GRUPUL DE LUCRU PENTRU PROTECŢIA PERSOANELOR ÎN CEEA CE PRIVEŞTE PRELUCRAREA DATELOR CU CARACTER PERSONAL

00461/13/RO
WP 202

Avizul nr. 02/2013 privind aplicațiile instalate pe dispozitivele inteligente

Adoptat la 27 februarie 2013

Acest grup de lucru a fost instituit în temeiul articolului 29 din Directiva 95/46/CE. Acesta este un organ consultativ european independent pentru protecţia datelor și a vieții private. Atribuțiile acestuia sunt descrise la articolul 30 din Directiva 95/46/CE și la articolul 15 din Directiva 2002/58/CE.

Secretariatul este asigurat de Direcţia C (Drepturi fundamentale și cetățenia Uniunii) a Comisiei Europene, Direcția Generală Justiţie, B-1049 Bruxelles, Belgia, biroul nr. MO-59 02/013.

Site: http://ec.europa.eu/justice/data-protection/index_ro.htm

Rezumat

În magazinele de aplicații există sute de mii de aplicații diferite disponibile pentru fiecare tip uzual de dispozitiv inteligent. S-a raportat că magazinele de aplicații sunt aprovizionate zilnic cu peste 1 600 de aplicații noi și că un utilizator mediu de telefoane inteligente descarcă 37 de aplicații. Astfel de aplicații pot fi furnizate utilizatorilor finali la costuri inițiale reduse sau fără costuri inițiale, adresându-se unui public format din doar câțiva indivizi sau din milioane de persoane.

Aplicațiile sunt capabile să colecteze cantități considerabile de date din dispozitivele inteligente (de exemplu, datele stocate în dispozitiv de către utilizatori și datele furnizate de diferiți senzori, cum ar fi datele de localizare) și să le prelucreze pentru a oferi utilizatorilor finali servicii noi și inovatoare. Cu toate acestea, aceleași surse de date pot fi prelucrate suplimentar, de obicei cu scopul de a furniza un flux de venituri într-o manieră care poate fi necunoscută sau nedorită de către utilizatorii finali.

Dezvoltatorii de aplicații care nu cunosc cerințele în materie de protecție a datelor pot crea riscuri semnificative la adresa vieții private și a reputației utilizatorilor de dispozitive inteligente. Principalele riscuri legate de protecția datelor cu caracter personal la care sunt expuși utilizatorii finali sunt lipsa de transparență și de cunoaștere a tipurilor de prelucrări operate de o aplicație și lipsa consimțământului în cunoștință de cauză din partea utilizatorilor finali înainte de prelucrarea datelor respective. Măsurile de securitate deficiente, o tendință evidentă de maximizare a datelor și elasticitatea scopurilor în care sunt colectate datele cu caracter personal contribuie, de asemenea, la apariția riscurilor cu privire la protecția datelor cu caracter personal în mediul actual al aplicațiilor.

Un risc ridicat la adresa protecției datelor cu caracter personal rezultă, de asemenea, din gradul de fragmentare a mediului de dezvoltare a aplicațiilor între numeroși actori, printre care se numără: dezvoltatorii de aplicații, proprietarii de aplicații, magazinele de aplicații, producătorii de sisteme de operare și de dispozitive (producătorii de SO și de dispozitive) și alți terți care pot fi implicați în colectarea și prelucrarea datelor cu caracter personal preluate din dispozitivele inteligente, cum ar fi furnizorii de instrumente analitice și de servicii de publicitate. Majoritatea concluziilor și recomandărilor din prezentul aviz se adresează dezvoltatorilor de aplicații (având în vedere că aceștia dețin cel mai mare control asupra modului exact de prelucrare sau de prezentare a informațiilor în cadrul aplicației), însă, de cele mai multe ori, pentru ca aceștia să poată atinge cele mai ridicate standarde în materie de confidențialitate și de protecție a datelor, trebuie să existe o colaborare cu alte părți din ecosistemul de aplicații. Acest aspect este important în special în ceea ce privește securitatea, în cazul căreia lanțul numeroșilor actori este la fel de puternic precum veriga sa cea mai slabă.

Numeroase tipuri de date disponibile pe dispozitivele mobile inteligente sunt date cu caracter personal. Cadrul juridic relevant este reprezentat de Directiva privind protecția datelor, în combinație cu protecția dispozitivelor mobile ca parte din sfera privată a utilizatorilor, prevăzută de Directiva asupra confidențialității și comunicațiilor electronice. Normele respective se aplică tuturor aplicațiilor destinate utilizatorilor de aplicații de pe teritoriul UE, indiferent de amplasarea dezvoltatorului sau a magazinului de aplicații.

În prezentul aviz, grupul de lucru clarifică cadrul juridic aplicabil prelucrării datelor cu caracter personal în ceea ce privește dezvoltarea, distribuția și utilizarea aplicațiilor instalate pe dispozitivele inteligente, cu axare pe cerința de obținere a consimțământului utilizatorilor

finali, principiile limitării scopului și minimizării datelor, necesitatea adoptării de măsuri de securitate corespunzătoare, obligația de a asigura informarea corectă a utilizatorilor finali, drepturile utilizatorilor finali, perioadele corespunzătoare de păstrare a datelor și, în special, prelucrarea echitabilă a datelor colectate de la copii și referitoare la aceștia.

Cuprins

1. Introducere 5
2. Riscuri legate de protecția datelor 6
3 Principii privind protecția datelor 8
3.1 Dreptul aplicabil 8
3.2 Datele cu caracter personal prelucrate de aplicații 9
3.3 Părțile implicate în prelucrarea datelor cu caracter personal 10
3.3.1 Dezvoltatorii de aplicații 11
3.3.2 Producătorii de SO și de dispozitive 12
3.3.3 Magazinele de aplicații 14
3.3.4 Terții 14
3.4 Temeiul juridic 17
3.4.1 Acordul prealabil instalării și prelucrării datelor cu caracter personal 17
3.4.2 Temeiuri juridice pentru prelucrarea datelor pe parcursul utilizării aplicației 19
3.5 Limitarea scopului și minimizarea datelor 20
3.6 Securitate 22
3.7 Informare 26
3.7.1 Obligația de informare și conținutul necesar 26
3.7.2 Forma informațiilor 28
3.8 Drepturile persoanei vizate 29
3.9 Perioadele de păstrare a datelor 30
3.10 Copiii 31
4 Concluzii și recomandări 32

1. Introducere

Aplicațiile sunt aplicații software proiectate adeseori pentru a îndeplini o anumită sarcină și pentru a fi instalate pe un anumit set de dispozitive inteligente, cum ar fi telefoanele inteligente, tabletele electronice și televizoarele conectate la internet. Acestea organizează informațiile într-o manieră corespunzătoare caracteristicilor specifice ale dispozitivului, interacționând îndeaproape cu caracteristicile echipamentului hardware și ale sistemului de operare instalate pe dispozitiv.

În magazinele de aplicații există sute de mii de aplicații diferite disponibile pentru fiecare tip uzual de dispozitiv inteligent. Aplicațiile deservesc o gamă variată de scopuri, inclusiv navigare pe internet, comunicare (e-mail, telefonie și mesagerie online), divertisment (jocuri, filme/video și muzică), rețele de socializare, servicii bancare și servicii de localizare. S-a raportat că magazinele de aplicații sunt aprovizionate zilnic cu peste 1 600 de aplicații noi[1] și că un utilizator mediu de telefoane inteligente descarcă 37 de aplicații[2]. Astfel de aplicații pot fi furnizate utilizatorilor finali la costuri inițiale reduse sau fără costuri inițiale, adresându-se unui public format din doar câțiva indivizi sau din milioane de persoane.

Sistemul subiacent de operare va include, de asemenea, structuri software sau de date importante pentru serviciile de bază oferite de dispozitivele inteligente, de exemplu, carnetul de adrese al unui telefon inteligent. Sistemul de operare este proiectat astfel încât să pună componentele respective la dispoziția aplicațiilor prin intermediul interfețelor de programare a aplicațiilor (*Application Programming Interfaces* – API). API oferă acces la o multitudine de senzori care pot fi prezenți pe dispozitivele inteligente, printre care se numără un giroscop, o busolă digitală și un accelerometru care indică viteza și direcția de mișcare, camere frontale și posterioare care filmează și fotografiază, precum și un microfon pentru înregistrări audio. De asemenea, dispozitivele inteligente pot să conțină senzori de proximitate[3] și să se conecteze prin diferite interfețe de rețea, inclusiv Wi-Fi, Bluetooth, NFC (*near field communication* - comunicare în câmp apropiat) sau Ethernet. În fine, poziția exactă se poate stabili prin intermediul serviciilor de geolocalizare [astfel cum se descrie în Avizul nr. 13/2011 privind serviciile de geolocalizare pe dispozitivele mobile inteligente emis de grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal (GL29)[4]]. Tipul, acuratețea și frecvența datelor furnizate de senzorii respectivi variază în funcție de dispozitivul utilizat și de sistemul de operare.

