REKOMENDACJA R (1999) 5

KOMITETU MINISTRÓW DLA PAŃSTW CZŁONKOWSKICH

W SPRAWIE OCHRONY PRYWATNOŚCI W INTERNECIE

WYTYCZNE W SPRAWIE OCHRONY OSÓB W ZAKRESIE GROMADZENIA I PRZETWARZANIA DANYCH OSOBOWYCH NA „INFOSTRADACH"

(przyjęta przez Komitet Ministrów 23 lutego1999 r. w czasie 660 spotkania Ministrów Delegatów)

Preambuła

Komitet Ministrów, na mocy artykułu 15.b Statutu Rady Europy,

Zważywszy, że celem Rady Europy jest urzeczywistnienie jak najściślejszego związku między jej Państwami Członkowskimi;

Zauważając rozwój nowych technologii i nowych usług komunikacji i informacji on line;

Świadomy faktu, że rozwój ten będzie znacząco wpływał na funkcjonowanie całości społeczeństwa oraz na stosunki międzyludzkie, w szczególności poprzez zwiększenie możliwości komunikowania się i wymiany informacji na poziomie krajowym i międzynarodowym;

Świadomy korzyści, jakie ten rozwój przynosi użytkownikom nowych technologii;

Uznając jednak, że rozwój technologii i rozpowszechnienie gromadzenia i przetwarzania danych osobowych w „infostradach" niosą ze sobą zagrożenie dla prywatności osób;

Uznając, że rozwój technologii umożliwia również przyczynienie się do poszanowania praw i podstawowych wolności, w szczególności prawa do prywatności, przy przetwarzaniu danych osobowych dotyczących osób fizycznych;

Świadomy konieczności rozwoju technik gwarantujących anonimowość osób, których dane dotyczą i poufność informacji wymienianych za pośrednictwem „infostrad", z poszanowaniem praw i wolności innych osób oraz wartości społeczeństwa demokratycznego;

Świadomy faktu, że komunikacja z użyciem nowych technologii informacji również podlega zasadom poszanowania praw człowieka i podstawowych wolności, w szczególności poszanowania prywatności i tajemnicy korespondencji, tak jak to gwarantuje artykuł 8 Europejskiej Konwencji Praw Człowieka;

Uznając, że gromadzenie, przetwarzanie, a szczególnie udostępnianie danych osobowych z użyciem nowych technologii informacji, zwłaszcza "infostrad", podlegają postanowieniom Konwencji o ochronie osób w zakresie zautomatyzowanego przetwarzania danych osobowych (Strasbourg, 1981, Seria traktatów europejskich nr 108) oraz rekomendacjom sektorowym

dotyczącym ochrony danych, w szczególności Rekomendacji Nr R (90) 19 w sprawie ochrony danych osobowych używanych dla celów związanych z płatnościami i innymi powiązanymi operacjami, Rekomendacji Nr R (91) 10 w sprawie udostępniania osobom trzecim danych osobowych będących w posiadaniu instytucji publicznych oraz Rekomendacji Nr R (95) 4 w sprawie ochrony danych osobowych w dziedzinie telekomunikacji, ze szczególnym uwzględnieniem usług telefonicznych;

Uznając, że należy uczulić użytkowników i dostawców usług internetowych w sprawie wdrożenia ogólnych postanowień wyżej wymienionej konwencji w odniesieniu do gromadzenia i przetwarzania danych osobowych na „infostradach";

Zaleca rządom Państw Członkowskich szerokie rozpowszechnienie wytycznych zawartych w załączniku do niniejszej rekomendacji, zwłaszcza wśród użytkowników i dostawców usług internetowych, jak również wśród wszystkich krajowych organów powołanych do czuwania nad przestrzeganiem przepisów o ochronie danych.

Załącznik do Rekomendacji R (99) 5 Komitetu Ministrów

dla Państw Członkowskich w sprawie ochrony prywatności w Internecie

Wytyczne w sprawie ochrony osób w zakresie gromadzenia i przetwarzania danych osobowych na "infostradach", które mogą być włączone lub dołączone do kodeksów postępowania

I. Wstęp

Niniejsze wytyczne zawierają zasady uczciwego postępowania, jakie powinny być przestrzegane w kwestii ochrony prywatności przez użytkowników i dostawców usług internetowych[1]. Zasady te mogą być zawarte w kodeksach postępowania.

