POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Incydent naruszenia ochrony danych i jego konsekwencje

Brak zgłoszenia naruszenia jest obecnie jedną z najczęstszych przyczyn kar nakładanych przez Prezesa Urzędu Ochrony Danych Osobowych (PUODO) na administratorów danych. Rejestrowanie oraz zgłaszanie organowi nadzorczemu naruszeń ochrony danych osobowych to jeden z podstawowych obowiązków, jakie nakłada na administratorów danych unijne rozporządzenie o ochronie danych. Ponadto RODO wymaga prowadzenia wewnętrznego rejestru takich naruszeń oraz wdrażania zabezpieczeń, które mają zapobiegać takim naruszeniom, a w razie ich zaistnienia obowiązkowego wdrożenia działań naprawczych.

Kiedy może wystąpić naruszenie ochrony danych?

Naruszeniem ochrony danych zgodnie z art. 4 pkt 12 RODO jest 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. Naruszenie musi dotyczyć danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez podmiot, którego dotyczy naruszenie. Natomiast skutkiem naruszenia może być zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych.

UODO w publikacji „Obowiązki administratorów związane z naruszeniami ochrony danych osobowych" wskazuje trzy główne grupy naruszeń:

- naruszenie poufności – polega na ujawnieniu danych osobowych nieuprawnionej osobie, np. przypadkowe wysłanie danych osobowych klienta do niewłaściwego działu firmy lub osoby postronnej,
- naruszenie dostępności – polega na czasowej bądź trwałej utracie lub zniszczeniu danych osobowych, np. zgubienie lub kradzież nośnika zawierającego bazy danych klientów administratora przy braku kopii zapasowej; w tym miejscu należy wspomnieć, że UODO zwraca uwagę, iż nie każda czasowa niedostępność danych jest od razu naruszeniem ochrony danych; będzie nią tylko taka niedostępność danych, która może stanowić ryzyko dla praw lub wolności osób fizycznych; jako przykład Urząd podaje np. brak dostępu do danych pacjentów w szpitalu, który może prowadzić do uniemożliwienia przeprowadzenia pilnej operacji,
- naruszenie integralności – polega na zmianie treści danych osobowych w sposób nieautoryzowany, np. pracownik zmienia nazwiska klientów poprzez dopisanie innej litery na końcu każdego z nich.

Postępowanie administratora

W związku z zaistnieniem naruszenia ochrony danych RODO przewiduje różne obowiązki, które obciążają administratorów danych. Ich zakres zależy od stopnia takiego naruszenia i skutków dla osób, których dotyczył incydent.

Przede wszystkim każdy administrator danych musi wprowadzić w swojej jednostce takie procedury, które będą umożliwiać szybkie wykrycie takiego naruszenia i ocenę naruszeń pod kątem wystąpienia ryzyka naruszenia praw i wolności osób fizycznych. Ponadto administrator musi prowadzić wewnętrzną ewidencję naruszeń, zgłaszać zaistniałe naruszenia organowi nadzorczemu, powiadamiać osoby, których dane dotyczą, o naruszeniu oraz podejmować działania mające na celu przeciwdziałanie skutkom naruszenia i zapobieganie im w przyszłości. Zgłoszenia do UODO należy dokonać nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Właśnie dlatego po zaistnieniu naruszenia ochrony danych administrator musi przeprowadzić analizę, której celem jest ustalenie, czy w wyniku naruszenia doszło do ryzyka naruszenia praw i wolności osób fizycznych czy nie.

Jeżeli naruszenie dotyczy danych osób w różnych krajach UE, Prezes UODO może być, ale nie musi być wiodącym (czyli właściwym dla administratora) organem nadzorczym. W przypadku transgranicznego naruszenia danych administrator powinien dokonać analizy, czy wiodącym organem nadzorczym w odniesieniu do czynności przetwarzania, które zostały objęte naruszeniem, jest Prezes UODO czy może inny europejski organ nadzorczy.

Ryzyko wystąpienia szkód

Z ryzykiem naruszenia praw lub wolności osób fizycznych mamy do czynienia wówczas, kiedy naruszenie może skutkować fizyczną, materialną lub niematerialną szkodą dla osób fizycznych, których dane naruszono. Jak tłumaczy UODO w swoim opracowaniu, szkodami takimi są np. dyskryminacja, kradzież tożsamości lub oszustwo dotyczące tożsamości, nadużycia finansowe, straty finansowe, nieuprawnione cofnięcie pseudonimizacji, utrata poufności danych osobowych chronionych tajemnicą zawodową, naruszenie dobrego imienia lub inne znaczące skutki gospodarcze lub społeczne dla danej osoby fizycznej. Jeżeli naruszenie dotyczy danych osobowych ujawniających pochodzenie etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych lub danych genetycznych, dotyczących zdrowia lub życia seksualnego, należy uznać, że występuje duże prawdopodobieństwo takiej szkody.

Jeśli w wyniku dokonania takiej analizy administrator danych uzna, że takie prawdopodobieństwo jest małe, wówczas nie ma obowiązku zgłoszenia naruszenia Prezesowi UODO. Wskazane naruszenie musi jednak wpisać do wewnętrznej ewidencji naruszeń. Co istotne, niezależnie od poziomu ryzyka, obowiązkiem administratora jest wprowadzenie środków zaradczych i naprawczych mających na celu zminimalizowanie ryzyka i zabezpieczenie danych osobowych w przyszłości.