---

1 Raportul ConceivablyTech din 19 august 2012, disponibil la următoarea adresă: www.conceivablytech.com/10283/business/apple-app-store-to-reach-1mapps-this-year-sort-of. Citat de Kamala D. Harris, procurorul general al Departamentului de Justiție din California, „Privacy on the go, Recommendations for the mobile ecosystem" din ianuarie 2013: http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.

2 Aceasta este o estimare globală pentru 2012 furnizată de ABI Research la următoarea adresă: http://www.abiresearch.com/press/smartphone-users-worldwide-will-download-37-apps-o

3 Un senzor care poate detecta prezența unui obiect fizic în lipsa contactului fizic. A se vedea: http://www.w3.org/TR/2012/WD-proximity-20121206/

4 A se vedea Avizul nr. 13/2011 al GL29 privind serviciile de geolocalizare pe dispozitivele mobile inteligente (mai 2011): http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf.

Prin intermediul API, dezvoltatorii de aplicații pot să colecteze încontinuu astfel de date, să acceseze și să scrie date de contact, să trimită e-mail-uri, SMS-uri sau mesaje pe rețelele de socializare, să citească/să modifice/să șteargă conținutul cartelelor SD, să înregistreze mesaje audio, să utilizeze camera foto și să acceseze fotografiile stocate, să citească starea și identitatea telefonului, să modifice parametrii generali ai sistemului și să împiedice intrarea telefonului în stare de veghe. De asemenea, API pot să furnizeze informații referitoare la dispozitivul în cauză prin intermediul unuia sau a mai multor identificatori unici, precum și informații privind alte aplicații instalate. Sursele respective de date pot fi prelucrate ulterior, în general în scopul de a genera un flux de venituri, într-o manieră care poate fi necunoscută sau nedorită de către utilizatorii finali.

Obiectivul prezentului aviz este de a clarifica cadrul juridic aplicabil prelucrării datelor cu caracter personal în contextul distribuției și al utilizării de aplicații pe dispozitivele inteligente și de a lua în considerare eventuala prelucrare ulterioară care poate avea loc în afara aplicațiilor, cum ar fi utilizarea datelor colectate pentru crearea de profiluri și vizarea utilizatorilor. Avizul analizează principalele riscuri legate de protecția datelor, furnizează o descriere a diferitelor părți implicate și evidențiază diferitele responsabilități juridice. Printre părțile implicate se numără dezvoltatorii de aplicații, proprietarii de aplicații, magazinele de aplicații, producătorii de dispozitive și de sisteme de operare (producătorii de dispozitive și de SO), precum și alți terți care pot fi implicați în colectarea și prelucrarea datelor cu caracter personal preluate din dispozitivele inteligente, cum ar fi furnizorii de instrumente analitice și de servicii de publicitate.

Prezentul aviz se concentrează pe cerința de obținere a consimțământului, principiile limitării scopului și minimizării datelor, necesitatea adoptării unor măsuri de securitate corespunzătoare, obligația de a asigura informarea corectă a utilizatorilor finali, drepturile utilizatorilor finali, perioadele corespunzătoare de păstrare a datelor și, în special, prelucrarea corectă a datelor colectate de la copii și referitoare la aceștia.

Domeniul de aplicare al prezentului aviz cuprinde numeroase tipuri de dispozitive inteligente diferite, vizând, în special, aplicațiile disponibile pentru dispozitivele mobile inteligente.

2. Riscuri legate de protecția datelor

Interacțiunea strânsă cu sistemul de operare permite aplicațiilor să acceseze o cantitate mult mai mare de date în comparație cu un browser tradițional[5]. Aplicațiile sunt capabile să colecteze cantități semnificative de date din dispozitivul mobil (date de localizare, date stocate în dispozitiv de către utilizatori și date furnizate de diferiți senzori) și să le prelucreze cu scopul de a oferi utilizatorilor finali servicii noi și inovatoare.

Un risc ridicat la adresa protecției datelor cu caracter personal rezultă din gradul de fragmentare a mediului de dezvoltare a aplicațiilor între numeroși actori. O informație poate fi transmisă din dispozitiv în timp real spre a fi prelucrată oriunde în lume sau pentru a fi copiată între diferite lanțuri de terți. Unele dintre cele mai cunoscute aplicații sunt dezvoltate de către companii de tehnologie importante, însă multe altele sunt proiectate de către întreprinderi mici

[5] Cu toate că, sub impulsul dezvoltatorilor de jocuri pe internet, browserele de calculator au un acces tot mai mare la datele furnizate de senzori cu privire la dispozitivele utilizatorilor finali.

nou-înființate. Un programator care vine cu o idee, fără a deține competențe de programare sau având competențe limitate, poate ajunge la un public de talie mondială într-o perioadă de timp foarte scurtă. Dezvoltatorii de aplicații care nu cunosc cerințele în materie de protecție a datelor cu caracter personal pot crea riscuri semnificative la adresa vieții private și a reputației utilizatorilor de dispozitive inteligente. În același timp, serviciile furnizate de către terți, cum ar fi serviciile de publicitate, cunosc o dezvoltare rapidă și, în cazul în care sunt integrate de către un dezvoltator de aplicații fără atenția cuvenită, există posibilitatea să divulge cantități semnificative de date cu caracter personal.

Principalele riscuri legate de protecția datelor cu caracter personal ale utilizatorilor finali sunt lipsa de transparență și de cunoaștere a tipurilor de prelucrări operate de o aplicație și lipsa consimțământului în cunoștință de cauză din partea utilizatorilor finali înainte de prelucrarea datelor respective. Măsurile de securitate deficiente, o tendință evidentă de maximizare a datelor și elasticitatea scopurilor în care sunt colectate datele cu caracter personal contribuie, de asemenea, la apariția riscurilor cu privire la protecția datelor cu caracter personal în mediul actual al aplicațiilor. O mare parte din riscurile respective au fost deja examinate și abordate de alte autorități internaționale de reglementare, cum ar fi Comisia Federală pentru Comerț (FTC) din SUA, Comisariatul pentru protecția vieții private din Canada și Procurorul General al Departamentului de Justiție din California[6].

- Un risc esențial în legătură cu protecția datelor este lipsa de transparență. Dezvoltatorii de aplicații sunt constrânși, prin caracteristicile propuse de producătorii sistemelor de operare și de magazinele de aplicații, să garanteze furnizarea unor informații cuprinzătoare, la momentul oportun, către utilizatorii finali. Cu toate acestea, nu toți dezvoltatorii de aplicații profită de aceste caracteristici, întrucât numeroase aplicații nu dețin o politică de confidențialitate sau nu reușesc să își informeze în mod clar potențialii utilizatori în legătură cu tipul de date cu caracter personal care pot fi prelucrate de aplicație și cu scopul în care urmează să fie prelucrate acestea. Lipsa de transparență nu se limitează la aplicațiile gratuite sau la cele deținute de dezvoltatori fără experiență, întrucât studiile recente au indicat că doar 61,3 % din cele mai importante 150 de aplicații propun o politică de confidențialitate[7].

- Lipsa de transparență este strâns legată de lipsa consimțământului exprimat liber și în cunoștință de cauză. După ce aplicația a fost descărcată, consimțământul se reduce, de cele mai multe ori, la o căsuță prin a cărei bifarea utilizatorul final indică acceptarea clauzelor și a condițiilor, fără a avea nici măcar opțiunea „Nu, mulțumesc”. Conform

[6] A se vedea, printre altele, raportul serviciilor FTC „Mobile Privacy Disclosures, Building Trust Through Transparency”, februarie 2013: http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf; raportul serviciilor FTC „Mobile Apps for Kids: Current Privacy Disclosures are Disappointing”, februarie 2012: http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf; raportul de urmărire „Mobile Apps for Kids: Disclosures Still Not Making the Grade”, decembrie 2012: http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf; raportul Comisariatului pentru protecția vieții private din Canada „Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps”, octombrie 2012: http://www.priv.gc.ca/information/pub/gd_app_201210_e.pdf; raportul procurorului general al Departamentului de Justiție al Californiei, Kamala D. Harris, „Privacy on the go, Recommendations for the mobile ecosystem”, ianuarie 2013: http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf

[7] Studiul FPF referitor la aplicațiile mobile, iunie 2012: http://www.futureofprivacy.org/wp-content/uploads/Mobile-Apps-Study-June-2012.pdf

unui studiu al GSMA din septembrie 2011, 92 % din utilizatorii de aplicații doresc să dispună de opțiuni mai detaliate[8].

- Măsurile deficiente de securitate pot conduce la prelucrarea neautorizată a datelor (sensibile) cu caracter personal, de exemplu, în cazul încălcării confidențialității datelor cu caracter personal la un dezvoltator de aplicații sau în cazul unor scurgeri de date cu caracter personal în aplicația respectivă.

