Warszawa, dn. 22 września 2026 r.

Czy każdy wniosek o dostęp do danych trzeba realizować?

19 marca 2026 r. Trybunał Sprawiedliwości Unii Europejskiej wydał wyrok w sprawie C-526/24, Brillen Rottler GmbH & Co. KG przeciwko TC, dotyczący granic korzystania z prawa dostępu do danych osobowych na podstawie RODO. Orzeczenie ma znaczenie nie tylko dla prawników i specjalistów ds. ochrony danych. Dotyka sytuacji, z którą w praktyce może spotkać każdy administrator: spółka, instytucja czy organizacja przetwarzająca dane klientów, pracowników lub subskrybentów. Sedno sprawy sprowadza się do pytania: gdzie kończy się korzystanie z uprawnień przyznanych przez RODO, a gdzie się zaczyna ich nadużycie?
Klient zapisuje się do newslettera, a kilkanaście dni później kieruje do firmy wniosek o szeroki dostęp do dotyczących go danych. Jednocześnie wskazuje, że jeśli jego żądanie nie zostanie spełnione, może wystąpić z roszczeniem odszkodowawczym. Czy administrator może w takiej sytuacji odmówić realizacji wniosku, czy znaczenie ma to, że jest to pierwsze żądanie dostępu złożone przez tę osobę i czy powinien „bać się" konieczności zapłaty odszkodowania?
Właśnie na te kwestie zwrócił uwagę TSUE w sprawie Brillen Rottler.

Stan faktyczny

W marcu 2023 r. mężczyzna oznaczony w wyroku jako TC, mieszkający w Austrii, zapisał się do newslettera niemieckiego przedsiębiorstwa optycznego Brillen Rottler, podając swoje dane osobowe i wyrażając zgodę na ich przetwarzanie. Kilkanaście dni później skierował do firmy formalny wniosek o dostęp do swoich danych na podstawie art. 15 RODO. Brillen Rottler odmówiło, uznając żądanie za nadmierne w rozumieniu art. 12 ust. 5 RODO. TC podtrzymał swoje żądanie i zażądał 1000 euro odszkodowania na podstawie art. 82 RODO. Firma wystąpiła do sądu, twierdząc, że TC stosuje powtarzalny schemat: zapisuje się do newsletterów, następnie składa wnioski o dostęp do danych, a w przypadku nieprawidłowości żąda odszkodowania. Na poparcie swoich twierdzeń wskazywała m.in. publikacje internetowe i biuletyny kancelarii prawnych.
Zdaniem Brillen Rottler RODO nie służyło w tym przypadku ochronie prywatności, lecz systematycznemu wyszukiwaniu uchybień administratorów. Sąd rejonowy w Arnsbergu powziął wątpliwości dotyczące wykładni przepisów RODO i skierował do TSUE pytania prejudycjalne. Trybunał odpowiedział, porządkując trzy ważne kwestie.

Czy i kiedy wniosek o dostęp do danych może być nadmierny?

Artykuł 12 ust. 5 RODO pozwala administratorowi odmówić realizacji żądania osoby, której dane dotyczą albo pobrać rozsądną opłatę, jeśli żądanie to jest ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter. Kluczowe słowo to ustawiczny, czyli powtarzający się. Rodziło ono pytanie: czy skoro przepis mówi o powtarzalności, to pierwszy w ogóle złożony wniosek zawsze musi być traktowany jako uprawniony?
Trybunał odpowiedział, że fraza „w szczególności ze względu na swój ustawiczny charakter" jest w przepisie tylko przykładem, a nie jedynym możliwym powodem uznania żądania za nadmierne. Tak więc liczba wniosków nie jest jedynym kryterium. Nawet pierwszy, jedyny wniosek złożony przez daną osobę teoretycznie może zostać uznany za nadmierny, jeśli okoliczności na to wskazują.
To nie oznacza jednak, że administratorzy dostali w ręce łatwe narzędzie do odmawiania dostępu każdemu, kto wydaje im się podejrzany. TSUE wyraźnie zastrzegł, że wyjątek z art. 12 ust. 5 RODO należy interpretować zawężająco: to znaczy, że administrator może się na niego powoływać tylko wyjątkowo, a próg dowodowy powinien być wysoki. Co więcej, to na administratorze, a nie na osobie

