

COMPLIANCE INSIGHTS

Vol. 105

Nadmiarowe ujawnienie danych osobowych przedstawicielom mediów



1. Dane ujawnione na konferencji

Spór między spółdzielnią mieszkaniową a jej członkinią przeniósł się do lokalnych mediów i internetu. Chcąc przedstawić opinii publicznej swoją wersję wydarzeń, zarząd zwołał konferencję prasową. Dziennikarzom przekazano kopię zawiadomienia o podejrzeniu popełnienia przestępstwa, zawierającą imię, nazwisko, numer PESEL i adres zamieszkania członkini spółdzielni. Dokument nie został wcześniej zanonimizowany, co doprowadziło do ujawnienia danych osobom nieuprawnionym.



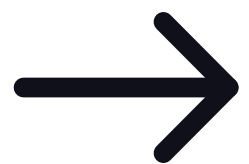
2. Upublicznienie ma swoje granice

Spółdzielnia argumentowała, że członkini wcześniej sama upubliczniła swoje dane, dlatego ryzyko związane z naruszeniem uznano za niskie. W toku postępowania administrator przyznał jednak, że nie wie, czy osoba ta opublikowała kopię zawiadomienia o podejrzeniu popełnienia przestępstwa ani czy weszła w jego posiadanie. Samo ogólne udostępnienie niektórych informacji przez osobę nie oznacza zatem, że administrator może ujawnić cały dokument i zawarte w nim dane.



3. Prawo prasowe to nie wyjątek

Spółdzielnia twierdziła również, że dane pozostawały bezpieczne, ponieważ dokument przekazano dziennikarzom zobowiązanym do zachowania rzetelności zawodowej. Dziennikarze nie występowali jednak o udostępnienie danych członkini spółdzielni, a Prawo prasowe nie uzasadniało przekazania im niezanonimizowanej kopii zawiadomienia. Zaufanie do odbiorcy nie zwalnia administratora z ograniczenia zakresu ujawnianych informacji ani z oceny ryzyka z perspektywy osoby, której dane dotyczą.



4. Prawo do ochrony danych pozostaje

Okoliczność, że wobec danej osoby złożono zawiadomienie o podejrzeniu popełnienia przestępstwa, nie daje administratorowi swobody w ujawnianiu jej danych. Nawet gdyby zarzuty zostały później potwierdzone, osoba ta nadal korzysta z ochrony przewidzianej w RODO. Ujawnienie numeru PESEL wraz z imieniem, nazwiskiem i adresem powinno być oceniane przez pryzmat możliwych konsekwencji dla tej osoby, a nie stawianych jej zarzutów.



5. Konieczna reakcja przed wystąpieniem szkody

To, że ujawnienie danych nie doprowadziło jeszcze do odnotowanej szkody, nie zwalnia administratora z działania. Znaczenie ma już sama możliwość wystąpienia kradzieży tożsamości, strat finansowych lub naruszenia dobrego imienia. Powiadomienie osoby, której dane dotyczą, nie jest przy tym formalnością. Ma umożliwić jej ocenę sytuacji i podjęcie środków zaradczych, zanim potencjalne ryzyko przerodzi się w rzeczywiste konsekwencje.



6. Spółdzielnia jako przedsiębiorca

NSA odniósł się także do odrębnej kwestii: czy spółdzielnia mieszkaniowa może być uznana za przedsiębiorcę na potrzeby nakładania kar na podstawie RODO. WSA miał w tym zakresie wątpliwości, jednak NSA ich nie podzielił. Uznał spółdzielnię za przedsiębiorcę w rozumieniu art. 83 ust. 4 RODO. Oznacza to, że znajduje wobec niej zastosowanie maksymalny limit kary przewidziany w tym przepisie dla przedsiębiorstw.



7. Wnioski dla administratorów

Każde naruszenie wymaga indywidualnej, udokumentowanej analizy. Powinna ona obejmować zakres i kontekst ujawnionych danych, możliwe skutki dla osoby, której dane dotyczą, oraz prawdopodobieństwo ich wystąpienia. Ogólny formularz lub lakoniczny wpis w rejestrze naruszeń nie zastąpią rzetelnej oceny. Jeżeli występują wątpliwości, administrator powinien poważnie rozważyć zgłoszenie naruszenia, zamiast zakładać, że brak dotychczasowej szkody oznacza brak ryzyka.



Compliance Insight



Mariusz Purgał

Partner

mariusz.purgal@kwkr.pl
+48 797 927 960



Maksymilian Skrzypek

Associate

maksymilian.skrzypek@kwkr.pl
+48 508 062 117

Zapraszamy do kontaktu