- Un alt risc pentru protecția datelor este legat de nerespectarea (din ignoranță sau intenționat) a principiului limitării scopului, conform căruia datele cu caracter personal pot fi colectate și prelucrate numai în scopuri specifice și legitime. Datele cu caracter personal colectate de aplicații pot fi distribuite la scară largă către o serie de terți în scopuri nedefinite sau elastice precum „cercetarea de piață". Aceeași nerespectare alarmantă se observă și în ceea ce privește principiul minimizării datelor. Studiile recente indică faptul că numeroase aplicații colectează cantități semnificative de date provenind de la telefoanele inteligente fără nicio legătură semnificativă cu funcționalitatea aparentă a aplicațiilor respective[9].

3 Principiile aplicabile în domeniul protecției datelor

3.1 Dreptul aplicabil

Cadrul juridic relevant al UE este reprezentat de Directiva privind protecția datelor (95/46/CE). Aceasta se aplică ori de câte ori utilizarea aplicațiilor instalate pe dispozitivele inteligente implică prelucrarea datelor cu caracter personal ale persoanelor fizice. Pentru a identifica dreptul aplicabil, este esențial să se identifice în primul rând rolul diferitelor părți interesate implicate: identificarea operatorului (operatorilor) procesului de prelucrare desfășurat prin intermediul aplicațiilor mobile este deosebit de importantă pentru stabilirea dreptului aplicabil. Stabilirea operatorului reprezintă un aspect decisiv care declanșează aplicarea legislației UE în domeniul protecției datelor, deși nu reprezintă singurul criteriu în acest sens. În conformitate cu articolul 4 alineatul (1) litera (a) din Directiva privind protecția datelor, dreptul intern al unui stat membru este aplicabil tuturor proceselor de prelucrare a datelor cu caracter personal desfășurate „în contextul stabilirii" operatorului pe teritoriul statului membru în cauză. În temeiul articolului 4 alineatul (1) litera (c) din Directiva privind protecția datelor, dreptul intern al unui stat membru este aplicabil, de asemenea, în cazul unui operator care *nu este stabilit* pe teritoriul Comunității și care utilizează echipamente situate pe teritoriul statului membru în cauză. Dat fiind că dispozitivul are o contribuție fundamentală la procesul de prelucrare a datelor cu caracter personal furnizate de către utilizator și referitoare la acesta, acest criteriu este de obicei îndeplinit[10]. Acest aspect este relevant însă numai în cazul în care operatorul nu este stabilit pe teritoriul UE.

---

[8] „*89 % [din utilizatori] consideră că este important să știe când datele lor cu caracter personal sunt făcute cunoscute de o aplicație și să dispună de posibilitatea de a închide aplicația respectivă.*" Sursă: studiul „User perspectives on mobile privacy", septembrie 2011: 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

[10] În măsura în care aplicația generează un trafic de date cu caracter personal către operatorii de date. Este posibil ca acest criteriu să nu fie îndeplinit în cazul în care datele sunt prelucrate doar la nivel local, chiar în dispozitiv.

În consecință, ori de câte ori o parte implicată în dezvoltarea, distribuția și operarea aplicațiilor este considerată a fi operatorul, aceasta răspunde, pe cont propriu sau împreună cu alte părți, de asigurarea respectării tuturor cerințelor prevăzute de Directiva privind protecția datelor. Identificarea rolului părților implicate în dezvoltarea aplicațiilor mobile va fi analizat pe larg în secțiunea 3.3 de mai jos.

Pe lângă Directiva privind protecția datelor, Directiva asupra confidențialității și comunicațiilor electronice (2002/58/CE, revizuită de Directiva 2009/136/CE) prevede un standard specific pentru toate părțile la nivel mondial care doresc să stocheze sau să acceseze informații stocate în dispozitivele utilizatorilor din Spațiul Economic European (SEE).

Articolul 5 alineatul (3) din Directiva asupra confidențialității și comunicațiilor electronice prevede că „*stocarea sau accesarea informațiilor stocate în echipamentul terminal al unui abonat sau utilizator este permisă doar cu condiția ca abonatul sau utilizatorul în cauză să fi primit informații clare și complete, în conformitate cu Directiva 95/46/CE,* inter alia*, cu privire la scopul prelucrării [...].”*

Deși multe din dispozițiilor Directivei asupra confidențialității și comunicațiilor electronice se aplică numai furnizorilor de servicii de comunicații electronice accesibile publicului și furnizorilor de rețele de comunicații publice de pe teritoriul Comunității, articolul 5 alineatul (3) se aplică fiecărei entități care stochează informații pe dispozitive inteligente sau citește informații de pe dispozitive inteligente. Acesta se aplică indiferent de natura entității respective (și anume, indiferent dacă programatorul individual este o entitate publică sau privată sau o corporație importantă sau dacă este vorba despre un operator de date, o persoană împuternicită de către operator sau un terț).

Cerința de obținere a consimțământului, prevăzută la articolul 5 alineatul (3), se aplică tuturor informațiilor, indiferent de natura datelor stocate sau accesate. Domeniul de aplicare nu se limitează la datele cu caracter personal; informațiile respective pot consta în orice tip de date stocate pe dispozitiv.

Cerința de obținere a consimțământului, prevăzută la articolul 5 alineatul (3) din Directiva asupra confidențialității și comunicațiilor electronice, se aplică serviciilor furnizate „*pe teritoriul Comunității*”, și anume, tuturor persoanelor fizice din Spațiul Economic European, indiferent de amplasarea furnizorului de servicii. Este important ca dezvoltatorii de aplicații să știe că ambele directive au un caracter juridic obligatoriu, și anume că drepturile indivizilor sunt inalienabile și că acestea nu se supun renunțărilor contractuale. Aceasta înseamnă că aplicabilitatea legislației europene în domeniul protecției vieții private nu poate fi exclusă printr-o declarație unilaterală sau printr-un acord contractual[11].

3.2 Datele cu caracter personal prelucrate de aplicații

Numeroase tipuri de date stocate pe un dispozitiv inteligent sau generate de un dispozitiv inteligent sunt date cu caracter personal. În conformitate cu considerentul 24 din Directiva asupra confidențialității și comunicațiilor electronice:

[11] De exemplu, declarații conform cărora se aplică doar dreptul unei jurisdicții din afara SEE.

„Echipamentul terminal al utilizatorului de rețele de comunicații electronice și orice informație stocată în acesta fac parte din sfera privată a utilizatorului protejată conform Convenției Europene pentru Protecția Drepturilor Omului și a Libertăților Fundamentale."

Acestea sunt considerate date cu caracter personal ori de câte ori se referă la o persoană fizică identificabilă în mod direct (de exemplu, prin intermediul numelui) sau indirect de către un operator sau un terț. Ele se pot referi la proprietarul dispozitivului sau la orice altă persoană, cum ar fi datele de contact ale prietenilor din carnetul de adrese[12]. Datele pot fi colectate și prelucrate pe dispozitiv sau, odată transferate, în orice altă parte, pe infrastructura dezvoltatorilor de aplicații sau a terților, prin intermediul unei conexiuni spre o API externă, în timp real și fără știrea utilizatorului final.

Exemple de astfel de date cu caracter personal care pot avea un impact semnificativ asupra vieții private a utilizatorilor și a altor persoane sunt următoarele:

- poziția exactă
- contacte
- identificatori unici ai dispozitivului și ai consumatorului (cum ar fi IMEI[13], IMSI[14], IUD[15] și numărul de telefon mobil)
- identitatea persoanei vizate
- identitatea telefonului (și anume, numele telefonului[16])
- cartea de credit și datele referitoare la plăți
- jurnalul de apeluri telefonice, SMS-uri sau mesagerie instantanee
- istoricul navigărilor
- e-mail
- datele de autentificare pentru serviciile societății informaționale (în special serviciile cu caracter social)
- fotografii și înregistrări video
- date biometrice (de exemplu, recunoașterea facială și modele de amprente digitale)

3.3 Părțile implicate în prelucrarea datelor cu caracter personal

În dezvoltarea, distribuția și operarea aplicațiilor sunt implicate numeroase părți diferite, fiecare dintre acestea putând avea diverse responsabilități în materie de protecție a datelor.

Pot fi identificate patru părți principale, și anume: (i) dezvoltatorii de aplicații (inclusiv proprietarii de aplicații)[17], producătorii de sisteme de operare și de dispozitive („operatorii de

[12] Datele pot fi (i) generate în mod automat de dispozitiv, pe baza caracteristicilor determinate în prealabil de producătorul de SO și/sau de dispozitive sau de furnizorul relevant de telefonie mobilă (de exemplu, date de geolocalizare, parametri de rețea, adresă IP); (ii) generate de utilizator prin intermediul aplicațiilor (liste de contact; notițe, fotografii); (iii) generate de aplicații (de exemplu, istoricul navigărilor)

[13] **Identitatea** internațională a echipamentului mobil (IMEI).

[14] **Identitatea** internațională de abonat mobil (IMSI).

[15] Identificatorul unic al dispozitivului (IUD).

