



Ochrona danych osobowych w UE



Źródło: <http://ec.europa.eu/justice/data-protection/media/photos/data-protection.jpg>

Polska jest w strukturach Unii Europejskiej od 1 maja 2004. Od tego czasu winno się zwracać uwagę nie tylko na zmiany w prawie krajowym, lecz również na te zachodzące w prawie wspólnotowym. Jednym z ważniejszych aspektów prawa unijnego jest ochrona danych osobowych. Jak wygląda? Jakie są jej podstawy prawne? Na co należy zwrócić szczególną uwagę? Właśnie tym zagadnieniom będzie poświęcony poniższy biuletyn.

Polska ustawa o ochronie danych osobowych w artykule szóstym informuje, że za dane osobowe należy uważać:

- „1. (...) wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
2. 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, kulturowe lub społeczne.
3. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań¹”

Dane osobowe to najprościej mówiąc informacje o osobie fizycznej. Nie jest wyszczególnione co jest danymi osobowymi, a czego do nich się nie zalicza. Te mogą mieć

¹ Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r.



formę cyfrową, alfabetyczną, zdjęć, dźwięku, video czy też danych biometrycznych jak odciski palców albo obraz tęczówki².

Drugim, ważnym pojęciem, kluczowym w zrozumieniu omawianego tematu są „dane osobowe wrażliwe”. Dane te są objęte szczególną ochroną. Co do zasady przetwarzanie ich jest zabronione, lecz w szczególnych, określonych w unormowaniach prawnych przypadkach jest dozwolone. Takimi wrażliwymi danymi są na przykład: poglądy polityczne, pochodzenie rasowe, orientacja seksualna, informacje o nałogach czy przynależność do organizacji religijnych³.

Jak są chronione dane osobowe w Unii Europejskiej

Gwarantem poszanowania danych osobowych we Wspólnocie są następujące akty prawne:

- Traktat o funkcjonowaniu Unii Europejskiej, artykuł 16
- Karta Praw Podstawowych, artykuł 8
- Traktat o Unii Europejskiej, artykuł 39
- Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995

Te dokumenty w całości lub we wskazanych fragmentach odnoszą się do kwestii ochrony danych osobowych. Wskazują, że taka ochrona dotyczy każdego obywatela Unii Europejskiej oraz, iż zainteresowane osoby muszą wyrazić zgodę co do przetwarzania danych lub ich podania. Akty prawne jednocześnie informują, że nad przestrzeganiem wyżej wspomnianych uwarunkowań powinien stać niezależny organ. Za taki uważa się Europejskiego Inspektora Danych Osobowych.

Urząd Europejskiego Inspektora Ochrony Danych Osobowych istnieje od 2001. Jego głównym zadaniem jest dbanie o to, aby wszystkie instytucje i organy Unii Europejskiej szanowały prawo obywateli do prywatności przy przetwarzaniu danych osobowych. „Przetwarzanie danych” czyli między innymi zbieranie informacji, ich zapis, niszczenie lub przesyłanie.

Europejski Inspektor Ochrony Danych współpracuje z Urzędnikami do spraw Ochrony Danych we wszystkich instytucjach i organach Unii Europejskiej, a także z Generalnymi Inspektorami Ochrony Danych Osobowych w krajach członkowskich.

Każdy obywatel, który ma podstawy twierdzić, że jego prywatność została naruszona powinien zwrócić się najpierw do osób przetwarzających jego dane, dopiero gdy to nie wystarczy winien skontaktować się z Inspektorem Ochrony Danych. Ostatnim etapem, gdy

² paiz.gov.pl, *Podstawowe definicje i pojęcia związane z ochroną danych osobowych*, s.2

³ nik.gov.pl, *NIK o danych osobowych*, <http://www.nik.gov.pl/aktualnosci/nik-o-danych-osobowych-debata.html>



skarżący nie zgodzi się z wydaną opinią przez Inspektora jest wniesienie sprawy do Trybunału Sprawiedliwości⁴

Dyrektywa z 1995 w znaczącym stopniu rozwiązała kwestię ochrony danych osobowych. Na dzień dzisiejszy wspomniana dyrektywa jest jednak niewystarczająca i coraz bardziej archaiczna. Związane jest to głównie ze zmianami do jakich doszło na gruncie nowych technologii, a także z tym, że przepisy w państwach unijnych różnią się od siebie.

