

Law in Brief



W kolejnym cyklu „Nieznajomość prawa szkodzi” podejmujemy problematykę przetwarzania danych osobowych w aplikacjach mobilnych. O tym, jak powinny wyglądać zapisy w polityce prywatności aplikacji czy serwisu internetowego, opowiada Generalny Inspektor Ochrony Danych Osobowych. Zwracamy również uwagę na nowe prawo konsumenckie, którego zmiana ma istotne znaczenie dla branży e-commerce. Zmiany prawa przybliży ekspert IP i e-commerce.

Paweł A. Kozyra
Dyrektor komunikacji
Comarch SA
Pawel.Kozyra@Comarch.pl



Twórcy aplikacji i dane osobowe

Rozmowa z Generalnym Inspektorem Ochrony Danych Osobowych, dr. Wojciechem Rafałem Wiewiórowskim.

Paweł A. Kozyra: *Atrakcyjne dla użytkownika funkcjonalności aplikacji to nie wszystko. O czym powinien pamiętać jej twórca, by spełniała wymogi prawne?*

dr Wojciech Rafał Wiewiórowski: Bezdyskusyjna jest transparentność przetwarzania danych osobowych. Osoba korzystająca z danego rozwiązania powinna, dzięki precyzyjnej informacji, mieć świadomość, a w konsekwencji zdać sobie sprawę, jakie jej dane i w jaki sposób będą wykorzystywane. GODO sugeruje, by ustawienia domyślne danej aplikacji, w sposób jak najdalej idący, chroniły prywatność osób. A każda inna do-

datkowa grupa danych, która jest pozyskiwana przez aplikację, wymagała dodatkowej zgody ze strony osoby z niej korzystającej. Niestety, algorytmy większości aplikacji są tworzone w ten sposób, że gromadzone są zarówno dane, które są niezbędne do działania takiej aplikacji, jak również te dane, które mogą być przydatne twórcom czy zarządzającemu aplikacją. Kolejna kwestia to poinformowanie, kto będzie miał dostęp do danych. Użytkownik czy twórca? Może to być również podmiot współpracujący z twórcą aplikacji, np. oferujący system operacyjny, na którym działa aplikacja.

PK: *Możemy także korzystać ze stworzonych przez organy ochrony danych lub przez organizacje pozarządowe podręczników zawierających precyzyjne wskazówki, jak postępować w tej materii.*

WW: Ogromna rola spoczywa też na GODO. Jednak skuteczność działań zależy przede wszystkim od współpracy z organizacjami środowiskowymi, w przypadku aplikacji – z ich deweloperami. Przełożenie regulacji napisanych językiem prawnym na język zrozumiały dla danej grupy zawodowej czy osób zainteresowanych tematem jest możliwe dzięki ścisłej współpracy z reprezentantami tego środowiska: izbami handlowymi, stowarzyszeniami zawodowymi czy start-upami. Podczas VIII Europejskiego Dnia Ochrony Danych Osobowych dyskutowaliśmy o edukacji cyfrowej rozumianej jako lifelong learning, czyli uczenie się przez całe życie, które powinno odnosić się do wszystkich etapów życia i ról, które pełni w społeczeństwie, a nie tylko edukacji szkolnej.

PK: *Czy istnieje system certyfikacji legalizujący, uwiarygadniający daną aplikację i potwierdzający jej zgodność z wymaganiami z zakresu ochrony danych osobowych?*

WW: Zdajemy sobie sprawę, że należy ten proces uregulować. Obecnie analizujemy praktyki innych krajów Unii Europejskiej w tej materii. W niektórych państwach uwiarygodnienia dokonuje sam rynek poprzez



dr Wojciech Rafał Wiewiórowski
Generalny Inspektor
Ochrony Danych
Osobowych

organizacje branżowe wspierane przez odpowiedników GODO w danym kraju. Mniej skomplikowanym rozwiązaniem jest system samocertyfikacji. Twórca aplikacji sam stwierdza, że przyjmuje pewne wymagania na siebie i wyraża zgodę na poddanie się kontroli organów ochrony danych, które mogą sprawdzić, czy spełnił wymagania w tym zakresie.

