GRUPA ROBOCZA ART. 29

00461/13/PL
WP 202

Opinia 02/2013 w sprawie aplikacji na urządzenia inteligentne

Przyjęta w dniu 27 lutego 2013 r.

Streszczenie

Istnieją setki tysięcy różnych aplikacji dostępnych w szeregu sklepów z aplikacjami dla każdego popularnego rodzaju urządzenia inteligentnego. Według uzyskanych informacji w sklepach z aplikacjami przybywa ponad 1 600 nowych aplikacji dziennie. Według doniesień przeciętny użytkownik smartfona pobiera 37 aplikacji. Aplikacje mogą być oferowane użytkownikom końcowym za niewielką opłatą lub bez żadnych kosztów bezpośrednich oraz mogą mieć grono użytkowników liczące tylko kilka osób lub wiele milionów osób.

Aplikacje mogą gromadzić duże ilości danych z urządzenia (np. dane przechowywane na urządzeniu przez użytkownika oraz dane z różnych czujników, w tym dane dotyczące lokalizacji), a także przetwarzać je w celu świadczenia nowych i innowacyjnych usług na rzecz użytkowników końcowych. Te same źródła danych mogą być jednak dalej przetwarzane, zwykle w celu zapewnienia źródła dochodów, w sposób, którego użytkownik końcowy może nie znać lub nie chcieć.

Podmioty opracowujące aplikacje nieświadome wymogów dotyczących ochrony danych mogą powodować znaczące ryzyko dla życia prywatnego i reputacji użytkowników urządzeń inteligentnych. Głównym czynnikiem ryzyka związanym z ochroną danych dla użytkowników końcowych jest brak przejrzystości i świadomości rodzajów przetwarzania, jakich może dokonywać aplikacja, w połączeniu z brakiem świadomej zgody użytkowników końcowych wyrażonej przed rozpoczęciem przetwarzania danych. Słabe środki bezpieczeństwa, wyraźna tendencja do maksymalizacji danych i elastyczność celów, w jakich gromadzi się dane osobowe, jeszcze bardziej przyczyniają się do występowania czynników ryzyka związanych z ochroną danych spotykanych w obecnym środowisku aplikacji.

Duże ryzyko dla ochrony danych wynika również ze stopnia rozdrobnienia rynku opracowywania aplikacji, na którym obecnych jest wiele podmiotów. Są to m.in. podmioty opracowujące aplikacje, właściciele aplikacji, sklepy z aplikacjami, producenci systemów operacyjnych i urządzeń oraz inne osoby trzecie, które mogą być zaangażowane w gromadzenie i przetwarzanie danych osobowych z urządzeń inteligentnych, takie jak analitycy i podmioty świadczące usługi reklamowe. Większość wniosków i zaleceń w niniejszej opinii jest skierowanych do podmiotów opracowujących aplikacje (z uwagi na fakt, że mają one największą kontrolę nad dokładnym sposobem przeprowadzania przetwarzania i prezentacji informacji w ramach aplikacji), które, aby mogły sprostać najwyższym normom w zakresie ochrony prywatności i danych, muszą jednak często współpracować z innymi stronami w środowisku aplikacji. Ma to szczególne znaczenie w dziedzinie bezpieczeństwa, w której łańcuch wielu podmiotów jest tylko tak mocny, jak jego najsłabsze ogniwo.

Wiele rodzajów danych dostępnych na inteligentnym urządzeniu przenośnym ma charakter danych osobowych. Właściwe ramy prawne stanowi dyrektywa o ochronie danych w połączeniu z dyrektywą o prywatności i łączności elektronicznej w części dotyczącej ochrony urządzeń przenośnych w odniesieniu do życia prywatnego użytkowników. Przepisy te mają zastosowanie do wszystkich aplikacji skierowanych do użytkowników aplikacji w UE, bez względu na lokalizację podmiotu opracowującego aplikacje lub sklepu z aplikacjami.

W niniejszej opinii grupa robocza omawia ramy prawne mające zastosowanie do przetwarzania danych osobowych w trakcie opracowywania, dystrybucji i wykorzystywania aplikacji do urządzeń inteligentnych, ze szczególnym uwzględnieniem wymagania dotyczącego zgody, zasad w zakresie ograniczenia celu i minimalizacji danych, potrzeby

podjęcia odpowiednich środków bezpieczeństwa, obowiązku prawidłowego informowania użytkowników końcowych, ich praw, rozsądnych okresów przechowywania, a zwłaszcza uczciwego przetwarzania danych zgromadzonych od dzieci oraz dotyczących dzieci.

Spis treści

1. Wprowadzenie

Aplikacje stanowią oprogramowanie użytkowe często zaprojektowane do konkretnego zadania i przeznaczone dla konkretnego zbioru inteligentnych urządzeń, takich jak smartfony, komputery typu tablet i telewizja internetowa. Organizują one informacje w sposób odpowiedni dla szczególnych cech charakterystycznych danego urządzenia i często wchodzą w ścisłe interakcje z elementami sprzętu komputerowego i właściwościami systemu operacyjnego obecnymi w urządzeniach.

Istnieją setki tysięcy różnych aplikacji dostępnych w szeregu sklepów z aplikacjami dla każdego popularnego rodzaju urządzenia inteligentnego. Aplikacje służą różnorodnym celom obejmującym przeglądanie internetu, komunikację (przesyłanie wiadomości e-mail, wiadomości telefonicznych i internetowych), rozrywkę (gry, filmy/video i muzykę), usługi sieci społecznościowych, usługi bankowe i usługi oparte na lokalizacji. Według uzyskanych informacji w sklepach z aplikacjami przybywa ponad 1 600 nowych aplikacji dziennie[1]. Przeciętny użytkownik smartfona pobiera 37 aplikacji[2]. Aplikacje mogą być oferowane użytkownikom końcowym za niewielką opłatą lub bez żadnych kosztów bezpośrednich oraz mogą mieć grono użytkowników liczące tylko kilka osób lub wiele milionów osób.

Podstawowy system operacyjny obejmuje również oprogramowanie lub struktury danych, które są ważne dla podstawowych usług urządzeń inteligentnych, na przykład książki adresowej smartfona. System operacyjny jest zaprojektowany, aby udostępniać wspomniane elementy składowe aplikacjom poprzez interfejsy programowania aplikacji (API). Interfejsy te oferują dostęp do wielu czujników, które mogą znajdować się w inteligentnych urządzeniach. Do czujników tych należą: żyroskop, kompas cyfrowy i przyspieszeniomierz mające informować o prędkości i kierunku ruchu, kamery z przodu i z tyłu umożliwiające kręcenie filmów i robienie fotografii oraz mikrofon do nagrywania dźwięku. Urządzenia inteligentne mogą również zawierać czujniki zbliżeniowe[3].Mogą one także łączyć się poprzez wiele interfejsów sieciowych, w tym Wi-Fi, Bluetooth, NFC lub Ethernet. Ponadto możliwe jest ustalenie dokładnej lokalizacji dzięki usługom geolokalizacyjnym (opisanym w opinii Grupy Roboczej Art. 29 13/2011 w sprawie usług geolokalizacyjnych w inteligentnych urządzeniach przenośnych[4]). Rodzaj, dokładność i częstotliwość wspomnianych danych z czujników różnią się w zależności od urządzenia i systemu operacyjnego.

---

1 Sprawozdanie w ConceivablyTech z dnia 19 sierpnia 2012 r., dostępne na stronie internetowej www.conceivablytech.com/10283/business/apple-app-store-to-reach-1mapps-this-year-sort-of. Cytowane przez Kamalę D. Harris, prokurator generalną Departamentu Sprawiedliwości stanu Kalifornia, „Privacy on the go, Recommendations for the mobile ecosystem", styczeń 2013, http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.

2 Są to dane szacunkowe na poziomie ogólnoświatowym za 2012 r. instytutu ABI Research, http://www.abiresearch.com/press/smartphone-users-worldwide-will-download-37-apps-o.

3 Czujnik mogący wykrywać obecność przedmiotów bez kontaktu fizycznego. Zob.: http://www.w3.org/TR/2012/WD-proximity-20121206/.

4 Zob. Opinia 13/2011 w sprawie usług geolokalizacyjnych w inteligentnych urządzeniach przenośnych Grupy Roboczej Art. 29 (maj 2011 r.), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_pl.pdf.

Poprzez interfejsy programowania aplikacji podmioty opracowujące aplikacje są w stanie gromadzić takie dane w sposób ciągły, uzyskiwać dostęp do danych kontaktowych i je zapisywać, wysyłać wiadomości e-mail, SMS lub wiadomości sieci społecznościowych, czytać/modyfikować/usuwać zawartość karty SD, nagrywać dźwięk, korzystać z kamery i uzyskiwać dostęp do przechowywanych fotografii, odczytywać informacje dotyczące stanu i tożsamości telefonu, modyfikować ustawienia systemu globalnego oraz uniemożliwiać przechodzenie telefonu w stan uśpienia. Interfejsy programowania aplikacji mogą również dostarczać informacje odnoszące się do samego urządzenia poprzez jeden lub większą liczbę niepowtarzalnych kodów identyfikacyjnych oraz informacje o innych zainstalowanych aplikacjach. Te same źródła danych mogą być dalej przetwarzane, zwykle w celu zapewnienia źródła dochodów, w sposób, którego użytkownik końcowy może nie znać lub nie chcieć.

Celem niniejszej opinii jest wyjaśnienie ram prawnych mających zastosowanie do przetwarzania danych osobowych w zakresie dystrybucji i wykorzystywania aplikacji do urządzeń inteligentnych oraz rozważenie dalszego przetwarzania, jakie może mieć miejsce poza aplikacją, takiego jak wykorzystywanie zgromadzonych danych w celu budowy profilów lub określania grup docelowych użytkowników. W opinii analizuje się kluczowe czynniki ryzyka związane z ochroną danych, przedstawia się opis różnych zaangażowanych stron oraz podkreśla się różne zobowiązania prawne. Zagadnienia te odnoszą się do podmiotów opracowujących aplikacje, właścicieli aplikacji, sklepów z aplikacjami, producentów systemów operacyjnych i urządzeń oraz innych osób trzecich, które mogą być zaangażowane w gromadzenie i przetwarzanie danych osobowych z urządzeń inteligentnych, takich jak analitycy i podmioty świadczące usługi reklamowe.

W opinii uwzględniono w szczególności wymaganie dotyczące zgody, zasady w zakresie ograniczenia celu i minimalizacji danych, potrzebę podjęcia odpowiednich środków bezpieczeństwa, obowiązek prawidłowego informowania użytkowników końcowych, ich prawa, rozsądne okresy przechowywania, a zwłaszcza uczciwe przetwarzanie danych zgromadzonych od dzieci oraz dotyczących dzieci.

Zakres ten ma zastosowanie do wielu różnych rodzajów urządzeń inteligentnych, ale dotyczy w szczególności dostępnych aplikacji do inteligentnych urządzeń przenośnych.

2. Czynniki ryzyka związane z ochroną danych

Ścisła interakcja z systemem operacyjnym pozwala aplikacji na dostęp do znacznie większej ilości danych niż ma to miejsce w przypadku tradycyjnej przeglądarki internetowej[5]. Aplikacje mogą gromadzić duże ilości danych z urządzenia (dane dotyczące lokalizacji, dane przechowywane w urządzeniu przez użytkownika oraz dane z różnych czujników), a także przetwarzać je w celu świadczenia nowych i innowacyjnych usług na rzecz użytkowników końcowych.

Duże zagrożenie dla ochrony danych wynika z poziomu rozdrobnienia środowiska wynikającego z działalności wielu podmiotów, które zajmują się opracowywaniem aplikacji. Pojedynczy element danych można w czasie rzeczywistym przekazać z urządzenia w celu

[5] Mimo że przeglądarki internetowe oparte na stacjach roboczych zdobywają szerszy dostęp do danych sensorycznych dotyczących urządzeń użytkowników końcowych, napędzanych przez podmioty opracowujące gry internetowe.

przetwarzania go na całym świecie lub kopiowania między łańcuchami osób trzecich. Niektóre z najpopularniejszych aplikacji są opracowywane przez najważniejsze podmioty zajmujące się technologiami, ale wiele innych jest projektowanych przez małe przedsiębiorstwa rozpoczynające działalność. Pojedynczy programista z pomysłem i niewielkimi wcześniej zdobytymi umiejętnościami lub bez takich umiejętności w zakresie programowania może w krótkim czasie dotrzeć do grona odbiorców na całym świecie. Podmioty opracowujące aplikacje nieświadome wymogów dotyczących ochrony danych mogą powodować znaczące ryzyko dla życia prywatnego i reputacji użytkowników urządzeń inteligentnych. Jednocześnie usługi osób trzecich, takie jak reklama, rozwijają się gwałtownie, co w przypadku, gdy są one integrowane przez podmiot opracowujący aplikacje bez należytej uwagi, może spowodować ujawnienie znacznych ilości danych osobowych,

Głównym czynnikiem ryzyka związanym z ochroną danych dla użytkowników końcowych jest brak przejrzystości i świadomości rodzajów przetwarzania, jakich może dokonywać aplikacja, w połączeniu z brakiem świadomej zgody użytkowników końcowych wyrażonej przed rozpoczęciem przetwarzania danych. Słabe środki bezpieczeństwa, wyraźna tendencja do maksymalizacji danych i elastyczność celów, w jakich gromadzi się dane osobowe, jeszcze bardziej przyczyniają się do występowania czynników ryzyka związanych z ochroną danych spotykanych w obecnym środowisku aplikacji. Wiele ze wspomnianych zagrożeń zostało już zbadanych i ograniczonych przez inne międzynarodowe organy regulacyjne, takie jak amerykańska Federalna Komisja Handlu, Kanadyjski Urząd Komisarza ds. Prywatności oraz Prokurator Generalny Departamentu Sprawiedliwości stanu Kalifornia[6].

- Głównym ryzykiem związanym z ochroną danych jest brak przejrzystości. Aby zapewnić udostępnienie kompleksowych informacji użytkownikowi końcowemu w odpowiednim czasie, podmioty opracowujące aplikacje są ograniczone właściwościami udostępnionymi przez producentów systemów operacyjnych i sklepy z aplikacjami. Nie wszystkie podmioty opracowujące aplikacje wykorzystują jednak wspomniane właściwości, ponieważ wiele aplikacji nie posiada polityki prywatności lub nie informuje swoich ewentualnych użytkowników w zrozumiały sposób o rodzaju danych osobowych, jakie dana aplikacja może przetwarzać, ani o celu tego przetwarzania. Brak przejrzystości nie ogranicza się do darmowych aplikacji lub aplikacji będących własnością niedoświadczonych podmiotów, ponieważ w niedawnym badaniu stwierdzono, że tylko 61,3 % z czołowych 150 aplikacji zapewnia politykę prywatności[7].