[16] Utilizatorii au tendința de a-și denumi telefoanele cu numele lor real: „iPhone-ul lui Ion Popescu".

[17] Grupul de lucru utilizează terminologia comună de „dezvoltatori de aplicații", însă subliniază faptul că termenul nu se limitează la programatorii sau dezvoltatorii tehnici de aplicații, ci include proprietarii de aplicații, și anume, companiile și organizațiile care solicită dezvoltarea aplicațiilor și care determină scopul acestora.

SO și de dispozitive")[18], (iii) magazinele de aplicații (distribuitorul de aplicații) și, în fine, (iv) alte părți implicate în prelucrarea datelor cu caracter personal. În anumite cazuri, responsabilitățile în materie de protecție a datelor sunt partajate, în special atunci când aceeași entitate este implicată la diferite niveluri, de exemplu, în cazul în care producătorul de SO controlează și magazinul de aplicații.

De asemenea, utilizatorii finali trebuie să își asume răspunderea corespunzătoare în cazul în care creează și stochează date cu caracter personal cu ajutorul dispozitivelor mobile. Dacă prelucrarea datelor respective are loc exclusiv în scopuri proprii sau casnice, Directiva privind protecția datelor nu se aplică [articolul 3 alineatul (2)], iar utilizatorul este scutit de obligațiile oficiale în materie de protecție a datelor. Dacă utilizatorii decid totuși să împărtășească datele prin intermediul aplicației, de exemplu, prin punerea informațiilor respective la dispoziția unui public format dintr-un număr nedefinit de persoane[19] cu ajutorul unei aplicații de socializare în rețea, aceștia prelucrează informațiile în afara domeniului de aplicare al condițiilor de scutire în scopuri casnice[20].

3.3.1 Dezvoltatorii de aplicații

Dezvoltatorii de aplicații creează aplicații și/sau le pun la dispoziția utilizatorilor finali. Din această categorie fac parte organizațiile din sectorul public și privat care externalizează dezvoltarea aplicațiilor, precum și companiile și persoanele care creează și dezvoltă astfel de aplicații. Dezvoltatorii proiectează și/sau creează software-ul care va fi instalat pe telefoanele inteligente, stabilind astfel măsura în care aplicația respectivă va accesa și prelucra diferitele categorii de date cu caracter personal din dispozitiv și/sau prin intermediul resurselor informatice aflate la distanță (unitățile informatice ale dezvoltatorilor de aplicații sau ale terților).
În măsura în care dezvoltatorul de aplicații stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal din dispozitivele inteligente, acesta constituie operatorul de date, astfel cum este definit la articolul 2 litera (d) din Directiva privind protecția datelor. În acest caz, dezvoltatorul de aplicații trebuie să respecte toate dispozițiile Directivei privind protecția datelor cu caracter personal. Principalele dispoziții sunt explicate la secțiunile 3.4-3.10 din prezentul aviz.

Inclusiv în cazul în care se aplică scutirea în scopuri casnice pentru un utilizator, dezvoltatorul de aplicații este în continuare responsabil, în calitate de operator de date, dacă prelucrează datele în scopuri proprii. Acest lucru este relevant, de exemplu, în cazul în care aplicația necesită accesul la întregul carnet de adrese cu scopul de a furniza serviciul respectiv (mesagerie instantanee, apeluri telefonice, apeluri video).

Responsabilitățile dezvoltatorului de aplicații vor fi limitate în mod semnificativ în cazul în care nu se prelucrează și/sau nu se fac publice date cu caracter personal în afara dispozitivului sau dacă dezvoltatorul de aplicații a adoptat măsurile tehnice și organizaționale

---

[18] În anumite cazuri, producătorul de SO este unul și același cu producătorul dispozitivului, în timp ce, în alte cazuri, producătorul dispozitivului este o companie diferită de furnizorul de SO.

[19] A se vedea jurisprudența Curții de Justiție a Uniunii Europene, hotărârea din 6 noiembrie 2003 în cauza C-101/01 *Proces penal împotriva BodilLindqvist* și hotărârea din 16 decembrie 2008 în cauza C-73/07 *Tietosuojavaltuutettu/SatakunnanMarkkinapörssiOy și SatamediaOy*.

[20] A se vedea Avizul nr. 5/2009 al GL29 privind socializarea în rețea online (iunie 2009): http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_ro.pdf

corespunzătoare pentru a se asigura că datele sunt anonimizate în mod ireversibil și agregate pe dispozitiv înainte ca acestea să părăsească dispozitivul în cauză.

În orice caz, dacă dezvoltatorul de aplicații obține accesul la informațiile care sunt stocate în dispozitiv, se aplică, de asemenea, Directiva asupra confidențialității și comunicațiilor electronice, iar dezvoltatorul de aplicații trebuie să respecte cerința de obținere a consimțământului, prevăzută la articolul 5 alineatul (3) din directivă.

În măsura în care dezvoltatorul de aplicații a externalizat, integral sau parțial, prelucrarea datelor către un terț, iar terțul respectiv își asumă rolul de persoană împuternicită de către operator, atunci dezvoltatorul de aplicații trebuie să respecte toate obligațiile legate de utilizarea unei persoane împuternicite de către operator. Aceasta ar include, de asemenea, utilizarea unui furnizor de servicii de informatică dematerializată („cloud computing”) (de exemplu, pentru stocarea externă a datelor)[21].

În măsura în care dezvoltatorul de aplicații permite terților accesul la datele de utilizator (cum ar fi o rețea de publicitate care accesează datele privind poziția geografică a dispozitivului cu scopul de a furniza servicii de publicitate comportamentală), acesta trebuie să apeleze la mecanismele corespunzătoare pentru a respecta cerințele aplicabile în conformitate cu cadrul juridic al UE. În cazul în care terțul accesează datele stocate în dispozitiv, se aplică obligația de obținere a consimțământului, prevăzută la articolul 5 alineatul (3) din Directiva asupra confidențialității și comunicațiilor electronice. De asemenea, în cazul în care terțul prelucrează date cu caracter personal în scopuri proprii, aceasta poate fi operator comun de date împreună cu dezvoltatorul de aplicații și, prin urmare, trebuie să respecte principiul limitării scopului și obligațiile în materie de securitate[22] în ceea ce privește partea prelucrării ale cărei scopuri și mijloace le determină. Întrucât pot exista diferite tipuri de acorduri, de natură atât comercială, cât și tehnică, între dezvoltatorii de aplicații și terți, responsabilitatea fiecărei părți va trebui să fie stabilită de la caz la caz, luându-se în considerare circumstanțele specifice ale prelucrării în cauză.

Un dezvoltator de aplicații poate utiliza bibliotecile terțului cu ajutorul unui software care furnizează funcționalități comune, cum ar fi, de exemplu, o bibliotecă pentru o platformă de jocuri sociale. Dezvoltatorul de aplicații trebuie să se asigure că utilizatorii au cunoștință de orice prelucrare a datelor de către bibliotecile în cauză și, în cazul în care au loc astfel de prelucrări, că prelucrarea datelor respective respectă cadrul juridic al UE, inclusiv, dacă este relevant, prin obținerea consimțământului din partea utilizatorilor. În acest sens, dezvoltatorii de aplicații trebuie să prevină utilizarea funcționalităților ascunse utilizatorilor.

3.3.2 Producătorii de SO și de dispozitive

Producătorii de SO și de dispozitive ar trebui considerați, de asemenea, operatori de date (și, dacă este relevant, operatori comuni) în ceea ce privește orice prelucrare a datelor cu caracter personal în scopuri proprii, cum ar fi buna funcționare a dispozitivului, securitatea etc. În

[21] A se vedea Avizul nr. 05/2012 al GL29 privind „cloud computing” (iulie 2012): http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_ro.pdf.

[22] A se vedea Avizul nr. 2/2010 al GL29 privind publicitatea comportamentală online (iunie 2010): http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_ro.pdf și Avizul nr. 1/2010 al GL29 privind conceptele de „operator” și „persoană împuternicită de către operator” (februarie 2010): http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_ro.pdf

categoria respectivă s-ar încadra datele generate de utilizatori (de exemplu, datele de contact ale utilizatorilor în momentul înregistrării), datele generate în mod automat de dispozitiv [de exemplu, în cazul în care dispozitivul deține o funcționalitate „apelare acasă” (*phone home*) necesară pentru localizare] sau datele cu caracter personal prelucrate de către producătorul de SO sau de dispozitive care rezultă din instalarea sau utilizarea aplicațiilor respective. În cazul în care producătorii de SO sau de dispozitive furnizează o funcționalitate suplimentară, cum ar fi o facilitate de salvare de rezervă sau de localizare la distanță, aceștia ar putea fi considerați, în egală măsură, operatori de date în ceea ce privește prelucrarea datelor cu caracter personal în acest scop.