Użytkownicy powinni być świadomi odpowiedzialności dostawców usług internetowych i odwrotnie. Jest więc zalecane, aby użytkownicy i dostawcy usług internetowych przeczytali ten tekst w całości, mimo, że jest on podzielony na kilka części tak, aby łatwiej było się nim posługiwać. Może Państwa dotyczyć jedna lub więcej części niniejszego tekstu.

Posługiwanie się Internetem wiąże się z odpowiedzialnością za każdą czynność i z zagrożeniem dla prywatności. Ważne jest, aby postępować w taki sposób, aby być bezpiecznym i utrzymywać dobre stosunki z innymi ludźmi. Niniejsze wytyczne zawierają kilka praktycznych wskazówek dotyczących ochrony prywatności, ale nie zwalniają z konieczności zapoznania się z obowiązującymi Państwa prawami i obowiązkami.

Należy pamiętać, że poszanowanie prywatności jest podstawowym prawem każdej istoty ludzkiej, która może być również chroniona przepisami o ochronie danych. A więc najlepiej byłoby sprawdzić państwa sytuację prawną.

II. Do użytkowników

1. Pamiętajcie, że Internet nie jest bezpieczny. Jednakże istnieją i rozwijają się nowe środki umożliwiające zwiększenie ochrony waszych danych[2]. Używajcie więc wszelkich dostępnych środków do ochrony waszych połączeń, takich jak legalnie dostępne szyfrowanie poufnej poczty elektronicznej jak również własne kody dostępu do komputera[3].
2. Pamiętajcie, że każda dokonana transakcja, każda wizyta na stronie internetowej, pozostawiają ślady. Te „elektroniczne ślady" mogą zostać użyte bez waszej wiedzy do stworzenia profilu waszej osoby i waszych zainteresowań. Jeżeli nie życzycie sobie, aby został utworzony wasz profil, powinniście używać najnowszych dostępnych technik, dających możliwość otrzymywania ostrzeżenia za każdym razem, gdy zostawiacie ślad i możliwość odmówienia zostawienia śladu. Możecie również żądać informacji dotyczącej zasad działania różnych programów i stron pod względem ochrony danych i wybierać takie, które rejestrują małą ilość danych, lub są dostępne z zachowaniem anonimowości.
3. Anonimowy dostęp i korzystanie z usług i płatności stanowią najlepszą ochronę prywatności. Poszukajcie informacji o środkach technicznych, jakimi osiąga się tę anonimowość, jeżeli to konieczne[4].
4. Pełna anonimowość nie jest możliwa ze względu na ograniczenia prawne. W tym przypadku, jeżeli prawo na to zezwala, możecie używać pseudonimu, w ten sposób wasza prawdziwa tożsamość będzie znana tylko waszemu dostawcy usług internetowych.
5. Podawajcie waszemu dostawcy usług internetowych czy jakiejkolwiek innej osobie tylko te dane, które są konieczne dla realizacji określonego celu, o którym zostaliście poinformowani. Bądźcie szczególnie ostrożni w sprawie kart kredytowych i numerów rachunków bankowych, które łatwo mogą być nielegalnie użyte w ramach Internetu.
6. Pamiętajcie, że wasz adres elektroniczny jest daną osobową i że ktoś może chcieć się nim posłużyć do różnych celów, takich jak umieszczenie w książce telefonicznej czy w spisie użytkowników. Nie wahajcie się zapytać, jaki jest cel tych książek i ich inne zastosowanie. Możecie zażądać, aby wasz adres został usunięty, jeżeli nie życzycie sobie figurować w tych książkach lub w tych spisach.

