Dr Marlena Wach
RADCA PRAWNY W KANCELARII DOMAŃSKI ZAKRZEWSKI PALINKA SP. K.,
ADIUNKT, SZKOŁA WYŻSZA PSYCHOLOGII SPOŁECZNEJ

Kilka uwag na temat nowych obowiązków dostawców usług w związku z implementacją dyrektyw 2009/140/WE oraz 2009/136/WE

Nadmierna ochrona w nowelizacji Prawa telekomunikacyjnego

W dyskusji nad neutralnością i nowymi obowiązkami dostawców usług telekomunikacyjnych należy uwzględnić fakt, iż wypełnianie obowiązków w zakresie bezpieczeństwa oraz integralności sieci i usług związane jest de facto z zarządzaniem ruchem. Zarządzanie to jest już zatem praktykowane, więc dalsza dyskusja dobrze, aby miała na celu doprecyzowanie i ujednolicenie szczegółowych zasad zarządzania oraz ustalenie ich wzajemnego oddziaływania.

Projekt nowelizacji Prawa telekomunikacyjnego ma na celu implementację dyrektyw 2009/140/WE oraz 2009/136/WE, które zostały przyjęte przez Parlament Europejski i Radę 25 listopada 2009 r. Dyrektywy te zmieniają poprzednie regulacje telekomunikacyjne tworzące tzw. pakiet dyrektyw 2002. Zmieniona została m.in. dyrektywa 2002/58/WE dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej. Nowelizacja Prawa telekomunikacyjnego 18 stycznia 2012 r. została przyjęta przez komitet Rady Ministrów do spraw europejskich i projekt ma trafić pod obrady stałego komitetu Rady Ministrów.

Ochrona użytkowników

Nowe przepisy mają lepiej chronić użytkowników, tym samym nakładają dodatkowe obowiązki na przedsiębiorców telekomunikacyjnych. Wskazuje się wielokrotnie w różnych publikacjach dotyczących tego zagadnienia, iż umowa o świadczenie usług telekomunikacyjnych i regulamin będą bardziej rozbudowane, a przez to nieczytelne. Wprowadzenie wielu obowiązków informacyjnych stanowi kontynuację szerszej polityki Komisji Europejskiej realizowanej nie tylko w stosunku do sektora telekomunikacyjnego, ale też np. sektora finansowego[1]. Objawia się też ona w przyjęciu przez Parlament Europejski dyrektywy o prawach konsumenta (*The Consumer Rights Directive* 20011/83/EU[2]). Przepisy tej nowej dyrektywy muszą zostać wprowadzone najpóźniej do końca 2013 r. przez państwa członkowskie.

Nowa dyrektywa wprowadza m.in. wspólne dla wszystkich państw członkowskich definicje konsumenta i sprzedawcy oraz wspólny zbiór zasad, od których państwa członkowskie mogą odstąpić tylko w szczególnych przypadkach. Dyrektywa ta wskazuje na najważniejsze informacje, jakie przedsiębiorcy mają obowiązek przekazywać konsumentom przed zawarciem umowy. Reguluje też szczególne wymogi i zasady dotyczące umów zawieranych na odległość

[1] Zob. nowa ustawa z 12 maja 2011 r. o kredycie konsumenckim w zakresie formularza informacyjnego.
[2] Zob. http://ec.europa.eu/justice/consumer-marketing/rights-contracts/directive/index_en.htm

oraz poza lokalem przedsiębiorstwa. Ma ona na celu – analogicznie do regulacji z sektora telekomunikacyjnego – ochronę przed ukrytymi opłatami i kosztami, większą przejrzystość cen. Warto także podkreślić, że dyrektywa ta ma charakter horyzontalny, czyli państwa członkowskie zobowiązane są do przyjęcia jej wprost w całości. Propozycje zmiany dyrektywy o handlu elektronicznym (2000/31/WE, *E-commerce Directive*[3]) zmierzają w podobnym kierunku.

Podobnie jak znacząca większość osób wypowiadających się na wskazany temat, uważam, że proponowane zmiany w projekcie nowelizacji Prawa telekomunikacyjnego mające na celu ochronę użytkownika idą zbyt daleko i są czasami wewnętrznie sprzeczne. Na przykład trudno, aby jeszcze bardziej rozbudowana umowa czy regulamin świadczenia usług telekomunikacyjnych były zarazem przejrzyste, czytelne i zrozumiałe. Na powyższe europejskie tendencje wskazuję jednak, aby nie tracić szerokiego spojrzenia na to zagadnienie. Prowadzi to też do pytania o przyszłe sprzeczności czy też powielanie się przepisów w zakresie obowiązków informacyjnych. Sytuacja taka może wystąpić, zwłaszcza gdy będzie możliwość zawierania online umów o świadczenie usług telekomunikacyjnych (drogą elektroniczną, za pomocą formularza dostępnego na stronie internetowej przedsiębiorcy).