Aplicațiile care necesită accesul la datele de geolocalizare trebuie să utilizeze serviciile de localizare ale SO. În cazul în care o aplicație utilizează geolocalizarea, SO poate colecta date cu caracter personal cu scopul de furniza aplicațiilor informații de geolocalizare, putând lua în considerare, de asemenea, utilizarea datelor respective în vederea îmbunătățirii propriilor servicii de localizare. În ultimul caz menționat, SO este operatorul de date.

De asemenea, producătorii de SO și de dispozitive răspund de interfața de programare a aplicațiilor (API), care permite prelucrarea datelor cu caracter personal de către aplicație pe dispozitivul inteligent. Dezvoltatorul de aplicații va putea să acceseze caracteristicile și funcțiile respective puse la dispoziție de către producătorii de SO și de dispozitive prin intermediul API. Întrucât producătorii de SO și de dispozitive stabilesc mijloacele (și amploarea) accesului la datele cu caracter personal, aceștia trebuie să se asigure că dezvoltatorul de aplicații dispune de un control suficient de detaliat pentru ca accesul să poată fi furnizat numai la datele care sunt necesare pentru funcționarea aplicației. De asemenea, producătorii de SO și de dispozitive ar trebui să se asigure că accesul respectiv poate fi revocat într-o manieră simplă și eficace.

Conceptul privind „luarea în considerare a vieții private începând cu momentul conceperii” (*privacy by design*) este un principiu important la care se face trimitere în mod indirect în Directiva privind protecția datelor[23] și care, împreună cu principiul privind „luarea în considerare a vieții private în setările standard” (*privacy by default*), este menționat cu mai multă claritate în Directiva asupra confidențialității și comunicațiilor electronice[24]. Conform acestuia, producătorii de dispozitive sau de aplicații au obligația de a integra protecția datelor încă din momentul conceperii. Luarea în considerare a vieții private începând cu momentul conceperii este necesară în mod explicit pentru proiectarea echipamentelor de telecomunicații, astfel cum se prevede în Directiva privind echipamentele hertziene și echipamentele terminale de telecomunicații[25]. Prin urmare, producătorii de SO și de dispozitive, împreună cu magazinele de aplicații, dețin o responsabilitate importantă în ceea ce privește garantarea protecției datelor cu caracter personal și a vieții private a utilizatorilor de aplicații. Aceasta include garantarea disponibilității mecanismelor corespunzătoare de informare și educare a

[23] A se vedea considerentul 46 și articolul 17.

[24] A se vedea articolul 14 alineatul (3).

[25] Directiva 1999/5/CE din 9 martie 1999 privind echipamentele hertziene și echipamentele terminale de telecomunicații și recunoașterea reciprocă a conformității acestora. Jurnalul Oficial al Comunităților Europene nr. L 91/10 din 7.4.1999. Articolul 3 alineatul (3) litera (c) prevede că Comisia Europeană poate dispune ca dispozitivele utilizatorului final să fie construite astfel încât să prezinte garanții pentru asigurarea protecției datelor cu caracter personal și a vieții private a utilizatorilor și a abonaților.

utilizatorilor finali cu privire la ceea ce pot face aplicațiile și la tipul de date care pot fi accesate, precum și la furnizarea setărilor corespunzătoare care permit utilizatorilor aplicației să modifice parametrii procesului de prelucrare a datelor[26].

3.3.3 Magazinele de aplicații

Fiecare dintre cele mai răspândite tipuri de dispozitive inteligente deține propriul magazin de aplicații, fiind frecvente cazurile în care un anumit SO este strâns legat de un anumit magazin de aplicații. Adeseori, magazinele de aplicații prelucrează plățile inițiale pentru aplicații, putând să se ocupe și de achizițiile integrate în aplicații și, în consecință, să solicite înregistrarea utilizatorului cu nume, adresă și date financiare. Aceste date identificabile (în mod direct) pot fi combinate cu datele referitoare la achiziții și obișnuințele de utilizare, precum și cu datele citite din dispozitiv sau generate de acesta (cum ar fi identificatorii unici). În vederea prelucrării datelor cu caracter personal în cauză, magazinele de aplicații constituie probabil operatorul de date, inclusiv dacă raportează astfel de informații dezvoltatorilor de aplicații. În cazul în care magazinele de aplicații prelucrează descărcarea unei aplicații a unui utilizator final, istoricul accesărilor sau o facilitate similară destinată restaurării aplicațiilor descărcate anterior, acestea constituie, de asemenea, operatorul de date în ceea ce privește prelucrarea datelor cu caracter personal în acest scop.

Un magazin de aplicații înregistrează datele de identificare a conectărilor, precum și istoricul aplicațiilor achiziționate. De asemenea, acesta solicită utilizatorului să furnizeze numărul cărții de credit, care va fi stocat împreună cu contul de utilizator. În cazul operațiilor respective, magazinul de aplicații este operatorul de date.

Dimpotrivă, este posibil ca site-urile care permit instalarea pe dispozitiv a unei aplicații descărcate fără o autentificare prealabilă să nu prelucreze date cu caracter personal.

Magazinele de aplicații se află în poziția importantă de a permite dezvoltatorilor de aplicații să furnizeze informații corespunzătoare cu privire la aplicații, inclusiv tipurile de date care pot fi prelucrate de aplicațiile respective și scopurile în care sunt prelucrate acestea. Magazinele de aplicații pot asigura respectarea normelor respective prin intermediul politicii de acces (pe baza controalelor ex-ante sau ex-post). În colaborare cu producătorul de SO, magazinul de aplicații poate dezvolta un cadru pentru a permite dezvoltatorilor de aplicații să furnizeze note de informare coerente și semnificative (cum ar fi simboluri care reprezintă anumite tipuri de acces la datele furnizate de senzori) și să le afișeze în mod vizibil în catalogul magazinului de aplicații.

3.3.4 Terții

În procesul de prelucrare a datelor cu caracter personal prin intermediul aplicațiilor sunt implicați numeroși terți.

[26] Grupul de lucru salută recomandările în acest sens din raportul serviciilor FTC intitulat „Mobile Privacy Disclosures”, menționat la nota de subsol nr. 6 de mai sus, de exemplu, la pagina 15: „[…] *platformele se află în poziția unică de a divulga cantități semnificative de date între aplicații, fiind încurajate să facă acest lucru. În conformitate cu observațiile formulate în cadrul atelierului de lucru, acestea pot lua în considerare, în egală măsură, divulgarea informațiilor respective la diferite momente în timp […]*.”

De exemplu, numeroase aplicații libere sunt plătite prin intermediul publicității care poate include, fără a se limita la aceasta, publicitatea contextuală sau personalizată, care poate avea loc prin mecanisme de urmărire precum module cookie sau alți identificatori ai dispozitivului. Publicitatea poate consta într-un spațiu publicitar în cadrul aplicației, reclame în afara aplicației, furnizate prin modificarea setărilor de navigare, plasarea de pictograme pe dispozitivul mobil sau organizarea personalizată a conținutului aplicației (de exemplu, rezultate de căutare sponsorizate).

Publicitatea în domeniul aplicațiilor este furnizată, în general, prin intermediul rețelelor de publicitate și al intermediarilor similari care pot avea legătură sau care pot fi identici cu producătorul de SO sau cu magazinul de aplicații. Astfel cum se subliniază în Avizul nr. 2/2010[27] al GL29, publicitatea online implică de cele mai multe ori prelucrarea datelor cu caracter personal prevăzută la articolul 2 din Directiva privind protecția datelor și interpretată de grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal, instituit în temeiul articolului 29[28].

Alte exemple de terți sunt furnizorii de instrumente analitice și furnizorii de servicii de comunicații. Furnizorii de instrumente analitice permit dezvoltatorilor să obțină mai multe informații privind utilizarea, popularitatea și utilitatea aplicațiilor acestora. Furnizorii de servicii de comunicații[29] pot juca, de asemenea, un rol important în stabilirea setărilor standard și a actualizărilor de securitate ale diferitelor dispozitive, putând prelucra date referitoare la utilizarea aplicațiilor respective. Personalizarea acestora („branding”) poate afecta potențialele măsuri tehnice și funcționale care pot fi aplicate de utilizator pentru a-și proteja datele cu caracter personal.

În comparație cu dezvoltatorii de aplicații, terții pot juca două tipuri de roluri: unul constă în executarea operațiunilor pentru proprietarul aplicației, de exemplu, în scopul de a integra instrumente analitice chiar în aplicație. În acest caz, atunci când acționează exclusiv în numele dezvoltatorului de aplicații și nu prelucrează date în scopuri proprii și/sau nu împărtășesc datele respective cu dezvoltatorii, terții acționează mai degrabă ca persoană împuternicită de către operator.