Jeżeli ryzyko wystąpienia naruszenia praw i wolności osób fizycznych jest wysokie, to oprócz wpisu w ewidencji naruszeń i zgłoszenia naruszenia ochrony danych do PUODO, w niektórych przypadkach będzie konieczne powiadomienie o naruszeniu osób, których dane dotyczą. Jak informuje UODO, opis charakteru naruszenia jest istotnym elementem informacji przekazywanej osobom, których dane dotyczą. Powinien on być na tyle szczegółowy i jasny, aby osoby, do których jest kierowany, mogły zrozumieć, co się stało z ich danymi osobowymi, dlaczego oraz co to dla nich oznacza.

Zawiadomienie osób fizycznych nie jest wymagane, gdy:

- 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,
- administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, np. administrator zorientował się, że przesyłka zawierająca dane osobowe została zaadresowana na niewłaściwy adres i skontaktował się z operatorem pocztowym, który nie dopuścił do dostarczenia jej wskazanemu początkowo adresatowi,
- wymagałoby ono niewspółmiernie dużego wysiłku; w takim jednak przypadku będzie musiał zostać wydany publiczny komunikat lub inny podobny środek, za pomocą którego osoby, których dane dotyczą, zostaną poinformowane w równie skuteczny sposób, np. dokumentacja zawierająca dane osobowe była prowadzona jedynie w wersji papierowej i uległa zalaniu; w takim przypadku administrator musi wydać publiczny komunikat, w którym osoby fizyczne zostaną poinformowane o naruszeniu.

Dokumentowanie incydentów

RODO w art. 33 ust. 5 nakłada na administratorów danych obowiązek dokumentowania wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Użyte w tym artykule sformułowanie „wszelkich naruszeń" oznacza, że ewidencja powinna obejmować wszystkie naruszenia spełniające kryteria określone w definicji zawartej w art. 4 pkt 12 RODO. Są to zarówno naruszenia, które nie wymagały dokonania zgłoszenia, jak i te podlegające temu obowiązkowi.

Jeżeli chodzi o sposób prowadzenia ewidencji, to Grupa Robocza Art. 29 stoi na stanowisku, że administrator może zdecydować o dokumentowaniu naruszeń w rejestrze czynności przetwarzania prowadzonym zgodnie z art. 30 RODO. Nie ma wymogu prowadzenia osobnego rejestru naruszeń, gdy informacje dotyczące naruszenia można łatwo zidentyfikować i przedłożyć na żądanie.

2. Dokonanie zgłoszenia do Prezesa UODO

Naruszenie ochrony danych może zdarzyć się w każdym podmiocie. Jeżeli takie zdarzenie będzie miało miejsce i np. dojdzie do wysłania dokumentów zawierających dane osobowe na inny adres czy zagubienia niezabezpieczonych urządzeń informatycznych zawierających takie dane, wówczas reakcja administratora danych ma decydujące znaczenie. Jednym z jego obowiązków może być dokonanie zgłoszenia takiego incydentu do Prezesa Urzędu Ochrony Danych Osobowych.

Administrator ma 72 godziny

W przypadku naruszenia ochrony danych osobowych administrator powinien bez zbędnej zwłoki, w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, zgłosić je organowi nadzorczemu. W Polsce taką funkcję pełni Prezes UODO. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Takiego zgłoszenia administrator danych nie musi dokonywać, jeżeli jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Administratorzy danych często mają wątpliwości, jak powinni postąpić, gdy w przeciągu tych 72 godzin nie mają jeszcze pełnej wiedzy na temat zaistniałego incydentu, a co za tym idzie, ich zgłoszenie może być niepełne. W takim przypadku, jak informuje UODO, w ciągu pierwszych 72 godzin trzeba przekazać to, co już udało się ustalić. Natomiast należy niezwłocznie uzupełnić zgłoszenie o nowe informacje, gdy tylko administrator danych ustali kolejne szczegóły związane z zaistniałym naruszeniem.

Takie zgłoszenie musi co najmniej:

- opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
- zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
- opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
- opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków; np. w przypadku naruszenia polegającego na zagubieniu lub kradzieży niezabezpieczonych (niezaszyfrowanych) urządzeń informatycznych z danymi osobowymi (smartfony, komputery przenośne) możliwymi działaniami naprawczymi mogą być: skuteczne szyfrowanie pamięci urządzeń/plików z danymi osobowymi (zgodne z aktualną wiedzą techniczną) oraz dodatkowe (mechanizmy weryfikacji użytkownika np. hasło, PIN).

W zależności od rodzaju zgłoszenia określa się, czy jest to zgłoszenie:

- kompletne/jednorazowe – kiedy administrator posiada pełny obraz naruszenia i ma wszystkie informacje o tym co, gdzie, kiedy i w jakim zakresie wydarzyło się w związku z naruszeniem,
- wstępne – kiedy administrator nie posiada jeszcze wszystkich danych dotyczących naruszenia, a grozi mu przekroczenie terminu 72 godzin wymaganych do zgłoszenia naruszenia,
- uzupełniające/zmieniające – jeśli po wypełnieniu zgłoszenia wstępnego udało się administratorowi danych uzyskać brakujące informacje i chce je złożyć do urzędu lub w przypadku gdy informacje udzielone w zgłoszeniu kompletnym/jednorazowym okazały się błędne i chce je zaktualizować.