Dotychczasowa Dyrektywa narzucała jedynie wymagania odnośnie celowości, a państwa członkowskie same wprowadzały odpowiednie przepisy. Rodziło to różnice w implementowaniu i stosowaniu owej dyrektywy, a co za tym idzie - różny poziom ochrony danych w poszczególnych państwach członkowskich⁵.

W związku z powyższym przedstawiciele państw Unii Europejskiej postanowili zająć się tą kwestią i obecnie trwają prace nad reformą „prywatności” we Wspólnocie. Znaczący wkład we wprowadzanie zmian ma Viviane Reding, komisarz Unii Europejskiej do spraw sprawiedliwości, praw podstawowych i obywatelstwa. To właśnie komisarz podkreśla, iż „reforma ma pomóc w budowaniu zaufania do usług internetowych, ponieważ ludzie będą lepiej poinformowani o swoich prawach i będą mieli lepszą kontrolę nad swoimi danymi. Reforma pozwoli to osiągnąć ułatwiając jednocześnie życie przedsiębiorcom i ograniczając ich koszty.”⁶ Aktualnie toczą się debaty nad kształtem tej reformy.

Viviane Reding postuluje, iż:

1. „Reforma przepisów dotyczących ochrony danych osobowych musi znaleźć się w dzienniku ustaw. Chciałabym, żeby w 2014 r. prace nad kwestiami ochrony danych osobowych odbywały się na pełnych obrotach.”
2. „Reforma nie powinna zawierać rozróżnienia na sektor prywatny i państwowy. Obywatele mogliby po prostu nie zrozumieć takiego podziału w czasach, gdy sektor publiczny zbiera, porównuje, a czasem nawet sprzedaje dane osobowe. Poza tym takie rozróżnienie jest bardzo trudne w świetle tego, że samorząd terytorialny może nabyć przestrzeń do przechowywania danych na prywatnej chmurze”
3. „Przepisy określające zasady danych osobowych lub wpływające na prywatność wymagają publicznej debaty, ponieważ odnoszą się do swobód obywatelskich w Internecie”

⁴ europa.eu, Europejski inspektor ochrony danych, http://europa.eu/about-eu/institutions-bodies/edps/index_pl.htm

⁵ http://ec.europa.eu/polska/wroclaw/spotkania/2013/130131_widok_pl.htm

⁶ mac.gov.pl, Ochrona Danych Osobowych, <https://mac.gov.pl/wp-content/uploads/2013/05/Ochrona-danych-osobowych-broszura-informacyjna-MAC.pdf>



4. „Gromadzenie danych osobowych powinno mieć określony cel i być ograniczone w swoim zasięgu do tego, co jest proporcjonalne. Nie można akceptować nadzoru ogólnego nad danymi z zakresu łączności elektronicznej”
5. „Przepisy muszą być jasne i aktualne. Państwa członkowskie nie mogą polegać na przestarzałych przepisach, opracowanych w innej rzeczywistości technologicznej, tworząc zasady dotyczące nowoczesnych systemów nadzoru”
6. „Na kwestie bezpieczeństwa narodowego należy powoływać się z umiarem. Praktyka ta powinna być raczej wyjątkiem, a nie zasadą”
7. „Prawdziwy nadzór nie może mieć miejsca bez udziału organów wymiaru sprawiedliwości. Nadzór wykonawczy jest dobry. Nadzór parlamentarny jest niezbędny. Nadzór sądowy jest kluczowy”
8. „Wiadomość dla naszych przyjaciół w Stanach Zjednoczonych. Przepisy dotyczące ochrony danych osobowych powinny mieć zastosowanie bez względu na obywatelstwo danej osoby. Stosowanie różnych standardów wobec obywateli danego państwa i cudzoziemców nie ma uzasadnienia biorąc pod uwagę otwarty charakter Internetu⁷”

Jak pokazuje tych osiem punktów, główny nacisk kładzie się na kwestie związane z ujednoczeniem przepisów, zastosowaniem ich do przedsiębiorstw, które niekoniecznie mają swoją siedzibę na terenie Unii Europejskiej, lecz świadczą usługi dla obywateli Wspólnoty jak np. Facebook czy Twitter.