---

[6] Zob. między innymi sprawozdanie służb Federalnej Komisji Handlu (FTC) „Mobile Privacy Disclosures, Building Trust Through Transparency", luty 2013 r., http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf, sprawozdanie służb Federalnej Komisji Handlu (FTC) „Mobile Apps for Kids: Current Privacy Disclosures are Disappointing", luty 2012 r., http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf oraz sprawozdanie uzupełniające, „Mobile Apps for Kids: Disclosures Still Not Making the Grade", grudzień 2012 r., http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf, Kanadyjskie Urzędy Komisarza ds. Ochrony Prywatności, „Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps", październik 2012 r., http://www.priv.gc.ca/information/pub/gd_app_201210_e.pdf, Kamala D. Harris, prokurator generalna Departamentu Sprawiedliwości stanu Kalifornia, „Privacy on the go, Recommendations for the mobile ecosystem", styczeń 2013 r., http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.

[7] Badanie aplikacji mobilnych z czerwca 2012 r. Forum Przyszłości Prywatności (FPF) http://www.futureofprivacy.org/wp-content/uploads/Mobile-Apps-Study-June-2012.pdf.

- Brak przejrzystości jest ściśle związany z brakiem swobodnej i świadomej zgody osoby zainteresowanej. Kiedy aplikacja zostaje pobrana, wyrażenie zgody często ogranicza się do zaznaczenia okienka wskazującego, że użytkownik końcowy akceptuje warunki, bez możliwości wyboru opcji „Nie, dziękuję". Według badania przedsiębiorstwa GSMA z września 2011 r. 92 % użytkowników aplikacji chciałoby mieć wybór opierający się na bardziej szczegółowych informacjach[8].

- Słabe środki bezpieczeństwa mogą prowadzić do bezprawnego przetwarzania (wrażliwych) danych osobowych, na przykład, jeżeli podmiot opracowujący aplikacje doświadcza przypadku naruszenia danych osobowych lub jeżeli z samej aplikacji następuje wyciek danych.

- Inne ryzyko związane z ochroną danych dotyczy nieprzestrzegania (z powodu niewiedzy lub celowo) zasady ograniczenia celu, która wymaga, aby dane osobowe były gromadzone i przetwarzane wyłącznie w określonych i zgodnych z prawem celach. Dane osobowe gromadzone przez aplikacje mogą być rozpowszechniane na szeroką skalę szeregowi osób trzecich w nieokreślonych lub szeroko zdefiniowanych celach, takich jak „badanie rynku". Takie samo alarmujące nieprzestrzeganie ma miejsce w odniesieniu do zasady minimalizacji danych. Ostatnie badania wykazało, że wiele aplikacji gromadzi duże ilości danych ze smartfonów bez żadnego znaczącego związku z podstawową funkcjonalnością aplikacji[9].

3 Zasady ochrony danych

3.1 Prawo właściwe

Odpowiednimi ramami prawnymi UE jest dyrektywa 95/46/WE o ochronie danych. Stosuje się ją w każdym przypadku, w którym wykorzystywanie aplikacji na urządzenia inteligentne pociąga za sobą przetwarzanie danych osobowych osób fizycznych. W celu określenia prawa właściwego, kluczowe jest po pierwsze określenie roli różnych zaangażowanych zainteresowanych stron: określenie administratora lub administratorów danych w odniesieniu do przetwarzania dokonywanego za pomocą aplikacji mobilnych jest szczególnie istotne w odniesieniu do prawa właściwego. Elementem decydującym o zastosowaniu przepisów UE o ochronie danych jest miejsce prowadzenia działalności gospodarczej przez administratora danych, chociaż nie jest to jedynym kryterium. Zgodnie z art. 4 ust. 1 lit. a) dyrektywy o ochronie danych prawo krajowe państwa członkowskiego ma zastosowanie w odniesieniu do każdego przetwarzania danych osobowych odbywającego się „w kontekście prowadzenia przez administratora danych działalności gospodarczej" na terytorium państwa członkowskiego. Na mocy art. 4 ust. 1 lit. c) dyrektywy o ochronie danych prawo krajowe państwa członkowskiego ma zastosowanie również w przypadkach, w których administrator danych *nie prowadzi działalności gospodarczej* na terytorium Wspólnoty, a wykorzystuje środki znajdujące się na terytorium wymienionego państwa członkowskiego. Ponieważ urządzenie jest instrumentem w przetwarzaniu danych osobowych pochodzących od

[8] „89 % [użytkowników] uważa, że ważne jest posiadanie wiedzy o tym, kiedy aplikacja wymienia ich informacje osobiste, oraz możliwości wyłączenia tej funkcji". Źródło: „User perspectives on mobile privacy", wrzesień 2011 r., http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/futuresightuserperspectivesonuserprivacy.pdf.

[9] Wall Street Journal, „Your Apps Are Watching You", http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html.

użytkownika i go dotyczących, zazwyczaj wspomniane kryterium jest spełnione[10]. Ma to znaczenie jedynie w przypadku, gdy administrator danych nie prowadzi działalności gospodarczej w UE.

W rezultacie za każdym razem, gdy stronę zaangażowaną w opracowywanie, dystrybucję i działanie aplikacji uznaje się za administratora danych, taka strona jest odpowiedzialna, samodzielnie lub wspólnie z innymi podmiotami, za zapewnienie zgodności ze wszystkimi wymaganiami przedstawionymi w dyrektywie o ochronie danych. Określenie roli stron zaangażowanych w aplikacje mobilne przeanalizowano dalej w sekcji 3.3 poniżej.

Oprócz dyrektywy o ochronie danych, dyrektywa o prywatności i łączności elektronicznej (2002/58/WE, w wersji zmienionej przez 2009/136/WE) ustanawia szczegółowe normy dla wszystkich stron na całym świecie, które chcą przechowywać informacje lub uzyskiwać dostęp do informacji przechowywanych na urządzeniach użytkowników w Europejskim Obszarze Gospodarczym (EOG).

Artykuł 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej stanowi, że przechowywanie informacji lub uzyskanie dostępu do informacji już przechowywanych w urządzeniu końcowym abonenta lub użytkownika [jest] dozwolone wyłącznie pod warunkiem że dany abonent lub użytkownik wyraził zgodę zgodnie z dyrektywą 95/46/WE po otrzymaniu jasnych i wyczerpujących informacji, między innymi o celach przetwarzania. (…)

Chociaż wiele przepisów dyrektywy o prywatności i łączności elektronicznej stosuje się jedynie do dostawców publicznie dostępnych usług łączności elektronicznej oraz dostawców publicznych sieci łączności we Wspólnocie, art. 5 ust. 3 ma zastosowanie do każdego podmiotu, który umieszcza informacje na urządzeniu inteligentnym lub odczytuje je z tego urządzenia. Ma on zastosowanie bez względu na charakter podmiotu (tj. na to, czy jest on podmiotem publicznym lub prywatnym, indywidualnym programistą lub wielką korporacją, a także na to, czy jest on administratorem danych, przetwarzającym lub osobą trzecią).

Wymaganie wyrażenia zgody określone w art. 5 ust. 3 ma zastosowanie do wszystkich informacji bez względu na charakter przechowywanych danych lub danych, do których uzyskuje się dostęp. Zakres nie ogranicza się do danych osobowych, może to być każdy rodzaj informacji przechowywanych na urządzeniu.

Wymaganie wyrażenia zgody określone w art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej ma zastosowanie do usług oferowanych „we Wspólnocie", to znaczy wszystkim osobom mieszkającym w Europejskim Obszarze Gospodarczym niezależnie od lokalizacji usługodawcy. Istotne jest, aby podmioty opracowujące aplikacje wiedziały, że obie dyrektywy stanowią prawa nadrzędne z uwagi na fakt, że prawa jednostki są niezbywalne i nie podlegają zrzeczeniu się na podstawie umowy. Oznacza to, że nie można wyłączyć stosowania europejskiego prawa do prywatności poprzez jednostronną deklarację lub porozumienie umowne[11].

[10] W zakresie, w jakim aplikacja generuje przesył danych osobowych do administratorów danych. Wspomniane kryterium może nie być spełnione, jeżeli dane są przetwarzane jedynie lokalnie, na samym urządzeniu.

[11] Przykładowo, oświadczenia, że stosuje się prawo właściwe spoza EOG.

3.2 Dane osobowe przetwarzane przez aplikacje

Wiele rodzajów danych przechowywanych na urządzeniu inteligentnym lub generowanych przez nie to dane osobowe. Zgodnie z motywem 24 dyrektywy o prywatności i łączności elektronicznej:

> „Wyposażenie terminali użytkowników sieci łączności elektronicznej oraz informacje przechowywane na tych urządzeniach stanowią część prywatnej sfery użytkowników podlegającej ochronie na mocy Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności".

Są to dane osobowe zawsze, kiedy odnoszą się do osoby fizycznej, która jest bezpośrednio (na przykład poprzez nazwisko) lub pośrednio możliwa do zidentyfikowania przez administratora danych lub osobę trzecią. Mogą one być powiązane z właścicielem urządzenia lub jakąkolwiek inną osobą, na przykład z danymi kontaktowymi znajomych w książce adresowej[12]. Dane mogą być gromadzone i przetwarzane na urządzeniu lub, po przekazaniu, gdzie indziej w infrastrukturze podmiotów opracowujących aplikacje lub osób trzecich poprzez połączenie z zewnętrznym interfejsem programowania aplikacji w czasie rzeczywistym bez wiedzy użytkownika końcowego.

Przykłady takich danych osobowych, które mogą mieć znaczący wpływ na życie prywatne użytkowników oraz innych osób, są następujące:

- lokalizacja;
- kontakty;
- niepowtarzalne kody identyfikacyjne wyrobu i klienta (takie jak numer IMEI[13], IMSI[14], UDID[15] oraz numer telefonu przenośnego);
- tożsamość osoby, której dane dotyczą;
- tożsamość telefonu (tj. nazwa telefonu[16]);
- dane karty kredytowej i płatności;
- dzienniki połączeń telefonicznych, SMS-y lub komunikatory internetowe;
- historia przeglądania;
- wiadomości e-mail;
- dane uwierzytelniające usług społeczeństwa informacyjnego (zwłaszcza usług o cechach społecznych);
- fotografie i filmy;
- dane biometryczne (np. wzory z systemów rozpoznawania twarzy i wzory odcisków palców).

---

[12] Dane mogą być (i) automatycznie generowane przez urządzenie na podstawie właściwości określonych uprzednio przez producenta systemu operacyjnego lub urządzenia lub przez właściwego operatora telefonii ruchomej (np. dane geolokalizacyjne, ustawienia sieci, adres IP); (ii) generowane przez użytkownika poprzez aplikacje (wykazy kontaktów, notatki, fotografie); (iii) generowane przez aplikacje (np. historia przeglądania).

[13] Międzynarodowy **numer fabryczny** mobilnego aparatu telefonicznego.

[14] Międzynarodowy **numer tożsamości** telefonicznej abonenta mobilnego.

[15] Niepowtarzalny **kod identyfikacyjny** wyrobu.

[16] Użytkownicy zazwyczaj nazywają telefony swoim prawdziwym nazwiskiem: „iPhone Jana Kowalskiego".

3.3 Strony zaangażowane w przetwarzanie danych

Wiele różnych stron jest zaangażowanych w opracowywanie, dystrybucję i działanie aplikacji, a każda z nich może mieć różne zobowiązania w zakresie ochrony danych.

Można zidentyfikować cztery główne strony. Są to: (i) podmioty opracowujące aplikacje (w tym właściciele aplikacji)[17], (ii) producenci systemów operacyjnych i urządzeń[18]; (iii) sklepy z aplikacjami (dystrybutor aplikacji), a ponadto (iv) inne strony zaangażowane w przetwarzanie danych osobowych. W niektórych przypadkach odpowiedzialność w zakresie ochrony danych jest wspólna, szczególnie, kiedy ten sam podmiot jest zaangażowany na wielu etapach, na przykład w sytuacji, gdy producent systemu operacyjnego kontroluje również sklep z aplikacjami.

Użytkownicy końcowi także mogą odegrać pewną rolę, biorąc stosowną odpowiedzialność w zakresie, w jakim tworzą i przechowują dane osobowe za pośrednictwem swoich urządzeń przenośnych. Jeżeli takie przetwarzanie służy wyłącznie celom osobistym lub celom gospodarstwa domowego, dyrektywa o ochronie danych nie ma zastosowania (art. 3 ust. 2) i użytkownik jest zwolniony z formalnych obowiązków w zakresie ochrony danych. Jeżeli użytkownicy postanawiają jednak wymieniać dane za pośrednictwem aplikacji, na przykład upubliczniając informacje nieokreślonej liczbie osób[19], korzystając z aplikacji sieci społecznościowej, przetwarzają oni informacje w zakresie wykraczającym poza warunki zwolnienia z uwagi na cele gospodarstwa domowego[20].

3.3.1 Podmioty opracowujące aplikacje

Podmioty opracowujące aplikacje tworzą aplikacje lub udostępniają je użytkownikom końcowym. Kategoria te obejmuje organizacje sektora prywatnego i publicznego, które zlecają na zewnątrz opracowanie aplikacji, a także te przedsiębiorstwa oraz osoby fizyczne budujące i tworzące aplikacje. Opracowują one lub tworzą oprogramowanie, które będzie funkcjonowało na smartfonach, i w ten sposób decydują o zakresie, w jakim dana aplikacja będzie uzyskiwała dostęp do różnych kategorii danych osobowych na urządzeniu lub poprzez zdalne zasoby obliczeniowe (jednostki obliczeniowe podmiotów opracowujących aplikacje lub osób trzecich) oraz przetwarzała te dane.

W zakresie, w jakim podmiot opracowujący aplikacje określa cele i sposoby przetwarzania danych osobowych na urządzeniach inteligentnych, jest on administratorem danych jak określono w art. 2 lit. d) dyrektywy o ochronie danych. W takim przypadku musi on przestrzegać przepisów całej dyrektywy o ochronie danych. Kluczowe przepisy wyjaśniono w pkt 3.4-3.10 niniejszej opinii.

---

[17] Grupa Robocza stosuje powszechną terminologię podmiotów opracowujących aplikacje, jednak podkreśla, że przedmiotowy termin nie ogranicza się do programistów lub podmiotów opracowujących aplikacje pod względem technologicznym, ale obejmuje właścicieli aplikacji, to jest przedsiębiorstwa i organizacje, które zlecają opracowywanie aplikacji oraz określają ich cele.

[18] W niektórych przypadkach producent systemu operacyjnego pokrywa się z producentem urządzenia, podczas gdy w innych wypadkach producentem urządzenia jest inne przedsiębiorstwo niż producent systemu operacyjnego.

[19] Zob. sprawy Trybunału Sprawiedliwości, sprawa C-101/01 Postępowanie karne przeciwko Bodil Lindqvist, wyrok z dnia 6 listopada 2003 r. oraz sprawa C-73/07 Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy i Satamedia Oy, wyrok z dnia 16 grudnia 2008 r.

[20] Zob. Opinia 5/2009 w sprawie portali społecznościowych Grupy Roboczej Art. 29 (czerwiec 2009 r.) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_pl.pdf#h2-5.