Zgłoszenia można dokonać na cztery sposoby:

- elektronicznie poprzez wypełnienie dedykowanego formularza elektronicznego dostępnego bezpośrednio na platformie Biznes.gov.pl,
- elektronicznie poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą ePUAP:/UODO/SkrytkaESP,
- elektronicznie poprzez wysłanie wypełnionego formularza za pomocą pisma ogólnego dostępnego na platformie Biznes.gov.pl lub na platformie epuap.gov.pl,
- tradycyjną pocztą, wysyłając wypełniony formularz na adres Urzędu.

Najczęstsze błędy w zgłoszeniach

UODO w opracowaniu „Dotychczasowe doświadczenia w zakresie zgłaszania naruszeń ochrony danych osobowych i zawiadamiania o nich osób, których dane dotyczą", dostępnym na stronie internetowej www.uodo.gov.pl, wskazuje na najczęstsze błędy popełniane przez administratorów danych dokonujących zgłoszeń incydentów. Wśród nich wymienia m.in. nierzetelne, zdawkowe przekazywanie informacji, które uniemożliwia ocenę prawdopodobieństwa wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych. Do błędów tych zalicza się też wypełnianie zgłoszeń w sposób rutynowy, podanie niewłaściwej liczby osób, której dane są zagrożone naruszeniem, podanie niewłaściwej kategorii danych, wskazanie niewłaściwego poziomu ryzyka czy też niewłaściwego czasu zaistnienia naruszenia. Oprócz tego UODO zwraca uwagę na częsty brak przeprowadzenia prawidłowej oceny ryzyka naruszenia praw lub wolności osób fizycznych. Ponadto wskazuje, iż zgodnie z art. 33 ust. 3 RODO, administrator powinien w zgłoszeniu podać tylko kategorie danych osobowych, których dotyczy naruszenie. Niewłaściwą praktyką jest podawanie w zgłoszeniu konkretnych imion, nazwisk lub adresów zamieszkania osób, których dane dotyczą.

Wdrożenie obsługi naruszeń według UODO

1. Opracowanie procedury postępowania z naruszeniem.
2. Ustalenie zasad przekazywania informacji (różne kanały komunikacji) – wewnętrzny formularz zgłoszenia.
3. Zbudowanie świadomości poprzez szkolenie pracowników.
4. Wprowadzenie checklisty pozwalającej ocenić wpływ naruszenia na podmiot.

Wybrane fragmenty dedykowanego formularza elektronicznego dotyczące szczegółów naruszenia

4. Charakter naruszenia

4A. Opisz szczegółowo na czym polegało naruszenie

.....

4B. Na czym polegało naruszenie?

☐ a) Zgubienie lub kradzież nośnika/urządzenia ☐ b) Dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji ☐ c) Korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy ☐ d) Nieuprawnione uzyskanie dostępu do informacji ☐ e) Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń ☐ f) Złośliwe oprogramowanie ingerujące w poufność, integralność lub dostępność danych ☐ g) Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing)	☐ h) Nieprawidłowa anonimizacja danych osobowych w dokumencie ☐ i) Nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora ☐ j) Niezamierzona publikacja ☐ k) Dane osobowe wysłane do niewłaściwego odbiorcy ☐ l) Ujawnienie danych niewłaściwej osoby ☐ m) Ustne ujawnienie danych osobowych

4C. Działanie złośliwego oprogramowania (odpowiedz na poniższe pytania, jeśli w sekcji 4B zaznaczono pole f)

a) Jeśli w ocenie administratora doszło wyłącznie do naruszenia dostępności danych, w jaki sposób stwierdzono, że nie doszło do naruszenia ich poufności? (w sytuacji gdy np. dane nie zostały pobrane przez osobę nieupoważnioną, a jedynie zaszyfrowane w sposób uniemożliwiający uzyskanie do nich dostępu)

.....

b) Czy, a jeżeli tak, to w jakiej formie, złośliwe oprogramowanie poinformowało o konieczności uiszczenia opłaty w celu odzyskania dostępu do danych (podaj nazwę złośliwego oprogramowania, sposób poinformowania, żądaną kwotę, kanał komunikacji, sposób zapłaty oraz termin)

.....

c) Jeżeli doszło do utraty dostępności danych, to czy administrator był w posiadaniu kopii zapasowej, jeśli tak – to w jakim czasie ją przywrócił?

.....

UWAGA: Jeżeli zgłoszenie naruszenia dotyczy podejrzanych załączników, phishingu, szantażu czy działania złośliwego oprogramowania, rozważ zgłoszenie zdarzenia do CERT Polska pod adresem https://incydent.cert.pl/. Dokonanie takiego zgłoszenia jest szczególnie zalecane w przypadku, kiedy odpowiedzi na powyższe pytania są utrudnione bądź niemożliwe.
O fakcie zgłoszenia incydentu do CERT Polska poinformuj w zgłoszeniu uzupełniającym Prezesa UODO (pkt 1 formularza) podając datę zgłoszenia, jego numer oraz ewentualnie informacje na temat incydentu otrzymane od CERT Polska).

