Naruszenia ochrony danych

w świetle ogólnego rozporządzenia o ochronie danych

experto24.pl

Spis treści

Data 25 maja 2018 r. zapadnie w pamięć wszystkim osobom, które zajmują się tematem ochrony danych osobowych w Europie. Jest to data rozpoczęcia stosowania ogólnego rozporządzenia o ochronie danych (dalej: rodo). Nowe prawo zasadniczo zmienia zasady ochrony danych osobowych, jakie powinny być stosowane przez każdą organizację przetwarzającą dane osobowe. Każde z państw Unii Europejskiej może wydać odpowiednie akty związane z doprecyzowaniem rodo, ale jedynie w zakresie wskazanym przez rozporządzenie. Prawo w zakresie ochrony danych osobowych nie będzie więc identyczne w każdym kraju członkowskim, jednakże na pewno będzie większa spójności i jednolitość.

Zmiany w zakresie ochrony danych osobowych w polskim prawodawstwie były jak najbardziej konieczne. Ustawa o ochronie danych osobowych oraz akty prawne wydane na jej podstawie były w pewnych kwestiach anachroniczne i trudne do stosowania. Jako przykład takich wymagań można wskazać chociażby wymóg posiadania zgody w formie pisemnej na przetwarzanie danych wrażliwych czy konieczność wskazania obszarów przetwarzania danych w dokumentacji opisującej przetwarzanie danych osobowych. Rodzaj odpowiedzialności (odpowiedzialność karna) przyjętej w naszej ustawie również nie zdaje egzaminu. Jak wynika z analiz sprawozdań Generalnego Inspektora Ochrony Danych Osobowych (GIODO), sprawy z ochrony danych osobowych nawet jeżeli trafią do prokuratury, to są zazwyczaj umarzane z uwagi na niską szkodliwość społeczną czynu. Taka sytuacja prowadzi do częstych naruszeń prawa do ochrony danych osobowych z uwagi na akceptację ryzyka prawnego z nim związanego. Celem przyjęcia rodo jest zaś ograniczenie naruszeń związanych z przetwarzaniem danych osobowych.

Naruszenie – co to jest?

Zgodnie z definicją językową naruszeniem jest postępowanie lub zaniechanie postępowania prowadzące do niedochowania przyjętych norm. Mogą to być zarówno normy prawne, techniczne, jak i społeczne czy też takie jak ISO. Przez naruszenie danych osobowych rozumie się przypadkowe lub bezprawne zniszczenie, utratę, zmianę, nieuprawnione ujawnienie lub dostęp do danych osobowych przetwarzanych przez administratora danych lub procesora.

Naruszenie przepisów rodo może prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych, w szczególności: jeżeli przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną. Ogólne rozporządzenie o ochronie danych kładzie duży nacisk na oszacowanie możliwości naruszenia praw i wolności i podjęcie niezbędnych działań, a w szczególności wdrożenie niezbędnych środków w celu zabezpieczenia przetwarzanych danych osobowych.

Bez wątpienia do naruszenia rodo może dojść w związku z celowym działaniem lub zaniechaniem podmiotu przetwarzającego dane osobowe. Pewne wątpliwości budzi jednak nieumyślne działanie takiego podmiotu. Obecnie takie nieumyślne działanie stanowi naruszenie ustawy o ochronie danych osobowych, a w szczególności jest to naruszenia zasady bezpieczeństwa. W rodo nie ma jasnego wskazania w tym zakresie. Analizując jednak przepisy rodo, należy postawić wniosek, iż naruszenie może być również nieumyślne. Wskazuje na to definicja naruszenia ochrony danych osobowych zawarta w art. 4 pkt 12 rodo. Zgodnie z nim „naruszenie ochrony danych osobowych" 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. Wprost jest więc wskazane, że do naruszenia może dojść przypadkowo, co niewątpliwie jest wskazaniem, że naruszenie

może być nieumyślne. Przykładem takiego naruszenia może być przypadkowe wysłanie za pośrednictwem poczty elektronicznej tabelki z danymi osobowymi nie do docelowego odbiorcy tylko do innej osoby – poprzez wpisanie błędnego adresu e-mail.