Nawet jeżeli do użytkownika ma zastosowanie zwolnienie z uwagi na cele gospodarstwa domowego, podmiot opracowujący aplikacje w dalszym ciągu jest odpowiedzialny jako administrator danych, jeżeli przetwarza dane do swoich własnych celów. Ma to na przykład znaczenie, kiedy aplikacja wymaga dostępu do całej książki adresowej, aby świadczyć daną usługę (komunikatory internetowe, połączenia telefoniczne, połączenia wideo).

Odpowiedzialność podmiotu opracowującego aplikacje będzie znacząco ograniczona, jeżeli żadne dane osobowe nie są przetwarzane lub udostępniane na zewnątrz urządzenia, lub jeżeli podmiot opracowujący aplikacje podjął stosowne środki techniczne i organizacyjne w celu nieodwracalnego zanonimizowania danych oraz zagregowania ich na samym urządzeniu, zanim jakiekolwiek dane zostaną przesłane z tego urządzenie.

W każdym przypadku, jeżeli podmiot opracowujący dane uzyskuje dostęp do informacji przechowywanych na urządzeniu, ma zastosowanie również dyrektywa o prywatności i łączności elektronicznej i podmiot opracowujący dane musi przestrzegać wymagania wyrażenia zgody przewidzianego w art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej.

W zakresie, w jakim podmiot opracowujący dane zleca na zewnątrz część lub całość faktycznego przetwarzania danych osobie trzeciej, oraz w zakresie, w jakim ta osoba trzecia przyjmuje rolę przetwarzającego, podmiot opracowujący aplikacje musi przestrzegać wszystkich zobowiązań związanych ze korzystaniem z usług przetwarzającego. Obejmuje to również korzystanie z usług dostawcy przetwarzania danych w chmurze obliczeniowej (np. w celu przechowywania danych na zewnątrz)[21].

W zakresie, w jakim podmiot opracowujący aplikacje zezwala na dostęp do danych użytkowników osobom trzecim (takim jak dostawcy reklam uzyskujący dostęp do danych geolokalizacyjnych urządzenia w celu dostarczania reklamy behawioralnej), musi on stosować odpowiednie mechanizmy w celu przestrzegania wymagań mających zastosowanie na podstawie ram prawnych UE. Jeżeli osoba trzecia uzyskuje dostęp do danych przechowywanych na urządzeniu, ma zastosowanie obowiązek uzyskania świadomej zgody określonej w art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej. Ponadto, jeżeli osoba trzecia przetwarza dane osobowe do swoich własnych celów, może ona być również współadministratorem danych wraz z podmiotem opracowującym aplikacje i w związku z tym musi zapewnić przestrzeganie zasady ograniczenia celu oraz obowiązków dotyczących zachowania bezpieczeństwa[22] w odniesieniu do części przetwarzania, dla której określa ona cele i środki. Ponieważ między podmiotami opracowującymi dane a osobami trzecimi mogą istnieć różne rodzaje uzgodnień, zarówno handlowych, jak i technicznych, stosowną odpowiedzialność każdej ze stron należy ustalać odrębnie dla każdego przypadku, uwzględniając szczególne okoliczności przedmiotowego przetwarzania.

---

[21] Zob. Opinia 05/2012 na temat przetwarzania danych w chmurze obliczeniowej Grupy Roboczej Art. 29 (lipiec 2012 r.), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_pl.pdf#h2-5.

[22] Zob. Opinia 2/2010 w sprawie internetowej reklamy behawioralnej Grupy Roboczej Art. 29 (czerwiec 2010 r.), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_pl.pdf#h2-5 oraz Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający" Grupy Roboczej Art. 29 (luty 2010 r.), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_pl.pdf#h2-5.

Podmiot opracowujące aplikacje może korzystać z bibliotek osoby trzeciej za pomocą oprogramowania oferującego powszechne funkcje, takie jak na przykład biblioteka dla społecznościowej platformy gier. Podmiot opracowujący dane musi dopilnować, aby użytkownicy wiedzieli o każdym przetwarzaniu danych dokonywanym przez takie biblioteki, oraz aby takie przetwarzanie danych było zgodne z ramami prawnymi UE, w tym w stosownych przypadkach, poprzez uzyskanie zgody użytkownika. W tym sensie podmioty opracowujące aplikacje musza zapobiegać korzystaniu z funkcji, które są ukryte przed użytkownikiem.

3.3.2 Producenci systemów operacyjnych i urządzeń

Producentów systemów operacyjnych i urządzeń również należy uznać za administratorów (i w stosownych przypadkach, jako współadministratorów) w odniesieniu do wszelkich danych osobowych przetwarzanych do ich własnych celów, takich jak sprawne funkcjonowanie urządzenia, bezpieczeństwo itp. Obejmuje to dane generowane przez użytkownika (np. dane o użytkowniku podane przy rejestracji), dane generowane automatycznie przez urządzenie (np. jeżeli urządzenie posiada funkcję nawiązywania połączenia z producentem pozwalającą na ustalenie jego lokalizacji) lub dane osobowe przetwarzane przez producenta systemu operacyjnego lub urządzenia wynikające z instalacji lub korzystania z aplikacji. W przypadku, gdy producent systemu operacyjnego lub urządzenia zapewnia dodatkową funkcję, taką jak kopia zapasowa lub zdalne ustalanie lokalizacji obiektu, jest on również administratorem danych osobowych przetwarzanych w tym celu.

Aplikacje wymagające dostępu do geolokalizacji muszą korzystać z usług lokalizacyjnych systemu operacyjnego. Gdy aplikacja wykorzystuje geolokalizację, system operacyjny może gromadzić dane osobowe w celu dostarczenia informacji geolokalizacyjnych do aplikacji oraz może skorzystać z tych danych w celu poprawy własnych usług lokalizacyjnych. Do tego ostatniego celu system operacyjny jest również administratorem.

Producent systemu operacyjnego i urządzenia jest również odpowiedzialny za interfejs programowania aplikacji (API) umożliwiający przetwarzanie danych osobowych przez aplikacje na urządzeniu inteligentnym. Podmiot opracowujący aplikacje może uzyskiwać dostęp do tych właściwości i funkcji, które producenci systemów operacyjnych i urządzeń udostępniają poprzez interfejsy programowania aplikacji. Ponieważ producenci systemów operacyjnych i urządzeń określają sposoby (i zakres) uzyskiwania dostępu do danych osobowych, muszą zapewnić podmiotom opracowującym aplikacje wystarczającą przesiewowość kontroli, tak aby dostępu udzielano jedynie do tych danych, które są niezbędne do funkcjonowania aplikacji. Producenci systemów operacyjnych i urządzeń powinni również zapewnić możliwość cofnięcia tego dostępu w prosty i skuteczny sposób.

Koncepcja „uwzględnienia ochrony prywatności już w fazie projektowania" jest ważną zasadą, do której pośrednio odniesiono się w dyrektywie o ochronie danych[23] i którą wraz z „domyślną ochroną prywatności" jaśniej określono w dyrektywie o prywatności i łączności elektronicznej[24]. Wymaga ona od producentów urządzenia lub aplikacji uwzględnienia ochrony danych od samego początku ich projektowania. Uwzględnienie ochrony prywatności już w fazie projektowania jest wyraźnie wymagane w odniesieniu do projektowania sprzętu telekomunikacyjnego zgodnie z dyrektywą w sprawie urządzeń radiowych i końcowych

[23] Zob. motyw 46 i art. 17.
[24] Zob. art. 14 ust. 3.

urządzeń telekomunikacyjnych[25]. W związku z tym na producentach systemów operacyjnych i urządzeń oraz sklepach z aplikacjami ciąży istotna odpowiedzialność za zapewnienie zabezpieczeń w celu ochrony danych osobowych i prywatności użytkowników aplikacji. Obejmuje to zapewnienie dostępności stosownych mechanizmów mających na celu informowanie i edukowanie użytkowników końcowych o tym, co mogą robić aplikacje oraz do jakich danych mogą uzyskiwać dostęp, a także zapewnienie stosownych ustawień, aby użytkownicy aplikacji mogli zmienić parametry przetwarzania[26].

3.3.3 Sklepy z aplikacjami

Każde z najpowszechniej wykorzystywanych urządzeń inteligentnych posiada własny sklep z aplikacjami i często ma miejsce sytuacja, w której konkretny system operacyjny jest głęboko zintegrowany z konkretnym sklepem z aplikacjami. Sklepy z aplikacjami często przetwarzają płatności z góry za aplikacje oraz mogą również wspierać zakupy w ramach aplikacji i w ten sposób wymagać rejestracji użytkownika z podaniem danych dotyczących jego nazwiska, adresu i danych finansowych. Wspomniane dane (bezpośrednio) możliwe do identyfikacji mogą być połączone z danymi dotyczącymi zachowania przy zakupie i korzystaniu oraz z danymi odczytanymi z urządzenia lub generowanymi przez nie (takimi jak niepowtarzalne kody identyfikacyjne). W przypadku przetwarzania takich danych osobowych sklepy z aplikacjami prawdopodobnie będą administratorami danych, w tym, gdy przekazują takie informacje z powrotem podmiotom opracowującym aplikacje. W przypadku, gdy sklep z aplikacjami przetwarza aplikacje pobrane przez użytkownika lub historię stosowania, lub podobne funkcje mające na celu przywrócenie wcześniej pobranych aplikacji, musi on być również administratorem przetwarzanych w tym celu danych osobowych.

Sklep z aplikacjami zapisuje dane logowania oraz historię wcześniej zakupionych aplikacji. Wymaga również od użytkownika podania numeru karty kredytowej, który będzie przechowywany na koncie użytkownika. Sklep z aplikacjami jest administratorem w odniesieniu do tych operacji.

Z drugiej strony może okazać się, że strony internetowe, które pozwalają na pobieranie aplikacji do zainstalowania na urządzeniu bez żadnego uwierzytelnienia, nie przetwarzają żadnych danych osobowych.

Ze względu na swoją pozycję, sklepy z aplikacjami odgrywają istotną rolę w umożliwianiu podmiotom opracowującym aplikacje dostarczanie odpowiednich informacji o aplikacji, w tym o rodzajach danych, jakie aplikacja może przetwarzać, oraz w jakich celach. Sklepy z aplikacjami mogą wdrażać przedmiotowe zasady poprzez swoją politykę przyjmowania (opartą na kontrolach *ex ante* lub *ex post*). We współpracy z producentem systemu operacyjnego sklep z aplikacjami może opracować ramy w celu umożliwienia podmiotom

[25] Dyrektywa 1999/5/WE z dnia 9 marca 1999 r. w sprawie urządzeń radiowych i końcowych urządzeń telekomunikacyjnych oraz wzajemnego uznawania ich zgodności. Dz.U. L 91, z 7.4.1999, s. 10. Art. 3 ust. 3 lit. c) stanowi, że Komisja Europejska może zdecydować, że urządzenia użytkowników końcowych mają być tak skonstruowane, aby miały wbudowane systemy zabezpieczające w celu zapewnienia ochrony danych osobowych i prywatności subskrybenta.

[26] Grupa Robocza z zadowoleniem przyjmuje zalecenia Federalnej Komisji Handlu w tym względzie, przedstawione w sprawozdaniu służb „Mobile Privacy Disclosures", o którym mowa w przypisie 6 powyżej, na przykład na s. 15: „(…) platformy znajdują się w wyjątkowej pozycji umożliwiającej zapewnianie spójnego ujawniania we wszystkich aplikacjach i są zachęcane do postępowania w ten sposób. Zgodnie z uwagami z warsztatów, mogą one również uznawać dokonywanie przedmiotowych ujawnień w wielu punktach w czasie (…)".

opracowującym aplikacje przekazywania spójnych i znaczących powiadomień informacyjnych (takich jak symbole przedstawiające pewne rodzaje dostępu do danych sensorycznych) oraz wyświetlanie ich w widocznym miejscu w katalogu sklepu z aplikacjami.

3.3.4 Osoby trzecie

Istnieje wiele różnych osób trzecich zaangażowanych w przetwarzanie danych poprzez korzystanie z aplikacji.

Przykładowo wiele darmowych aplikacji jest opłacanych z reklam, które mogą być między innymi reklamą kontekstową lub zindywidualizowaną, możliwą dzięki usługom śledzenia, takim jak pliki *cookie* lub inne kody identyfikacyjne wyrobu. Reklama może składać się z bannera wewnątrz aplikacji, reklam poza aplikacją zapewnianym przez modyfikację ustawień przeglądarki lub umieszczania ikon na mobilnych stacjach roboczych lub dostarczanych poprzez zindywidualizowaną zawartość aplikacji (np. sponsorowane wyniki wyszukiwania).

Reklamy dla aplikacji są zasadniczo zapewniane przez sieci reklamowe i podobnych pośredników, który mogą być związani z producentem systemu operacyjnego lub ze sklepem z aplikacjami lub mogą stanowić ten sam podmiot, co oni. Jak określono w opinii 2/2010[27] Grupy Roboczej Art. 29 reklama internetowa często pociąga za sobą przetwarzanie danych osobowych zgodnie z tym, co określono w art. 2 dyrektywy o ochronie danych i zgodnie z wykładnią przedstawionej przez Grupę Roboczą Art. 29[28].

Innymi przykładami osób trzecich są dostawcy usług analitycznych i dostawcy usług łączności. Dostawcy usług analitycznych umożliwiają podmiotom opracowującym aplikacje zyskanie wglądu w stosowanie, popularność i używalność ich aplikacji. Dostawcy usług łączności[29] również mogą odgrywać ważną rolę w określaniu domyślnych ustawień i aktualizacji zabezpieczeń wielu urządzeń oraz mogą przetwarzać dane o wykorzystywaniu aplikacji. Ich personalizacja („marka") może mieć konsekwencje w odniesieniu do ewentualnych środków technicznych i funkcjonalnych, jakie może zastosować użytkownik w celu ochrony swoich danych osobowych.

W porównaniu do podmiotów opracowujących aplikacje osoby trzecie mogą odgrywać dwa rodzaje ról: jedną z nich jest wykonywanie operacji dla właściciela aplikacji, na przykład świadczenie usług analitycznych w ramach aplikacji. W takim przypadku, kiedy działają one wyłącznie w imieniu właściciela aplikacji i nie przetwarzają danych do swoich własnych celów ani nie wymieniają danych z podmiotami opracowującymi, prawdopodobnie działają jako przetwarzający.

Druga rola polega na gromadzeniu informacji ze wszystkich aplikacji w celu świadczenia dodatkowych usług: zapewnianiu danych liczbowych z zakresu analizy na większą skalę (popularność aplikacji, zindywidualizowane rekomendacje) lub unikanie wyświetlania tej

---

[27] Opinia 2/2010 w sprawie internetowej reklamy behawioralnej Grupy Roboczej Art. 29 (czerwiec 2010 r.), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_pl.pdf#h2-5.

[28] Zob. również interpretację pojęcia danych osobowych w opinii 4/2007 w sprawie pojęcia danych osobowych Grupy Roboczej Art. 29 (czerwiec 2007 r.), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_pl.pdf#h2-5.