4D. Przyczyna naruszenia

☐ Wewnętrzne działanie niezamierzone	☐ Wewnętrzne działanie zamierzone
☐ Zewnętrzne działanie niezamierzone	☐ Zewnętrzne działanie zamierzone

4E. Charakter

☐ Naruszenie poufności danych
Nieuprawnione lub przypadkowe ujawnienie bądź udostępnienie danych
☐ Naruszenie integralności danych
Wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania
☐ Naruszenie dostępności danych
Brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez osobę do tego uprawnioną

4F. Dzieci

☐ Naruszenie dotyczy przetwarzania danych w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.
(opcjonalnie)

(...)

8. Możliwe konsekwencje

8A. Uszczerbek fizyczny, majątkowy, niemajątkowy lub inne znaczące konsekwencje dla osoby, której dane dotyczą

☐ Utrata kontroli nad własnymi danymi osobowymi
☐ Ograniczenie możliwości realizowania praw z art. 15-22 RODO
☐ Ograniczenie możliwości realizowania praw
☐ Dyskryminacja
☐ Kradzież lub sfałszowanie tożsamości
☐ Strata finansowa
☐ Naruszenie dobrego imienia
☐ Utrata poufności danych osobowych chronionych tajemnicą zawodową
☐ Nieuprawnione odwrócenie pseudonimizacji
☐ Inne
Opisz poniżej inne skutki naruszenia prawa do ochrony danych osoby, której dane dotyczą:
.....

3. Kontrole i uprawnienia Prezesa UODO

Prezes Urzędu Ochrony Danych Osobowych jako polski organ nadzorczy nakłada na administratorów danych administracyjne kary pieniężne, które w indywidualnym przypadku mają być skuteczne, proporcjonalne i odstraszające, ale też są sygnałem dla innych podmiotów, jak ważna jest współpraca z UODO. Prezes UODO może kontrolować doraźnie różne podmioty, co do których otrzymał np. sygnał o stwierdzonych nieprawidłowościach przy przetwarzaniu danych. Kontrolę może wszcząć również w wyniku uzyskanego od administratora danych zgłoszenia naruszenia ochrony danych, w celu kontroli podjętych przez administratora działań np. w zakresie powiadomienia osób, których dane były przetwarzane i podjętych działań naprawczych.

Kompetencje Prezesa UODO

Do Prezesa UODO należy nie tylko monitorowanie przestrzegania przepisów unijnego rozporządzenia o ochronie danych (RODO), ale także kontrola przestrzegania innych, zarówno unijnych, jak i krajowych przepisów o ochronie danych, w tym przepisów polskiej ustawy o ochronie danych, jak również przepisów innych ustaw i rozporządzeń wykonawczych dotyczących ochrony danych osobowych.

Krajowa ustawa o ochronie danych osobowych wyróżnia trzy rodzaje kontroli, jaką może prowadzić Prezes Urzędu. Należą do nich kontrole:

- planowa – prowadzona zgodnie z zatwierdzonym przez Prezesa Urzędu planem kontroli,
- doraźna – na podstawie uzyskanych przez Prezesa Urzędu informacji,
- sprawowana w ramach monitorowania przestrzegania stosowania rozporządzenia 2016/679.

Obowiązek prowadzenia przez Prezesa Urzędu kontroli planowej i sporządzenie planu kontroli wynika więc wyraźnie z przepisów. Przy czym nie określają one szczegółowych wymogów w tym zakresie, pozostawiając organowi swobodę, gdy chodzi o ukształtowanie planu kontroli (kontrole planowane na 2023 r. – patrz ramka).

Natomiast jeśli chodzi o kontrolę doraźną, to może ona zostać podjęta pomimo tego, że nie była przewidziana w planie kontroli. Potrzeba jej przeprowadzenia może wynikać z informacji, jakie uzyskał organ nadzorczy o stwierdzonych nieprawidłowościach w zakresie przetwarzania danych. Takie informacje mogą pochodzić ze źródeł powszechnie dostępnych lub od osób zainteresowanych, które zwracają uwagę PUODO na pewne nieprawidłowości. Oczywiście najpopularniejszym wskazaniem do przeprowadzenia kontroli będzie skarga osoby, której dane dotyczą, na administratora przetwarzającego jej dane, w ocenie tej osoby w sposób nieprawidłowy.

Jak wygląda kontrola?

Kontrolę przeprowadza upoważniony przez Prezesa UODO pracownik Urzędu lub członek bądź pracownik organu nadzorczego państwa członkowskiego UE w przypadku, o którym mowa w art. 62 RODO, czyli dokonywania wspólnych operacji nadzorczych. Kontrolę przeprowadza się po okazaniu imiennego upoważnienia wraz z legitymacją służbową, a w przypadku kontrolującego z innego kraju członkowskiego – po okazaniu imiennego upoważnienia wraz z dokumentem potwierdzającym tożsamość. Prezes Urzędu może upoważnić do udziału w kontroli osobę posiadającą wiedzę specjalistyczną, jeżeli przeprowadzenie czynności kontrolnych wymaga takiej wiedzy.

