Odpowiedzialność za naruszenie ochrony danych osobowych

Ogólne rozporządzenie o ochronie danych (RODO) nałożyło na administratorów i podmioty przetwarzające szereg nowych obowiązków w zakresie przetwarzania danych osobowych. Równolegle do obowiązków, zmieniły się również zasady ponoszenia odpowiedzialności za naruszenia przepisów ochrony danych osobowych. Brak zgodności z przepisami RODO może prowadzić nie tylko do odpowiedzialności administracyjnej egzekwowanej przez organ nadzoru, ale również do odpowiedzialności cywilnoprawnej, dochodzonej w postępowaniu sądowym. Co więcej, kolejny rodzaj odpowiedzialności, tym razem karną, wprowadza *Ustawa o ochronie danych osobowych*.

Odpowiedzialność administracyjna

Najczęstszym rodzajem komentowanej odpowiedzialności za naruszenie przepisów RODO jest odpowiedzialność administracyjna. A właściwie wysokość **pieniężnych kar administracyjnych**, które mogą zostać nałożone przez krajowe organy nadzoru. Zależnie od okoliczności każdego indywidualnego przypadku, kary pieniężne nakładane są obok lub zamiast środków naprawczych.

Nałożenie przez organ nadzoru kar pieniężnych lub obowiązku zastosowania właściwych środków naprawczych następuje po przeprowadzeniu postępowania administracyjnego. Postępowanie administracyjne może być natomiast wynikiem złożonej przez podmiot danych skargi lub przeprowadzonej kontroli.

RODO wyróżnia **dwa przedziały kar pieniężnych**:

- do **10 mln euro**, a w przypadku przedsiębiorstwa do **2 % jego całkowitego rocznego światowego obrotu** z poprzedniego roku obrotowego,
- do **20 mln euro**, a w przypadku przedsiębiorstwa do **4 % jego całkowitego rocznego światowego obrotu** z poprzedniego roku obrotowego.

Wyższa kara przewidziana jest m.in. za naruszenie podstawowych zasad przetwarzania danych osobowych czy naruszenie podstawowych obowiązków względem osób, których dane dotyczą, takich jak obowiązek informacyjny czy obowiązek związany z prawem do usunięcia danych.

Ustawa o ochronie danych osobowych przewiduje jednak mniejsze kary dla podmiotów sektora finansów publicznych:

- jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1–12 i 14 *Ustawy o finansach publicznych*, instytutu badawczego i Narodowego Banku Polskiego – w wysokości do **100 000 złotych** (tj. np. szkoły, uczelnie, szpitale, ZUS, gminy, NFZ, sądy),

- jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 13 *Ustawy o finansach publicznych* – w wysokości do **10 000 złotych** (tj. np. teatry, opery, filharmonie, kina, muzea, biblioteki, domy kultury, galerie sztuki).

Oznacza to, że w razie naruszenia przepisów RODO, administracja będzie dużo łagodniej potraktowana niż przedsiębiorcy. Jest to jednak działanie usprawiedliwione. Administracja nie dysponuje bowiem własnymi środkami pieniężnymi, więc żeby zapłacić ewentualną karę, będzie musiała te środki wydzielić z tego, czym dysponuje na realizację swoich ustawowych zadań. Pomimo kary obowiązek ich realizacji pozostanie, zmniejszy się natomiast budżet. W tym wypadku tymi którzy na tym stracą, będą przede wszystkim obywatele. Mimo że pomniejszona, kara pieniężna i tak pozwoli na ukaranie podmiotu i działań osób, których zaniedbania doprowadziły do jej nałożenia.

Należy zaznaczyć, że samo stwierdzenie naruszeń przepisów RODO, które stanowią podstawę do nałożenia kary pieniężnej, nie obliguje organu do sięgnięcia po ten rodzaj sankcji. Organ zawsze ma bowiem możliwość zastosowania środków naprawczych o charakterze niepieniężnym. Jeżeli naruszenie jest niewielkie lub jeżeli grożąca kara pieniężna stanowiłaby dla administratora nieproporcjonalne obciążenie, organ zamiast tego może udzielić upomnienia.

Organ nadzoru decydując o tym czy nałożyć karę pieniężną oraz ustalając jaka ewentualnie ma być jej wysokość, bierze pod uwagę:

- charakter, wagę oraz czas trwania naruszenia,
- umyślność lub nieumyślność naruszenia,
- działania podjęte dla zminimalizowania szkody,
- stopień odpowiedzialności z uwzględnieniem wdrożonych środków technicznych i organizacyjnych,
- wszelkie mające znaczenie wcześniejsze naruszenia,
- sposób, w jaki dowiedział się o naruszeniu,
- zastosowanie się do wcześniej nałożonych środków naprawczych,
- stosowanie kodeksów postępowania,
- wszelkie inne czynniki obciążające lub łagodzące.