[29] Dostawców usług łączności obowiązują również sektorowe obowiązki w zakresie ochrony danych, które wykraczają poza zakres niniejszej opinii.

samej reklamy temu samemu użytkownikowi. Kiesy osoby trzecie przetwarzają dane osobowe do swoich własnych celów, działają jak administratorzy i w związku z tym muszą przestrzegać wszystkich mających zastosowanie przepisów dyrektywy o ochronie danych[30].W przypadku reklamy behawioralnej administrator musi uzyskać ważną zgodę użytkownika na gromadzenie i przetwarzanie danych osobowych, składających się przykładowo z analizy i kombinacji danych osobowych, oraz tworzenia lub wykorzystywania profili. Jak wcześniej wyjaśniła Grupa Robocza Art. 29 w opinii 2/2012 w sprawie internetowej reklamy behawioralnej taką zgodę najlepiej uzyskać stosując mechanizmy uprzedniego wyrażenia zgody.

Przedsiębiorstwo zapewnia właścicielom aplikacji i reklamodawcom wskaźniki poprzez stosowanie instalacji śledzenia wbudowanych w aplikacje przez podmiot opracowujący aplikację. W związku z tym instalacje śledzenia należące do danego przedsiębiorstwa można zainstalować na wielu aplikacjach i urządzeniach. Jedną z jej usług jest informowanie podmiotów opracowujących aplikacje o innych aplikacjach wykorzystywanych przez danego użytkownika, poprzez ściąganie niepowtarzalnego kodu identyfikacyjnego. Przedsiębiorstwo określa środki (tj. instalacje śledzenia) i cele swoich narzędzi przed zaoferowaniem ich podmiotom opracowującym aplikacje, reklamodawcom i innym podmiotom, a zatem działa jako administrator.

W zakresie, w jakim osoby trzecie uzyskują dostęp lub przechowują informacje na urządzeniu inteligentnym, muszą one przestrzegać wymagania wyrażenia zgody określonego w art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej.

W tym kontekście ważne jest odnotowanie, że użytkownicy mają zasadniczo ograniczone możliwości w zakresie instalowania na urządzeniach inteligentnych oprogramowania, które kontrolowałoby przetwarzanie danych osobowych, co jest powszechne w środowisku internetowym opartym na stacjach roboczych. Jako alternatywa dla wykorzystywania plików *cookie* HTTP osoby trzecie często uzyskują dostęp do niepowtarzalnych kodów identyfikacyjnych w celu wyodrębnienia (grup) użytkowników i świadczenia na ich rzecz ukierunkowanych usług, w tym reklam. Ponieważ użytkownicy nie mogą usunąć lub zmienić wielu z tych kodów identyfikacyjnych (takich jak IMEI, IMSI, MSISDN[31] oraz specyficznych niepowtarzalnych kodów identyfikacyjnych wyrobu), wspomniane osoby trzecie mają potencjał do przetwarzania znaczących ilości danych osobowych bez kontroli sprawowanej przez użytkownika końcowego.

[30] Opinia 2/2010 w sprawie internetowej reklamy behawioralnej Grupy Roboczej Art. 29, s. 10–11.
[31] Cyfrowa sieć usług zintegrowanych na stacje ruchome.

3.4 Podstawa prawna

W celu przetworzenia danych osobowych wymagana jest podstawa prawna, jak wymieniono w art. 7 dyrektywy o ochronie danych. W art. 7 wyróżniono sześć różnych podstaw prawnych przetwarzania danych: jednoznacznie udzielona zgoda osoby, której dane dotyczą; konieczność przetwarzania w celu realizacji umowy z osobą, której dane dotyczą; ochrona istotnych interesów osoby, której dane dotyczą; konieczność przetwarzania w celu zapewnienia zgodności z obowiązkiem prawnym; (w odniesieniu do organów publicznych) konieczność przetwarzania w celu realizacji zadania wykonywanego w interesie publicznym i konieczność przetwarzania ze względu na uzasadnione interesy (związane z działalnością gospodarczą).

W odniesieniu do przechowywania informacji lub uzyskiwania dostępu do informacji przechowywanych już w urządzeniu inteligentnym w art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej (zawierającym wymóg uzyskania zgody na umieszczenie w urządzeniu i pozyskanie informacji z urządzenia) określono bardziej szczegółowe ograniczenie podstawy prawnej, którą można uwzględnić.

3.4.1 Zgoda poprzedzająca instalację i przetwarzanie danych osobowych

W przypadku aplikacji główną podstawą prawną mającą zastosowanie jest zgoda. Przy instalacji aplikacji informacje są umieszczane na urządzeniu użytkownika końcowego. Wiele aplikacji korzysta także z dostępu do danych przechowywanych na urządzeniu, kontaktów w książce adresowej, obrazów, filmów i innych osobistych dokumentów. We wszystkich tych przypadkach zgodnie z art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej wymaga się zgody użytkownika oraz zapewnienia jasnych i wyczerpujących informacji przed umieszczeniem informacji w urządzeniu i ich pozyskaniem z urządzenia.

Należy zauważyć różnicę pomiędzy zgodą wymaganą na umieszczenie jakichkolwiek informacji w urządzeniu i odczyt informacji z urządzenia a zgodą wymaganą do posiadania podstawy prawnej na przetwarzanie różnych rodzajów danych osobowych. Chociaż oba wymogi dotyczące zgody mają zastosowanie jednocześnie, każdy w oparciu o inną podstawę prawną, oba podlegają warunkom, zgodnie z którymi zgoda musi być dobrowolna, konkretna i świadoma (zgodnie z definicją zawartą w art. 2 lit. h) dyrektywy o ochronie danych). W związku z tym obydwa rodzaje zgody można w praktyce połączyć podczas instalacji albo zanim aplikacja zacznie zbierać dane osobowe z urządzenia, pod warunkiem, że użytkownikowi uświadomiono jednoznacznie, na co wyraża zgodę.

Wiele sklepów z aplikacjami zapewnia podmiotom opracowującym aplikacje możliwość informowania użytkowników końcowych o podstawowych właściwościach aplikacji przed instalacją i wymaga działania potwierdzającego ze strony użytkownika przed pobraniem i instalacją aplikacji (tj. naciśnięcie przycisku „instaluj”). Podczas gdy działanie takie może w pewnych okolicznościach spełniać wymaganie wyrażenia zgody zawarte w art. 5 ust. 3, prawdopodobnie nie może ono zapewnić wystarczających informacji, aby stanowiło ważne wyrażenie zgody na przetwarzanie danych osobowych. Zagadnienie to zostało uprzednio omówione przez Grupę Roboczą Art. 29 w opinii 15/2011 w sprawie definicji zgody[32].

[32] Opinia 15/2011 w sprawie definicji zgody Grupy Roboczej Art. 29 (lipiec 2011 r.), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_pl.pdf#h2-5.

W kontekście urządzeń inteligentnych zgoda „dobrowolna” oznacza, że użytkownik musi mieć możliwość zaakceptować lub odrzucić przetwarzanie danych osobowych. W związku z tym, jeżeli aplikacja ma przetwarzać dane osobowe, użytkownik musi mieć swobodę zaakceptowania lub odrzucenia tego przetwarzania. Użytkownik nie powinien być stawiany w sytuacji, w której na ekranie pojawia się jedynie wariant umożliwiający zakończenie instalacji, czyli „Tak, akceptuję”. Musi być dostępny wariant „Anuluj” lub inny sposób wstrzymania instalacji.

Zgoda „świadoma” oznacza, że osoba, której dane dotyczą, musi posiadać do swojej dyspozycji niezbędne informacje w celu dokonania dokładnej oceny[33].W celu uniknięcia wszelkiej dwuznaczności informacje muszą być udostępnione przed przetworzeniem jakichkolwiek danych osobowych. Uwzględnia to także przetwarzanie danych, które mogło mieć miejsce podczas instalacji, np. na potrzeby diagnostyki lub śledzenia. Zawartość i formę takich informacji omówiono w pkt 3.7 niniejszej opinii.

Zgoda „konkretna” oznacza, że oświadczenie woli musi odnosić się do przetwarzania szczególnej pozycji danych lub ograniczonej kategorii przetwarzania danych. Z tego powodu naciśnięcia przycisku „instaluj” nie można uznać za ważne wyrażenie zgody na przetwarzanie danych osobowych, ponieważ zgoda nie może być ogólnie sformułowanym upoważnieniem. W niektórych przypadkach istnieje możliwość, by użytkownicy udzielali szczegółowej zgody, gdy zgoda jest potrzebna dla każdego rodzaju danych, do których aplikacja ma uzyskać dostęp[34].Takie podejście spełnia dwa ważne wymagania prawne - po pierwsze, odpowiednie poinformowanie użytkownika o ważnych elementach usługi oraz, po drugie, zapytanie o konkretną zgodę w odniesieniu do każdego z elementów[35]. Alternatywne podejście, w którym podmiot opracowujący aplikacje wymaga od użytkowników zaakceptowania obszernego zbioru warunków lub obszernej polityki prywatności nie stanowi konkretnej zgody[36].

Pojęcie zgody konkretnej odnosi się także do praktyki śledzenia zachowania użytkowników przez reklamodawców lub jakąkolwiek inną osobę trzecią. Ustawienia domyślne zapewniane przez systemy operacyjne i aplikacje nie mogą zawierać jakiejkolwiek funkcji śledzenia, aby umożliwić użytkownikom wyrażenie konkretnej zgody na ten rodzaj przetwarzania danych. Wspomniane ustawienia domyślne nie mogą być obchodzone przez osoby trzecie, jak to często ma obecnie miejsce w przypadku mechanizmów „Nie śledź” umieszczonych w przeglądarkach.

---

[33] *Idem* s. 19.

[34] Szczegółowa zgoda oznacza, że osoby mogą drobiazgowo (konkretnie) kontrolować funkcje przetwarzania danych osobowych oferowane przez aplikację i decydować, które z nich chcą włączyć.

[35] Konieczność takiej szczegółowej zgody potwierdziły także służby Federalnej Komisji Handlu w swoim najnowszych sprawozdaniu (przypis 6 powyżej), s. 15–16 : „[...] platformy powinny uwzględnić zapewnienie ujawnień »dokładnie na czas« i uzyskanie natychmiastowej potwierdzającej zgody na gromadzenie innej zawartości, którą wielu konsumentów uznałoby za szczególnie chronioną w wielu kontekstach, takiej jak fotografie, kontakty, pozycje w kalendarzu, nagrania zawartości audio lub video”.

[36] *Idem*, s. 34–35: „Ogólna zgoda bez dokładnego wskazania celu przetwarzania danych, na które osoba, które dane dotyczą, zgadza się nie spełnia tego wymogu. Oznacza to, że informacje dotyczące celu przetwarzania nie mogą być zawarte w postanowieniach ogólnych, lecz w osobnej klauzuli dotyczącej zgody”.

Przykłady konkretnej zgody

Aplikacja udziela informacji na temat pobliskich restauracji. Aby możliwa była jej instalacja, podmiot opracowujący aplikacje musi uzyskać zgodę. Aby uzyskać dostęp do danych geolokalizacyjnych, podmiot opracowujący aplikacje musi osobno prosić o zgodę, np. podczas instalacji lub przed uzyskaniem dostępu do geolokalizacji.
Konkretna zgoda oznacza, że zgoda musi być ograniczona do konkretnego celu polegającego na poinformowaniu użytkownika o pobliskich restauracjach. Dostęp do danych dotyczących lokalizacji z urządzenia można w związku z tym uzyskać jedynie, gdy użytkownik wykorzystuję aplikację w tym celu. Zgoda użytkownika na przetwarzania danych geolokalizacyjnych nie stanowi pozwolenia dla aplikacji na ciągłe gromadzenie danych dotyczących lokalizacji z urządzenia. Dalsze przetwarzanie tego rodzaju wymaga dodatkowych informacji i osobnej zgody.

Podobnie, aby aplikacja komunikacyjna mogła uzyskać dostęp do listy kontaktów, użytkownik musi mieć możliwość wybrania kontaktów, z którymi chce się skomunikować, zamiast udzielać dostępu do całej książki adresowej (w tym danych kontaktowych osób niebędących użytkownikami usługi, które nie mogły wyrazić zgody na przetwarzanie danych ich dotyczących).

Należy zauważyć, że nawet gdy zgoda spełnia trzy warunki opisane powyżej, to nie stanowi ona jednak pozwolenia na przetwarzanie nieuczciwe i niezgodne z prawem. Jeżeli cel przetwarzania danych jest nadmierny lub nieproporcjonalny, nawet jeżeli użytkownik wyraził zgodę, podmiot opracowujący aplikacje nie będzie miał ważnej podstawy prawnej i prawdopodobnie naruszy przepisy dyrektywy o ochronie danych.

Przykład nadmiernego i niezgodnego z prawem przetwarzania danych

Aplikacja budzika oferuje dodatkową właściwość, za pomocą której użytkownik może wydać komendę głosową, aby uciszyć budzik lub wprowadzić go w tryb „drzemki". W tym przykładzie zgoda na nagrywanie będzie ograniczona do czasu, w którym budzik wydaje dźwięki. Wszelkie monitorowanie, zapisywanie lub nagrywanie dźwięku w czasie, gdy budzik nie dzwoni, zostałoby prawdopodobnie uznane za nadmierne lub niezgodne z prawem.

W przypadku aplikacji zainstalowanych na urządzeniu domyślnie (zanim użytkownik końcowy stał się właścicielem) lub innego przetwarzania dokonywanego przez system operacyjny, które opiera się na zgodzie jako podstawie prawnej, administratorzy muszą starannie rozważyć, czy zgoda jest rzeczywiście ważna. W wielu przypadkach należy uwzględnić osobny mechanizm udzielania zgody, być może przy pierwszym uruchomieniu aplikacji, w celu umożliwienia administratorowi pełnego poinformowania użytkownika końcowego. Gdy dane należą do szczególnych kategorii danych określonych w art. 8 dyrektywy o ochronie danych, zgoda musi być wyraźna.

Ponadto użytkownicy muszą mieć możliwość wycofania swojej zgody w prosty i skuteczny sposób. Kwestię tę omówiono w sekcji 3.8 niniejszej opinii.

3.4.2 Podstawa prawna przetwarzania danych podczas korzystania z aplikacji

Jak wyjaśniono powyżej, zgoda jest konieczną podstawą prawną pozwalającą podmiotowi opracowującemu aplikacje na zgodne z prawem odczytywanie lub zapisywanie informacji, a w konsekwencji na przetwarzanie danych osobowych. W następnym etapie podczas korzystania z aplikacji podmiot opracowujący aplikacje może powołać się na inne podstawy

prawne w odniesieniu do innych rodzajów przetwarzania danych, o ile nie dotyczy to przetwarzania szczególnie chronionych danych osobowych.

Wspomniane podstawy prawne mogą być konieczne do realizacji umowy z osobą, której dane dotyczą, lub konieczne dla uzasadnionych interesów (związanych z działalnością gospodarczą) (art. 7 lit. b) i f) dyrektywy o ochronie danych.