Czynności kontrolnych dokonuje się w obecności kontrolowanego lub osoby przez niego upoważnionej, co ma na celu zapewnienie czynnego udziału tej osoby w czynnościach kontrolnych. Kontrola może odbyć się pod nieobecność kontrolowanego lub osoby przez niego upoważnionej, po okazaniu legitymacji służbowej i upoważnienia osobie czynnej w lokalu przedsiębiorstwa lub przywołanemu świadkowi, jeżeli jest funkcjonariuszem publicznym, niebędącemu jednak pracownikiem UODO ani osobą podlegającą wyłączeniu z udziału w kontroli.

Kontrolujący w ramach wykonywanych czynności kontrolnych ma prawo wstępu w godzinach od 6^{00} do 22^{00} na grunt oraz do budynków, lokali lub innych pomieszczeń. Ma również prawo wglądu do dokumentów i informacji mających bezpośredni związek z zakresem przedmiotowym kontroli. Może prowadzić oględziny miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych. Ma prawo żądać złożenia pisemnych lub ustnych wyjaśnień oraz przesłuchiwać w charakterze świadka osoby w zakresie niezbędnym do ustalenia stanu faktycznego oraz zlecać sporządzanie ekspertyz i opinii.

Kontrolowany zapewnia kontrolującemu oraz osobom upoważnionym do udziału w kontroli warunki i środki niezbędne do sprawnego przeprowadzenia kontroli, a w szczególności sporządza we własnym zakresie kopie lub wydruki dokumentów oraz informacji zgromadzonych na nośnikach, w urządzeniach lub systemach, tzn. z wykorzystaniem własnego sprzętu i na własny koszt. Kontrolowany ma obowiązek potwierdzić sporządzane kopie lub wydruki za zgodność z oryginałem. Kontrolę prowadzi się nie dłużej niż 30 dni od dnia okazania kontrolowanemu lub innej osobie wskazanej w przepisach imiennego upoważnienia do przeprowadzenia kontroli oraz legitymacji służbowej lub innego dokumentu potwierdzającego tożsamość.

Wysokie kary

RODO wprowadza wysokie kary za naruszenie jego przepisów. Art. 83 stanowi, że administracyjnej karze pieniężnej w wysokości do 10 mln euro, a w przypadku przedsiębiorstwa – w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, podlega brak wdrożenia przez administratora lub podmiot przetwarzający odpowiednich środków technicznych i organizacyjnych w celu ochrony przetwarzanych danych osobowych. Z kolei administracyjnej karze pieniężnej w wysokości do 20 mln euro, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, podlega m.in. naruszenie podstawowych zasad przetwarzania, w tym warunków uzyskania zgody od osób, których dane są przetwarzane.

Polska ustawa o ochronie danych osobowych w zakresie administracyjnych kar pieniężnych odsyła bezpośrednio do unijnego rozporządzenia, obniżając jedynie wysokość kar dla instytucji publicznych. Prezes UODO może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 100 tys. zł na jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1–12 i pkt 14 ustawy o finansach publicznych (Dz. U. z 2022 r. poz. 1634 ze zm.). Kary pieniężne w wysokości do 10 tys. zł Prezes UODO może nakładać na jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 13 ustawy o finansach publicznych, czyli na państwowe i samorządowe instytucje kultury.

Kary pieniężne nie są jedynymi środkami, które mogą być stosowane przez Prezesa UODO. RODO przewiduje również inne środki, które mogą być wykorzystywane zamiast kary pieniężnej lub razem z nią. Takimi środkami mogą być m.in. udzielenie upomnienia administratorowi lub podmiotowi przetwarzającemu czy nakazanie mu spełnienia żądania osoby, której dane dotyczą, wynikającego z praw przysługujących jej na mocy RODO.

Szczegółowy plan kontroli sektorowych UODO na 2023 r. obejmuje:

1. Organy przetwarzające dane osobowe w Systemie Informacyjnym Schengen i Wizowym Systemie Informacyjnym – przetwarzanie danych osobowych SIS/VIS na podstawie przepisów ustawy o udziale Rzeczpospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym (Dz. U. z 2021 r. poz. 1041), aktów wykonawczych oraz przepisów Unii Europejskiej.
2. Podmioty przetwarzające dane osobowe przy użyciu aplikacji mobilnych – sposób zabezpieczenia i udostępniania danych osobowych przetwarzanych w związku z użytkowaniem aplikacji.
3. Podmioty przetwarzające dane osobowe przy użyciu aplikacji internetowych (webowych) – sposób zabezpieczenia i udostępniania danych osobowych przetwarzanych w związku z użytkowaniem aplikacji.

4. Środki i zabezpieczenia pozwalające uniknąć naruszeń

Każdy administrator danych ma obowiązek wdrożenia odpowiednich i skutecznych środków ochrony danych, a także powinien być w stanie wykazać, że czynności przetwarzania są zgodne z unijnym rozporządzeniem oraz że są skuteczne. Środki te powinny uwzględniać charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych.