PK: *Jak powinny wyglądać zapisy w polityce prywatności aplikacji czy serwisu internetowego, w których zostaną uregulowane kwestie przetwarzania danych osobowych?*

WW: Z treści zgody na przetwarzanie danych osobowych powinno w sposób niebudzący wątpliwości wynikać, w jakim celu, w jakim zakresie i przez kogo dane osobowe będą przetwarzane. Wyrażający zgodę musi mieć pełną świadomość tego, na co się godzi. Zgoda może być odwołana w każdym czasie. Można też dodać, że ewentualne wątpliwości należy zgłaszać do GODO.

PK: *Jakie warunki prawne muszą spełnić polscy twórcy aplikacji internetowych, które zbierają dane o korzystających z nich użytkownikach (np. wymuszając konieczność udostępnienia listy znajomych, treści SMS-ów)?*

WW: Należy rozróżnić dwie sytuacje. Pierwsza dotyczy instytucji publicznych. One prowadząc działania w mediach społecznościowych, czy udostępniając aplikacje, nie mogą wymagać od użytkownika żadnych innych danych, które nie są konieczne do wykonania zadania publicznego w ich obszarze. Gwarantuje nam to Konstytucja RP. W art. 7 istnieje nakaz, by organy władzy publicznej działały tylko na podstawie i w granicach prawa. W art. 51 natomiast czytamy, że nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawa. Druga sytuacja dotyczy podmiotów prywatnych. Każdy, kto korzysta ze świadczonych przez nie usług, sam decyduje o przekazaniu informacji na swój temat. Oczywiście wcześniej musi zostać prawidłowo poinformowany o zakresie i celu przetwarzania danych. I jeśli się na to godzi, wtedy ponosi wszelkie konsekwencje swojej decyzji, również tej nietrafnej.

PK: *Użytkownik, rejestrując swój profil na Facebooku, zmuszony jest zaakceptować regulamin (umowa adhezyjna przez przystąpienie) lub zrezygnować z korzystania z takiego serwisu. Jakie jest prawo właściwe do rozpatrywania sporów, czynów niedozwolonych czy kwestii danych osobowych w serwisach społecznościowych?*

WW: Przy korzystaniu z serwisów internetowych możemy mieć do czynienia zarówno z kwestiami dotyczącymi ochrony danych osobowych, jak i zagadnieniami związanymi z ochroną praw konsumenckich. Klasyczne spory konsumenckie są rozpatrywane przez sądy polskie. Jeżeli chodzi o ochronę danych osobowych, to Unia Europejska od dawna stoi na stanowisku, że w przypadku serwisów internetowych kierujących swoje usługi do osób z terytorium UE i działających na terytorium UE ewentualne spory powinny być rozstrzygane na podstawie prawa unijnego w sądach na obszarze UE. To nie oznacza, że zawsze będą rozpatrywane w kraju zamieszkania osoby. Najwięksi dostawcy usług internetowych zazwyczaj mają swoje przedstawicielstwa na terenie UE, przede wszystkim w Irlandii i Wielkiej Brytanii, ale mają też swoje oddziały krajowe, jak np. Google, który ma oddział w Polsce. Oddziały te mają jednak swoje specjalizacje. Istotne jest więc to, gdzie ma siedzibę administrator serwisu i gdzie zlokalizowane są urządzenia służące do pozyskiwania danych. Jako przykład podam przypadek firmy Google, której polski oddział nie obsługuje zagadnień prawnych związanych z ochroną danych i tym samym z zasady Google podlega właściwości irlandzkiego odpowiednika GODO. Tym niemniej w jednym przypadku usługa Google poddana była kontroli GODO. To sytuacja pozyskiwania danych osobo-

wych na potrzeby projektu Street View – niektóre elementy infrastruktury Google, np. samochody wyposażone w rejestratory obrazów, były bowiem zlokalizowane na terytorium Polski i tu bezpośrednio przetwarzały dane.