Wspomniane podstawy prawne są ograniczone do przetwarzania danych, które nie są danymi szczególnie chronionymi konkretnego użytkownika, i w związku z tym można się na nie powołać jedynie w zakresie, w jakim określone przetwarzanie danych jest ściśle konieczne do wykonania wybranej usługi lub, w przypadku art. 7 lit. f), jedynie gdy takie interesy nie są podporządkowane interesom związanym z podstawowymi prawami i wolnościami osoby, której dane dotyczą.

Przykłady umownej podstawy prawnej

Użytkownik wyraża zgodę na instalację aplikacji mobilnej bankowości. W celu wykonania wniosku o dokonanie płatności bank nie musi pytać o osobną zgodę użytkownika na ujawnienie jego imienia i nazwiska oraz numeru rachunku bankowego odbiorcy płatności. Ujawnienie to jest ściśle konieczne w celu wykonania umowy z tym konkretnym użytkownikiem i w związku z tym bank posiada podstawę prawną w art. 7 lit. b) dyrektywy o ochronie danych. To samo rozumowanie ma zastosowanie do aplikacji komunikacyjnych; gdy dostarczają one istotnych informacji, takich jak nazwa rachunku, adres e-mail lub numer telefonu, innej osobie, z którą użytkownik chce się skomunikować, ujawnienie jest w sposób oczywisty konieczne do wykonania umowy.

3.5 Ograniczenie celu i minimalizacja danych

Fundamentalnymi zasadami będącymi podstawą dyrektywy o ochronie danych są ograniczenie celu i minimalizacja danych. Ograniczenie celu umożliwia użytkownikom podjęcie świadomej decyzji o powierzeniu danej stronie swoich danych osobowych, ponieważ dowiedzą się oni, w jaki sposób ich dane są wykorzystywane i będą mogli oprzeć się na opisie ograniczonego celu, by zrozumieć, w jakim celu ich dane zostaną wykorzystane. Cele przetwarzania danych muszą w związku z tym być dobrze opisane i zrozumiałe dla przeciętnego użytkownika nieposiadającego wiedzy specjalistycznej z zakresu prawa lub techniki.

Jednocześnie ograniczenie celu wymaga, aby podmioty opracowujące aplikacje znały dobrze swoją działalność gospodarczą w ogólnych zarysach, zanim rozpoczną gromadzenie danych osobowych od użytkowników. Dane osobowe można przetwarzać tylko w takich celach, które zakładają ich rzetelne i zgodne z prawem przetwarzanie (art. 6 ust. 1 dyrektywy o ochronie danych), i cele te muszą być określone przed rozpoczęciem przetwarzania danych.

Zasada ograniczenia celu wyłącza nagłe zmiany głównych warunków przetwarzania.

Na przykład, jeżeli aplikacja pierwotnie miała na celu umożliwienie użytkownikom wysyłanie sobie wzajemnie wiadomości e-mail, lecz podmiot opracowujący aplikacje zdecydował zmienić swój model biznesowy i połączył adresy e-mail swoich użytkowników z numerami telefonów użytkowników innej aplikacji. W takim przypadku odpowiedni administratorzy powinni indywidualnie skontaktować się z wszystkimi użytkownikami i uzyskać ich uprzednią jednoznaczną zgodę w odniesieniu do nowego celu przetwarzania ich danych osobowych.

Ograniczenie celu idzie w parze z zasadą minimalizacji danych. W celu zapobieżenia niekoniecznemu lub potencjalnie niezgodnemu z prawem przetwarzaniu danych podmioty opracowujące aplikacje muszą starannie rozważyć, które dane są ściśle konieczne do wykonania pożądanej funkcji.

Aplikacje mogą uzyskiwać dostęp do wielu funkcji urządzenia i z związku z tym są zdolne do robienia wielu rzeczy, w tym wysyłania niewidocznych SMS-ów (*stealth SMS*), uzyskiwania dostępu do obrazów i całej książki adresowej. Wiele sklepów z aplikacjami wspiera (pół)automatyczne aktualizacje, dzięki którym podmiot opracowujący aplikacje może włączyć nowe właściwości i udostępnić je przy minimalnym udziale lub bez udziału użytkownika końcowego.

Grupa robocza podkreśla na tym etapie, że osoby trzecie uzyskujące dostęp do danych użytkowników za pośrednictwem aplikacji muszą przestrzegać zasad ograniczenia celu i minimalizacji danych. Niepowtarzalnych, często niezamienialnych, identyfikatorów urządzeń nie należy stosować w celach reklamowych (ukierunkowanych według zainteresowań) lub analitycznych ze względu na brak możliwości wycofania zgody przez użytkowników. Podmioty opracowujące aplikacje powinny zapewnić zapobieganie niezamierzonemu rozrostowi funkcji poprzez niewprowadzanie zmian w przetwarzaniu podczas przechodzenia z jednej wersji aplikacji na inną bez przedstawienia użytkownikom końcowym właściwych powiadomień z informacjami i zapewnienia im możliwości wycofania się z przetwarzania lub z całej usługi. Użytkownikom należy także zaoferować techniczne możliwości weryfikacji oświadczeń dotyczących zadeklarowanych celów poprzez umożliwienie im dostępu do danych dotyczących przepływu informacji na zewnątrz poprzez aplikację w odniesieniu do przepływu spowodowanego przez użytkownika.

Informacje i kontrola dokonywana przez użytkownika są kluczowymi elementami mającymi na celu zapewnienie poszanowania zasad minimalizacji danych i ograniczenia celu.

Dostęp do podstawowych danych znajdujących się na urządzeniu za pomocą interfejsu programowania aplikacji daje producentom systemów operacyjnych i urządzeń oraz sklepom z aplikacjami możliwość egzekwowania szczegółowych zasad i oferowania użytkownikom końcowym stosownych informacji. Na przykład producenci systemów operacyjnych i urządzeń powinni oferować interfejs programowania aplikacji umożliwiający dokładną kontrolę w celu rozróżnienia każdego rodzaju tych danych i zapewnienia podmiotom opracowującym aplikacje możliwości żądania dostępu jedynie do tych danych, które są ściśle konieczne do (zgodnego z prawem) funkcjonowania ich aplikacji. Rodzaje danych, do których dostępu żąda podmiot opracowujący aplikacje, mogą wtedy być wyraźnie przedstawione w sklepie z aplikacjami, aby poinformować użytkownika przed instalacją.

W tym kontekście kontrola dostępu do danych przechowywanych w urządzeniu opiera się na innych mechanizmach:

a) producenci systemów operacyjnych i urządzeń oraz sklepy z aplikacjami określają **zasady**, które należy stosować, aby można było umieścić aplikacje w danym sklepie z aplikacjami: podmioty opracowujące aplikacje muszą przestrzegać tych zasad lub podjąć ryzyko, że ich aplikacja nie będzie dostępna w tych sklepach[37];
b) **interfejsy programowania aplikacji** systemów operacyjnych określają standardowe metody dostępu do danych przechowywanych na telefonie, do którego aplikacje mają dostęp. Mają one także wpływ na gromadzenie danych po stronie serwera;
c) **kontrole *ex ante*** – wprowadzone kontrole wykonywane przed zainstalowaniem aplikacji[38];
d) **kontrole *ex post*** – kontrole realizowane po zainstalowaniu aplikacji.

3.6 Bezpieczeństwo danych

Zgodnie z art. 17 dyrektywy o ochronie danych administratorzy i przetwarzający muszą podjąć konieczne środki organizacyjne i techniczne, aby zapewnić ochronę przetwarzanych danych osobowych. W wyniku tego środki muszą podjąć wszystkie podmioty zidentyfikowane w sekcji 3.3, każdy zgodnie ze swoją rolą i zakresem odpowiedzialności.

Cel związany z wypełnieniem obowiązku w zakresie bezpieczeństwa jest dwojaki. Umożliwi ona użytkownikom bardziej rygorystyczną kontrolę ich danych oraz zwiększy poziom zaufania do podmiotów faktycznie obsługujących dane użytkowników.

Podmioty opracowujące aplikacje, sklepy z aplikacjami, producenci systemów operacyjnych i urządzeń oraz osoby trzecie w celu wypełnienia swoich odpowiednich obowiązków w zakresie bezpieczeństwa jako administratorzy muszą wziąć pod uwagę zasadę uwzględniania ochrony prywatności już w fazie projektowania i jako opcję domyślną. Wymaga to ciągłej oceny zarówno istniejącego, jak i przyszłego ryzyka w zakresie ochrony danych oraz wdrożenia i oceny skutecznych środków ograniczających ryzyko, w tym minimalizacji danych.

Podmioty opracowujące aplikacje

Istnieje wiele publicznie dostępnych wytycznych dotyczących bezpieczeństwa aplikacji mobilnych publikowanych przez producentów systemów operacyjnych i urządzeń oraz przez niezależne osoby trzecie, np. Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji[39].

Przegląd najlepszych praktyk bezpieczeństwa w opracowywaniu aplikacji znajduje się poza zakresem niniejszej opinii; grupa robocza chciałaby jednak skorzystać z okazji, by dokonać

[37] Urządzenia z usuniętymi ograniczeniami umożliwiają instalację aplikacji poza oficjalnymi sklepami; urządzenia korzystające z systemu operacyjnego Android również pozwalają na instalację aplikacji z innych źródeł.
[38] Ze szczególnym przypadkiem instalacji zainstalowanych fabrycznie.
[39] Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji „Smartphone Secure Development Guideline". http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/smartphone-secure-development-guidelines.

przeglądu tych praktyk, które mogą mieć poważny wpływ na podstawowe prawa użytkowników aplikacji.

Ważną decyzją, którą należy podjąć przed zaprojektowaniem aplikacji jest kwestia miejsca, w którym dane będą przechowywane. W niektórych przypadkach dane użytkownika są przechowywane w urządzeniu, lecz podmioty opracowujące aplikacje mogą wykorzystać także architekturę klient-serwer. Oznacza to, że dane osobowe są przenoszone lub kopiowane do systemów usługodawcy. Przechowywanie i przetwarzanie danych w urządzeniu daje użytkownikom końcowym największą kontrolę nad tymi danymi, np. umożliwiając im usunięcie danych, jeżeli wycofają swoją zgodę na ich przetwarzanie. Bezpieczne przechowywanie danych na zewnątrz może jednak pomóc w odzyskiwaniu danych w następstwie utraty lub kradzieży urządzenia. Możliwe są także metody pośrednie.

Podmioty opracowujące aplikacje muszą zidentyfikować jasno opisaną politykę w zakresie sposobów opracowywania i dystrybucji oprogramowania. Producenci systemów operacyjnych i urządzeń także mają swoją rolę polegającą na promowaniu bezpiecznego przetwarzania danych przez aplikacje, co zostanie omówione poniżej. Ponadto podmioty opracowujące aplikacje i sklepy z aplikacjami muszą opracować i wprowadzić otoczenie sprzyjające bezpieczeństwu wraz z narzędziami zapobiegającymi rozprzestrzenianiu się szkodliwych aplikacji i umożliwiającymi łatwe instalowanie/odinstalowywanie każdej aplikacji.

Dobre praktyki, które można wprowadzić podczas opracowywania aplikacji, uwzględniają minimalizację liczby wierszy i złożoności kodu oraz wdrożenie kontroli w celu wykluczenia możliwości niezamierzonego przeniesienia danych lub narażenia ich integralności. Ponadto wszelkie informacje wejściowe należy zatwierdzać w celu uniemożliwienia przepełnienia buforu lub ataków typu *injection*. Pozostałymi mechanizmami bezpieczeństwa, które warto wymienić, są odpowiednie strategie zarządzania aktualizacjami bezpieczeństwa oraz przeprowadzanie regularnych, niezależnych audytów systemu bezpieczeństwa. Dodatkowo kryteria dotyczące opracowywania aplikacji powinny uwzględniać domyślne wdrożenie zasady przydzielania jak najmniejszych uprawnień, zgodnie z którą aplikacje mogą mieć dostęp jedynie do danych, które są im faktycznie potrzebne, aby udostępnić użytkownikowi daną funkcję. Podmioty opracowujące aplikacje i sklepy z aplikacjami powinny zachęcać użytkowników za pomocą ostrzeżeń do uzupełniania tych dobrych praktyk w zakresie opracowywania pozytywnymi praktykami użytkowników, takimi jak aktualizacja aplikacji do najbardziej aktualnej wersji oraz przypomnienie, by nie stosować tych samych haseł do różnych usług.

Na etapie opracowywania aplikacji podmioty opracowujące aplikacje muszą także podjąć środki mające na celu uniemożliwienie nieautoryzowanego dostępu do danych osobowych poprzez zapewnienie ochrony danych w stosownych przypadkach zarówno podczas przesyłania, jak i przechowywania.

Aplikacje mobilne powinny działać w konkretnych miejscach w pamięci urządzeń (piaskownicach (*sandboxes*)[40]) w celu zmniejszenia konsekwencji działania złośliwego oprogramowania/szkodliwych aplikacji. W bliskiej współpracy z producentami systemów operacyjnych i urządzeń lub sklepami z aplikacjami podmioty opracowujące aplikacje muszą wykorzystywać dostępne mechanizmy w celu umożliwienia użytkownikom sprawdzenia,

[40] Piaskownica jest mechanizmem bezpieczeństwa służącym do oddzielania działających programów.

jakie dane są wykorzystywane przez określone aplikacje, a także selektywnego przyznawania lub pozbawiania uprawnień. Stosowanie funkcji ukrytych nie powinno być dozwolone.

Podmioty opracowujące aplikacje muszą starannie rozważyć metody identyfikacji i uwierzytelniania użytkowników. Nie powinni oni stosować trwałych (związanych z urządzeniem) identyfikatorów, lecz zamiast nich, związane z aplikacją lub tymczasowe identyfikatory urządzeń o niskiej entropii, aby uniknąć śledzenia użytkowników wraz z upływem czasu. Należy uwzględnić sprzyjające prywatności mechanizmy uwierzytelniania. Przy uwierzytelnianiu użytkowników podmioty opracowujące aplikacje muszą skupić się szczególnie na zarządzaniu identyfikatorami użytkowników i hasłami. Hasła muszą być przechowywane w postaci szyfrowanej i bezpiecznie, jako kryptograficzna funkcja skrótu. Udostępnienie użytkownikom testu siły wybranego hasła jest także użyteczną techniką zachęcania do stosowania lepszych haseł (kontrola entropii). W stosownych przypadkach (dostęp do danych szczególnie chronionych, lecz także dostęp do opłaconych zasobów) można przewidzieć ponowne uwierzytelnienie, również za pomocą wielu czynników lub różnych kanałów (np. kodu dostępu wysyłanego za pomocą SMS-a) lub stosowanie danych uwierzytelnienia związanych z użytkownikiem końcowym (zamiast urządzenia). Przy wyborze identyfikatorów sesji należy stosować nieprzewidywalne ciągi, w miarę możliwości w połączeniu z informacjami kontekstowymi, takimi jak data i godzina, lecz także adres IP lub dane globalizacyjne.

