Oświadczenie Europejskiej Rady Ochrony Danych dotyczące zmiany rozporządzenia w sprawie prywatności i łączności elektronicznej oraz jego wpływu na ochronę osób fizycznych w zakresie prywatności i poufności komunikacji

Organy ds. ochrony danych Unii Europejskiej, zjednoczone w Europejskiej Radzie Ochrony Danych (EROD), uznają rewizję obowiązującej dyrektywy o prywatności i łączności elektronicznej (2002/58/WE, zmienionej dyrektywą 2009/136/WE) za ważną, konieczną i wymagającą szybkiego zakończenia. Począwszy od 2009 r. bardzo rozpowszechniły się usługi komunikacyjne oparte na IP, znane jako usługi OTT (*over-the-top*), które nie są objęte obowiązującą dyrektywą. Aby zapewnić użytkownikom końcowym ochronę poufności komunikacji przy korzystaniu z tych nowych usług, a także aby stworzyć równe warunki działania dla dostawców łączności elektronicznej i usług funkcjonalnie równoważnych, wzywamy Komisję Europejską, Parlament i Radę do współpracy w celu szybkiego przyjęcia nowego rozporządzenia w sprawie prywatności i łączności elektronicznej („rozporządzenie o e-prywatności"), które powinno zastąpić obecnie obowiązującą dyrektywę jak najszybciej po wejściu w życie ogólnego rozporządzenia o ochronie danych („RODO") w maju tego roku.

Biorąc pod uwagę przebieg prac nad wnioskiem, a także z myślą o współprawodawcach, EROD postanowiła udzielić dalszych porad i wyjaśnień dotyczących pewnych konkretnych kwestii związanych z poprawkami proponowanymi przez współprawodawcę.

1. Poufność komunikacji elektronicznej wymaga szczególnej ochrony wykraczającej poza przepisy RODO.

Poufność komunikacji (nowoczesny odpowiednik tradycyjnej tajemnicy korespondencji) jest prawem podstawowym chronionym na mocy art. 7 Karty praw podstawowych Unii Europejskiej, wdrożonym już dyrektywą o prywatności i łączności elektronicznej. Prawo do zachowania poufności musi być stosowane do każdego rodzaju przekazu elektronicznego, niezależnie od sposobu jego wysłania, czy to w trakcie przesyłu, czy w oczekiwaniu na przesył, na każdym etapie od wysłania do doręczenia. Ochrony wymaga również integralność urządzeń końcowych każdego użytkownika.

Łączność elektroniczna to w naszych nowoczesnych społeczeństwach podstawa działalności w wielu istotnych dziedzinach, wspierająca korzystanie z licznych praw podstawowych – wolności myśli, sumienia, wyznania, wypowiedzi, informacji, zgromadzeń, stowarzyszeń itp. Konieczne jest zatem skuteczniejsze zapewnienie poufnego i neutralnego charakteru usług przekazywania wiadomości.

Biorąc pod uwagę powszechność i znaczenie łączności elektronicznej w naszym życiu cyfrowym, wiadomości elektroniczne niejednokrotnie zawierają lub ujawniają szczególne kategorie danych osobowych, czy to bezpośrednio, czy choćby tylko ze względu na nagromadzenie i połączenie treści i metadanych, co pozwala na wyciąganie bardzo dokładnych wniosków na temat życia prywatnego poszczególnych osób. Wiąże się to z wysokim ryzykiem dla praw i wolności osób i wymaga w związku z tym odpowiedniego podejścia.

Z tego względu w pełni popieramy środki przewidziane w proponowanym rozporządzeniu, polegające na szeroko ujętych zakazach, ograniczonych wyjątkach i wymogu uzyskania zgody. Rozporządzenie o e-prywatności nie powinno zatem zezwalać na przetwarzanie treści i metadanych pochodzących z łączności elektronicznej na ogólnie sformułowanych podstawach, takich jak „prawnie uzasadnione interesy", które wykraczają poza zakres konieczny do świadczenia usługi łączności elektronicznej. Rozporządzenie nie powinno również umożliwiać przetwarzania metadanych pochodzących z łączności elektronicznej do celów wykonania umowy, a więc nie powinno przewidywać wyjątku dotyczącego ogólnie tego celu, ponieważ określa ono już dokładnie, jakie rodzaje przetwarzania są w tym celu dozwolone (np. przetwarzanie do w celu naliczania opłat).