Zadaniem organu jest stosowanie takich sankcji, aby były w każdym indywidualnym przypadku **skuteczne, proporcjonalne i odstraszające.**

Jeżeli w wyniku analizy naruszenia organ zdecyduje się zrezygnować z kary pieniężnej jako zbyt rygorystycznej w danym przypadku, może on zamiast tego zastosować wspomniane już **środki naprawcze** do których zaliczamy:

- udzielanie upomnień,
- nakazanie spełnienia żądania osoby, której dane dotyczą, wynikającego z przysługujących jej praw,

- nakazanie dostosowania operacji przetwarzania do przepisów RODO, a w stosownych przypadkach wskazanie sposobu i terminu,
- nakazanie zawiadomienia osoby, której dane dotyczą, o naruszeniu,
- wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania,
- nakazanie sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania oraz nakazanie powiadomienia o tych czynnościach odbiorców, którym ujawniono dane osobowe,
- cofnięcie certyfikacji lub nakazanie podmiotowi certyfikującemu cofnięcia lub nieudzielania certyfikacji,
- nakazanie zawieszenia przepływu danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej.

Odpowiedzialność cywilnoprawna

Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia RODO, ma prawo uzyskać od administratora danych lub podmiotu przetwarzającego **odszkodowanie za poniesioną szkodę**. Wszczęcie postępowania sądowego jest możliwe niezależnie od skarg złożonych do organu nadzoru. Regulacja zawarta w art. 82 RODO ma charakter wyłącznie prywatnoprawny i dotyczy bezpośredniej relacji pomiędzy administratorem lub podmiotem przetwarzającym a podmiotem danych.

Administrator lub podmiot przetwarzający poniesie odpowiedzialność w przypadku **wystąpienia łącznie** następujących przesłanek:

- poniesienia przez osobę, której dane dotyczą **szkody** (majątkowej lub niemajątkowej),
- **naruszenia** przez administratora lub procesora przepisów RODO,
- zaistnienia **związku pomiędzy szkodą a naruszeniem**,
- wystąpienia **winy** w naruszeniu RODO.

Zgodnie z postanowieniami motywu 146, przetwarzanie dokonywane w sposób naruszający RODO obejmuje także przetwarzanie, które narusza **akty delegowane i wykonawcze** przyjęte na jego mocy oraz **prawo państwa członkowskiego** je doprecyzowujące. Tym samym, szkoda podmiotu danych może być spowodowana nie tylko niezgodnością postępowania z zasadami przetwarzania wskazanymi w RODO, ale również m.in. w *Ustawie o ochronie danych osobowych*, bądź *Ustawie o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia*. Warto przy tym pamiętać, że ostatnia z powołanych ustaw wprowadza zmiany w wielu przepisach sektorowych takich jak np. *Kodeks Pracy* czy *Prawo bankowe*.

Ciężar dowodu wystąpienia naruszenia spoczywa na podmiocie danych. Biorąc jednakże pod uwagę zasadę rozliczalności, administrator musi być w stanie wykazać przestrzeganie przez siebie przepisów ochrony danych osobowych. Sprowadzi się to zatem do tego, że ciężar udowodnienia zgodności przetwarzania zostanie przeniesiony na administratora, po przedstawieniu przez podmiot danych dowodów na wystąpienie naruszenia.

Odpowiedzialność solidarna

Jeżeli w tym samym procesie przetwarzania danych osobowych uczestniczy więcej niż jeden podmiot, ich odpowiedzialność będzie miała charakter **solidarny**. Ma to na celu przede wszystkim zapewnienie osobie, której dane dotyczą rzeczywiste uzyskanie odszkodowania lub zadośćuczynienia.

Administrator lub podmiot przetwarzający, który zapłacił odszkodowanie za całą wyrządzoną szkodę, ma prawo żądania od pozostałych podmiotów uczestniczących w tym przetwarzaniu, zwrotu części kwoty odszkodowania odpowiadającej części szkody, za którą ponoszą odpowiedzialność (**roszczenie regresowe**).

Podmiot przetwarzający odpowiada wyłącznie za szkody spowodowane niedopełnieniem przez niego obowiązków, które nakłada na niego RODO oraz za działania wbrew zgodnym z prawem instrukcjom administratora. Tym samym, o odpowiedzialności procesora możemy mówić w następujących przypadkach:

- przepisy RODO nakładały na procesora obowiązki, których niewykonanie lub nienależyte wykonanie spowodowało szkodę,
- procesor działał niezgodnie ze zgodnymi z prawem instrukcjami administratora,
- procesor świadomie działał zgodnie z niezgodnymi z prawem instrukcjami administratora.