Podmioty opracowujące aplikacje powinny mieć także na uwadze wymogi określone w dyrektywie o prywatności i łączności elektronicznej dotyczące naruszeń danych osobowych i konieczności aktywnego informowania użytkowników. Podczas gdy wymogi te mają obecnie zastosowanie jedynie do podmiotów świadczących publicznie dostępne usługi komunikacji elektronicznej, oczekuje się, że obowiązek ten zostanie rozszerzony na wszystkich administratorów (oraz przetwarzających) w drodze przyszłego rozporządzenia o ochronie danych zgodnie z wnioskami Komisji (COM 2012/0011/COD). Takie rozwiązanie zwiększa dodatkowo konieczność posiadania i ciągłej oceny szczegółowego „planu bezpieczeństwa" obejmującego gromadzenie, przechowywanie i przetwarzanie wszelkich danych osobowych w celu zapobiegania występowaniu naruszeń i uniknięcia poważnych kar pieniężnych przewidzianych w takich przypadkach. Plan bezpieczeństwa musi także przewidywać m.in. zarządzanie słabościami oraz terminowe i bezpieczne udostępnianie wiarygodnych wersji bez błędów.

Odpowiedzialność podmiotów opracowujących aplikacje za bezpieczeństwo ich produktów nie kończy się na dostarczeniu na rynek działającej wersji. Aplikacje, jak każde oprogramowanie, mogą zawierać wady i luki w zakresie bezpieczeństwa, a podmioty opracowujące aplikacje muszą opracować poprawki lub aktualizacje, aby zaradzić tym wadom, a także udostępnić je podmiotom, które mogą je udostępnić użytkownikom, lub dokonać tego samodzielnie.

Sklepy z aplikacjami

Sklepy z aplikacjami są ważnym pośrednikiem pomiędzy użytkownikami końcowymi a podmiotami opracowującymi aplikacje i powinny uwzględnić szereg solidnych i skutecznych kontroli aplikacji przed dopuszczeniem ich na rynek. Powinny przedstawiać informacje na temat kontroli, które faktycznie przeprowadzają, a także uwzględnić informacje dotyczące rodzaju przeprowadzanych kontroli zgodności ochrony danych.

Podczas gdy środek ten nie jest w 100 % skuteczny, jeżeli chodzi o eliminację rozprzestrzeniania szkodliwych aplikacji, ze statystyk wynika, że praktyka ta w znacznym stopniu zmniejsza występowanie szkodliwych funkcji w „oficjalnych" sklepach z aplikacjami[41]. Aby poradzić sobie z dużą liczbą dostarczanych codziennie aplikacji, mechanizm ten mógłby zyskać na dostępności automatycznych narzędzi analizy oraz dzięki wdrożeniu kanałów wymiany informacji pomiędzy ekspertami z zakresu bezpieczeństwa oraz specjalistami z zakresu oprogramowania, a także wdrożeniu skutecznych procedur i polityki rozwiązywania zgłoszonych problemów.

Oprócz przeglądu aplikacji przed dopuszczeniem do sprzedaży w sklepie z aplikacjami należy je także objąć mechanizmem wizerunku publicznego. Aplikacje nie powinny być jedynie oceniane przez użytkowników na podstawie tego, jak są „fajne", lecz także na podstawie ich funkcjonalności, ze specjalnym odniesieniem do mechanizmów zachowania prywatności i bezpieczeństwa. Ponadto mechanizmy wizerunku powinny być opracowane w sposób zapobiegający fałszywej ocenie. Mechanizmy kwalifikacji i wizerunku aplikacji mogą być skuteczne w budowaniu wspólnego zaufania pomiędzy różnymi podmiotami, zwłaszcza jeżeli dane są wymieniane przez dużą liczbę osób trzecich.

Sklepy z aplikacjami często wdrażają metodę zdalnego odinstalowania szkodliwych lub niepewnych aplikacji. Mechanizm ten, jeżeli nie został właściwie zaprojektowany, może stanowić utrudnienie w umożliwieniu użytkownikom bardziej rygorystycznej kontroli swoich danych. W związku z tym chroniący prywatność sposób odinstalowania aplikacji przez sklep z aplikacjami powinien być oparty na informowaniu i zgodzie użytkownika. Ponadto, z bardziej praktycznego punktu widzenia, kanały informacji zwrotnych powinny zostać udostępnione użytkownikom w celu zgłaszania problemów bezpieczeństwa związanych z ich aplikacjami oraz zgłaszania skuteczności jakiejkolwiek procedury zdalnego usuwania.

Podobnie jak podmioty opracowujące aplikacje sklepy z aplikacjami powinny być świadome przyszłych zobowiązań dotyczących powiadomień o naruszeniu danych osobowych oraz współpracować z podmiotami opracowującymi aplikacje w celu zapobiegania takim naruszeniom.

Producenci systemów operacyjnych i urządzeń

Producenci systemów operacyjnych i urządzeń są także ważną stroną w określeniu norm minimalnych i najlepszych praktyk wśród podmiotów opracowujących aplikacje, nie tylko w zakresie bezpieczeństwa podstawowego oprogramowania oraz interfejsów programowania aplikacji, lecz także w zakresie udostępnianych narzędzi, wytycznych i materiałów referencyjnych. Producenci systemów operacyjnych i urządzeń powinni udostępnić solidne i dobrze znane algorytmy szyfrowania i wspierać odpowiednie długości klucza. Powinni także udostępnić podmiotom opracowującym aplikacje solidne i bezpieczne mechanizmy uwierzytelniania (np. stosowanie certyfikatów poświadczonych przez zaufane organy certyfikacji w celu uwierzytelnienia zdalnego zasobu). Umożliwi to, by podmioty opracowujące aplikacje uniknęły konieczności tworzenia własnych mechanizmów

[41] „Hey, You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets", Y Zhou i in., Network and Distributed System Security Symposium (NDSS) 2012 r.

uwierzytelniania. W praktyce jest to często słabo wdrażane i może stanowić poważną słabość[42].

Dostępem do danych osobowych i ich przetwarzaniem przez aplikacje należy zarządzać za pomocą klas wbudowanych w interfejs programowania aplikacji i metod umożliwiających właściwe kontrole i zabezpieczenia. Producenci systemów operacyjnych i urządzeń powinni dopilnować, aby metody i funkcje umożliwiające aplikacjom dostęp do danych osobowych zawierały właściwości mające na celu wdrożenie wniosków o szczegółową zgodę. Podobnie należy podjąć działania mające na celu wyłączenie lub ograniczenie dostępu do danych osobowych poprzez wykorzystanie funkcji niskiego poziomu lub innych środków, które mogą posłużyć do obchodzenia kontroli i zabezpieczeń wbudowanych w interfejs programowania aplikacji.

Producenci systemów operacyjnych muszą także opracować wyraźne ścieżki audytu w urządzeniach, tak aby użytkownicy końcowi mogli wyraźnie widzieć, które aplikacje miały dostęp do danych na ich urządzeniach.

Wszystkie strony muszą szybko reagować na słabości w zakresie bezpieczeństwa w odpowiednim czasie, by użytkownicy końcowi nie byli niepotrzebnie narażeni na wady bezpieczeństwa. Niestety niektórzy producenci systemów operacyjnych i urządzeń (oraz operatorzy sieci telekomunikacyjnych przy dystrybucji markowych urządzeń) nie świadczą długoterminowego wsparcia w odniesieniu do wersji systemu operacyjnego, pozostawiając użytkowników bez ochrony przed powszechnie znanymi słabościami w zakresie bezpieczeństwa. Producenci systemów operacyjnych i urządzeń wraz z podmiotami opracowującymi aplikacje muszą z góry zapewniać użytkownikom informacje dotyczące czasu oczekiwania na regularne aktualizacje związane z bezpieczeństwem. Powinni także informować użytkowników jak najwcześniej o tym, czy rozwiązanie problemu w zakresie bezpieczeństwa wymaga dokonania aktualizacji.

Osoby trzecie

Powyższe elementy i uwagi dotyczące bezpieczeństwa muszą być także stosowane przez osoby trzecie przy gromadzeniu i przetwarzaniu danych osobowych do ich własnych celów, zwłaszcza przez reklamodawców i podmioty świadczące usługi analityczne. Obejmuje to również bezpieczną transmisję i szyfrowane przechowywanie wyjątkowych identyfikatorów urządzeń i użytkowników oraz pozostałych danych osobowych.

3.7 Informacje

3.7.1 Obowiązek informowania i wymagana zawartość

Zgodnie z art. 10 dyrektywy o ochronie danych każda osoba, której dane dotyczą, ma prawo znać tożsamość administratora przetwarzającego jej dane osobowe. Ponadto w kontekście aplikacji użytkownik końcowy ma prawo wiedzieć, jaki rodzaj danych osobowych jest

[42] Niedawno wskazano, że brak wizualnych wskaźników bezpieczeństwa w odniesieniu do wykorzystania SSL/TLS i nieodpowiednie wykorzystanie SSL/TLS może być wykorzystane do przeprowadzenia ataków typu *Main-in-the-Middle* (MITM). Według niedawnych badań łączna zainstalowana baza aplikacji, które zostały potwierdzone jako podatne na ataki typu MITM, zawiera kilka milionów użytkowników. „Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security", Bernd Freisleben i Matthew Smith, 19th ACM Conference on Computer and Communications Security (ACM CCS 2012).

przetwarzany i w jakim celu dane zostaną wykorzystane. Jeżeli dane osobowe użytkownika gromadzone są od innych podmiotów w środowisku aplikacji (jak opisano w sekcji 3.3 niniejszej opinii), użytkownik końcowy, zgodnie z art. 11 dyrektywy o ochronie danych, ma mimo to prawo do uzyskania informacji o takim przetwarzaniu danych w taki sam sposób. W związku z tym przy przetwarzaniu danych osobowych odpowiedni administrator musi przedstawić potencjalnym użytkownikom co najmniej o następujące informacje:

— kim jest (tożsamość i dane kontaktowe);
— dokładne kategorie danych osobowych, które podmiot opracowujący aplikacje będzie gromadził i przetwarzał;
— dlaczego (dokładnie do jakich celów);
— czy dane będą ujawnione osobom trzecim;
— jak użytkownicy mogą wykonywać swoje prawa w zakresie wycofania zgody i usunięcia danych.

Dostępność tego rodzaju informacji dotyczących przetwarzania danych osobowych jest kluczowa, aby uzyskać od użytkownika zgodę na przetwarzanie danych. Zgoda jest ważna jedynie, gdy osoba została najpierw poinformowana o głównych elementach przetwarzania danych. Zapewnienie takich informacji dopiero po rozpoczęciu przetwarzania danych osobowych przez aplikację (co ma często miejsce w trakcie instalacji) uznaje się za niewystarczające i nieważne w świetle prawa. Zgodnie ze sprawozdaniem służb Federalnej Komisji Handlu grupa robocza podkreśla konieczność zapewnienia informacji w momencie, w którym są one ważne dla konsumentów, tuż przed rozpoczęciem gromadzenia takich informacji przez aplikacje. Uzyskanie informacji o danych, które są przetwarzane jest szczególnie ważne, biorąc pod uwagę szeroki dostęp do czujników i struktur danych w urządzeniu, który na ogół posiadają aplikacje, przy czym w wielu przypadkach taki dostęp nie jest intuicyjnie oczywisty. Odpowiednie informacje są także bardzo istotne, gdy aplikacja przetwarza szczególne kategorie danych osobowych, np. dotyczących stanu zdrowia, przekonań politycznych, orientacji seksualnej itd. Ponadto podmiot opracowujący aplikacje powinien wyraźnie rozróżnić informacje obowiązkowe i nieobowiązkowe, a system powinien umożliwiać użytkownikowi odmowę dostępu do informacji nieobowiązkowych za pomocą domyślnych wariantów chroniących prywatność.

W odniesieniu do tożsamości administratora użytkownicy muszą wiedzieć, kto jest prawnie odpowiedzialny za przetwarzanie ich danych osobowych i jak można skontaktować się z administratorem. W przeciwnym wypadku nie są oni w stanie wykonać swoich praw, takich jak prawo do (zdalnego) dostępu do przechowywanych informacji na ich temat. Ze względu na rozdrobniony charakter środowiska aplikacji istotne jest, aby każda aplikacja miała jeden punkt kontaktowy ponoszący odpowiedzialność za całość przetwarzania danych przez aplikację. Użytkownik końcowy nie powinien być zmuszany do badania stosunków pomiędzy podmiotami opracowującymi aplikacje i innymi stronami przetwarzającymi dane osobowe za pomocą aplikacji.

W odniesieniu do celu lub celów użytkownicy końcowi muszą zostać odpowiednio poinformowani, które dane są gromadzone na ich temat i dlaczego. Użytkownikom należy także wyjaśnić za pomocą jasnego i prostego języka, czy dane mogą zostać ponownie wykorzystane przez inne strony, a jeżeli tak, to w jakim celu. Szeroko zdefiniowane cele, takie jak „innowacyjność produktu” są niewłaściwe do celów informowania użytkowników. Należy w prosty sposób stwierdzić, czy użytkownicy będą pytani o wyrażenie zgody na udostępnianie danych osobom trzecim w celu reklamowym lub analitycznym. Na sklepach z

aplikacjami spoczywa istotny obowiązek zapewnienia dostępności i łatwego dostępu do tych informacji w odniesieniu do każdej aplikacji.

Na sklepach z aplikacjami spoczywa istotny obowiązek zapewnienia odpowiednich informacji. Zdecydowanie zaleca się stosowanie wskaźników wizualnych lub ikon odnoszących się do sposobów wykorzystania danych w celu poinformowania użytkowników o rodzajach przetwarzania danych.

Oprócz powyższego minimalnego zakresu informacji koniecznych w celu uzyskania zgody od użytkownika aplikacji grupa robocza, mając na względzie rzetelne przetwarzanie danych osobowych, stanowczo zaleca, by administratorzy udostępnili użytkownikom informacje dotyczące następujących kwestii:

- proporcjonalności w odniesieniu do rodzajów danych zgromadzonych lub danych, do których uzyskano dostęp, znajdujących się na urządzeniu;
- okresów zatrzymywania danych;
- środków bezpieczeństwa podejmowanych przez administratora.

Grupa robocza zaleca również, aby podmioty opracowujące aplikacje uwzględniły informacje dotyczące swojej polityki prywatności skierowanej do użytkowników europejskich, sposobu zapewnienia zgodności aplikacji z europejskim prawem w zakresie ochrony danych, w tym możliwego przesłania danych osobowych z Europy do np. Stanów Zjednoczonych oraz tego czy i w jaki sposób aplikacja jest w tym przypadku zgodna z zasadami bezpiecznego transferu danych osobowych (program Safe Harbor).

3.7.2 Forma informacji

Istotny zakres informacji dotyczących przetwarzania danych musi być dostępny dla użytkowników przed instalacją aplikacji, poprzez sklep za aplikacjami. Po drugie, właściwe informacje dotyczące przetwarzania danych muszą być także dostępne wewnątrz aplikacji po zainstalowaniu.

Sklepy z aplikacjami jako współadministratorzy wraz z podmiotami opracowującymi aplikacje w odniesieniu do informacji muszą dopilnować, by każda aplikacja zapewniała istotne informacje dotyczące przetwarzania danych. Sklepy powinny sprawdzić hiperłącza do załączonych stron zawierających informacje dotyczące prywatności i usunąć aplikacje z uszkodzonymi hiperłączami lub w jakikolwiek innych sposób niedostępnymi informacjami dotyczącymi przetwarzania danych.