EROD podkreśla, że metadane pochodzące z łączności elektronicznej mogą być nadal przetwarzane bez zgody osoby, której dane dotyczą, pod warunkiem ich rzeczywistej anonimizacji[1]. EROD zachęca dostawców usług łączności elektronicznej do korzystania z tej możliwości w celu tworzenia innowacyjnych usług przy jednoczesnym zachowaniu prywatności.

2. Dyrektywa o prywatności i łączności elektronicznej już obowiązuje.

Ochrona poufności komunikacji to już istniejące prawo. W dyrektywie o prywatności i łączności elektronicznej z 2002 r., zmienionej w 2009 r., ustanowiono już ogólny zakaz przetwarzania treści i metadanych pochodzących z łączności elektronicznej. Działania takie są dopuszczalne wyłącznie:

- za uprzednią zgodą użytkownika, lub
- jeżeli spełniają jeden z wyjątków przewidzianych w dyrektywie o prywatności i łączności elektronicznej (transmisja komunikatu lub naliczanie opłat).

Usługi transmisji wykorzystywane do świadczenia usług w trybie maszyna-maszyna także są objęte zakresem obecnej dyrektywy. Przepisy te zachowano w proponowanym rozporządzeniu. Również ochrona urządzeń końcowych jest już przysługującym prawem. Wykorzystanie możliwości urządzeń końcowych użytkownika w zakresie przechowywania danych odbywa się w sposób neutralny pod względem technologicznym. Dlatego też nie tylko pliki cookie, ale wszystkie technologie śledzenia podlegają już zgodzie użytkownika lub jednemu z wyjątków określonych w dyrektywie o prywatności i łączności elektronicznej.

Ponadto proponowane rozporządzenie zmienione przez współprawodawców wprowadza kilka nowych wyjątków zaproponowanych przez Grupę Roboczą Art. 29[2], takich jak aktualizacje w zakresie bezpieczeństwa i pomiar odbiorców. Wyjątki te dotyczą konkretnych rodzajów przetwarzania, stanowiących bardzo ograniczone zagrożenie dla prywatności użytkowników.

[1] Zgodnie z definicją w WP216, przy czym dane poddane pseudonimizacji pozostają danymi osobowymi.

[2] Zob. opinie Grupy Roboczej WP194 oraz WP240.

3. Proponowane rozporządzenie ma na celu zapewnienie jego jednolitego stosowania we wszystkich państwach członkowskich oraz w odniesieniu do wszystkich rodzajów administratorów danych.

Obecna dyrektywa o prywatności i łączności elektronicznej nie ma zastosowania do usług łączności elektronicznej oferowanych przez dostawców działających w internecie, mimo że świadczą oni usługę równoważną pod względem funkcjonalnym.
Dostawcy ci będą jednak objęci zakresem proponowanego rozporządzenia. EROD podkreśla, że rozszerzenie zakresu stosowania rozporządzenia na usługi równoważne pod względem funkcjonalnym, w tym tzw. usług OTT, jest istotnym elementem reformy. Należy unikać wszelkich proponowanych zmian w projekcie rozporządzenia, które mogłyby podważyć ten cel (np. wszelkich propozycji zmierzających do ograniczenia zakresu ochrony do danych komunikacyjnych w trakcie przesyłu), aby zagwarantować wszystkim dostawcom równe warunki działania.
Proponowane rozporządzenie ma również zastosowanie niezwłocznie po zebraniu danych dotyczących zachowania użytkownika, bez względu na to, czy utworzył on konto w celu skorzystania z usługi. Takie podejście nie tylko zapewni użytkownikom usług ochronę, na jaką zasługują, ale także umożliwi uczciwą konkurencję między administratorami danych. Należy zauważyć, że zgoda, którą należy uzyskać na mocy rozporządzenia o e-prywatności, ma takie samo znaczenie jak zgoda na podstawie RODO. W szczególności wymóg dobrowolnego charakteru zgody uniemożliwi usługodawcom stosowanie tzw. *cookie walls*[3], a obowiązek uzyskania konkretnej zgody stworzy równe warunki działania dla usługodawców, niezależnie od tego, czy użytkownik był zalogowany.
Ponadto ustanowienie szczególnych sankcji za naruszenie rozporządzenia o e-prywatności, w połączeniu z rozszerzonym zakresem terytorialnym (oba te środki stanowią odzwierciedlenie przepisów RODO), zapewni organom ochrony danych skuteczne uprawnienia, które umożliwią im egzekwowanie stosowania rozporządzenia w odniesieniu do wszystkich narzędzi komunikacji elektronicznej wykorzystywanych przez użytkowników z UE.