Warto również pamiętać, że rodo często posługuje się pojęciem naruszenia praw lub wolności, które jest pojęciem szerszym od naruszenia ochrony danych osobowych. Wynika to z analizy definicji użytej w art. 4 rodo, która sprowadza się na kwestii związanych zapewnieniem bezpieczeństwa przetwarzanym danym. W rodo zdefiniowano szeroki katalog zasad związanych z ochroną danych osobowych i oprócz zasady bezpieczeństwa wskazany takie zasady jak rzetelność, adekwatność, legalność, celowość czy okresowość. Podmiot, przetwarzając dane osobowe, może naruszyć więc nie tylko zasadę bezpieczeństwa, ale również pozostałe zasady, co może prowadzić do naruszenia praw lub wolności. Ogólne rozporządzenie o ochronie danych nakłada pewne obowiązki w zależności od tego, czy mamy do czynienia z naruszeniem ochrony danych osobowych, czy też z naruszeniem praw i wolności.

Naruszenia norm rodo może dopuścić się zarówno administrator danych, jak i podmiot przetwarzający. W rodo została wprowadzona nowa definicja, której nie ma w naszej obecnie ustawie, a mianowicie współadministrator. Analizując zakres jego odpowiedzialności, należy wskazać, że jest ona taka sama jak administratora danych. Współadministrator, dopuszczając się naruszenia, jest więc traktowany tak samo jak administrator danych. Naruszenia może dopuścić się osoba upoważniona. Osobą upoważnioną może być pracownik lub współpracownik administratora danych czy podmiotu przetwarzającego. Zgodnie z art. 32 ust. 4. rodo administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora. W kwestii wyjaśnienia pojęcia polecenia można odwołać się do poleceń służbowych w zakresie czynności wykonywanych przez pracowników lub odnieść się do zakresu czynności wskazanych w upoważnieniu do przetwarzania danych osobowych. Naruszeniem byłoby więc działanie lub zaniechanie pracownika wykraczające poza polecenia służbowe oraz zakres

czynności wskazanych w upoważnieniu. Jako naruszenie należałoby również traktować częściowe wykonanie poleceń administratora danych w zakresie przetwarzania danych osobowych. Taka wykładnia komentowanego przepisu prowadzi do konstrukcji odpowiedniego wzoru upoważnienia, który określiłby zakres czynności związanych z przetwarzaniem danych osobowych.
W polskim systemie prawa naruszenie norm wynikających z ustawy może prowadzić nie tylko do naruszenia przepisów do ochrony danych osobowych, ale również innych przepisów. Analogiczna sytuacja będzie miała miejsce po 25 maja 2018 r., kiedy ustawa przestanie obowiązywać, a ochrona danych osobowych zacznie być regulowana bezpośrednio przez rodo.

Na początku należy wskazać, że naruszenie zasad ochrony danych osobowych może prowadzić do naruszenia dóbr osobistych. Katalog dób osobistych został wskazany w art. 23 Kodeksu cywilnego. Wskazany artykuł zawiera katalog dóbr osobistych, do których można zaliczyć: swobodę sumienia, nazwisko lub pseudonim, wizerunek, tajemnicę korespondencji, nietykalność mieszkania, twórczość naukową, artystyczną, wynalazczą i racjonalizatorską. Wskazany powyżej katalog dóbr osobistych ma charakter dynamiczny, zmieniający się wraz ze zmianami stosunków społecznych. Do wyżej wymienionego katalogu można zaliczyć również prywatność. Jest to szczególnie istotne z uwagi na to, iż naruszenie ochrony danych osobowych może prowadzić właśnie do naruszenia prywatności, czego przykładem może być np. niezamówiony marketing. Ocena, czy w danej sytuacji doszło do naruszenia dóbr osobistych, następuje w oparciu o kryteria obiektywne. Ocena nie zależy więc od subiektywnych odczuć osoby, która twierdzi, że doszło do naruszenia jej prawa do prywatności, lecz od obiektywnej czynników, które mogą zostać potwierdzone w przewodzie cywilnym. Inaczej mówiąc, nie zawsze to co wydaje się nam naruszeniem naszej prywatności, będzie tym naruszeniem w świetle przepisów Kodeksu cywilnego. Nie każde naruszenie ochrony danych osobowych będzie też stanowiło naruszenie prawa do prywatności.