Obowiązki administratora

Podmioty przetwarzające dane osobowe są zobowiązane przestrzegać przepisów RODO i co za tym idzie – muszą być w stanie wykazać, że tych regulacji przestrzegają. Dlatego administrator powinien przyjąć wewnętrzne polityki i wdrożyć środki, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych. Takie środki mogą polegać m.in. na minimalizacji przetwarzania danych osobowych, jak najszybszej pseudonimizacji danych osobowych, przejrzystości co do funkcji i przetwarzania danych osobowych, umożliwieniu osobie, której dane dotyczą, monitorowania przetwarzania danych, umożliwieniu administratorowi tworzenia i doskonalenia zabezpieczeń.

RODO stanowi, że w celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z jego przepisami administrator lub podmiot przetwarzający powinni oszacować ryzyko właściwe dla przetwarzania oraz wdrożyć środki – takie jak szyfrowanie – minimalizujące to ryzyko. Środki takie powinny zapewnić odpowiedni poziom bezpieczeństwa, w tym poufność, a także uwzględniać stan wiedzy technicznej oraz koszty ich wdrożenia w stosunku do ryzyka i charakteru danych osobowych podlegających ochronie. Oceniając ryzyko w zakresie bezpieczeństwa danych, należy wziąć pod uwagę ryzyko związane z przetwarzaniem danych osobowych – takie jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych – i mogące w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych.

Wskazówki wynikające z RODO

RODO jest aktem prawnym neutralnym technologicznie. Oznacza to, że nie wskazuje, jakie środki i zabezpieczenia powinny być stosowane przez administratorów danych. Postęp technologiczny jest coraz szybszy i przepisy nie byłyby w stanie nadążyć za zmianami. Ustawodawca unijny stworzył więc akt, który ma być aktem obowiązującym przez wiele lat.

To administrator danych podejmuje decyzję o tym, jakie środki i zabezpieczenia będą u niego w jednostce wdrożone. Taką decyzję podejmuje w oparciu o wiedzę na temat tego, jakie dane przetwarza, w jakich zbiorach i systemach, na jakie zagrożenia są narażone przetwarzane dane. Administrator danych powinien więc – uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze – wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. Stosowanymi zabezpieczeniami mogą być:

- pseudonimizacja i szyfrowanie danych osobowych,
- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Wspomniana pseudonimizacja oznacza przetworzenie danych osobowych w taki sposób, aby nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

Wśród wymienionych przykładowo środków znalazła się zdolność do zapewnienia poufności, integralności i odporności systemów i usług przetwarzania. Za bezpieczeństwo danych przetwarzanych w systemach komputerowych odpowiada administrator i podmiot przetwarzający, którzy powinni zapewnić aktualne oprogramowania oraz regularne testowanie środków bezpieczeństwa.

O konieczności aktualizowania stosowanych w jednostce programów komputerowych informuje Urząd Ochrony Danych Osobowych na stronie www.uodo.gov.pl. Z informacji tych wynika, że: „Aktualizacje są nieodłącznym aspektem w świecie informatycznym, dlatego należy zdawać sobie sprawę z tego, że regularne aktualizowanie programów antywirusowych, oprogramowania typu firewall, przeglądarek, a także innych aplikacji i całych systemów operacyjnych, z których korzystamy na co dzień, jest jednym z kluczowych warunków zapewniających bezpieczną i stabilną pracę naszego komputera".

Poza tym trzeba pamiętać o opracowaniu odpowiednich regulaminów pracy z systemami informatycznymi, sprzętem komputerowym, korzystania z poczty elektronicznej, pracy z nośnikami elektronicznymi zawierającymi dane osobowe, korzystania z internetu. Ze wszystkimi tymi regulaminami należy zapoznać pracowników i inne osoby, które przetwarzają dane osobowe.

5. Naruszenie ochrony danych w biurze rachunkowym

Prowadzimy biuro rachunkowe. Mamy zawarte umowy powierzenia z kilkoma różnymi pracodawcami. Jeden z pracowników wysłał przez pomyłkę dokumenty dotyczące jednego z klientów do wszystkich pozostałych podmiotów, których dane przetwarzamy. Jak powinniśmy postąpić w sytuacji wystąpienia u nas naruszenia ochrony danych osobowych?

Administrator danych ponosi odpowiedzialność za przetwarzanie danych osobowych przez niego samego lub w jego imieniu. Oznacza to, że mimo zawarcia umowy powierzenia, na administratorze danych nadal ciążą obowiązki związane z ochroną przekazywanych danych osobowych. Dlatego tak ważne jest wybieranie tylko tych podmiotów przetwarzających, które gwarantują taką ochronę przetwarzanym danym. W szczególności posiadają wiedzę fachową, wiarygodność i zasoby niezbędne do wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom RODO, w tym wymogom bezpieczeństwa przetwarzania (motyw 81 RODO). Ponadto administrator ma obowiązek wdrożenia odpowiednich i skutecznych środków oraz powinien być w stanie wykazać, że czynności przetwarzania są zgodne z RODO oraz, że są skuteczne. Natomiast zgodnie z art. 28 ust. 3 lit. f) RODO, umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający, uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z tych obowiązków.