Dostęp do informacji o tym, jak przetwarzane są nasze dane osobowe ma być łatwiejszy, a odpowiedzialność wśród podmiotów, które przetwarzają dane ma znacznie wzrosnąć oraz prawem każdego obywatela będzie możliwość wniesienia skargi o tym, że doszło do naruszenia przepisów rozporządzenia we własnym kraju niezależnie od tego w którym z krajów Unii Europejskiej jego dane są przetwarzane⁸.

Reforma unijnych przepisów dot. ochrony danych osobowych

Prace nad reformą unijnych przepisów odnoszących się do ochrony danych osobowych z 1995 r. zostały zainicjowane 25 stycznia 2012 r., a ich koniec przewiduje się na wiosnę 2016 roku⁹.

Reforma przyniesie głęboką harmonizację prawa na poziomie wspólnotowym, ustanowi jednakowe standardy ochrony danych w całej Unii, wzmocni prawa jednostek w tym zakresie, wprowadzi na terenie UE spójny system egzekwowania przepisów dotyczących ochrony

⁷ europa.eu, *Dzień ochrony danych osobowych: Wiceprzewodnicząca Reding wzywa do opracowania nowego porozumienia w sprawie ochrony danych osobowych dla Europy*, http://europa.eu/rapid/press-release_IP-14-70_pl.htm

⁸ mac.gov.pl, *Ochrona Danych Osobowych*, <https://mac.gov.pl/wp-content/uploads/2013/05/Ochrona-danych-osobowych-broszura-informacyjna-MAC.pdf>

⁹ wiadomosci.ngo.pl, *Dzień Ochrony Danych Osobowych 2014: Potrzebne nowe porozumienie w UE*, <http://wiadomosci.ngo.pl/wiadomosci/957622.html>



danych osobowych, jak i wzmocni współpracę krajowych organów administracji w tej tematyce¹⁰.

Komisarz Reding zwróciła również uwagę na wspomniany wyżej problem związany z dyrektywą z 1995 roku - wprowadzenie w poszczególnych państwach członkowskich wielu, często bardzo różnych przepisów. Dlatego też nowe proponowane przepisy będą mieć formę rozporządzenia, czyli będą obowiązywać we wszystkich państwach członkowskich i nie będą pozostawiać miejsca na różne interpretacje.

„Chcemy mieć na naszym kontynencie jeden system i jednolite zasady, takie same dla wszystkich. Jest to niezbędne, aby w pełni wykorzystywać możliwości, jakie daje wspólny rynek, liczący 500 milionów konsumentów – podkreślała wiceprzewodnicząca KE. – Jeśli ludzie będą ufać, że ich dane są wykorzystywane zgodnie z przepisami, będą chcieli je przekazywać. Dzięki temu świat cyfrowy będzie mógł funkcjonować. Konieczne jest zapewnienie równowagi między biznesem i obywatelami, a debata, która się właśnie toczy, pozwoli ją uzyskać.”¹¹

Françoise Le Bail (dyrektorka ds. sprawiedliwości w Komisji Europejskiej) przedstawiła główne założenia projektu rozporządzenia:

1. Osoby fizyczne uzyskają łatwiejszy dostęp do własnych danych i będą mogły sprawniej przekazywać swoje dane osobowe od jednego usługodawcy do drugiego (prawo do przenoszenia danych);
2. „Prawo do bycia zapomnianym” pomoże ludziom lepiej zarządzać ryzykiem związanym z ochroną danych w internecie. Osoby fizyczne będą miały możliwość usunięcia swoich danych, jeżeli nie będzie istnieć uzasadniona podstawa do ich zachowania.
3. Nastąpi uproszczenie procesu przekazywania danych do krajów trzecich.

Pakiet dotyczący ochrony danych to ambitna inicjatywa, mająca na celu wprowadzenie podstawowego prawa jednostki do prywatności w błyskawicznie ewoluującym świecie technologii. Zawierać będzie szeroką gamę środków:

- Prawo bycia zapomnianym

Komisja Europejska proponuje, by każdy mógł złożyć wniosek o wykasowanie swoich danych osobistych, jeśli nie chce, by były dalej przetwarzane. Jednak część eurodeputowanych chce usunąć ten zapis, uznając go za niemożliwy do wprowadzenia.