7. Bądźcie ostrożni wobec stron, które proszą o więcej danych niż to konieczne do uzyskania dostępu do strony lub do przeprowadzenia transakcji albo nie wyjaśniają, dlaczego jest im potrzebna całość dotyczących was danych.
8. Pamiętajcie, że w grę wchodzi wasza odpowiedzialność prawna za przetwarzanie danych, na przykład gdy nielegalnie coś pobieracie lub wysyłacie i że, nawet jeżeli używacie pseudonimu, można was zidentyfikować.
9. Nie wysyłajcie złośliwych wiadomości, może to obrócić się przeciwko wam i mieć konsekwencje prawne.
10. Wasz dostawca usług internetowych jest odpowiedzialny za prawidłowe używanie danych. Zapytajcie go, jakie dane gromadzi, w jaki sposób i dla jakich celów. Ponawiajcie to pytanie co jakiś czas. Żądajcie ich zmiany, jeżeli okażą się nieprawidłowe lub ich usunięcia, jeżeli są zbyt obszerne, nie są uaktualnione lub nie są już konieczne. Żądajcie od dostawcy usług internetowych, aby poinformował inne strony, którym przekazał wasze dane[5].
11. Jeżeli nie jesteście zadowoleni ze sposobu, w jaki wasz aktualny dostawca usług internetowych gromadzi, przetwarza, przechowuje lub udostępnia wasze dane i jeżeli odmawia zmiany swojego postępowania, pomyślcie o zmianie dostawcy. Jeżeli uważacie, że wasz dostawca usług internetowych nie przestrzega zasad dotyczących ochrony danych, możecie poinformować właściwy organ lub podjąć kroki prawne.
12. Zapoznajcie się z zagrożeniami dla prywatności i dla bezpieczeństwa w Internecie, jak również o dostępnych środkach służących zmniejszeniu tych zagrożeń.
13. Jeżeli zamierzacie wysyłać dane do innego kraju, powinniście mieć świadomość tego, że dane te mogą tam być słabiej chronione. Jeżeli dotyczy to waszych własnych danych, oczywiście macie pełną swobodę ich przekazania mimo wszystko. Jednakże, zanim wyślecie do innego kraju dane dotyczące innych osób, poinformujcie się, na przykład w waszym organie ochrony danych, o możliwości dokonania takiego przekazania[6]. Jeżeli jest taka konieczność, możecie zwrócić się do odbiorcy danych, aby zapewnił gwarancje[7] niezbędne dla zapewnienia ochrony danych.

III. Do dostawców usług internetowych

1. Stosujcie odpowiednie procedury i dostępne technologie, najlepiej poświadczone certyfikatem, gwarantujące prywatność osób, których dane dotyczą (nawet, jeżeli nie

są one użytkownikami Internetu), a w szczególności integralność i poufność danych, jak również bezpieczeństwo fizyczne i logiczne sieci i usług dostarczanych w sieci.

2. Informujcie użytkowników o zagrożeniach dla prywatności wynikających z używania Internetu zanim się zarejestrują lub rozpoczną używać serwisu. Może to dotyczyć zagrożeń dotyczących integralności danych, ich poufności, bezpieczeństwa sieci lub innych zagrożeń prywatności, takich jak gromadzenie lub rejestrowanie danych bez ich wiedzy.
3. Informujcie użytkowników o środkach technicznych, jakich mogą zgodnie z prawem używać, aby zmniejszyć zagrożenia dotyczące bezpieczeństwa dotyczących ich danych i połączeń, takich jak szyfrowanie i podpis elektroniczny. Proponujcie te środki techniczne za cenę odpowiednią do kosztów, aby nie była zniechęcająca.
4. Przed przyjęciem abonamentu i podłączeniem użytkownika do Internetu poinformujcie go o sposobach dostępu, korzystania z serwisów i ich opłacania w sposób anonimowy (na przykład za pomocą kart przedpłaconych). Ze względu na ograniczenia prawne nie można zapewnić pełnej anonimowości. Wobec tego, jeżeli prawo na to zezwala, zaoferujcie możliwość korzystania z pseudonimów. Informujcie użytkowników o istnieniu programów umożliwiających wyszukiwanie i surfowanie po Internecie z zachowaniem anonimowości. Skonfigurujcie wasz system tak, aby używanie danych nie było konieczne, lub było ograniczone do minimum.
5. Nie czytajcie, nie zmieniajcie i nie usuwajcie wiadomości wysyłanych do kogoś innego.
6. Nie pozwalajcie na jakąkolwiek ingerencję w treść wiadomości, chyba, że taka ingerencja jest dozwolona prawem i wykonywana jest przez organ administracji publicznej.
7. Nie gromadźcie, nie przetwarzajcie i nie przechowujcie danych o użytkownikach, chyba, że jest to konieczne dla ściśle określonych celów zgodnych z prawem.
8. Nie udostępniajcie danych osobom trzecim, chyba, że udostępnienie jest przewidziane prawem[8].
9. Nie przechowujcie danych przez okres dłuższy niż jest to konieczne dla osiągnięcia celu przetwarzania[9].
10. Nie używajcie danych do promowania i sprzedawania waszych własnych usług, chyba, że osoba, poinformowana przez was, nie zgłosiła sprzeciwu lub, w przypadku przetwarzania danych o połączeniach lub danych szczególnie chronionych, udzieliła wyraźnej zgody.