żądającej dostępu, spoczywa ciężar wykazania, że żądanie rzeczywiście jest nadmierne. Sam fakt, że ktoś skorzystał ze swojego prawa szybko po nawiązaniu relacji z firmą, niczego jeszcze nie przesądza. Trybunał odwołał się do ugruntowanej w prawie unijnym koncepcji nadużycia prawa. Aby stwierdzić, że dane zachowanie stanowi nadużycie, trzeba wykazać łącznie dwa elementy:

- **obiektywny**: mimo formalnego spełnienia wszystkich przesłanek przewidzianych w przepisach, cel, jakiemu ten przepis ma służyć, w rzeczywistości nie jest realizowany. Celem prawa dostępu z art. 15 RODO, jak przypomniał Trybunał, odwołując się do motywu 63 preambuły, jest umożliwienie osobie zorientowania się, jakie dane są o niej przetwarzane oraz sprawdzenie zgodności tego przetwarzania z prawem, tak by mogła ewentualnie skorzystać z innych uprawnień (sprostowania, usunięcia, sprzeciwu itd.).
- **subiektywny**: wola uzyskania korzyści wynikającej z przepisów Unii poprzez sztuczne stworzenie warunków wymaganych do jej uzyskania. Administrator musi wykazać, że osobie nie chodziło wcale o poznanie sposobu przetwarzania jej danych, tylko o stworzenie podstawy do żądania odszkodowania.

TSUE wskazał konkretne okoliczności, które sąd krajowy powinien wziąć pod uwagę, oceniając, czy do takiego nadużycia doszło:

- czy osoba podała dane, mimo że nie była do tego w ogóle zobowiązana,
- w jakim celu dane zostały podane,
- ile czasu upłynęło między podaniem danych a złożeniem wniosku o dostęp,
- całościowe zachowanie tej osoby.

Trybunał odniósł się też do argumentu Brillen Rottler dotyczącego publicznie dostępnych informacji (artykułów, wpisów na blogach, biuletynów prawniczych) sugerujących, że TC systematycznie stosuje ten sam schemat wobec różnych firm. TSUE potwierdził, że tego typu informacje mogą być brane pod uwagę przy ocenie, czy doszło do nadużycia, ale wyłącznie jako element wspierający, potwierdzony innymi okolicznościami sprawy. Same doniesienia medialne czy wpisy na forach nie wystarczą. Ostatecznie to do krajowego sądu należy teraz ocena, czy w konkretnym przypadku TC rzeczywiście działał w złej wierze, czy po prostu skorzystał ze swojego ustawowego prawa: tylko szybciej i bardziej stanowczo, niż firma by sobie tego życzyła.

Czy odszkodowanie należy się tylko za przetwarzanie?

Druga grupa pytań dotyczyła art. 82 ust. 1 RODO, który przyznaje prawo do odszkodowania za szkodę majątkową lub niemajątkową w wyniku naruszenia rozporządzenia. Pojawiła się wątpliwość: czy odszkodowanie przysługuje tylko wtedy, gdy szkoda wynika bezpośrednio z niezgodnego z prawem *przetwarzania* danych, czy również wtedy, gdy naruszenie polega na czymś innym, na przykład na samej odmowie udzielenia dostępu do danych, bez żadnej dodatkowej operacji na danych?

TSUE odpowiedział jasno, że prawo do odszkodowania nie jest ograniczone wyłącznie do szkód wynikających z przetwarzania danych. Przepis art. 82 ust. 1 RODO wskazuje ogólnie na naruszenie rozporządzenia. Naruszenie prawa dostępu z art. 15 RODO (a więc np. bezpodstawna odmowa udzielenia informacji) samo w sobie może rodzić prawo do odszkodowania, nawet jeśli nie towarzyszy mu żadna nowa, nielegalna operacja na danych osobowych. Jeśli więc firma bezpodstawnie odmówi komuś dostępu do jego danych, może się narazić na roszczenie odszkodowawcze, niezależnie od tego, czy same dane były przetwarzane w sposób wadliwy.

Czym jest szkoda niemajątkowa w tym kontekście?