- Wyrażna zgoda

¹⁰ http://ec.europa.eu/polska/wroclaw/spotkania/2013/130131_widok_pl.htm

¹¹ http://ec.europa.eu/polska/news/130513_reding_boni_debata_pl.htm



W propozycji KE zawarty jest przepis, według którego firma mogłaby przetwarzać prywatne dane osób tylko po uprzednim wyrażeniu przez nie wyrażonej zgody (może być cofnięta w każdym momencie). Sprawozdawca Jan Philipp Albrecht (Zieloni, Greens/EFA) chce, by Parlament zastrzegł, że zgoda obowiązuje jedynie w przypadku pierwotnego powodu gromadzenia danych.

- Profilowanie

To analizowanie i przewidywanie wydajności pracy, sytuacji ekonomicznej, lokalizacji, zdrowia, preferencji, niezawodności lub zachowania, bazujące na automatycznym przetwarzaniu danych osobowych. Poseł Albrecht proponuje, by było to możliwe tylko i wyłącznie za udzieleniem zgody, lub w wyjątkowych, prawnie określonych przypadkach.

- Pozostałe zagadnienia

Firmy i władze publiczne powinny w jasny sposób wytłumaczyć zasady, jakimi kierują się podczas ochrony zebranych danych, oraz przewidzieć funkcję inspektora ochrony danych, jeśli w przedsiębiorstwie pracuje więcej niż 250 osób (wg. propozycji Komisji). Albrecht uważa, że przepis ten powinien zostać zmieniony i inspektor powinien być obecny w firmach, które rocznie przetwarzają dane przynajmniej 500 osób. Według KE, za wszelkie naruszenia, przewidywane będą kary w wysokości do miliona euro, lub 2 proc. rocznego obrotu firmy.

Wiele kontrowersji budzi zaplanowane w dyrektywie – prawo do bycia zapomnianym. Viviane Reding wyjaśniła, że prawo europejskie, w tym klauzula dot. prawa do bycia zapomnianym, nie narusza prawa do informacji i osoby publiczne nie będą mogły domagać się usunięcia informacji prasowych na swój temat, powołując się na prawo do bycia zapomnianym.

Interes publiczny powinien, jej zdaniem, dominować również w relacjach posiadacza danych osobowych z przetwarzającymi ją instytucjami publicznymi, które w określonych sytuacjach, np. klęski żywiołowej, powinny móc przetwarzać dane osobowe w sposób uzasadniony interesem publicznym (akcja poszukiwawcza, działania związane z odbudową zniszczonego terenu itd.). Również poziom ochrony obywatela powinien być zróżnicowany w zależności od potencjalnego zagrożenia. Prywatność i dane osobowe powinny uzyskać wyższy stopień ochrony w relacjach z gigantami rynku internetowego.¹²

Celem jest przyjęcie nowych regulacji przed wiosennymi wyborami do PE w 2014 r.

Parlament Europejski pracując nad poważną reformą ochrony danych obywateli UE udostępnia porady jak być bezpieczniejszym online. Oto one:

1. Nie odpowiadaj, kiedy pytają

¹² http://ec.europa.eu/polska/news/130513_reding_boni_debata_pl.htm



To, że Cię pytają, nie znaczy, że musisz odpowiadać. Jeżeli zakładasz tylko konto mailowe, nie musisz mieć obszernego profilu. A jeśli przyłączasz się do portalu społecznościowego, możesz ograniczyć ilość informacji o sobie do minimum. Jeżeli musisz podać swój e-mail, a nie potrzebujesz odpowiedzi, zawsze możesz podać zmyślony adres.

2. „Ciasteczka” są najlepsze, kiedy możesz je zjeść

Upewnij się, że tylko te strony internetowe, które odwiedzasz, będą mogły zbierać informacje w formie plików cookies („ciasteczek”). W tym celu ustaw swoją przeglądarkę tak, aby odrzucała pliki cookies z innych źródeł. W ten sposób zmniejszysz ryzyko kradzieży informacji przez bezwzględnych hakerów, np. za pomocą nieprawdziwych reklam umieszczanych na odwiedzanych przez Ciebie stronach

3. Hasło to nie przepustka

Sprawdź, czy Twoje hasła chronią Twoje dane i czy nie są przepustką do Twoich danych osobowych. Nie używaj wszędzie tego samego hasła, nie podawaj jako hasła nazwy użytkownika stosowanej na innej stronie, hakerzy mogą to wychwycić. Używaj cyfr i liter (w tym wielkich) w kombinacjach, które nie są wyrazami słownikowym