11. Jesteście odpowiedzialni za prawidłowe używanie danych. Na waszej stronie głównej ogłoście w sposób jasny i widoczny, jaka jest wasza polityka w kwestii prywatności. Ta wskazówka powinna kierować za pomocą linku do szczegółowego objaśnienia stosowanych przez was praktyk dotyczących prywatności. Zanim użytkownik rozpocznie korzystanie z serwisu, kiedy odwiedza waszą stronę i za każdym razem, gdy o to zapyta, poinformujcie go o waszej tożsamości, o tym, jakie dane gromadzicie i przechowujecie, w jaki sposób, dla jakich celów i przez jaki okres je przechowujecie. W razie potrzeby poproście go o wyrażenie zgody. Na wniosek osoby, której dane dotyczą poprawcie bez zwłoki dane niepoprawne, usuńcie je, jeżeli są zbyt obszerne, nieaktualne lub nie są już konieczne i zaprzestańcie przetwarzania, jeżeli użytkownik wyrazi sprzeciw. Poinformujcie osoby trzecie, którym udostępniliście dane o wszelkich dokonanych modyfikacjach. Unikajcie jakiegokolwiek gromadzenia danych bez wiedzy osoby, której one dotyczą.
12. Informacja przekazywana użytkownikowi musi być dokładna i uaktualniona.
13. Zastanówcie się dobrze przed opublikowaniem danych na waszej stronie! Taka publikacja mogłaby stanowić naruszenie prywatności innych osób i może ona być zabroniona.
14. Przed wysłaniem danych do innego państwa zasięgnijcie informacji, na przykład w organie ochrony danych, w sprawie możliwości przystąpienia do tej operacji[10]. W razie potrzeby konieczne będzie otrzymanie od odbiorcy danych zapewnienia o wprowadzeniu odpowiednich gwarancji[11] dla ochrony tych danych.

IV. Wyjaśnienia i pomoc

1. Za każdym razem gdy jest mowa w niniejszym tekście o “dostawcach” lub “dostawcach usług”, dotyczy to również innych podmiotów działających w Internecie, takich jak dostawcy dostępu, zawartości, sieci, autorów programów wyszukiwarek, koordynatorów forów internetowych lub “info-kiosków” itd.
2. Należy pamiętać o upewnieniu się co do tego, czy wasze prawa są przestrzegane. Mechanizmy feedback oferowane na forach internetowych, stowarzyszenia dostawców usług internetowych, organy ochrony danych lub inne instytucje są ważnymi środkami służącymi zapewnieniu przestrzegania tych wytycznych. Skontaktujcie się z nimi, jeżeli potrzebujecie wyjaśnień lub chcecie uzyskać pomoc.

3. Niniejsze wytyczne mają zastosowanie do wszelkiego rodzaju “infostrad”.

---

[1] Patrz część IV, ustęp 1
[2] Termin “dane” dotyczy danych osobowych i oznacza wszelkie informacje, które dotyczą was lub innych osób.
[3] Na przykład używajcie hasła i często je zmieniajcie.
[4] Na przykład używając publicznych kiosków internetowych lub przedpłaconych kart dostępu i kart płatniczych.
[5] Przepisy o ochronie danych, podobnie jak art. 5 Konwencji o ochronie danych w zakresie zautomatyzowanego przetwarzania danych osobowych Rady Europy stanowią, że ten, kto przetwarza dane jest odpowiedzialny za dokładność i za aktualność danych.
[6] Ustawodawstwo wielu państw w Europie zakazuje przekazywania danych do państwa nie zapewniającego odpowiedniego lub równoważnego poziomu ochrony danych. Przewidziane są jednak wyjątki, zwłaszcza, jeżeli osoba, której dane dotyczą wyraziła zgodę na przekazanie jej danych do takich państw.
[7] Gwarancje te mogą być rozwijane i/lub przedstawiane zwłaszcza w umowach dotyczących przekazywania danych za granicę.
[8] Na ogół przepisy dotyczące ochrony danych dopuszczają udostępnianie osobom trzecim pod różnymi warunkami, w szczególności:
- Danych szczególnie chronionych i danych o połączeniach, pod warunkiem, że osoba, której dane dotyczą udzieliła wyraźnej zgody;
- Innych danych, jeżeli udostępnienie jest konieczne dla osiągnięcia zgodnego z prawem celu lub gdy osoba, której dane dotyczą nie wyraziła sprzeciwu.

[9] Na przykład nie przechowujcie danych do fakturowaniu, chyba, że jest to przewidziane prawem.
[10] Patrz przypis 6.
[11] Patrz przypis 7.