Cel de-al doilea rol constă în colectarea informațiilor din diverse aplicații cu scopul de a furniza servicii suplimentare: furnizarea de cifre analitice la scară mai largă (popularitatea aplicațiilor, recomandări personalizate) sau evitarea afișării aceleiași reclame pentru același utilizator. În cazul în care terții prelucrează date cu caracter personal în scopuri proprii, acestea acționează în calitate de operatori de date, prin urmare, trebuie să respecte toate dispozițiile aplicabile ale Directivei privind protecția datelor cu caracter personal[30]. În cazul publicității comportamentale, operatorul de date trebuie să obțină consimțământul valabil al utilizatorului pentru colectarea și prelucrarea datelor cu caracter personal, constând, de

---

[27] Avizul nr. 2/2010 al GL29 privind publicitatea comportamentală online (iunie 2010): http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_ro.pdf

[28] A se vedea, de asemenea, interpretarea conceptului de date cu caracter personal din Avizul nr. 4/2007 al GL29 privind conceptul de date cu caracter personal (iunie 2007), disponibil la următoarea adresă: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_ro.pdf

[29] Furnizorii de servicii de comunicații trebuie să respecte, la rândul lor, obligațiile de protecție a datelor specifice sectorului în care operează și care depășesc domeniul de aplicare al prezentului aviz.

[30] Avizul nr. 2/2010 al GL29 privind publicitatea comportamentală online, p. 10-11.

exemplu, în analiza și combinarea datelor respective și în crearea și/sau aplicarea de profiluri. În conformitate cu cele menționate anterior în Avizul nr. 2/2012 privind publicitatea comportamentală online, adoptat de GL29, cea mai bună modalitate de obținere a unui astfel de consimțământ constă în utilizarea mecanism de „opt-in" (consimțământ acordat expres) prealabil.

O companie furnizează metrici pentru proprietarii de aplicații și agențiile de publicitate prin intermediul utilizării mecanismelor de urmărire integrate de către dezvoltatorul de aplicații în aplicații. Prin urmare, mecanismele de urmărire ale companiei pot fi instalate pe numeroase aplicații și dispozitive. Unul dintre serviciile furnizate constă în informarea dezvoltatorilor de aplicații cu privire la alte aplicații utilizate de către un utilizator prin intermediul colectării unui identificator unic. Compania definește mijloacele (și anume, mecanismele de urmărire) și scopurile instrumentelor sale înainte de a le furniza dezvoltatorilor de aplicații, agențiilor de publicitate și altor părți, acționând, prin urmare, în calitate de operator de date.

În măsura în care terții accesează sau stochează informații din dispozitivul inteligent, aceștia trebuie să respecte cerința de obținere a consimțământului, prevăzută la articolul 5 alineatul (3) din Directiva asupra confidențialității și comunicațiilor electronice.

În acest context, este important de remarcat faptul că, în general, utilizatorii dispun pe dispozitivele inteligente de posibilități limitate de instalare a unui software care să controleze prelucrarea datelor cu caracter personal, astfel cum se obișnuiește în mediul online în cazul computerelor de birou. Ca alternativă la utilizarea modulelor cookie HTTP, terții accesează adeseori identificatori unici pentru a selecta anumiți utilizatori (anumite grupuri de utilizatori) și pentru a le propune servicii special concepute pentru ei, inclusiv reclame. Întrucât o mare parte dintre identificatorii respectivi nu pot fi eliminați sau modificați de către utilizatori (cum ar fi IMEI, IMSI, MSISDN[31] și identificatorii unici ai dispozitivelor adăugați de sistemul de operare), terții în cauză pot prelucra cantități semnificative de date cu caracter personal fără ca utilizatorul final să aibă vreun control asupra acestor prelucrări.

[31] Rețeaua numerică cu integrare de servicii pe stațiile mobile.

3.4 Temeiul juridic

Prelucrarea datelor cu caracter personal poate avea loc numai dacă există unul dintre temeiurile juridice prevăzute la articolul 7 din Directiva privind protecția datelor. Articolul 7 deosebește șase temeiuri juridice pentru prelucrarea datelor: persoana vizată și-a dat consimțământul neechivoc, prelucrarea este necesară pentru executarea unui contract la care subiectul datelor este parte, prelucrarea este necesară în scopul protejării interesului vital al persoanei vizate, prelucrarea este necesară pentru îndeplinirea unei obligații legale, (pentru autoritățile publice) prelucrarea este necesară pentru aducerea la îndeplinire a unei sarcini de interes public și prelucrarea este necesară pentru realizarea intereselor (comerciale) legitime.

În ceea ce privește stocarea informațiilor sau obținerea accesului la informațiile deja stocate pe dispozitivul inteligent, articolul 5 alineatul (3) din Directiva asupra confidențialității și comunicațiilor electronice (și anume cerința de obținere a consimțământului pentru introducerea/extragerea de informații într-un/dintr-un dispozitiv) impune o limită/restricție mai detaliată cu privire la temeiurile juridice care pot fi luate în considerare.

3.4.1 Acordul prealabil pentru instalarea și prelucrarea datelor cu caracter personal

În cazul aplicațiilor, principalul temei juridic aplicabil este consimțământul utilizatorului. În momentul instalării unei aplicații, în dispozitivul utilizatorului final sunt introduse informații. Numeroase aplicații accesează, de asemenea, datele stocate în dispozitiv, contactele din carnetul de adrese, fotografiile, filmele și alte documente personale. În toate aceste cazuri, articolul 5 alineatul (3) din Directiva asupra confidențialității și comunicațiilor electronice prevede obținerea consimțământului utilizatorului, în urma unei informări clare și complete, înainte de introducerea/extragerea de informații în/din dispozitiv.

Trebuie subliniată distincția dintre consimțământul necesar pentru introducerea/extragerea de informații în/din dispozitiv și consimțământul necesar în scopul de a se dispune de temei juridic pentru prelucrarea diferitelor tipuri de date cu caracter personal. Deși ambele cerințe privind consimțământul sunt aplicabile simultan, fiecare având un alt temei juridic, ambele tipuri de consimțământ trebuie să fie liber acordate, specifice și clare [astfel cum se prevede la articolul 2 litera (h) din Directiva privind protecția datelor]. Prin urmare, cele două tipuri de consimțământ pot fi combinate în practică, fie în timpul instalării, fie înainte ca aplicația să înceapă să colecteze date cu caracter personal din dispozitiv, cu condiția ca utilizatorului să i se aducă la cunoștință fără echivoc pentru ce anume își dă consimțământul.

Numeroase magazine de aplicații oferă dezvoltatorilor de aplicații posibilitatea de a informa utilizatorii finali cu privire la caracteristicile de bază ale unei aplicații înainte de instalare și de a solicita din partea acestora un răspuns pozitiv înainte de descărcarea și instalarea aplicației respective (și anume, făcând clic pe butonul „instalare”). În timp ce un astfel de răspuns poate, în anumite circumstanțe, să îndeplinească cerința de obținere a consimțământului prevăzută la articolul 5 alineatul (3), este improbabil ca acesta să furnizeze suficiente informații astfel încât să reprezinte un consimțământ valabil pentru prelucrarea datelor cu caracter personal. Acest subiect a fost discutat anterior în Avizul nr. 15/2011 al GL29 privind definiția consimțământului[32].

[32] Avizul nr. 15/2011 al GL29 privind definiția consimțământului (iulie 2011): http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_ro.pdf

În contextul dispozitivelor inteligente, „liber acordat” înseamnă că un utilizator trebuie să aibă posibilitatea de a accepta sau refuza prelucrarea datelor sale cu caracter personal. Prin urmare, în cazul în care o aplicație trebuie să prelucreze date cu caracter personal, un utilizator trebuie să aibă libertatea de a accepta sau refuza acest lucru. Utilizatorul nu ar trebui să se găsească în fața unui ecran pe care se afișează doar opțiunea „Da, accept” cu scopul de a finaliza instalarea aplicației. Ar trebui să existe și o opțiune „Anulare” sau orice altă opțiune de oprire a instalării.

„Clar” înseamnă că persoana vizată trebuie să dispună de informațiile necesare pentru a lua o hotărâre în cunoștință de cauză[33]. Pentru a evita orice ambiguitate, informațiile respective trebuie puse la dispoziție înainte de prelucrarea datelor cu caracter personal. Aceasta include prelucrarea datelor care poate avea loc pe parcursul instalării, de exemplu, în scopul deparazitării sau al urmăririi. Conținutul și forma informațiilor respective sunt detaliate în secțiunea 3.7 din prezentul aviz.

„Specific” înseamnă că manifestarea de voință trebuie să se refere la prelucrarea unor anumite date sau a unei categorii limitate de date. Din acest motiv, un simplu clic pe butonul „Instalare” nu poate fi considerat un consimțământ valabil pentru prelucrarea datelor cu caracter personal din cauza faptului că un consimțământ nu poate fi exprimat printr-o autorizație formulată în mod general. În anumite situații, utilizatorii pot oferi un consimțământ detaliat, în cazul în care este necesar un consimțământ pentru fiecare tip de date care urmează să fie accesate de către aplicație[34]. O astfel de abordare îndeplinește două cerințe juridice importante, în primul rând, de informare corespunzătoare a utilizatorului cu privire la aspectele importante ale serviciului și, în al doilea rând, de solicitare a consimțământului specific pentru fiecare aspect în cauză[35]. Cealaltă abordare adoptată de către dezvoltatorii de aplicații, prin care utilizatorilor li se solicită să accepte un set complex de clauze și condiții și/sau politica de confidențialitate, nu constituie un consimțământ specific[36].