Przykładem takiego naruszenia obecnie jest brak zarejestrowania zbioru danych osobowych u GIODO co stanowi naruszenie ustawy, nie prowadzi jednak do naruszenia prawa do prywatności. Analogiczną

sytuacją związaną z naruszeniem rodo będzie brak rejestru czynności przetwarzania danych, który stanowi naruszenie rodo, ale nie prowadzi do naruszenia prywatności.

Obecnie dochodzenie swoich praw na tle naruszenia prawa do prywatności wymaga złożenia pozwu do sądu cywilnego. W samej ustawie nie ma wprost narzędzi do dochodzenia odszkodowań czy też zadośćuczynień związanych z naruszeniem ochrony danych osobowych. W rodo znajdziemy już wprost przepisy odnoszące się do możliwości dochodzenia ochrony prawnej przed sądem, jeżeli osoba, której dane dotyczą, uzna, że jej prawa przysługujące na mocy niniejszego rozporządzenia zostały naruszone w wyniku przetwarzania danych osobowych z naruszeniem niniejszego rozporządzenia.

Ogólne rozporządzenie o ochronie danych wskazuje, iż pozwanym może być zarówno administrator danych, jak i podmiot przetwarzający. Osoba, której dane zostały naruszone, ma prawo do wniesienia środka ochrony prawnej. Do takich środków można zaliczyć pozew w postępowaniu cywilnym. Zgodnie z art. 79 ust. 2 rodo środek ochrony prawnej wnosi się do sądu państwa członkowskiego, w którym administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną. Dopuszczalne jest również wszczęcie postępowania przed sądem państwa członkowskiego, w którym osoba, której dane dotyczą, ma miejsce zwykłego pobytu, chyba że administrator lub podmiot przetwarzający są organami publicznymi państwa członkowskiego wykonującymi swoje uprawnienia publiczne. Osoba fizyczna może sama dochodzić swoich roszczeń lub wyznaczyć reprezentanta. Nowością wynikającą z rodo jest możliwość umocowania organizacji lub zrzeszenia do reprezentowania interesów osoby fizycznej. Przytoczone podmioty muszą jednak spełniać pewne kryteria wskazana w art. 80 ust. 1 rodo. Do tych kryteriów można zaliczyć niezarobkowy charakter, powołanie zgodnie z prawem państwa członkowskiego, odpowiednio określone cele statutowe leżące w interesie publicznym i działanie w dziedzinie ochrony praw i wolności osób, których dane dotyczą, w związku z ochroną ich danych osobowych.
Tego typu norma wprost wskazuje na powołanie wyspecjalizowanych podmiotów (fundacji lub zrzeszeń), które będą działały w imieniu osób fizycznych, których prawa w zakresie ochrony danych

osobowych zostały naruszone. Te podmioty nie tylko będą mogły ubiegać się o odszkodowania, ale również złożyć skargę do organu nadzoru, którym zgodnie z projektem polskiej ustawy o ochroni e danych osobowych ma być Prezes Urzędu Ochrony Danych Osobowych.

Artykuł 82 ust. 1 rodo wprost wskazuje na możliwość otrzymania odszkodowania od administratora danych lub podmiotu przetwarzającego. Odszkodowanie jest przyznawane w związku z naruszeniem rodo, co jak już wskazano wcześniej jest szerszym pojęciem niż naruszanie ochrony danych osobowych. Osoba fizyczna będzie więc mogła dochodzić odszkodowania również w sytuacji jeżeli wykaże, że zostały naruszone inne zasady niż zasada bezpieczeństwa. W prowadzonym postępowaniu, zgodnie z ciężarem dowodu to powód (osoba, której dane dotyczą) będzie musiała jednak wykazać, iż na skutek naruszenia poniosła szkodę. Ogólne rozporządzenie o ochronie danych nie wprowadza rozróżnienia na szkodę (naruszenie materialne) oraz krzywdę (naruszenie niematerialne). Administrator danych lub podmiot przetwarzający nie odpowiadają za powstała szkodę, jeżeli wskażą, że naruszenie nie powstało z ich winy – art. 82 ust 3 rodo. Jednakże w tym celu konieczne jest wykazanie, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody.

