytut Dietetyki i Promocji Zdrowia Katarzyna Kaszyca” (adres stałego miejsca wykonywania działalności: ul. Kosztowska 27, 41-409 Mysłowice).
- 3) Naruszenie ochrony danych / naruszenie - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

2. Integralną częścią Instrukcji stanowi *Raport w związku z naruszeniem ochrony danych osobowych* (załącznik Nr 1). Raport opracowuje Administrator lub osoba przez niego upoważniona. Wszystkie naruszenia są ewidencjonowane. Za ewidencję naruszeń przyjmuje się zbiór raportów, o których mowa w niniejszym punkcie.

3. W przypadku stwierdzenia naruszenia:

- a. zabezpieczenia systemu informatycznego,
 - b. technicznego stanu urządzeń,
 - c. zawartości dokumentów lub baz zawierających dane osobowe,
 - d. jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych,
 - e. innych zdarzeń mogących mieć wpływ na naruszenie bezpieczeństwa danych osobowych,
- każdy pracownik lub zleceniobiorca Administratora jest obowiązany niezwłocznie powiadomić o tym fakcie Administratora lub osobę przez niego upoważnioną do przyjmowania takich zgłoszeń.

4. Do czasu pojawienia się w miejscu naruszenia Administratora lub osoby przez niego upoważnionej bądź uzyskania od nich poleceń co do dalszego postępowania, należy niezwłocznie:

- a. podjąć czynności niezbędne do zapobieżenia niepożądanym skutkom zaistniałego naruszenia lub ich maksymalnego ograniczenia, a następnie uwzględnić w działaniu również potrzebę ustalenia przyczyn naruszenia i jego sprawców i postępować tak, by ustalenia tych okoliczności nie utrudnić;
 - b. rozważyć wstrzymanie bieżącej pracy, w szczególności na urządzeniu dotkniętym naruszeniem, lub pracy biurowej w ogóle jeżeli wydaje się to potrzebne (np. w celu zabezpieczenia miejsca zdarzenia);
 - c. zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę naruszenia;
 - d. podjąć inne działania przewidziane i określone w instrukcjach technicznych stosownie do objawów i komunikatów towarzyszących naruszeniu;
 - e. podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej;
 - f. zastosować się do odpowiednich instrukcji i regulaminów, jeśli odnoszą się one do zaistniałego przypadku;
 - g. udokumentować wstępnie zaistniałe naruszenie;
 - h. nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu zgłoszenia naruszenia Administratorowi lub osobie upoważnionej, a następnie wykonywać ich polecenia.
5. Po przybyciu na miejsce naruszenia lub w miarę możliwości z wykorzystaniem środków porozumiewania się na odległość, Administrator lub osoba przez niego upoważniona:
- a. rozpoznaje zaistniałą sytuację i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Administratora;
 - b. może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem;
 - c. nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza wewnętrznej struktury Administratora.
6. Po przywróceniu prawidłowego stanu należy przeprowadzić szczegółową analizę w celu określenia przyczyny naruszenia bezpieczeństwa informacji oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
- a. Jeżeli przyczyną zdarzenia był błąd osoby zatrudnionej przy przetwarzaniu danych osobowych w systemie informatycznym, należy pouczyć ją o prawidłowym postępowaniu, a także rozważyć przeprowadzenie dodatkowego szkolenia osób biorących udział przy przetwarzaniu danych.
 - b. Jeżeli przyczyną było uaktywnienie złośliwego oprogramowania, należy ustalić źródło jego pochodzenia oraz wykonać lub zaktualizować zabezpieczenia antywirusowe.
 - c. Jeżeli przyczyną zdarzenia było rażące zaniedbanie ze strony osoby zatrudnionej przy przetwarzaniu danych osobowych, należy rozważyć wyciągnięcie odpowiednich konsekwencji zgodnie z przepisami kodeksu pracy lub umowy wiążącej tę osobą z Administratorem.

- d. Jeżeli przyczyną zdarzenia było włamanie w celu pozyskania bazy danych osobowych, należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających w celu zapewnienia skuteczniejszej ochrony danych osobowych.
- e. Jeżeli przyczyną zdarzenia był zły stan urządzeń lub wadliwy sposób działania oprogramowania, należy niezwłocznie przeprowadzić kontrolne czynności serwisowo - programowe.

7. Administrator lub osoba przez niego upoważniona dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który zawiera w szczególności opis okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja w postaci raportu musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania przez Administratora art. 33 RODO.

Raport, o którym mowa powyżej, składa się do ewidencji naruszeń.

Administrator lub osoba przez niego upoważniona, celem uwzględnienia w raporcie wszystkich istotnych okoliczności dotyczących naruszenia, powinna przy sporządzaniu raportu posilkować się, oprócz wzoru Raportu, również formularzem zgłoszenia naruszenia Prezesowi Urzędu Ochrony Danych Osobowych dostępnym na stronie internetowej Prezesa Urzędu Ochrony Danych Osobowych, nawet jeśli naruszenie takiemu zgłoszeniu nie podlega. Formularz taki stanowi załącznik do niniejszej Instrukcji (Załącznik Nr 2).

8. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Administrator lub osoba przez niego upoważniona zasięga niezbędnych opinii i proponuje postępowanie naprawcze, a w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych.
9. Zaistniałe naruszenie może stać się przedmiotem szczegółowej analizy prowadzonej przez zespół powołany przez Administratora. Analiza ta, powinna zawierać wszechstronną ocenę zaistniałego naruszenia, wskazanie odpowiedzialnych za wystąpienie naruszenia osób, wnioski co do ewentualnych przedsięwzięć, których podjęcie powinno zapobiec podobnym naruszeniom w przyszłości.
10. Raport, o którym mowa w pkt. 2 i 7 niniejszej Instrukcji, sporządza się i załącza do ewidencji w każdym przypadku stwierdzenia naruszenia, niezależnie od tego czy zastosowanie mają procedury opisane w pkt. 11 i 12 niniejszej Instrukcji.
11. W ciągu 72 godzin po stwierdzeniu naruszenia, naruszenie to należy zgłosić do Organu Nadzorczego, chyba, że jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
12. W przypadku gdy z analizy naruszenia wyniknie, że naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Zawiadomienia takiego nie dokonuje się gdy:
- a. Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności

środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

- b. Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby;
- c. wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Raport nr/.....			
w związku z naruszeniem ochrony danych osobowych			
Data wystąpienia naruszenia		Godzina wystąpienia naruszenia	
Osoba powiadamiająca o zaistniałym zdarzeniu (Imię i nazwisko, stanowisko)			
Lokalizacja naruszenia (ewentualnie dane kontaktowe podmiotu przetwarzającego, u którego doszło do naruszenia)			
Charakterystyka naruszenia bezpieczeństwa, oraz okoliczności towarzyszące			
Działania zaradcze podjęte niezwłocznie przez osoby znajdujące się na miejscu ujawnienia naruszenia			
Działania zaradcze podjęte po kontakcie z administratorem lub osobą przez niego upoważnioną			
Ustalone przyczyny wystąpienia zdarzenia			
Skutki wystąpienia naruszenia			
Decyzja co do zgłoszenia naruszenia do Prezesa Urzędu Ochrony Danych Osobowych wraz z uzasadnieniem, oraz ewentualną datą i godziną dokonania zawiadomienia			
Decyzja co do poinformowania osób których dane dotyczą, wraz z uzasadnieniem oraz ewentualną datą i wskazaniem formy takiego zawiadomienia			
Data i podpis Administratora lub osoby upoważnionej			