Grupa robocza zaleca, aby informacje dotyczące przetwarzania danych osobowych były także dostępne i łatwe do zlokalizowania np. w sklepie z aplikacjami i najlepiej na zwykłych stronach internetowych podmiotu opracowującego aplikacje odpowiedzialnego za daną aplikację. Niedopuszczalna jest sytuacja, w której użytkownicy są zmuszeni szukać w sieci informacji dotyczących polityki przetwarzania danych dotyczącej aplikacji zamiast uzyskać informacje bezpośrednio od podmiotu opracowującego aplikacje lub innego administratora.

Każda aplikacja powinna posiadać co najmniej czytelną, zrozumiałą i łatwo dostępną politykę prywatności, w której zawarto wszystkie powyższe informacje. Wiele aplikacji nie spełnia wymogu minimalnej przejrzystości. Według badania Forum Przyszłości Prywatności z czerwca 2012 r. 56 % płatnych aplikacji i prawie 30 % darmowych aplikacji nie ma polityki prywatności.

Aplikacje, które nie przetwarzają lub nie są przeznaczone do przetwarzania danych osobowych, powinny zawierać jasne stwierdzenie na ten temat w swojej polityce prywatności.

Istnieją oczywiście ograniczenia ilości informacji, jaką można przedstawić na małym ekranie, ale nie jest to powód do nieinformowania użytkowników końcowych we właściwy sposób. Można skorzystać z szeregu strategii, aby zapewnić świadomość użytkowników w zakresie kluczowych elementów usługi. Grupa robocza widzi korzyści w zastosowaniu not o układzie warstwowym opisanych przez Grupę Roboczą Art. 29 w opinii 10/2004[43], w których nota wstępna skierowana do użytkownika zawiera minimum informacji wymaganych przez ramy prawne UE, a dalsze informacje są dostępne poprzez hiperłącza prowadzące do całej polityki prywatności. Informacje należy przedstawić bezpośrednio na ekranie, w formie łatwo dostępnej i wyraźnie widocznej. Oprócz zrozumiałych informacji odpowiednich dla małych ekranów urządzeń przenośnych użytkownicy muszą mieć możliwość skorzystania z odsyłaczy do bardziej rozległych wyjaśnień, np. zawartych w polityce prywatności, dotyczących sposobu wykorzystania danych osobowych przez aplikację, tego, kto jest administratorem i gdzie użytkownik może wykonać swoje prawa.

Podejście to można połączyć z zastosowaniem ikon, obrazów, filmów i dźwięku oraz wykorzystać kontekstowe powiadomienia w czasie rzeczywistym, gdy aplikacja uzyskuje dostęp do książki adresowej lub fotografii[44].Wspomniane ikony muszą być znaczące, tj. wyraźne, zrozumiałe same przez się i niedwuznaczne. Jasne jest więc, że producent systemu operacyjnego ponosi znaczną współodpowiedzialność za ułatwienie stosowania ikon tego rodzaju.

Podmioty opracowujące aplikacje są ekspertami w programowaniu i opracowywaniu złożonych interfejsów na małe ekrany, grupa robocza wzywa więc przemysł do wykorzystania tego kreatywnego talentu, aby dostarczyć więcej kreatywnych rozwiązań w celu skutecznego informowania użytkowników na urządzeniach przenośnych. W celu dopilnowania, by informacje były faktycznie zrozumiałe dla użytkowników nieposiadających wiedzy technicznej lub prawniczej, grupa robocza (zgodnie ze sprawozdaniem służb Federalnej Komisji Handlu) stanowczo zaleca testowanie przez konsumentów wybranych strategii informowania[45].

3.8 Prawa osoby, której dane dotyczą

Zgodnie z art. 12 i 14 dyrektywy o ochronie danych podmioty opracowujące aplikacje i pozostali administratorzy w środowisku aplikacji mobilnych muszą umożliwić użytkownikom aplikacji wykonywanie ich prawa dostępu do danych, ich zmiany i usunięcia oraz prawa sprzeciwu wobec przetwarzania danych. Jeżeli użytkownik wykonuje swoje prawo dostępu, administrator musi zapewnić użytkownikowi informacje dotyczące przetwarzanych danych i źródła tych danych. Jeżeli administrator podejmuje zautomatyzowane decyzje w oparciu o połączone dane, musi on także poinformować użytkownika o zasadach podejmowania tych decyzji. Może mieć to miejsce w przypadkach, w których ocenia się wyniki lub postępowanie

[43] Opinia Grupy Roboczej w sprawie dalszej harmonizacji zasad informowania Art. 29 10/2004 (lipiec 2004), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_pl.pdf#h2-5.

[44] Na przykład ikona ostrzeżenia dotycząca przetwarzania danych geolokalizacyjnych stosowana w urządzeniach iPhone.

[45] Sprawozdanie służb Federalnej Komisji Handlu, przypis 6 powyżej, s. 16.

użytkownika, np. w oparciu o dane finansowe lub dane zdrowotne, lub inne dane profilowe. Na wniosek użytkownika administrator danych dla danej aplikacji musi także umożliwić poprawienie, usunięcie lub zablokowanie danych osobowych, jeżeli są one niekompletne, niedokładne lub zostały przetworzone niezgodnie z prawem.

Aby użytkownicy mogli sprawować kontrolę nad przetwarzaniem swoich danych osobowych, aplikacje muszą wyraźnie i widocznie informować użytkowników o istnieniu wspomnianych mechanizmów dostępu i poprawy. Grupa Robocza Art. 29 zaleca opracowanie i wdrożenie prostych, lecz bezpiecznych narzędzi dostępu *online*. Narzędzia dostępu powinny być dostępne najlepiej w każdej aplikacji lub poprzez umieszczenie hiperłącza do funkcji *online*, dzięki której użytkownicy mogą uzyskać natychmiastowy dostęp do wszystkich danych przetwarzanych na ich temat wraz z koniecznymi wyjaśnieniami. Podobne inicjatywy zastosowali dostawcy usług *online*, np. różne tablice lub inne mechanizmy dostępu.

Konieczność łatwego dostępu *online* jest szczególnie ważna w przypadku aplikacji przetwarzających bogate profile użytkowników, takie jak aplikacje służące do tworzenia sieci kontaktów, aplikacje społecznościowe i komunikacyjne, lub aplikacje przetwarzające dane szczególnie chronione i dane finansowe. Oczywiście dostęp powinien zostać udzielony jedynie, jeżeli ustalono tożsamość osoby, której dane dotyczą, w celu uniemożliwienia wycieku danych do osób trzecich. Obowiązek weryfikacji prawidłowej tożsamości nie powinien jednak prowadzić do dodatkowego, nadmiernego gromadzenia danych osobowych na temat osoby, której dane dotyczą. W wielu przypadkach może wystarczyć uwierzytelnienie zamiast (pełnej) identyfikacji.

Ponadto użytkownicy zawsze powinni mieć możliwość wycofania swojej zgody w łatwy i nieobciążający sposób. Osoba, której dane dotyczą, może wycofać zgodę na przetwarzanie danych na kilka różnych sposobów i z kilku różnych powodów. W najlepszym przypadku możliwość wycofania zgody powinna być dostępna za pośrednictwem wspomnianych wyżej łatwo dostępnych mechanizmów. Musi istnieć możliwość odinstalowania aplikacji i w związku z tym usunięcia wszystkich danych osobowych, także z serwerów administratora. W celu umożliwienia użytkownikom usunięcia ich danych przez podmiot opracowujący aplikacje ważne jest, aby producent systemu operacyjnego zapewnił sygnał dla podmiotu opracowującego aplikacje natychmiast po odinstalowaniu aplikacji przez użytkownika. Taki sygnał można zapewnić poprzez interfejs programowania aplikacji. Z zasady po odinstalowaniu aplikacji przez użytkownika podmiot opracowujący aplikacje nie ma podstawy prawnej, aby kontynuować przetwarzanie danych osobowych dotyczących danego użytkownika i w związku z tym musi on usunąć wszelkie dane. Podmiot opracowujący aplikacje chcący zatrzymać pewne dane, np. w celu ułatwienia ponownej instalacji aplikacji, musi oddzielnie zapytać o zgodę w procesie odinstalowywania, zwracając się do użytkownika o wyrażenie zgody na określony dodatkowy okres zatrzymywania. Jedynym wyjątkiem od tej zasady są ewentualne obowiązki prawne co do zatrzymania części danych do szczególnych celów, np. obowiązki podatkowe odnoszące się do transakcji finansowych[46].

[46] Grupa robocza przypomina wszystkim podmiotom związanym z usługami społeczeństwa informacyjnego, takimi jak aplikacje, że europejski obowiązek zatrzymywania danych (dyrektywa 2006/24/WE) nie ma do nich zastosowania i w związku z tym nie można się powoływać na ten obowiązek jako podstawę prawną do kontynuacji przetwarzania danych dotyczących użytkowników aplikacji po usunięciu przez nich tych aplikacji. Grupa robocza korzysta z okazji, aby podkreślić wyjątkowo ryzykowny charakter danych o ruchu, które jako takie wymagają specjalnych środków ostrożności i zabezpieczeń, jak wskazano w sprawozdaniu Grupy Roboczej Art. 29 w sprawie egzekwowania dyrektywy w sprawie zatrzymywania danych (WP172), w

3.9 Okresy zatrzymywania

Podmioty opracowujące aplikacje muszą rozważyć zatrzymywanie danych zgromadzonych za pomocą aplikacji oraz występujące w tym kontekście ryzyko związane z ochroną danych. Szczegółowe terminy będą zależeć od celu aplikacji i znaczenia danych dla użytkownika końcowego. Na przykład w przypadku kalendarza, dziennika lub aplikacji udostępniającej fotografie harmonogram zatrzymywania zostanie oddany pod kontrolę użytkownika końcowego, natomiast w przypadku aplikacji nawigacyjnej wystarczające może być przechowywanie jedynie 10 ostatnio odwiedzonych lokalizacji. Podmioty opracowujące aplikacje powinny także wziąć pod uwagę dane użytkowników, którzy długo nie korzystali z aplikacji Ci użytkownicy mogli stracić swoje urządzenie przenośne lub przejść na inne urządzenie bez aktywnego odinstalowania wszystkich aplikacji na urządzeniu pierwotnym. Podmioty opracowujące aplikacje powinny w związku z tym uprzednio zdefiniować okres nieaktywności, po którym konto będzie traktowane jako wygasłe, i zagwarantować, że użytkownik zostanie powiadomiony o takim terminie. Po upływie tego okresu administrator powinien powiadomić użytkownika i umożliwić mu odzyskanie danych osobowych. Jeżeli użytkownik nie odpowie na powiadomienie, dane osobowe dotyczące użytkownika i korzystania z aplikacji powinny zostać bezpowrotnie zanonimizowane lub usunięte. Okres przypomnienia zależy od celu aplikacji i miejsca przechowywania danych. Jeżeli dane są przechowywane na urządzeniu, np. najlepszy wynik w grze, dane można zatrzymywać do momentu odinstalowania aplikacji. Jeżeli sytuacja dotyczy danych wykorzystywanych tylko raz do roku, takich jak informacje dotyczące kurortu narciarskiego, okres przypomnienia może wynosić 15 miesięcy.

3.10 Dzieci

Dzieci są zagorzałymi użytkownikami aplikacji, zarówno na własnych urządzeniach, jak i na urządzeniach udostępnianych (np. należących do rodziców, rodzeństwa lub znajdujących się w placówce edukacyjnej); wyraźnie istnieje też duży i różnorodny rynek aplikacji skierowanych do dzieci. Jednocześnie dzieci posiadają ograniczone pojęcie i wiedzę lub w ogóle nie rozumieją i nie mają wiedzy odnośnie do zakresu i szczególnie chronionego charakteru danych, do których aplikacje mogą mieć dostęp, lub zakresu udostępniania danych osobom trzecim w celach reklamowych.

Grupa robocza omówiła dogłębnie kwestię przetwarzania danych osobowych dzieci w opinii 2/2009 w sprawie ochrony danych osobowych dzieci, dlatego w niniejszym punkcie odniesie się jedynie do kilku czynników ryzyka i zaleceń związanych szczególnie z aplikacjami[47].

Podmioty opracowujące aplikacje i pozostali administratorzy powinni zwracać uwagę na ograniczenie wiekowe określające dzieci lub nieletnich w ustawodawstwie krajowym, gdzie

---

którym to przypadku wszystkie właściwe zainteresowane strony wezwano do wdrożenia odpowiednich środków bezpieczeństwa.

[47] Opinia 2/2009 w sprawie ochrony danych osobowych dzieci (Ogólne wytyczne i szczególny przypadek szkół), WP160, z dnia 11 lutego 2009 r., http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_pl.pdf#h2-5.

zgoda rodziców jest warunkiem zgodnego z prawem przetwarzania informacji przez aplikacje[48].

Gdy zgoda może zostać legalnie uzyskana od nieletniego i aplikacja jest przeznaczona do wykorzystywania przez dziecko lub nieletniego, administrator powinien zwrócić uwagę na możliwość ograniczonego zrozumienia informacji dotyczących przetwarzania danych i nieprzywiązywania nadmiernej wagi do tych informacji przez nieletniego. Ze względu na ich ogólną podatność i biorąc pod uwagę, że dane osobowe muszą być przetwarzane rzetelnie i zgodnie z prawem, administratorzy kierujący swoje produkty do dzieci powinni jeszcze uważniej przestrzegać zasad minimalizacji danych i ograniczenia celu. W szczególności administratorzy nie powinni przetwarzać danych dzieci na potrzeby reklamy behawioralnej, zarówno bezpośrednio, jak i pośrednio, ponieważ będzie to wykraczać poza zakres rozumienia dziecka i w związku z tym będzie wykraczać poza granice przetwarzania zgodnego z prawem.

Grupa robocza podziela obawy przedstawione przez Federalną Komisję Handlu w sprawozdaniu jej służb w sprawie aplikacji mobilnych dla dzieci[49].

Podmioty opracowujące aplikacje, we współpracy ze sklepami z aplikacjami oraz producentami systemów operacyjnych i urządzeń, powinny przedstawiać właściwe informacje w sposób prosty, w języku odpowiednim do wieku. Administratorzy powinni także w szczególności powstrzymać się od gromadzenia danych dotyczących rodziców lub członków rodziny dziecka będącego użytkownikiem, takich jak informacje finansowe lub informacje na temat szczególnych kategorii danych, takich jak dane medyczne.

4 Wnioski i zalecenia

Wiele rodzajów danych dostępnych na inteligentnym urządzeniu przenośnym ma charakter danych osobowych. Właściwe ramy prawne stanowi dyrektywa o ochronie danych w połączeniu ze szczególnym wymaganiem dotyczącym zgody zawartym w art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej. Przepisy te mają zastosowanie do wszystkich aplikacji skierowanych do użytkowników aplikacji w UE, bez względu na lokalizację podmiotu opracowującego aplikacje lub sklepu z aplikacjami.