Termenul „specific” se referă, de asemenea, la practica de urmărire a comportamentului utilizatorului de către agenții de publicitate și de către orice alt terț. Setările standard furnizate de SO și de aplicații trebuie să fie concepute astfel încât să se evite orice urmărire, în scopul de a permite utilizatorilor să își dea consimțământul specific pentru acest tip de prelucrare a datelor. Trebuie ca aceste setări standard să nu poată fi eludate de către terți, cum se întâmplă de obicei cu mecanismele „Nu urmări” (*Do Not Track*) integrate în browsere.

---

33 Idem, p. 19.

34 Consimțământ detaliat înseamnă că persoanele pot controla cu precizie (în mod specific) funcțiile de prelucrare a datelor cu caracter personal propuse de aplicație pe care doresc să le activeze.

35 Necesitatea obținerii unui astfel de consimțământ detaliat este prevăzută în mod expres de serviciile FTC în raportul lor cel mai recent (nota de subsol nr. 6 de mai sus), p. 15-16: „[…] *platformele ar trebui să aibă în vedere divulgarea de informații la timp și obținerea consimțământului explicit pentru colectarea altor conținuturi pe care majoritatea consumatorilor le-ar putea considera sensibile în numeroase contexte, cum ar fi fotografii, contacte, intrări în calendar sau înregistrări audio sau video.*”

36 Idem, p 34-35: „*Consimțământul general fără o indicare precisă a scopului prelucrării pentru care persoana vizată își dă acordul nu respectă această cerință, ceea ce înseamnă că informațiile privind obiectivul prelucrării nu trebuie incluse în dispozițiile generale, ci într-o clauză separată privind consimțământul.”*

Exemple de consimțământ specific

O aplicație furnizează informații cu privire la restaurantele din apropiere. Înainte de instalare, dezvoltatorul aplicației trebuie să obțină consimțământul utilizatorului. Pentru a accesa datele de geolocalizare, dezvoltatorul de aplicații trebuie să solicite separat consimțământul utilizatorului, de exemplu, în cursul instalării sau înainte de accesarea datelor de geolocalizare.
„Specific" înseamnă că acordul trebuie să se limiteze la scopul specific de informare a utilizatorului cu privire la restaurantele din apropiere. Prin urmare, datele de localizare din dispozitiv pot fi accesate numai atunci când utilizatorul folosește aplicația în acest scop. Consimțământul utilizatorului în legătură cu prelucrarea datelor de geolocalizare nu permite aplicației să colecteze încontinuu date de localizare din dispozitivul în cauză. Prelucrarea ulterioară a datelor ar necesita informații suplimentare și un consimțământ separat.

În mod similar, pentru ca o aplicație de comunicații să acceseze lista de contacte, utilizatorul trebuie să fie capabil să selecteze contactele cu care dorește să comunice în loc să ofere accesul la întregul carnet de adrese (inclusiv datele de contact ale persoanelor care nu sunt utilizatori ai serviciului respectiv și care nu și-au exprimat consimțământul cu privire la prelucrarea datelor care le privesc).

Cu toate acestea, trebuie remarcat faptul că, deși consimțământul întrunește cele trei aspecte descrise mai sus, acesta nu constituie o autorizație pentru o prelucrare neechitabilă și ilegală. În cazul în care scopul prelucrării datelor este excesiv și/sau disproporționat, în pofida consimțământului utilizatorului, dezvoltatorul de aplicații nu dispune de un temei juridic și încalcă, cel mai probabil, Directiva privind protecția datelor.

Exemplu de prelucrare excesivă și ilegală a datelor

O aplicație de tip „alarmă" propune utilizatorului opțiunea de a utiliza o comandă vocală pentru anularea sau amânarea alarmei. În acest exemplu, consimțământul de înregistrare se limitează la durata în care alarma este în funcțiune. Orice monitorizare sau înregistrare audio pe durata în care alarma nu este în funcțiune ar fi considerată excesivă și ilegală.

În ceea ce privește aplicațiile instalate pe dispozitiv în mod implicit (înainte ca utilizatorul să intre în posesia acestuia) sau alt tip de prelucrare întreprinsă de SO care necesită un consimțământ ca temei juridic, operatorii de date trebuie să fie atenți dacă respectivul consimțământ este într-adevăr valabil. În numeroase cazuri, ar trebui avut în vedere un mecanism separat de obținere a consimțământului, eventual atunci când aplicația este pornită pentru prima oară, cu scopul de a oferi operatorilor de date suficiente posibilități de a furniza informații complete utilizatorului final. În cazul în care datele respective reprezintă categorii speciale de date, astfel cum se prevede la articolul 8 din Directiva privind protecția datelor, consimțământul trebuie să fie unul explicit.

Nu în ultimul rând, utilizatorii trebuie să dispună de posibilitatea de a-și retrage consimțământul într-o manieră simplă și eficace. Mai multe detalii în acest sens sunt disponibile în secțiunea 3.8 din prezentul aviz.

3.4.2 Temeiuri juridice pentru prelucrarea datelor în cursul utilizării aplicației

Astfel cum se explică mai sus, consimțământul reprezintă temeiul juridic necesar prin care dezvoltatorului de aplicații i se permite să citească și/sau să scrie informații în mod legal și, prin urmare, să prelucreze date cu caracter personal. Într-o etapă ulterioară, pe parcursul

utilizării aplicației, dezvoltatorul de aplicații poate invoca alte temeiuri juridice pentru alte tipuri de prelucrare a datelor atât timp cât acest lucru nu implică prelucrarea datelor sensibile cu caracter personal.

Astfel de temeiuri juridice pot consta în faptul că prelucrarea este necesară pentru executarea unui contract la care subiectul datelor este parte sau pentru realizarea intereselor (comerciale) legitime, în conformitate cu articolul 7 literele (b) și (f) din Directiva privind protecția datelor.

Temeiurile juridice în cauză se limitează la prelucrarea datelor nesensibile cu caracter personal ale unui anumit utilizator, putând fi invocate numai în măsura în care prelucrarea anumitor date este strict necesară pentru efectuarea serviciului dorit sau, în conformitate cu articolul 7 litera (f), numai cu condiția ca interese comerciale să nu prejudicieze interesul sau drepturile și libertățile fundamentale ale persoanei vizate.

Exemple de temeiuri juridice contractuale

Un utilizator își acordă consimțământul pentru instalarea unei aplicații de servicii bancare mobile. În vederea îndeplinirii solicitării de efectuare a unei plăți, banca nu necesită consimțământul separat al utilizatorului pentru comunicarea numelui și a numărului său de cont destinatarului plății. Informația respectivă este necesară exclusiv pentru executarea contractului la care utilizatorul este parte, prin urmare, banca deține un temei juridic în conformitate cu articolul 7 litera (b) din Directiva privind protecția datelor. Același raționament se aplică în cazul aplicațiilor de comunicații; în cazul în care acestea furnizează informații esențiale precum numele contului, adresa de e-mail sau numărul de telefon unei alte persoane cu care utilizatorul dorește să comunice, divulgarea informațiilor respective este în mod evident necesară pentru executarea contractului.

3.5 Limitarea scopului și minimizarea datelor

Principiile fundamentale care stau la baza Directivei privind protecția datelor cu caracter personal constau în limitarea scopului și minimizarea datelor. Limitarea scopului permite utilizatorilor să ia o decizie deliberată de încredințare a datelor lor cu caracter personal unui terț, urmând să fie informați cu privire la modul în care sunt utilizate datele respective și să se bazeze pe descrierea limitativă a scopului pentru a înțelege în ce scopuri urmează să fie utilizate datele respective. Prin urmare, scopurile în care sunt prelucrate datele trebuie să fie bine definite și înțelese de către un utilizator obișnuit care nu deține cunoștințe specializate juridice sau tehnice.

În același timp, limitarea scopului presupune ca dezvoltatorii de aplicații să aibă o viziune de ansamblu clară asupra obiectului lor de activitate înainte de a începe să colecteze datele cu caracter personal ale utilizatorilor. Datele cu caracter personal pot fi prelucrate numai în scopuri echitabile și legale [articolul 6 alineatul (1) litera (a) din Directiva privind protecția datelor], care trebuie definite înainte de prelucrarea datelor respective.

Principiul limitării scopului exclude modificările bruște cu privire la condițiile esențiale ale procesului de prelucrare.

De exemplu, în cadrul unei aplicații care vizează inițial să permită utilizatorilor să își trimită e-mail-uri unul altuia, dezvoltatorul decide să își modifice modelul comercial și să fuzioneze adresele de e-mail ale utilizatorilor săi cu numerele de telefon ale utilizatorilor unei alte aplicații. Operatorii de date respectivi ar trebui ulterior să îi abordeze individual pe toți utilizatorii și să le solicite consimțământul prealabil și neechivoc pentru noul scop de prelucrare a datelor cu caracter personal.