W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Podmiot przetwarzający, a takim jest niewątpliwie biuro rachunkowe, po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi. „Bez zbędnej zwłoki" oznacza najszybciej jak to możliwe. Przy czym warto w zawieranych umowach powierzenia dokonać zapisu takiego terminu wywiązywania się z obowiązku informowania administratora o wystąpieniu incydentu naruszenia ochrony danych. Prezes UODO na stronie www.uodo.gov.pl zwraca uwagę, że jeżeli podmiot przetwarzający świadczy usługi na rzecz wielu administratorów, a dany incydent wywiera wpływ na wszystkich z nich, podmiot przetwarzający jest zobowiązany do zgłoszenia naruszenia bez zbędnej zwłoki każdemu z tych administratorów. Należy pamiętać, że brak odpowiedniego działania po stronie podmiotu przetwarzającego w sytuacji naruszenia ochrony danych osobowych może skutkować zastosowaniem przez Prezesa UODO wobec podmiotu przetwarzającego uprawnień określonych w art. 58 RODO. Urząd Ochrony Danych Osobowych zwraca uwagę, iż nie wszystkie podmioty, przy pomocy których administratorzy przetwarzają dane osobowe, gwarantują odpowiednie bezpieczeństwo danych osobowych oraz szybkie i skuteczne rozwiązania służące prawidłowemu wywiązywaniu się z obowiązków określonych w art. 33 i art. 34 RODO.

Przykład

U podmiotu przetwarzającego doszło do naruszenia ochrony danych osobowych, co wymaga podjęcia działań mających na celu jak najszybsze zablokowanie nieuprawnionego dostępu do tych danych. Naruszenie to dotyczy danych przetwarzanych w ramach powierzenia.

W związku z zaistniałym zdarzeniem administrator powinien wydać odpowiednie polecenie podmiotowi przetwarzającemu i zadbać o to, aby żądania organu nadzorczego wydane w stosunku do niego zostały jak najszybciej i skutecznie zrealizowane.

8. Opóźnienie w powiadomieniu Prezesa UODO o naruszeniu

Jednostka, jako administrator danych, nie powiadomiła Prezesa UODO w ciągu 72 godzin o naruszeniu ochrony danych. Nie miała bowiem wszystkich niezbędnych informacji, by to zrobić. Czy można takie zawiadomienie wysłać w późniejszym terminie?

RODO w art. 33 ust. 1 wyraźnie stanowi, że w przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Przepis ten stanowi, że jeżeli administrator danych ma obowiązek zawiadomić Prezesa Urzędu Ochrony Danych Osobowych o wystąpieniu incydentu naruszenia ochrony danych (tj. istnieje ryzyko naruszenia praw lub wolności osób fizycznych), to powinien to zrobić bez zbędnej zwłoki, nie później niż w ciągu 72 godzin. Oczywiście powinno to nastąpić tak szybko, jak pozwalają na to okoliczności danej sprawy. Te 72 godziny, o których mówi RODO, liczy się od stwierdzenia przez administratora danych wystąpienia naruszenia podlegającego zgłoszeniu do PUODO.

Zgłoszenia można dokonać na 4 sposoby:

- elektronicznie poprzez wypełnienie dedykowanego formularza elektronicznego dostępnego bezpośrednio na platformie Biznes.gov.pl,
- elektronicznie poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą ePUAP:/UODO/SkrytkaESP,
- elektronicznie poprzez wysłanie wypełnionego formularza (dostępnego na stronie www.uodo.gov.pl), za pomocą pisma ogólnego dostępnego na platformie Biznes.gov.pl lub platformie epuap.gov.pl,
- tradycyjnie, wysyłając pocztą wypełniony formularz na adres UODO.

Jednocześnie z RODO wynika, że jeśli administrator danych przekazuje zgłoszenie do PUODO po upływie 72 godzin, musi wtedy dołączyć do tego zgłoszenia wyjaśnienie przyczyn opóźnienia. Może bowiem zdarzyć się, iż administrator danych nie dysponuje wszystkimi informacjami. W takiej sytuacji może brakujące informacje przekazywać sukcesywnie, tj. niezwłocznie po tym, jak wejdzie w ich posiadanie, np. ustali konkretną liczbę poszkodowanych osób. Warto więc wysłać zgłoszenie wstępne obejmujące podstawowe informacje, które następnie zostaną uzupełnione w kolejnym zgłoszeniu tzw. uzupełniającym, zawierającym wszystkie niezbędne informacje.

6. Forma prowadzenia ewidencji naruszeń

Spółka przygotowuje ewidencję naruszeń ochrony danych. Jakie informacje o naruszeniu powinna zawierać taka ewidencja? Czy do takiej ewidencji należy wpisywać tylko te naruszenia, które podlegają zgłoszeniu do Prezesa UODO, czy wszystkie występujące w firmie incydenty?