4. Ty rozdajesz, inni sprzedają

Poszperaj trochę i przyjrzyj się profilom innych osób – to, co możesz przeczytać o nich, inni mogą przeczytać o Tobie. Zamieszczanie zdjęć też może być przyczyną kłopotów. Po wrzuceniu prywatnych zdjęć do sieci tracisz nad nimi kontrolę. Jesteś pewien, że chcesz podawać tyle informacji o sobie

5. Trzymaj swoje dane osobowe pod kluczem

Portale społecznościowe są żyłą złota dla łowców danych, więc nie ułatwaj im zadania i ustaw jak najwyższy poziom ochrony prywatności w swoim profilu. Podczas żywiołowej dyskusji może Ci się wymknąć więcej, niż byś chciał. Kontroluj więc, co piszesz, tak aby nie ujawniać swoich danych.

6. Zamknij jedne drzwi, zanim otworzysz następne

Pozostawanie zalogowanym na portalu społecznościowym lub na koncie bankowym to jak zostawianie otwartego samochodu: jesteś narażony na ataki hakerów. Unikaj ryzyka i wyloguj się, zanim zaczniesz buszować w sieci.

7. Kto się podczepił do twojej sieci?

Jeżeli korzystasz z sieci WiFi, upewnij się, czy nie wiesz pasażerów na gapę. Zabezpiecz swoją sieć solidnym hasłem albo włącz kodowanie WPA, które jest pewniejsze.

8. Bezpieczeństwo działa w obie strony

Starasz się, żeby Twój komputer był bezpieczny, zwracasz uwagę na informacje, które zamieszczasz online, ale co z tymi, którzy przechowują Twoje dane? Mogłeś ustawić na najwyższy poziom bezpieczeństwa, ale jeżeli jakaś strona nie jest w stanie bezpiecznie przechowywać Twoich danych, i tak jesteś narażony. Czy możesz ufać właścicielom stron i ich systemom bezpieczeństwa?

9. Ogranicz szkody



Zastanów się nad stosowaniem jednej metody płatności tylko do zakupów online. Ustaw niski limit kredytowy – jeżeli ktoś uzyska dostęp do Twojej karty, szkody będą mniejsze.¹³

10. Waga na drobny druk

Tak samo w sieci, jak i gdziekolwiek indziej: sprawdzaj, co podpisujesz. Przykładowo, niektóre umowy odnawiają się automatycznie i musisz je wcześniej wypowiedzieć, jeżeli nie chcesz, żeby Twoja karta kredytowa została ponownie obciążona.

Źródła:

Wymienione w przypisach

oraz

- <http://ec.europa.eu/justice/data-protection/minisite/>
- http://europa.eu/rapid/press-release_MEMO-14-60_en.htm
- <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:350:0060:0071:PL:PDF>
- http://ec.europa.eu/commission_2010-2014/reding/pdf/news/20131022-libe-data-protection_en.pdf
- http://ec.europa.eu/justice/data-protection/index_pl.htm
- http://ec.europa.eu/justice/newsroom/data-protection/news/120125_pl.htm
- <http://www.europarl.europa.eu/news/pl/news-room/content/20130719STO17438/html/Ochrona-danych-strze%C5%BC-swojej-prywatno%C5%9Bci>
- <http://www.europarl.europa.eu/news/pl/news-room/content/20130723STO17555/html/Ochrona-danych-kluczowe-zagadnienia>
- <http://www.europarl.europa.eu/news/pl/news-room/content/20120120STO35905/html/Jak-chroni%C4%87-nasz%C4%85-prywatno%C5%9B%C4%87-w-internecie>
- Odzyskaj kontrolę nad swoimi danymi osobowymi, KE 2012

Przygotował:

Punkt Informacji Europejskiej

Europe Direct – Poznań

przy Wielkopolskiej Izbie Rzemieślniczej w Poznaniu

al. Niepodległości 2, 61-874 Poznań

tel. 61 8521670

e-mail: europedirect-poznan@irpoznan.com.pl, www.europe-direct.poznan.pl

Projekt współfinansowany ze środków Komisji Europejskiej



¹³ <http://www.europarl.europa.eu/news/pl/news-room/content/20131003STO21413/html/Jak-chroni%C4%87-swoj%C4%85-prywatno%C5%9B%C4%87-w-sieci>