Sama utrata kontroli nad danymi osobowymi albo niepewność co do tego, czy dane są przetwarzane, mogą stanowić szkodę niemajątkową uzasadniającą odszkodowanie.

Tu Trybunał podtrzymał linię orzeczniczą wypracowaną we wcześniejszych sprawach (m.in. Sprawa C-300/21, Österreichische Post AG: Wyrok z dnia 4 maja 2023 r. - UI v. Österreichische Post AG) utrata kontroli nad danymi rzeczywiście może być uznana za szkodę niemajątkową, nawet jeśli nie doszło do żadnego konkretnego nadużycia tych danych. Nie ma też żadnego „progu minimalnego": sąd krajowy nie może uznać, że szkoda była „zbyt mała", by w ogóle się nią zajmować.
Jest jednak istotne zastrzeżenie: osoba domagająca się odszkodowania musi realnie wykazać, że taką szkodę poniosła. Samo twierdzenie „bałem się" czy „czułem niepewność" nie wystarczy. Trybunał podkreślił też coś, co ma szczególne znaczenie właśnie dla takich spraw jak ta z Brillen Rottler: związek przyczynowy między naruszeniem a szkodą może zostać przerwany zachowaniem samej osoby poszkodowanej. Jeśli to sama osoba świadomie i dobrowolnie doprowadziła do sytuacji, w której rzekomo utraciła kontrolę nad swoimi danymi, na przykład celowo podając dane administratorowi po to, by sztucznie stworzyć podstawę do żądania odszkodowania, to nie może potem powoływać się na tę utratę kontroli jako na szkodę.

Co oznacza ten wyrok w praktyce?
Dla administratorów danych (firm i instytucji)
Wyrok potwierdza, że administratorzy mogą bronić się przed oczywistymi nadużyciami prawa dostępu do danych, także gdy chodzi o pierwszy wniosek danej osoby. Jest to jednak wyjątkowe narzędzie, którego zastosowanie wymaga ostrożności. Samo podejrzenie, że „coś tu nie gra", nie wystarczy. Administrator powinien wykazać rzeczywisty zamiar nadużycia, opierając się na konkretnych okolicznościach i dowodach a znaczenie mogą mieć m.in.:

- okoliczności podania danych,
- tempo i sposób działania wnioskodawcy,
- wcześniejsze, podobne przypadki potwierdzone konkretnymi dowodami, np. publicznymi wpisami.

W praktyce warto dokładnie dokumentować całą korespondencję i unikać pochopnej odmowy realizacji wniosku.
Dla osób, których dane dotyczą
Wyrok potwierdza, że prawo dostępu do danych jest realnym i egzekwowalnym uprawnieniem. Naruszenie tego prawa może prowadzić do roszczenia odszkodowawczego, nawet jeśli nie doszło jednocześnie do niewłaściwego przetwarzania danych. Jednocześnie prawo dostępu nie powinno być wykorzystywane instrumentalnie do sztucznego generowania sporów i roszczeń finansowych. Sądy krajowe powinny badać, czy za żądaniem rzeczywiście stoi ochrona prywatności, czy też inne, w szczególności finansowe, cele.
Dla praktyki orzeczniczej i compliance:
Wyrok wpisuje się w szerszą linię orzeczniczą TSUE dotyczącą równoważenia praw osób, których dane dotyczą, z ochroną administratorów przed nadużywaniem uprawnień. Dla działów compliance i inspektorów ochrony danych oznacza to potrzebę analizowania nie tylko samej treści wniosku, ale również jego kontekstu. Każdy przypadek powinien być oceniany indywidualnie, a ewentualna odmowa powinna być oparta na konkretnych, możliwych do wykazania okolicznościach.
Wyrok w sprawie Brillen Rottler pokazuje, że RODO, choć często postrzegane jako sztywny, zbiór przepisów, w praktyce wymaga sporo wyważenia i indywidualnej oceny każdej sytuacji. Trybunał po raz kolejny przypomniał, że prawo do ochrony danych osobowych, nie jest prawem absolutnym i musi być stosowane z poszanowaniem zasady proporcjonalności oraz zakazu nadużywania prawa.

Gabriela Tokarska - młodsza specjalistka ds. ochrony danych osobowych w iSecure sp. z o.o.