Obowiązek prowadzenia ewidencji (rejestru) naruszeń ochrony danych wynika z art. 33 ust. 5 RODO, który stanowi, że administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu na weryfikowanie przestrzegania tego przepisu. Użyto w nim sformułowania «wszelkich naruszeń», co oznacza, że w takiej ewidencji powinny być odnotowywane wszystkie incydenty, które wystąpiły w związku z przetwarzaniem danych osobowych, bez względu na ich wagę i na to, czy podlegają zgłoszeniu do PUODO czy nie. Dostęp do takiej ewidencji, w razie ewentualnej kontroli, musi mieć organ nadzorczy zgodnie z wynikającą z RODO zasadą rozliczalności. Urząd Ochrony Danych Osobowych, powołując się na ustalenia Grupy Roboczej Art. 29, wskazuje, że w przypadku stwierdzenia przez administratora danych, iż dany incydent nie wymaga zgłoszenia do Prezesa UODO, konieczne jest odnotowanie tego faktu wraz ze wskazaniem przyczyny, dla której uznano, że zdarzenie nie niesie ryzyka naruszenia praw i wolności osób fizycznych. W takiej ewidencji powinny zostać zawarte okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Przy czym administrator danych może prowadzić taką ewidencję w formie osobnego dokumentu lub może on być częścią rejestru czynności przetwarzania prowadzonego zgodnie z art. 30 RODO.

Jak informuje Prezes UODO na stronie www.uodo.gov.pl, do naruszeń ochrony danych osobowych można zaliczyć:

- zmianę danych bez zgody osoby, której dane dotyczą,
- wysłanie danych do niewłaściwej osoby (np. poprzez niewłaściwe zaadresowanie poczty elektronicznej),
- utratę nośników danych (telefon, laptop, USB, teczki zawierające dane w wersji papierowej),
- nieuprawnione udostępnienie danych (np. telefonicznie rozmówca podaje się za pracownika policji czy urzędu, próbując uzyskać informacje),
- nieodpowiednie usuwanie danych (np. administrator postanawia pozbyć się starych komputerów i przed sprzedażą usuwa jedynie pliki na pulpicie i opróżnia kosz ze starych plików, jednak nie usuwa danych z dysku komputera).

Przykład ewidencji przypadków naruszenia ochrony danych osobowych

Data wystąpienia naruszenia	Rodzaj naruszenia	Miejsce naruszenia	Opis okoliczności naruszenia	Skutki naruszenia	Naruszenie podlegające zgłoszeniu do PUODO	Powiadomienie osób, których dane dotyczą	Działania zaradcze
1.06.2023 r.	Naruszenie dostępności	Poza siedzibą administratora	Zagubienie nośnika zawierającego umowę sprzedaży z danymi osobowymi klienta	Nie wystąpiły, nośnik został zaszyfrowany, a klucz dostępu znajduje się u administratora	Nie	Nie	Przeszkolono pracowników w zakresie wynoszenia nośników zawierających dane poza siedzibę firmy

7. Problemy z poinformowaniem osoby o naruszeniu jej danych

W firmie wystąpiło naruszenie ochrony danych osobowych jednego z klientów. Doszło do omyłkowego udostępnienia numeru PESEL nieuprawnionym osobom. Powiadomiliśmy o tym incydencie PUODO. Mamy jednak problem ze skontaktowaniem się z jedną z osób. Jakie kanały należy wykorzystać, by powiadomić osobę o naruszeniu danych?

Zgodnie z opinią Prezesa Urzędu Ochrony Danych Osobowych zagubienie dokumentacji zawierającej imię, nazwisko i numer PESEL powoduje wysokie ryzyko naruszenia praw i wolności. Takie dane mogą bowiem zostać wykorzystane np. w celu uzyskania przez osoby trzecie pożyczki bądź kredytu, do zawarcia różnego rodzaju umów (np. najmu nieruchomości), zarejestrowania karty pre-paid, korzystania ze świadczeń opieki zdrowotnej na podstawie skradzionych danych. W związku z tym Czytelnicy o takim naruszeniu powinni zawiadomić Prezesa UODO oraz osoby, których dane zagubiono.

Zasadniczo taka informacja powinna być przekazana tym osobom w formie pisemnej, a w wyjątkowych sytuacjach może być udzielona ustnie. Nieodebranie przez osobę, której dane dotyczą, informacji o naruszeniu, przesłanej za pomocą poczty tradycyjnej, powinno wskazywać administratorowi na konieczność podejmowania dalszych działań w celu skutecznego poinformowania tej osoby o naruszeniu.

Urząd Ochrony Danych Osobowych w wyjaśnieniach zawartych na stronie www.uodo.gov.pl, w zakładce „Zadania Inspektora Ochrony Danych" wyjaśnia, iż: „W sytuacji gdy bezpośrednie kanały komunikacji zawiodą, warto rozważyć wydanie publicznego komunikatu lub zastosowanie podobnego środka komunikacyjnego, za pomocą którego osoba, której dane dotyczą, zostanie skutecznie poinformowana. Przykładami metod zawiadamiania o naruszeniu ochrony danych są np.: wiadomości e-mail, SMS, wiadomości bezpośrednie, rzucające się w oczy banery lub powiadomienia na stronach internetowych, komunikacja pocztowa oraz rzucające się w oczy reklamy w mediach drukowanych".

W przypadku gdy administrator nie jest w stanie zawiadomić danej osoby fizycznej o naruszeniu, np. dlatego, że dane kontaktowe tej osoby, które posiada, są już nieaktualne, wówczas zgodnie z wytycznymi Grupy Roboczej Art. 29 powinien ją poinformować tak szybko, jak jest to rozsądnie wykonalne, gdy tylko uzyska dane kontaktowe.