Mamy wiec do czynienia z sytuacją, kiedy można zwolnić się z odpowiedzialności odszkodowawczej, jeżeli wykażemy, że naruszenie powstało nawet pomimo podjętych środków mających za zadanie zapobieżenie temu naruszeniu. Administrator danych oraz podmiot przetwarzający będzie jednak odpowiadał za naruszenia powstałe na skutek winy nieumyślnej (lekkomyślność). Na tego typu podejście wskazują też dotychczasowe przepisy prawa cywilnego oraz podejście sądów, które opiera odpowiedzialność przedsiębiorcy na podstawie ryzyka, a nie winy.

Naruszenie ochrony danych osobowych może stanowić również naruszenia obowiązków pracowniczych. Dotyczy to w szczególności naruszenie zasad bezpieczeństwa. Należy zaznaczyć, iż zarówno obecnie, jak i zgodnie z wymaganiami rodo zasada bezpieczeństwa obejmuje zarówno same dane osobowe, jak i sposoby zabezpieczenia tych danych. Naruszenie rodo tak jak wcześniej ustawy

może stanowić ciężkie naruszenie obowiązków pracowniczych, a wiec po przeprowadzonym postępowaniu dyscyplinarnym udzielnie upominania, nagany czy też zwolnienie dyscyplinarne pracownika.

Kiedy zdarzenie należy zakwalifikować jako naruszenie rzetelności

Artykuł 5 rodo dotyczący zasad przetwarzania danych osobowych jako jedną z pierwszych wymienia zasadę rzetelności. Zgodnie z językową wykładnią rzetelny to:

1. „wypełniający należycie swe obowiązki",
2. „taki, jaki powinien być, odpowiadający wymaganiom",
3. „zgodny z prawdą, wiarygodny".

Zasada rzetelności jest często zestawiana z zasadą przejrzystości, co może sugerować, oprócz definicji językowej na jej właściwą interpratacje. Rzetelne przetwarzanie polega więc na poinformowaniu osoby, której dane dotyczą, o elementach wskazanych w art. 13 oraz 14 rodo oraz stosowaniu ujawnionych elementów w praktyce.

Obowiązek zgłaszania naruszeń

Nowością na gruncie ochrony danych osobowych jest obowiązek zgłaszania naruszeń organowi nadzorczemu. Nie jest to całkowicie nowa instytucja. Obowiązek zgłaszania naruszeń związanych z naruszeniem danych osobowych jest nałożony przez art. 174a Prawa telekomunikacyjnego na dostawców publicznie dostępnych usług telekomunikacyjnych. Zgodnie z art. 33 rodo taki obowiązek będzie spoczywał na każdym podmiocie przetwarzającym dane osobowe. Generalną zasadą wynikającą z przytoczonego artykuł jest obowiązek zgłaszania naruszeń ochrony danych osobowych. Jak to jednak zostało już wskazane nie każde naruszenie rodo stanowi naruszenie ochrony danych osobowych. Naruszeniem ochrony danych osobowych jest naruszeniem bezpieczeństwa

prowadzącym do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Jest to szczególnie istotne z uwagi na to, iż rodo nakłada wyłącznie obowiązek zgłaszania naruszeń ochrony danych osobowych, a nie wszelkich naruszeń norm zawartych w rozporządzeniu. Obowiązek zgłaszania naruszeń spoczywa zarówno na administratorze danych, jak i na podmiocie przetwarzającym.

Autor:

Łukasz Onysyk

Stopka redakcyjna

Redaktor:	Wioleta Szczygielska
ISBN:	978-83-269-6667-5
E-book nr:	2HH0615
Wydawnictwo:	Wydawnictwo Wiedza i Praktyka sp. z o.o.
Adres:	03-918 Warszawa, ul. Łotewska 9a
Kontakt:	Telefon 22 518 29 29, faks 22 617 60 10, e-mail: *cok@wip.pl*
NIP:	526-19-92-256
Numer KRS:	0000098264 – Sąd Rejonowy dla m.st. Warszawy, Sąd Gospodarczy XIII Wydział Gospodarczy Rejestrowy. Wysokość kapitału zakładowego: 200.000 zł