

Czy klienci banków i sklepów internetowych mogą czuć się bezpiecznie?

Z Michałem Serzyckim, Generalnym Inspektorem Ochrony Danych Osobowych, rozmawia Katarzyna Supranowicz



– Jakie są regulacje prawne dotyczące ochrony danych osobowych?

Główne zasady dotyczące ochrony danych osobowych zawarte są w ustawie o Ochronie Danych Osobowych, która została uchwalona 29 sierpnia 1997 roku, a weszła w życie 30 kwietnia 1998 roku. Teraz obchodzimy dziesięciolecie obowiązywania ustawy. Niniejsza ustawa określa jedynie ogólne zasady przetwarzania danych osobowych, natomiast sprecyzowanie ich znajduje się w szczególnych wobec ustawy o ochronie danych osobowych przepisach prawa, np. w prawie bankowym czy telekomunikacyjnym. O ile więc te przepisy – nazwijmy je branżowe – regulują kwestie związane z przetwarzaniem danych osobowych, to należy je stosować, gdyż ustawa wprost do nich odsyła.

– Od tamtego czasu wiele się zmieniło w gospodarce, firmy inaczej funkcjonują, rozwinęła się ban-

kowość internetowa. Czy w związku z tym istnieje potrzeba nowelizacji ustawy?

Ustawa była wielokrotnie nowelizowana, m. in. ze względu na konieczność dostosowania jej przepisów do Dyrektywy 95/46 WE. Organy UE cały czas kontrolują, czy ustawy w poszczególnych krajach UE są w pełni spójne z tą dyrektywą. Jest ona najważniejszym europejskim aktem dotyczącym ochrony danych osobowych i Polska ustawa jest z nią zgodna. Do najnowszych projektu nowelizacji ustawy GODO zgłosił uwagi będące wynikiem dziesięcioletnich doświadczeń. Wprowadzane aktualnie zmiany ustawy mają na celu zagwarantowanie skuteczniejszej niż dotychczas ochrony danych osobowych. Podstawowym celem

projektu ustawy jest przyjęcie rozwiązań stosowania finansowych sankcji karnych wobec podmiotów naruszających przepisy ustawy. Według proponowanych zmian, za niewykonanie decyzji wydanych przez Generalnego Inspektora Ochrony Danych Osobowych, nakładane będą kary na osoby i instytucje, które w jakikolwiek sposób utrudniają działanie inspektorów GODO.

– W jaki sposób funkcjonuje system kontroli GODO i jakiego rodzaju kary są nakładane? Czy ich wysokość jest wspólna dla UE?

Każde państwo ustala własne wysokości kar i są one bardzo zróżnicowane. Ciekawym przykładem jest Hiszpania. Pieniądże na funkcjonowanie mojego hiszpańskiego odpowiednika i jego Biura pochodzą z kar, pozyskiwanych od podmiotów naruszających prawo do ochrony danych osobowych.

W Polsce, zgodnie z aktualnymi przepisami ustawy o ochronie danych osobowych, konsekwencją naruszenia jej przepisów jest kara grzywny, ograniczenia bądź pozbawienia wolności. Natomiast GODO nie ma prawa nakładania na podmioty naruszające przepisy ustawy o ochronie danych osobowych kar pieniężnych, ale będzie miał takie prawo nakładania kar pieniężnych w przypadku uchylenia proponowanych w niej zmian.

– Jakie organy sprawują kontrolę nad firmami i instytucjami w kwestii ochrony danych osobowych i jakimi narzędziami się posługują?

Jedynym ustawowym organem, który sprawuje nadzór nad zgodnym z prawem przetwarzaniem danych osobowych, jest GODO. Kontrolę sprawuje poprzez wykorzystywanie do tego celu wszelkich przewidzianych w ustawie środków, m.in. wydając decyzje administracyjne i rozpatruje skargi, prowadzi rejestry zbiorów danych osobowych, opiniuje projekty ustaw i rozporządzeń dotyczących ochrony danych osobowych oraz kontroluje zgodność przetwarzania danych z obowiązującymi przepisami. Kontrole u administratorów danych są wykonywane przez wyznaczonych do tego inspektorów. Protokół kontroli wraz z zawartymi w nim wnioskami pokontrolnymi, kierowany jest do podmiotu kontrolowanego, który ma czas na ustosunkowanie się do zawartych w dokumentach pokontrolnych – wskazanych przez inspektorów – wszystkich uchybień.

– W 2002 roku miał miejsce ogromny wyciek danych osobowych z serwisu aukcyjnego Allegro.pl, a w lutym bieżącego roku z serwisu KupBilet.pl. Jakie działania podjął GODO w tych sprawach i jakie są ich konsekwencje?

W związku z wyciekiem danych polegającym na tym, że wszystkie dane użytkowników portalu Allegro.pl były ogólnodostępne i tym samym zostały naruszone przepisy dotyczące bezpieczeństwa danych, GODO przeprowadził kontrolę. W związku ze stwierdzonymi w trakcie trwania postępowania kontrolnego nieprawidłowościami, Allegro.pl zostało zobowiązane do usunięcia uchybień. GODO w decyzji nakazał zastosowanie dodatkowych zabezpieczeń, m. in. poprzez wprowadzenie tzw. protokołu SSL, czyli systemu szyfrowania danych kodującego informację wpisywaną przez użytkowników Internetu.