Z uwagi na powyższe, niezmiernie istotne jest właściwe określenie obowiązków podmiotu przetwarzającego, które powinno nastąpić w zawartej między nim a administratorem umowie powierzenia przetwarzania danych osobowych.

W przypadku podpowierzenia danych osobowych pełną odpowiedzialność za naruszenie spowodowane działaniami subprocesora ponosić będzie pierwotny podmiot przetwarzający.

Odpowiedzialność **współadministratorów** będzie miała również charakter solidarny. Co istotne ich solidarna odpowiedzialność wobec podmiotu danych, nie może zostać wyłączona we wspólnych uzgodnieniach, o których mowa w art. 26 RODO.

Odpowiedzialność karna

RODO nie reguluje kwestii związanych z odpowiedzialnością karną w razie jego naruszenia. Motyw 149 preambuły wskazuje jednak, że państwa członkowskie powinny mieć możliwość ustanawiania przepisów przewidujących sankcje karne za naruszenie jego postanowień, w tym za naruszenie krajowych przepisów przyjętych na jego mocy i w jego granicach.

Odpowiedzialność karna za naruszenie regulacji dotyczących ochrony danych osobowych została ujęta przez polskiego prawodawcę w art. 107 *Ustawy o ochronie danych osobowych*. Zgodnie z tym przepisem, **ten kto przetwarza dane osobowe**, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega:

- **grzywnie**,
- **karze ograniczenia wolności**,
- **karze pozbawienia wolności do lat dwóch**, w przypadkach szczególnych kategorii danych osobowych, **do lat trzech**.

Z sytuacjami, kiedy **przetwarzanie danych jest niedopuszczalne** mamy do czynienia wówczas, gdy brak jest podstawy prawnej to przetwarzanie legalizującej. Wiąże się to zatem z naruszeniem art. 6 RODO (jeżeli przetwarzane są dane zwykłe) albo 9 RODO (jeżeli przetwarzane są szczególne kategorie danych). Należy przy tym również pamiętać o szczególnych warunkach przetwarzania danych osobowych dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa, a więc o art. 10 RODO.

Przetwarzanie danych przez osobę nieuprawnioną wiąże się z kolei z przypadkami, gdy osoba, która dane przetwarza pozostaje poza kręgiem podmiotów do tego upoważnionych, tj. w stosunku do przetwarzanych danych nie posiada statusu administratora, podmiotu przetwarzającego, dalszego podmiotu przetwarzającego lub nie dysponuje upoważnieniem do przetwarzania danych osobowych nadanym przez administratora.

Zgodnie z zasadami prawa karnego, odpowiedzialność karną na podstawie przepisów *Ustawy o ochronie danych osobowych* ponoszą zawsze **oznaczone osoby fizyczne**, którym ta odpowiedzialność może zostać przypisana. Kara pozbawienia wolności nie zostanie zatem orzeczona wobec administratora, lecz wobec jego pracownika, który dopuścił się niezgodnego z prawem przetwarzania danych osobowych.

Co istotne, przestępstwa wskazane w art. 107 *Ustawy o ochronie danych osobowych* mogą zostać popełnione wyłącznie **umyślnie**. Jeżeli zatem pracownik nie miał świadomości braku podstawy do przetwarzania danych, które procedował w ramach swoich obowiązków służbowych, ciężko mu taką odpowiedzialność będzie przypisać. Co innego w sytuacji umyślnego naruszenia przepisów, np. wyniesienie bazy danych poza strukturę administratora i jej sprzedaży.

Podsumowanie

Sankcje grożące za naruszenie zasad ochrony danych osobowych są dość dotkliwe. Mogą zostać nałożone nie tylko na administratora danych czy podmiot przetwarzający. Odpowiedzialność może spotkać również pracowników czy współpracowników tych podmiotów.

Do tej pory najwyższą karę za nieprzestrzeganie RODO nałożył francuski organ nadzoru. W styczniu br. Google zostało ukarane sankcją 50 mln euro. Jest to jasny sygnał, że czasy pobłażliwości w tym zakresie bezpowrotnie się skończyły, a ochrona danych osobowych powinna być traktowana bardzo poważnie. Również w Polsce.

Autor artykułu:

Małgorzata Zdunek, *ekspert ds. ochrony danych osobowych*

Źródła:

- 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 (ogólne rozporządzenie o ochronie danych)
- Ustawa z dnia 20 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000)
- Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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 (ogólne rozporządzenie o ochronie danych) – treść uchwalona 21 lutego 2019 r., przekazana Prezydentowi i Marszałkowi Senatu 22 lutego 2019 r.
- RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, Bielak-Jomaa Edyta (red.), Lubasz Dominik (red.)
- Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz, Litwiński Paweł (red.), Barta Paweł, Kawecki Maciej