Zawiadomienie o naruszeniu danych osobowych

Nowelizacja ma doprecyzować obowiązki przedsiębiorców telekomunikacyjnych w przypadku naruszenia bezpieczeństwa sieci. Użytkownicy mają być bardziej chronieni przed spamem i zagrożeniem ujawnienia czy wykorzystania ich danych osobowych. Zgodnie z art. 174a nowelizacji w przypadku naruszenia danych osobowych abonentów lub użytkowników końcowych będących osobami fizycznymi dostawca usług telekomunikacyjnych bez zbędnej zwłoki, nie później niż w terminie trzech dni od stwierdzenia naruszenia, powinien zawiadomić o tym fakcie Generalnego Inspektora Ochrony Danych Osobowych (GIODO).

Zgodnie z projektem naruszeniem danych osobowych jest takie naruszenie bezpieczeństwa, które prowadzi do przypadkowego lub bezprawnego zniszczenia, utraty, zmiany, nieuprawnionego ujawnienia lub dostępu do danych osobowych przetwarzanych przez przedsiębiorcę telekomunikacyjnego w związku ze świadczeniem usług telekomunikacyjnych. Jednakże, gdyby naruszenie to miało niekorzystny wpływ na dane osobowe lub prywatność abonenta lub użytkownika końcowego będącego osobą fizyczną, dostawca nie później niż w terminie trzech dni od naruszenia będzie miał obowiązek zawiadomić go o takim naruszeniu. Zawiadomienie to nie jest konieczne, gdy dostawca wykaże, iż wdrożył przewidziane przepisami o ochronie danych osobowych odpowiednie techniczne i organizacyjne środki ochrony, które uniemożliwiają odczytanie danych przez osoby nieuprawnione oraz że środki te zostały zastosowane do danych, których ochrona została naruszona.

Zawiadomienie powinno zawierać m.in. opis charakteru naruszenia danych osobowych oraz zakładane ryzyko związane z naruszeniem, a także opis skutków naruszenia danych. Wprowadzenie tych obowiązków wiąże się z koniecznością poniesienia ze strony dostawcy usług telekomunikacyjnych dodatkowych kosztów. Ponadto ciekawym zobowiązaniem jest konieczność wskazania proponowanych przez dostawcę środków naprawczych. Dostawca ma także prowadzić rejestr naruszeń danych osobowych.

Bezpieczeństwo i integralność sieci i usług telekomunikacyjnych

Dodany został również nowy dział dotyczący bezpieczeństwa i integralności sieci i usług telekomunikacyjnych oraz przekazu komunikatów. W celu ich zapewnienia dostawca usług telekomunikacyjnych zobowiązany będzie do zastosowania środków technicznych i organizacyjnych odpowiednich do stopnia ryzyka. Będzie on miał też obowiązek

> „Nowelizacja ma doprecyzować obowiązki przedsiębiorców telekomunikacyjnych w przypadku naruszenia bezpieczeństwa sieci. Użytkownicy mają być bardziej chronieni przed spamem i zagrożeniem ujawnienia czy wykorzystania ich danych osobowych.

Nowe przepisy mają lepiej chronić użytkowników, tym samym nakładają dodatkowe obowiązki na przedsiębiorców telekomunikacyjnych. Wskazuje się często, iż umowa o świadczenie usług telekomunikacyjnych i regulamin będą bardziej rozbudowane, a tym samym nieczytelne.

[3] Zob. http://ec.europa.eu/internal_market/e-commerce/communication_2012_en.htm

> Uważam, podobnie jak większość osób wypowiadających się na ten temat, że proponowane zmiany w projekcie nowelizacji Prawa telekomunikacyjnego mające na celu ochronę użytkownika idą zbyt daleko i są czasami wewnętrznie sprzeczne. Na przykład trudno, aby jeszcze bardziej rozbudowana umowa czy regulamin świadczenia usług telekomunikacyjnych były zarazem przejrzyste, czytelne i zrozumiałe.