PK: *Czy prawo ma szansę lub powinno nadążyć za ekspansją nowych technologii?*

WW: Prawo nigdy nie będzie nadążało za rozwojem nowoczesnych technologii. Kiedy legislator próbował przewidzieć rozwój technologiczny, z reguły kończyło się to katastrofą. Tak było z dyrektywą oraz polską ustawą o podpisie elektronicznym. Próbowano w tych aktach przewidzieć kwestie rozwoju identyfikacji elektronicznej. Wymyślono rozwiązanie, które z punktu widzenia technicznego i prawnego było dobre, ale rynek nie chciał się rozwijać w tę stronę. To, że ustawodawca zawsze będzie gonił rozwijającą się czy uciekającą do przodu technologię, jest oczywiste. Zjawisko to będzie występowało zawsze. Jednak ważne jest, by monitorować, czy podstawowe zasady, które dotyczą choćby ochrony danych osobowych, są w tych nowych rozwiązaniach technologicznych stosowane. Trzeba też starać się, by przepisy nadążały za rozwojem technologicznym tam, gdzie jest to konieczne. Nie może to jednak polegać na dopasowaniu rozwiązań prawnych do konkretnych technologii czy do konkretnego modelu biznesowego, które w danym momencie istnieją na rynku. Nie wyobrażam sobie, byśmy tworzyli teraz prawo dotyczące cloud computingu, czyli przetwarzania danych w chmurze. Prawdopodobnie gdyby je stworzono, na rynku funkcjonowałyby już nowe rozwiązanie, które wymagałoby stworzenia innych reguł prawnych. W tym kontekście warto zaznaczyć, że przed nami kolejna wielka rewolucja – Internet przedmiotów. Na razie nie ma w tym zakresie regulacji prawnych. Niemniej prowadzony jest monitoring w tym zakresie, tak byśmy mogli wkroczyć w odpowiednim momencie, w którym będzie to niezbędne.

W jakim kraju należy dochodzić swoich praw, jeśli ich złamanie dopuścił się portal społecznościowy?

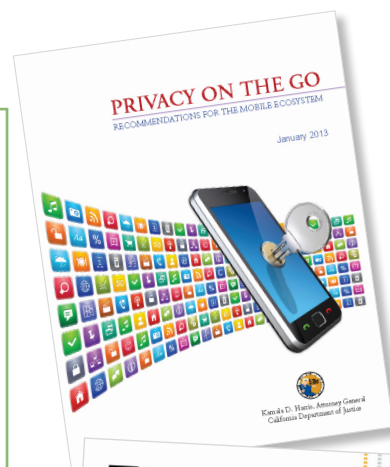


Pinterest: nie ustanowił swojego przedstawiciela w UE ze względu na toczący się spór o nazwę

Vimeo i Identi.ca: nie mają europejskiego przedstawiciela

Dobre praktyki, czyli jak tworzyć aplikacje, by były zgodne z prawem ochrony danych osobowych?

- » Opinia 02/2013 (WP 202) w sprawie aplikacji na urządzenia inteligentne przyjęta 27 lutego 2013 r. przez Grupę Roboczą Art. 29 zrzeszającą organy ochrony danych osobowych z państw członkowskich Unii Europejskiej;
- » „Privacy in mobile apps. Guidance for app developers” brytyjskiego organu ochrony danych (XII.2013 r.);
- » „Privacy On The Go. Recommendations For The Mobile Ecosystem” prokuratora generalnego Kalifornii (I.2013 r.);
- » „Best Practices for Mobile Application Developers” przygotowane przez Future of Privacy Forum oraz Center for Democracy & Technology;
- » „Mobile and Privacy. Privacy Design Guidelines for Mobile Application Development” przygotowane przez GSMA (2012 r.);
- » „Mobile privacy. A better practice guide for mobile app developers” przygotowane przez australijski organ ochrony danych (IX.2013 r.);
- » „Marketing Your Mobile App: Get It Right from the Start” opublikowane przez amerykańską Federalną Komisję Handlu (2012 r.);
- » „Une occasion à saisir : Développer des applis mobiles dans le respect du droit à la vie privée” przygotowane przez kanadyjskich rzeczników ochrony prywatności (2012 r.).



