Załącznik do zarządzenia Nr 33/2022
Wójta Gminy Tarnówka
z dnia 12 kwietnia 2022 r.

pieczątka

Instrukcja Postępowania w Sytuacji Naruszeń podczas przetwarzania dokumentacji w postaci tradycyjnej oraz elektronicznej

Administrator Danych Osobowych – Jacek Mościcki – Wójt Gminy Tarnówka

Zgodnie z art. 32 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 RODO) oraz zgodnie z USTAWĄ z dnia 10 maja 2018 r. o ochronie danych osobowych Dz. U. 2018 poz. 1000 Administrator Danych Osobowych wdraża dokument o nazwie: „**Instrukcja Postępowania w Sytuacji Naruszeń podczas przetwarzania dokumentacji w postaci tradycyjnej oraz elektronicznej".**

Istota naruszenia bezpieczeństwa informacji

Zagrożenia losowe zewnętrzne, w szczególności klęski żywiołowe, przerwy w zasilaniu mogą prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu.

Zagrożenia losowe wewnętrzne, w szczególności niezamierzone pomyłki operatorów, administratora systemu, awarie sprzętowe, błędy oprogramowania mogądoprowadzić do zniszczenia danych, zakłócenia ciągłość pracy systemu, naruszenia poufności danych.

Zagrożenia zamierzone, świadome i celowe najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na:

a) nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu),
b) nieuprawniony dostęp do systemu z jego wnętrza,
c) nieuprawniony przekaz danych,
d) pogorszenie jakości sprzętu i oprogramowania,
e) bezpośrednie zagrożenie materialnych składników systemu.

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to w szczególności:

a) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej, itp.,
b) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu,
c) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
d) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
e) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
f) stwierdzenie próby lub modyfikacji danych lub zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
g) wystąpienie niedopuszczalnej manipulacji danymi osobowymi w systemie,
h) ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń,
i) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.,
j) ujawnienie, istnienie nieautoryzowanych kont dostępu do danych,
k) podmienienie lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowanie lub skopiowanie danych osobowych,
l) rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

Za naruszenie ochrony danych w podmiocie uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), zdjęciach, płytach w formie niezabezpieczonej itp.

Postępowanie w przypadku naruszenia bezpieczeństwa informacji

Każdy pracownik podmiotu biorący udział w przetwarzaniu danych osobowych w systemie informatycznym (lub przetwarzanych w inny sposób) jest odpowiedzialny za bezpieczeństwo tych danych.

Każda osoba zatrudniona w podmiocie, która zauważyła zdarzenie mogące być przyczyną naruszenia ochrony danych osobowych lub mogących spowodować naruszenie bezpieczeństwa

danych, zobowiązana jest do natychmiastowego poinformowania Administratora Danych Osobowych.

Informacja o pojawieniu się zagrożenia lub wystąpieniu zagrożenia danych osobowych w podmiocie powinna być przekazywana przez pracownika osobiście, telefonicznie lub pocztą elektroniczną. Powinna zawierać imię i nazwisko osoby zgłaszającej oraz zauważone symptomy zagrożenia.

W przypadku gdy zgłoszenie o podejrzeniu zaistnienia incydentu otrzyma osoba inna niż Administrator Danych Osobowych, jest ona obowiązana poinformować o tym fakcie Administratora Danych Osobowych.

Każdy pracownik podmiotu, który stwierdzi fakt naruszenia bezpieczeństwa ma obowiązek:

a) podjąć czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość,
b) zaniechać wszelkich działań mogących uniemożliwić analizę wystąpienia naruszenia i udokumentowanie zdarzenia,
c) zabezpieczyć dostęp do miejsca lub urządzenia przez osoby trzecie,
d) wstrzymać pracę na komputerze na którym zaistniało naruszenie ochrony oraz nie uruchamiać bez koniecznej potrzeby komputerów i innych urządzeń, których funkcjonowanie w związku naruszeniem ochrony zostało wstrzymane,
e) podjąć stosownie do zaistniałej sytuacji, inne niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych,
f) powinien wstępnie udokumentować zaistniałe naruszenie.

Administrator Danych Osobowych niezwłocznie po uzyskaniu sygnału o naruszeniu danych osobowych, powinien:

a) zapoznać się z zaistniałą sytuacją i dokonać wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy podmiotu,
b) zapisać wszelkie informacje związane z danym zdarzeniem,
c) nawiązać kontakt ze specjalistami jeżeli zachodzi taka potrzeba,
d) przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej,
e) zażądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
f) poinformować o naruszeniu bezpieczeństwa danych osobowych Organ Nadzorczy oraz osoby, których dane są przetwarzane, a bezpieczeństwo zostało naruszone, chyba, że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Administrator Systemu Informatycznego powinien podjąć następujące działania zmierzające do wyjaśnienia zgłoszonego zdarzenia w systemie informatycznym:

a) wygenerować i wydrukować wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia,
b) przeprowadzić wywiady z pracownikami w celu ustalenia zaistniałych faktów,
c) przeprowadzić analizę poprawności funkcjonowania systemu informatycznego w podmiocie, jeżeli zgłoszone zdarzenie było związane z nieprawidłowym jego funkcjonowaniem,
d) przeprowadzić analizę zapisu zdarzeń w systemie informatycznym z uwzględnieniem zapisu operacji realizowanych przez użytkowników,

e) przeprowadzić analizę danych przetwarzanych w systemie informatycznym, jeżeli zgłoszone zdarzenie mogło być spowodowane utratą dostępności lub integralności przetwarzanych danych,
f) zabezpieczyć dane przetwarzane w systemie informatycznym dotkniętym incydentem, w szczególności dane konfiguracyjne tego systemu,
g) zabezpieczyć system informatyczny przed dalszym rozprzestrzenianiem się zagrożenia,
h) zebrać materiały pozwalające na wyjaśnienie przyczyn zaistnienia incydentu, jego charakteru i potencjalnych skutków.
i) zasięgnąć potrzebnych opinii i zaproponować działania naprawcze (w tym także ustosunkować się do kwestii ewentualnego odtworzenia danych z zabezpieczeń) oraz wznowienia terminu przetwarzania.

System informatyczny, którego prawidłowe działanie zostało odtworzone, powinien zostać poddany szczegółowej obserwacji w celu stwierdzenia całkowitego usunięcia symptomów incydentu.

W czasie jej trwania użytkowanie systemu informatycznego powinno być ograniczone do niezbędnego minimum.

Okres obserwacji jest uzależniony od charakteru incydentu i specyfiki systemu informatycznego jest on każdorazowo określany przez Administratora Systemu.

Sankcje karne

Wobec osoby, która w przypadku naruszenia bezpieczeństwa informacji nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne.

Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu bezpieczeństwa informacji nie wyklucza odpowiedzialności karnej tej osoby zgodnie z innymi regulacjami prawnymi.

Postanowienia końcowe

W sprawach nieuregulowanych niniejszą instrukcją odpowiednie zastosowanie mają reguły i procedury zawarte w dokumentach powiązanych podmiotu.

Instrukcja Postępowania w Sytuacji Naruszeń w podmiocie wchodzi w życie z dniem podpisania.

Zapisy tego dokumentu wchodzą w życie z dniem 12.04.2022 r.

Sporządził: Marcin Misztal – Inspektor Ochrony Danych Osobowych

Administrator Danych Osobowych:

.....

Data, podpis i pieczątka