4. Nowe rozporządzenie musi egzekwować wymóg uzyskania zgody używanie plików cookie i podobnych technologii oraz musi oferować dostawców usług narzędzia techniczne umożliwiające im uzyskanie tej zgody.

Zgodnie z wnioskiem Komisji Europejskiej art. 10 rozporządzenia ma zapewnić użytkownikom kontrolę nad wykorzystaniem możliwości ich urządzeń końcowych w zakresie przechowywania. Parlament zmodyfikował brzmienie art. 10 w celu wprowadzenia wymogu domyślnej ochrony prywatności w ustawieniach oprogramowania oraz dla zapewnienia rozwiązania technicznego służącego uzyskiwaniu ważnej zgody przez strony internetowe.
EROD w pełni popiera zaostrzenie tego artykułu i uważa, że powinien on wyraźnie odnosić się do systemów operacyjnych smartfonów, tabletów i wszelkich innych aplikacji klienckich, aby zagwarantować uwzględnianie w aplikacjach komunikacyjnych decyzji użytkowników niezależnie od środków technicznych.
Ponadto ustawienia ochrony prywatności powinny ułatwiać wyrażenie i wycofanie zgody w prosty, wiążący i możliwy do wyegzekwowania sposób wobec wszystkich stron, a użytkownicy powinni mieć możliwość dokonania przy instalacji jasnego wyboru, umożliwiającego im wyrażenie zgody, jeśli zechcą. Ponadto strony internetowe i aplikacje mobilne powinny mieć możliwość uzyskania zgody w sposób zgodny z RODO w ustawieniach prywatności.

5. Wnioski

[3] *Cookie wall* uniemożliwia dostęp do strony internetowej lub usługi użytkownikom, którzy nie wyrażają zgody na stosowanie plików cookie.

EROD uważa, że:

- Rozporządzenie o e-prywatności nie powinno prowadzić do obniżenia poziomu ochrony zapewnianej obecnie przez dyrektywę o prywatności i łączności elektronicznej.
- Rozporządzenie o e-prywatności powinno zapewniać ochronę wszystkich rodzajów łączności elektronicznej, w tym w ramach usług OTT, w sposób neutralny pod względem technologicznym.
- Przed przetwarzaniem danych pochodzących z łączności elektronicznej lub wykorzystaniem możliwości urządzeń końcowych użytkownika w zakresie przechowywania lub przetwarzania należy systematycznie uzyskiwać zgodę użytkownika w sposób wykonalny technicznie i możliwy do wyegzekwowania. Nie należy wprowadzać wyjątków umożliwiających przetwarzanie danych w oparciu o „prawnie uzasadniony interes" administratora danych ani w ogólnym celu wykonania umowy.
- Art. 10 powinien przewidywać skuteczny sposób uzyskiwania zgody na stronach internetowych i w aplikacjach mobilnych. W ogólniejszym ujęciu ustawienia powinny domyślnie chronić prywatność użytkowników, a zapytanie użytkownika o wybór ustawienia powinno następować po przedstawieniu mu stosownych i przejrzystych informacji. W tym względzie rozporządzenie powinno pozostać neutralne pod względem technicznym, aby jego stosowanie było spójne niezależnie od konkretnych okoliczności.
- W przypadku wprowadzenia jakichkolwiek doraźnych wyjątków rozważanych przez prawodawców, oprócz tych już uwzględnionych w projektach Komisji i Parlamentu, należy stosować najwyższy stopień kontroli. Szczególnie rygorystycznej kontroli wymagają wszelkie szeroko ujmowane wyjątki dotyczące przypadków, w których „organ publiczny" zwraca się o przetwarzanie danych; projekt nie powinien zezwalać na masowe monitorowanie lokalizacji użytkowników ani na przetwarzanie ich metadanych.
- Aby zapewnić dobrowolność zgody, jak wymaga tego RODO, dostęp do usług i funkcji nie może być uzależniony od zgody użytkownika na przetwarzanie danych osobowych lub informacji przetwarzanych przez urządzenia końcowe użytkownika bądź związanych z takimi urządzeniami, co oznacza, że należy wyraźnie zabronić stosowania *cookie walls*.
- Należy zachęcać do stosowania danych pochodzących z łączności elektronicznej poddanych rzeczywistej anonimizacji.
- Wymienione zmiany zapewnią ochronę prywatności użytkowników końcowych we wszelkich odnośnych kontekstach oraz zapobiegną wszelkim zakłóceniom konkurencji.