Rozdrobniony charakter środowiska aplikacji, szeroki zakres możliwości dostępu technicznego do danych przechowywanych lub generowanych na urządzeniach przenośnych i brak świadomości prawnej wśród podmiotów opracowujących aplikacje stwarzają szereg poważnych czynników ryzyka związanych z ochroną danych w odniesieniu do użytkowników aplikacji. Wspomniane czynniki ryzyka obejmują brak przejrzystości i brak świadomości wśród użytkowników aplikacji, słabe środki bezpieczeństwa, niewłaściwe mechanizmy zgody, tendencje do maksymalizacji danych oraz szeroko zdefiniowane cele przetwarzania danych.

---

[48] W państwach członkowskich UE ograniczenie wiekowe znajduje się w przedziale od 12 do 18 lat.

[49] Sprawozdanie służb Federalnej Komisji Handlu „Mobile Apps for Kids: Current Privacy Disclosures are Disappointing" (luty 2012 r.), http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf. „Podczas gdy służby napotkały na różnorodny zbiór aplikacji dla dzieci stworzonych przez setki różnych podmiotów opracowujących aplikacje, to znalazły niewiele lub nie znalazły w ogóle na rynkach aplikacji informacji o praktykach gromadzenia i udostępniania danych stosowanych przez te aplikacje".

Obowiązki w zakresie ochrony danych pokrywają się pomiędzy różnymi stronami zajmującymi się opracowaniem, dystrybucją i możliwościami technicznymi aplikacji. Większość wniosków i zaleceń jest skierowanych do podmiotów opracowujących aplikacje (ponieważ mają oni największą kontrolę nad dokładnym sposobem przetwarzania danych lub przedstawiania informacji w aplikacji), lecz często, aby osiągnąć najwyższe normy prywatności i ochrony danych, muszą oni współpracować z innymi stronami w środowisku aplikacji, takimi jak producenci systemów operacyjnych i urządzeń, sklepy z aplikacjami i osoby trzecie, takie jak podmioty świadczące usługi analityczne i sieci reklamowe.

Podmioty opracowujące aplikacje muszą

- mieć świadomość obowiązków powierzonych im z racji pełnienia funkcji administratora i realizować je podczas przetwarzania danych pochodzących od użytkowników i dotyczących użytkowników;
- mieć świadomość obowiązków powierzonych im z racji pełnienia funkcji administratora i realizować je podczas zawierania umów z przetwarzającymi, jeżeli zlecają na zewnętrz gromadzenie i przetwarzanie danych osobowych twórcom, programistom i np. podmiotom świadczącym usługi przechowywania w chmurze;
- zwracać się z pytaniem o zgodę, zanim aplikacja rozpocznie pobieranie lub umieszczanie informacji w urządzeniu, tj. przed instalacją aplikacji. Zgoda musi być dobrowolna, konkretna i świadoma;
- zwracać się z pytaniem o szczegółową zgodę w odniesieniu do każdego rodzaju danych, do których aplikacja będzie chciała uzyskać dostęp; co najmniej w odniesieniu do kategorii lokalizacji, kontaktów, niepowtarzalnego kodu identyfikacji wyrobu, tożsamości osoby, której dane dotyczą, tożsamości telefonu, danych dotyczących kart kredytowych i płatności, telefonii i SMS-ów, historii przeglądania, wiadomości E-mail, danych uwierzytelniających w sieciach społecznościowych i biometrii;
- mieć świadomość, że zgoda nie uzasadnia nadmiernego lub nieproporcjonalnego przetwarzania danych;
- zapewnić dobrze zdefiniowane i zrozumiałe cele przetwarzania danych przed instalacją aplikacji, nie zmieniać tych celów bez ponownego wyrażenia zgody; zapewniać wyczerpujące informacje w przypadkach, w których informacje będą wykorzystywane na potrzeby osób trzecich, takie jak reklama lub analizy;
- umożliwiać użytkownikom wycofanie zgody i odinstalowanie aplikacji oraz usunięcie danych w stosownych przypadkach;
- przestrzegać zasadę minimalizacji danych i gromadzić tylko te dane, które są ściśle konieczne do wykonywania wybranej funkcji;
- podejmować konieczne środki organizacyjne i techniczne, aby zapewnić ochronę przetwarzanych danych osobowych na wszystkich etapach opracowywania i wdrażania aplikacji (uwzględnianie prywatności już w fazie projektowania), jak opisano w sekcji 3.6 niniejszej opinii;
- zapewnić jeden punkt kontaktowy dla użytkowników aplikacji;
- zapewnić czytelną, zrozumiałą i łatwo dostępną politykę prywatności, która zawiera co najmniej następujące informacje dla użytkowników:
  - kim są podmioty opracowujące aplikacje (tożsamość i dane kontaktowe);
  - dokładne kategorie danych osobowych, które aplikacja będzie gromadzić i przetwarzać;
  - dlaczego przetwarzanie danych jest konieczne (w jakich dokładnych celach);
  - czy dane będą ujawniane osobom trzecim (nie ma to być ogólny opis, lecz szczegółowe wyjaśnienie tego, komu dane zostaną ujawnione),

— jakie prawa mają użytkownicy w zakresie wycofania zgody i usunięcia danych,

- umożliwić użytkownikom aplikacji wykonywanie ich prawa dostępu do danych, ich poprawienia i usunięcia oraz prawa do sprzeciwu wobec przetwarzania danych, a także poinformować ich o istnieniu tych mechanizmów;
- określić rozsądny okres zatrzymywania danych zgromadzonych przez aplikację i określić z góry okres nieaktywności, po którym konto będzie traktowane jako wygasłe;
- w odniesieniu do aplikacji skierowanych do dzieci: zwrócić uwagę na ograniczenie wiekowe określające dzieci lub nieletnich w ustawodawstwie krajowym, wybrać najbardziej restrykcyjne podejście do przetwarzania danych z pełnym poszanowaniem zasad minimalizacji danych i ograniczenia celu, powstrzymać się od przetwarzania danych osobowych dzieci na potrzeby reklamy behawioralnej, zarówno bezpośrednio, jak i pośrednio, oraz powstrzymać się od gromadzenia od dzieci danych dotyczących ich krewnych lub przyjaciół.

Grupa robocza zaleca, aby podmioty opracowujące aplikacje

- zapoznały się z właściwymi wytycznymi dotyczącymi szczególnych czynników ryzyka i środków w zakresie bezpieczeństwa;
- aktywnie informowały użytkowników o naruszeniach danych osobowych zgodnie z wymogami dyrektywy o prywatności i łączności elektronicznej;
- informowały użytkowników na temat proporcjonalności w odniesieniu do rodzajów danych zgromadzonych na urządzeniu lub danych, do których uzyskano dostęp, okresach zatrzymywania oraz zastosowanych środkach bezpieczeństwa;
- opracowały narzędzia umożliwiające użytkownikom dostosowanie okresów zatrzymywania do ich danych osobowych w oparciu o ich szczególne preferencje i kontekst, w przeciwieństwie do oferowania uprzednio określonych warunków zatrzymywania;
- uwzględniły w polityce prywatności informacje odnoszące się do użytkowników europejskich;
- opracowały i wdrożyły proste, lecz skuteczne narzędzia dostępu *online* dla użytkowników bez gromadzenia dodatkowych nadmiernych danych osobowych;
- wraz z producentami systemów operacyjnych i urządzeń oraz sklepami z aplikacjami wykorzystały swój talent i twórczo opracowały innowacyjne rozwiązania mające na celu odpowiednie informowanie użytkowników za pomocą urządzeń przenośnych, np. poprzez system not informacyjnych o układzie warstwowym połączonych ze znaczącymi ikonami.

Sklepy z aplikacjami muszą

- mieć świadomość obowiązków powierzonych im z racji pełnienia funkcji administratora i realizować je podczas przetwarzania danych pochodzących od użytkowników i dotyczących użytkowników;
- egzekwować obowiązek podmiotu opracowującego aplikacje w zakresie informacji, w tym w odniesieniu do rodzajów danych, do których aplikacja może mieć dostęp i celu tego dostępu, a także kwestii, czy dane są udostępniane osobom trzecim;
- zwracać szczególną uwagę na aplikacje skierowane do dzieci w celu ochrony przed niezgodnym z prawem przetwarzaniem ich danych, a w szczególności egzekwować obowiązek przedstawiania stosownych informacji w prosty sposób, w języku dostosowanym do wieku;
- zapewnić szczegółowe informacje dotyczące kontroli dostarczania aplikacji, które są faktycznie wykonywane, w tym tych mających na celu ocenę kwestii związanych z prywatnością i ochroną danych.

Grupa robocza zaleca, aby sklepy z aplikacjami

- we współpracy z producentem systemu operacyjnego opracowały narzędzie kontroli dla użytkowników, takie jak symbole przedstawiające dostęp do danych znajdujących się na urządzeniu przenośnym i generowanych przez nie;
- objęły wszystkie aplikacje mechanizmem wizerunku publicznego;
- wdrożyły chroniący prywatność mechanizm zdalnego odinstalowania;
- zapewniły użytkownikom kanały informacji zwrotnych, aby mogli zgłaszać problemy związane z prywatnością lub bezpieczeństwem;
- współpracowały z podmiotami opracowującymi aplikacje w celu aktywnego informowania użytkowników na temat naruszeń danych osobowych;
- ostrzegały podmioty opracowujące aplikacje odnośnie do specyfiki prawa europejskiego zanim zgłoszą aplikację w Europie, np. w odniesieniu do wymagania wyrażenia zgody i w przypadku przeniesienia danych osobowych do państw spoza UE.

Producenci systemów operacyjnych i urządzeń muszą

- zaktualizować swoje interfejsy programowania aplikacji i interfejsy użytkownika, by udostępnić użytkownikom odpowiednią kontrolę w celu wyrażania ważnej zgody co do danych przetwarzanych przez aplikacje;
- wdrożyć mechanizm uzyskiwania zgody w swoich systemach operacyjnych przy pierwszym uruchomieniu aplikacji lub przy pierwszej próbie uzyskania dostępu przez aplikację do jednej z kategorii danych mających istotnych wpływ na prywatność;
- stosować zasady uwzględniania prywatności już w fazie projektowania, by uniknąć niejawnego monitorowania użytkownika;
- zapewnić bezpieczeństwo przetwarzania;
- zapewnić zgodność (domyślnych ustawień) fabrycznie zainstalowanych aplikacji z prawem europejskim w zakresie ochrony danych;
- zapewnić przesiewowy dostęp do danych, czujników i usług w celu dopilnowania, by podmiot opracowujący aplikacje miał dostęp jedynie do tych danych, które są konieczne dla jego aplikacji;
- zapewnić przyjazne dla użytkownika i skuteczne metody unikania śledzenia przez reklamodawców lub jakąkolwiek inną osobę trzecią. Ustawienia domyślne muszą umożliwiać uniknięcie jakiegokolwiek śledzenia;
- zapewnić dostępność odpowiednich mechanizmów informowania i edukacji użytkownika końcowego o tym, co mogą robić aplikacje i do jakich danych mogą mieć dostęp;
- zapewnić odzwierciedlenie każdej próby dostępu do kategorii danych w informacji dla użytkownika przed instalacją aplikacji: przedstawione kategorie muszą być jasne i zrozumiałe;
- wdrożyć otoczenie sprzyjające bezpieczeństwu wraz z narzędziami zapobiegającymi rozprzestrzenianiu się szkodliwych aplikacji i umożliwiającymi łatwe instalowanie/odinstalowywanie każdej funkcji.

Grupa robocza zaleca, aby producenci systemów operacyjnych i urządzeń

- umożliwili użytkownikom odinstalowanie aplikacji i zapewnili sygnał (np. poprzez interfejs programowania aplikacji) dla podmiotu opracowującego aplikacje w celu umożliwienia usunięcia właściwych danych użytkownika;
- systematycznie oferowali i ułatwiali regularne aktualizacje bezpieczeństwa;
- dopilnowali, aby metody i funkcje umożliwiające aplikacjom dostęp do danych osobowych zawierały właściwości mające na celu wdrożenie zapytań o szczegółową zgodę;

- aktywnie wspomagali rozwój ikon ostrzegających użytkowników o różnym wykorzystaniu danych przez aplikacje i ułatwiali korzystanie z nich;
- opracowali wyraźne ścieżki audytu w urządzeniach, tak aby użytkownicy końcowi mogli wyraźnie widzieć, które aplikacje miały dostęp do danych na ich urządzeniach, oraz przepływ informacji na zewnątrz każdej aplikacji w odniesieniu do przepływu spowodowanego przez użytkownika.

Osoby trzecie muszą

- mieć świadomość obowiązków powierzonych im z racji pełnienia funkcji administratora i realizować je podczas przetwarzania danych pochodzących od użytkowników i dotyczących użytkowników;
- zachować zgodność z wymaganiem wyrażenia zgody określonym w art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej przy odczytywaniu lub zapisywaniu danych na urządzeniach przenośnych we współpracy z podmiotami opracowującymi aplikacje lub sklepami z aplikacjami, które zapewniają użytkownikowi informacje dotyczące celów przetwarzania danych;
- nie obchodzić jakichkolwiek mechanizmów opracowanych w celu unikania śledzenia, jak obecnie często ma to miejsce w przypadku mechanizmów „Nie śledź" umieszczonych w przeglądarkach;
- jeżeli są podmiotami świadczącymi usługi komunikacyjne, przy wydawaniu markowych urządzeń, zapewnić wyrażenie ważnej zgody przez użytkowników fabrycznie zainstalowanych aplikacji i przyjąć odpowiedzialność związaną z określaniem niektórych właściwości urządzenia i systemu operacyjnego, np. ograniczając dostęp użytkownika do pewnych parametrów konfiguracji lub filtrując poprawki (w zakresie bezpieczeństwa i funkcjonowania) dostarczone przez producentów urządzeń i systemów operacyjnych;
- jeżeli są podmiotami świadczącymi usługi reklamowe, w szczególności unikać umieszczania reklam poza kontekstem aplikacji. Przykładem jest umieszczanie reklam poprzez modyfikacje ustawień przeglądarki lub umieszczanie ikon na pulpicie mobilnym. Powstrzymać się od stosowania niepowtarzalnego identyfikatora wyrobu lub abonenta na potrzeby śledzenia;
- powstrzymać się od przetwarzania danych dzieci na potrzeby reklamy behawioralnej, zarówno bezpośrednio jak i pośrednio. Stosować odpowiednie środki bezpieczeństwa. Uwzględnia to również bezpieczną transmisję i szyfrowane przechowywanie niepowtarzalnych identyfikatorów wyrobów i użytkowników oraz pozostałych danych osobowych.

Grupa robocza zaleca, aby osoby trzecie

- opracowały i wdrożyły proste, lecz skuteczne narzędzia dostępu *online* dla użytkowników bez gromadzenia dodatkowych nadmiernych danych osobowych;
- gromadziły i przetwarzały jedynie dane, które są spójne z kontekstem, w jakim użytkownik dostarczył dane.