Natomiast sprawa wycieku danych kibiców korzystających z portalu KupBilet.pl jest przedmiotem postępowania GODO i z końcem maja spodziewamy się jej zakończenia. W chwili obecnej czekamy na ustosunkowanie się strony do zarzutów zawartych w protokole pokontrolnym. Należy podkreślić, iż w obu przypadkach zawiódł system, a nie człowiek, tak jak w przypadku ostatniej czarnej serii wycieków danych które miały miejsce w Wielkiej Brytanii.

– Czy adres mailowy i hasło do poczty mailowej to dane osobowe? Od którego momentu możemy mówić o danych osobowych?

W świetle definicji zawartej w ustawie jest to bardzo trudne do stwierdzenia. Mówi ona bowiem, że w rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Zaś osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Zatem IP komputera w kafecie internetowej nie może stać się daną osobową w odróżnieniu od IP komputera np. w urzędzie, gdzie wiadomo, że korzysta z niego jedna konkretna osoba. Podobnie dzieje się z nazwiskiem – jeżeli posłużymy się nim w miejscu, gdzie duża liczba obywateli nosi to samo nazwisko, nie posłuży ono do identyfikacji konkret-

nej osoby, tym samym nie stanie się daną osobową. Internet jest z pewnością dobrodziejstwem, ale również szczególnym miejscem, w którym osoby niepożądane mają, przy braku odpowiednich zabezpieczeń, możliwość skojarzenia i połączenia informacji, np. adresu mailowego, hasła, numeru konta bankowego czy loginu tworząc w ten sposób profil osoby, który następnie może być wykorzystany w nieodpowiedni i niekorzystny dla niej sposób.

– Czy klienci sklepów, banków internetowych, użytkownicy aukcji mają prawo żądać dowodów i dokumentów potwierdzających właściwe zarządzanie ich danymi osobowymi?

Przepisy prawa jasno i wyraźnie wymagają zgody na zbieranie i wykorzystywanie danych osobowych, oraz podania informacji do jakiego celu i przez jakie instytucje będą wykorzystywane dane osób których dotyczą. Ustawa również gwarantuje dostęp do danych przetwarzanych przez administratorów danych. Natomiast w przypadku zbierania danych osobowych nie od osoby której dane dotyczą, administrator danych jest zobowiązany poinformować ją od kogo pozyskał dane, w jakim celu i zakresie będzie je wykorzystywał oraz o prawie żądania zaprzestania a także sprzeciwu wobec przetwarzania jej danych osobowych. Takie prawo daje nam art. 24 i 25 ustawy. Ponadto, każdej osobie przysługuje prawo do kontroli przetwarzania jej danych osobowych u administratora danych, jak również raz na pół roku prawo do uzyskania informacji o jej danych osobowych przetwarzanych w zbiorze.

– Skąd Generalny Inspektor otrzymuje informacje o nadużyciach? Częściej są to efekty kontroli czy informacje wpływające do Biura z zewnątrz?

Najwięcej takich informacji wynika z kierowanych do GODO skarg. Reagujemy na wszystkie sygnały świadczące o naruszeniu przepisów ustawy o ochronie danych osobowych i szczegółowo je badamy. Również pomagają nam w tym media, dzięki którym możemy błyskawicznie zareagować na nieprawidłowości

i wysłać kontrolę do instytucji w której one wystąpiły.

– Jak długo trwa postępowanie w takich sprawach?

Zgodnie z przepisami ustawy, postępowanie prowadzi się według kodeksu postępowania administracyjnego. Często długość postępowania nie zależy tylko od nas, ale od strony, która często nie dochowuje ustawowych terminów. Biorąc także pod uwagę zawilość niektórych spraw, prowadzone przez biuro postępowania przedłużają się.

– W jakiej branży zanotowano najwięcej uchybień?

Przez pierwszych kilka lat obowiązywania ustawy najwięcej problemów przysparzały nam firmy zajmujące się marketingiem bezpośrednim. Od ponad dwóch lat sytuacja uległa zdecydowanej poprawie. Dodatkowo, na lepsze poszanowanie prawa do ochrony danych osobowych przez firmy marketingowe wpłynęło porozumienie pomiędzy GODO a Stowarzyszeniem Marketingu Bezpośredniego. Ostatnio pojawił się z kolei poważny problem telemarketingu, czyli nękania abonentów telefonami z ofertami zakupu produktów i usług. W tej sytuacji, jeżeli dane zostały pozyskane poprzez zakup całej bazy, to jest to zgodne z prawem. Wówczas potencjalny klient powinien zostać o ty poinformowany i ma prawo wglądu do tych danych. Może również nie wyrazić zgody na oferowanie kolejnych towarów czy usług. Problem zaczyna się w sytuacji, gdy dane do celów marketingowych zbierane są z ogólnie dostępnych zbiorów, czyli np. z książek telefonicznych. Jeżeli numer telefonu znajduje się w książce telefonicznej i nie został zastrzeżony, to każda firma, zgodnie z prawem, może z tego numeru korzystać i oferować swoje usługi. Firm działających na zasadzie telemarketingu obecnie jest na tyle dużo, że nawet jeśli ktoś odmówi współpracy z jedną firmą, to za chwilę może zadzwonić przedstawiciel kolejnej firmy. Jesteśmy świadomi wagi problemu i przygotowani do zajęcia się nim i jednocześnie mamy świadomość, że będziemy musieli poprosić o pomoc również inne urzędy.