

# Nowe obowiązki dostawców usług telekomunikacyjnych

**OCHRONA PRYWATNOŚCI** Operatorzy muszą zawiadamiać generalnego inspektora ochrony danych osobowych oraz abonentów o naruszeniu danych osobowych i prowadzić rejestr takich zdarzeń.

**MICHAŁ KOŁTUNIAK**

Na dostawców publicznie dostępnych usług telekomunikacyjnych nałożone zostały nowe obowiązki. Wszystko za sprawą nowelizacji ustawy – Prawo telekomunikacyjne. Została ona poszerzona o art. 174a – 174d. W największym skrócie sprowadzają się one do tego, że przedsiębiorca nie tylko musi chronić dane osobowe swoich klientów (co oczywiście musiał robić już wcześniej), ale w przypadku wykrycia naruszenia ich bezpieczeństwa powiadomić o tym zainteresowanego oraz organ właściwy do ochrony danych osobowych, czyli generalnego inspektora danych osobowych.

## Trzy dni

I tak w myśl nowego art. 174a ust. 1 dostawca usług telekomunikacyjnych zawiadamia GODO o naruszeniu danych osobowych niezwłocznie, nie później niż w terminie trzech dni od stwierdzenia naruszenia. Ustęp 2 wyjaśnia, że przez naruszenie rozumie się przypadkowe lub bezprawne zniszczenie, utratę, zmianę, nieuprawnione ujawnienie lub dostęp do danych osobowych przetwarzanych przez przedsiębiorcę w zwią-

ku ze świadczeniem publicznie dostępnych usług. Z kolei ustęp trzeci wskazuje, że w przypadku, gdy naruszenie danych może mieć niekorzystny wpływ na prawa abonenta lub użytkownika końcowego (będącego osobą fizyczną), dostawca niezwłocznie (jednak także nie później niż w terminie 3 dni) po wykryciu tego naruszenia, zawiadamia o tym osobę zainteresowaną. Rodzić może pytanie to, co należy rozumieć pod pojęciem niekorzystnego wpływu na prawa abonenta (użytkownika końcowego). Jednak i tutaj przepisy dają wskazówki. W myśl art. 174a ust. 4 przez naruszenie danych, które może wywrzeć niekorzystny wpływ na prawa abonenta lub użytkownika końcowego będącego osobą fizyczną, rozumie się takie naruszenie, które w szczególności może skutkować nieuprawnionym posługiwaniem się danymi osobowymi, szkodą majątkową, naruszeniem dóbr osobistych, ujawnieniem tajemnicy bankowej lub innej ustawowo chronionej tajemnicy zawodowej.

## Szczegółowy opis

Przepisy, poza wskazaniem obowiązku zawiadomienia o zaistniałej sytuacji, wskazują również, jak należy sformułować zawiadomienie. Mówiąc

dokładniej, wskazują, co powinno się w nim znaleźć. I tak w myśl art. 174a ust. 7 i 8, zarówno zawiadomienie kierowane do generalnego inspektora ochrony danych osobowych, jak i to kierowane do abonenta powinny zawierać m.in.:

- opis charakteru naruszenia danych osobowych,
- dane kontaktowe dostawcy publicznie dostępnych usług telekomunikacyjnych,
- informację o zalecanych środkach mających na celu złagodzenie ewentualnych niekorzystnych skutków naruszenia,
- informację o działaniach podjętych przez dostawcę,
- opis skutków naruszenia oraz proponowanych przez dostawcę środków naprawczych.

Warto zaznaczyć, że zawiadomienie kierowane do GODO powinno dodatkowo zawierać informację o zakładanym ryzyku związanym z powstałym naruszeniem oraz o fakcie (lub jego braku) poinformowania abonenta o wystąpieniu naruszenia danych osobowych. Ponadto warto dodać, że w przypadku gdy przedsiębiorca nie poinformuje abonenta o naruszeniu, a GODO uzna, że w danym przypadku powinno to nastąpić, może nałożyć taki obowiązek na firmę w drodze wydania odpowiedniej decyzji.

## • KIEDY NIE TRZEBA INFORMOWAĆ

Od obowiązku powiadomienia abonenta lub użytkownika końcowego, którym jest osoba prywatna, o naruszeniu jest jeden wyjątek. Mianowicie przedsiębiorca telekomunikacyjny nie musi tego robić, jeżeli zastosował u siebie odpowiednie techniczne i organizacyjne środki ochrony. Muszą to być środki, które uniemożliwiają odczytanie danych przez osoby nieuprawnione oraz rzeczywiste były zastosowane do danych, których ochrona została naruszona. W praktyce chodzi więc o sytuację, w których pomimo naruszenia zasad ochrony danych i np. dostania się ich w niepowołane ręce, niemożliwe będzie ich odczytanie i powiązanie ich z konkretnymi osobami. Wyjątek ten wprowadza art. 174a ust. 5. ■

## Uwaga!

**Przedsiębiorca ma obowiązek prowadzenia rejestru naruszeń danych osobowych, w tym faktów towarzyszących naruszeniom, ich skutków i podjętych działań.** Zgodnie z art. 174d ust. 2 dostawca publicznie dostępnych usług telekomunikacyjnych może powierzyć w drodze umowy innemu przedsiębiorcy prowadzenie rejestru naruszeń danych osobowych.