Prawne wyzwania e-commerce

Rozmowa z Tomaszem Zalewskim, radcą prawnym, managerem praktyki IP i e-commerce, partnerem w kancelarii Wierzbowski Eversheds.

Paweł A. Kozyra: *W połowie roku czekają nas zmiany w zakresie prawa ochrony konsumentów, które istotnie wpłyną m.in. na działalność sklepów internetowych.*

Tomasz Zalewski: Dotyczy to głównie sprzedaży na odległość i związanych z tym obowiązków przedsiębiorców. Zmiany te będą pociągały za sobą konieczność dostosowania do nowych wymogów stron internetowych oraz regulaminów. Niektórzy będą zmuszeni renegotjować umowy ze swoimi dostawcami usług. Ponieważ te zmiany stanowią pierwsze od wielu lat tak poważne wyzwanie dla przedsiębiorców, w szczególności tych prowadzących sklepy internetowe, powinni oni jak najszybciej przeanalizować zasady swojej działalności i pomyśleć nad wprowadzeniem koniecznych zmian, których wbrew pozorom będzie całkiem sporo.

Tomasz Zalewski
radca prawny



WIERZBOWSKI EVERSHEADS

PK: *Nowe przepisy mają być pozbawione niezrozumiałego dla konsumenta języka prawniczego.*

TZ: W przepisach pojawia się wymóg, aby informacje udzielane konsumentowi były „czytelne i wyrażone prostym językiem”. Klauzule napisane w sposób trudny do zrozumienia dla laika typu „z zastrzeżeniem powszechnie obowiązujących przepisów prawa” przejdą do przeszłości. Zmianie ulegnie zakres informacji przedkontraktowej udzielanej konsumentowi. Rozszerzeniu z 11 do 21 rodzajów ulegnie katalog informacji przekazywanych konsumentowi, pojawi się m.in. informacja o kosztach zwrotu rzeczy w przypadku odstąpienia od umowy, które ponosi konsument.

PK: *Wydłużeniu ulegnie termin odstąpienia od umowy.*

TZ: Termin na wykonanie prawa konsumenta do odstąpienia od umowy zmieni się z 10 na 14 dni. Konsument, który będzie chciał skorzystać z takiego prawa, będzie mógł złożyć oświadczenie na gotowym formularzu. Przedsiębiorca obowiązany będzie (w terminie 14 dni) zwrócić konsumentowi wszystkie dokonane przez niego płatności, w tym koszty dostarczenia. Sprzedawca będzie zobowiązany zwrócić tylko równowartość najtańszego, standardowego sposobu dostawy. Należy pamiętać o konieczności poinformowania konsumenta o kosztach zwrotu rzeczy – w przeciwnym wypadku ponosi je przedsiębiorca.

PK: *Nowe regulacje to fundamentalne zmiany zasad odpowiedzialności za wady sprzedanej rzeczy.*

TZ: Zmiany te należy ocenić jako znacznie ułatwiające obrót i upraszczające stan prawny, który obecnie przewiduje dwa odrębnie uregulowane reżimy odpowiedzialności za wady rzeczy: odpowiedzialność kodeksową na zasadzie rękojmi i gwarancji oraz odpowiedzialność za niezgodność towaru z umową (na podstawie ustawy o sprzedaży konsumenckiej). Wprowadzone zmiany będą ważne zatem dla praktycznie wszystkich uczestników obrotu, w tym obrotu profesjonalnego (zwłaszcza że przepisy kodeksu cywilnego o rękojmi i gwarancji stosuje się i stosować się będzie nadal odpowiednio do umowy o dzieło i do umowy o roboty budowlane). Wszyscy będą musieli zweryfikować wzory stosowanych umów w zakresie odpowiedzialności za wady, nawet jeśli nie zawierają umów z konsumentami.