Można zastanowić się, jak do powyższych zobowiązań w zakresie naruszenia danych oraz zapewnienia bezpieczeństwa i integralności sieci i usług telekomunikacyjnych ma się neutralność. Idealna koncepcja neutralności sieci oznacza, że informacje w Internecie powinny być przekazywane w sposób bezstronny bez względu na treść, miejsce przeznaczenia lub źródło, a użytkownicy powinni mieć możliwość decydowania, jakich aplikacji, usług i sprzętu chcą używać. Zdaniem EIOD coraz częstsze wykorzystywanie technik monitorowania i inspekcji przez dostawców usług internetowych narusza neutralność sieci oraz poufność komunikacji.

informowania użytkowników o wystąpieniu szczególnego ryzyka naruszenia bezpieczeństwa sieci. Ponadto powinien powiadomić Prezesa UKE o każdym istotnym naruszeniu bezpieczeństwa lub integralności sieci lub usług, a także o podjętych działaniach i środkach naprawczych. Dodatkowo przedsiębiorcy telekomunikacyjni, zgodnie z projektem nowelizacji, mają publikować na swoich stronach internetowych aktualne informacje m.in. o potencjalnych zagrożeniach związanych z korzystaniem przez abonentów z usług telekomunikacyjnych czy rekomendowanych środkach ostrożności i najbardziej popularnych sposobach zabezpieczania telekomunikacyjnych urządzeń końcowych przed oprogramowaniem złośliwym lub szpiegującym.

Neutralność sieci

Można zastanowić się również, jak do powyższych zobowiązań w zakresie naruszenia danych oraz zapewnienia bezpieczeństwa i integralności sieci i usług telekomunikacyjnych ma się neutralność. Idealna koncepcja neutralności sieci oznacza, że informacje w Internecie powinny być przekazywane w sposób bezstronny bez względu na treść, miejsce przeznaczenia lub źródło, a użytkownicy powinni mieć możliwość decydowania, jakich aplikacji, usług i sprzętu chcą używać. Komisja Europejska opublikowała 8 lutego br. stanowisko Europejskiego Inspektora Ochrony Danych (EIOD) w sprawie neutralności sieci, zarządzania ruchem oraz ochrony prywatności i danych osobowych (2012/C 34/01). Zdaniem EIOD coraz częstsze wykorzystywanie technik monitorowania i inspekcji przez dostawców usług internetowych narusza neutralność sieci oraz poufność komunikacji. Nasuwa to poważne pytania dotyczące ochrony prywatności i danych osobowych użytkowników.

Inspektor podkreśla nasilającą się tendencję do monitorowania ruchu w celu zapobiegania zagrożeniom oraz efektywnego wykorzystania infrastruktury. Oprócz zgody zainteresowanych użytkowników dyrektywa 2002/58/WE o prywatności i łączności elektronicznej wskazuje, iż podstawę dla przetwarzania danych o ruchu i komunikacji przez dostawców usług internetowych stanowi (1) świadczenie usługi; (2) zapewnienie bezpieczeństwa usługi oraz (3) minimalizacja zatorów. Legalne są zatem techniki inspekcji oparte na nagłówkach IP, monitorowanie i filtrowanie danych o komunikacji, które służą wyłącznie zapewnieniu bezpieczeństwa oferowanych przez dostawcę usług. EIOD uważa zatem, że aktualne ramy prawne zezwalają dostawcom usług internetowych na zarządzanie ruchem ze względu na wskazane wyżej potrzeby, czyli w celu zapobiegania zagrożeniom i zapewnienia efektywności sieci. Inne cele (przykładowo słuchanie, nagrywanie, przechowywanie lub inne rodzaje przejęcia komunikatu lub nadzoru nad nim i związanych z nim danych o ruchu) wymagają wyraźnej, świadomej i swobodnej zgody użytkowników na monitorowanie przez dostawców przesyłanych za ich pośrednictwem komunikatów.

W dyskusji nad neutralnością i nowymi obowiązkami dostawców usług telekomunikacyjnych należy zatem także uwzględnić fakt, iż wypełnianie obowiązków w zakresie bezpieczeństwa oraz integralności sieci i usług związane jest de facto z zarządzaniem ruchem. Obecnie ma to już miejsce, a dalsza dyskusja w tym zakresie powinna mieć na celu doprecyzowanie szczegółowych zasad oraz ustalenie wzajemnego oddziaływania, priorytetów poszczególnych pakietów zarządzanych w ramach ujednoliconej polityki. Z kolei wprowadzając nowe obowiązki informacyjne wobec konsumentów, warto mieć na uwadze również unikanie powielania się lub sprzeczności między nimi. Ewentualnie należałoby za pomocą odesłań odpowiednio rozgraniczyć te obowiązki. <<