Principiul limitării scopului este inseparabil de principiul minimizării datelor. În vederea prevenirii unei prelucrări inutile și potențial ilegale a datelor, dezvoltatorii de aplicații trebuie să identifice cu atenție datele strict necesare pentru executarea funcționalității dorite.

Aplicațiile pot obține accesul la numeroase funcționalități ale dispozitivului, fiind capabile, prin urmare, să facă diverse lucruri cum ar fi trimiterea unui SMS cu număr ascuns, accesarea imaginilor și a întregului carnet de adrese. Numeroase magazine de aplicații oferă servicii de actualizare (semi)automată în cadrul cărora dezvoltatorul de aplicații poate să integreze caracteristici noi și să le pună la dispoziție printr-o interacțiune redusă sau fără interacțiune cu utilizatorul final.

Grupul de lucru subliniază în această etapă faptul că terții care obțin accesul la datele utilizatorului prin intermediul aplicațiilor trebuie să respecte principiile limitării scopului și minimizării datelor. Identificatorii unici ai dispozitivului, care de cele mai multe ori nu pot fi modificați, nu ar trebui utilizați în scopul publicității și/sau a instrumentelor analitice bazate pe interesele consumatorilor deoarece utilizatorii nu sunt în măsură să își revoce consimțământul. Dezvoltatorii de aplicații ar trebui să se asigure că se evită denaturarea funcțiilor și, în acest sens, să nu modifice prelucrarea datelor de la o versiune de aplicație la alta fără a-și informa în mod corespunzător utilizatorii finali și fără a le oferi acestora posibilitatea de a se retrage din procesul de prelucrare a datelor sau de a renunța la serviciul respectiv. De asemenea, utilizatorilor ar trebui să li se ofere mijloacele tehnice necesare pentru verificarea declarațiilor referitoare la scopurile declarate: acestora ar trebui să li se permită accesul la informațiile privind volumul traficului de ieșire pe aplicație în raport cu traficul inițiat de utilizator.

Informarea și controalele efectuate de către utilizatori reprezintă principalele caracteristici care asigură respectarea principiilor minimizării datelor și limitării scopului.

Accesul la datele subiacente din dispozitiv prin intermediul API oferă producătorilor de SO și de dispozitive, precum și magazinelor de aplicații posibilitatea de a pune în aplicare norme specifice și de a furniza informațiile corespunzătoare utilizatorilor finali. De exemplu, producătorii de SO și de dispozitive ar trebui să ofere o API care să facă obiectul unor controale precise cu scopul de a diferenția fiecare tip de date și de a garanta faptul că dezvoltatorii de aplicații pot solicita accesul numai la datele care sunt strict necesare pentru funcționarea (legală) a aplicației lor. Tipurile de date solicitate de către dezvoltatorul de aplicații pot fi afișate în mod vizibil în magazinul de aplicații cu scopul de a informa utilizatorii înainte de instalarea aplicației în cauză.

În acest sens, controlul accesului la datele stocate în dispozitiv se bazează pe diferite mecanisme:

a. Producătorii de SO și de dispozitive și magazinele de aplicații definesc **norme** care se aplică pentru prezentarea aplicațiilor în magazinul lor de aplicații:

dezvoltatorii de aplicații trebuie să respecte normele în cauză, în caz contrar riscând ca aplicațiile lor să nu fie disponibile în magazinele respective[37].

b. **API** ale sistemelor de operare definesc metode standard de acces la datele stocate în telefonul la care au acces aplicațiile. De asemenea, acestea au un impact asupra colectării de date la nivel de server.
c. **Controale ex-ante** – controale efectuate înainte de instalarea unei aplicații[38].
d. **Controale ex-post** – controale efectuate după instalarea unei aplicații.

3.6 Securitate

În conformitate cu articolul 17 din Directiva privind protecția datelor, operatorii și persoanele împuternicite de către operatori trebuie să adopte măsurile organizaționale și tehnice necesare pentru a garanta protecția datelor cu caracter personal pe care le prelucrează. În consecință, măsurile respective trebuie adoptate de către toți actorii identificați în secțiunea 3.3, în funcție de rolul și responsabilitatea fiecăruia dintre aceștia.

Respectarea obligației în materie de securitate are dublu obiectiv. Aceasta va permite utilizatorilor să exercite un control mai strict asupra datelor lor cu caracter personal și va spori nivelul de încredere în entitățile care gestionează efectiv datele cu caracter personal ale utilizatorilor.

Pentru a-și respecta obligațiile în materie de securitate în calitate de operatori de date, dezvoltatorii de aplicații, magazinele de aplicații, producătorii de SO și de dispozitive și terții trebuie să țină seama de principiile privind luarea în considerare a vieții private începând cu momentul conceperii și luarea în considerare a vieții private în setările standard. Aceasta necesită o evaluare continuă atât a riscurilor existente, cât și a riscurilor viitoare în ceea ce privește protecția datelor, precum și punerea în aplicare și evaluarea unor măsuri eficace de atenuare, printre care minimizarea datelor.

Dezvoltatorii de aplicații

Există numeroase orientări destinate publicului referitoare la securitatea aplicațiilor mobile, publicate de către producătorii de SO și de dispozitive și de către terți independenți, de exemplu, Agenția europeană pentru securitatea rețelelor și a informațiilor (ENISA)[39].

Domeniul de aplicare al prezentului aviz nu include revizuirea tuturor celor mai bune practici în materie de securitate în ceea ce privește dezvoltarea aplicațiilor; cu toate acestea, grupul de lucru profită de această ocazie pentru a trece în revistă practicile care pot avea un impact grav asupra drepturilor fundamentale ale utilizatorilor de aplicații.

Este foarte important ca înainte de proiectarea unei aplicații să se stabilească unde vor fi stocate datele. În anumite cazuri, datele utilizatorilor sunt stocate în dispozitiv, însă dezvoltatorii de aplicații pot, de asemenea, să utilizeze o arhitectură client-server. Aceasta

---

[37] Dispozitivele de deblocare permit instalarea de aplicații în afara magazinelor oficiale; dispozitivele Android permit, de asemenea, instalarea de aplicații din alte surse.

[38] În special în cazul aplicațiilor instalate în prealabil.

[39] ENISA, „Smartphone Secure Development Guideline”: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/smartphone-secure-development-guidelines.

înseamnă că datele cu caracter personal sunt transferate sau copiate în sistemele furnizorului de servicii. Varianta în care datele sunt stocate și prelucrate pe dispozitiv oferă utilizatorilor finali cel mai mare control asupra datelor respective, permițându-le, de exemplu, să șteargă datele în cazul în care își retrag consimțământul referitor la prelucrarea acestora. Cu toate acestea, stocarea în siguranță a datelor într-un loc la distanță poate ajuta la recuperarea datelor în cazul în care dispozitivul este pierdut sau furat. Soluții intermediare sunt de asemenea posibile.

Dezvoltatorii de aplicații trebuie să identifice politici clare referitoare la modalitatea de dezvoltare și distribuire a software-ului. De asemenea, producătorii de SO și de dispozitive trebuie să promoveze prelucrarea în siguranță a datelor de către aplicații, care va fi detaliată în cele ce urmează. În al doilea rând, dezvoltatorii de aplicații și magazinele de aplicații trebuie să proiecteze și să introducă un mediu sigur, cu instrumente care să prevină răspândirea aplicațiilor dăunătoare și care să permită instalarea/dezinstalarea cu ușurință a fiecărui tip de aplicație în parte.

Printre bunele practici care pot fi utilizate în faza de proiectare a unei aplicații se numără minimizarea liniilor și a complexității codului, precum și efectuarea de verificări pentru a exclude posibilitatea ca datele să fie transferate sau compromise în mod neintenționat. În plus, toate intrările de date ar trebui validate pentru a se preveni depășirea capacității memoriei tampon sau atacurile tip injecție. Alte mecanisme de securitate care merită menționate includ aplicarea unor strategii corespunzătoare de administrare a corecțiilor programelor informatice folosite în materie de securitate și efectuarea de audituri periodice și independente în materie de securitate a sistemelor. De asemenea, criteriile de proiectare a aplicațiilor ar trebui să includă punerea în aplicare a principiului celui mai mic privilegiu implicit potrivit căruia aplicațiile pot accesa numai datele strict necesare pentru punerea la dispoziția utilizatorului a unei anumite funcționalități. Dezvoltatorii de aplicații și magazinele de aplicații ar trebui să încurajeze, de asemenea, utilizatorii, prin intermediul avertizărilor, să completeze bunele practici de proiectare cu practici virtuoase ale utilizatorilor, cum ar fi actualizarea aplicațiilor la cele mai recente versiuni disponibile și atenționări referitoare la evitarea reutilizării acelorași parole pentru servicii diferite.

Pe parcursul etapei de proiectare a aplicației, dezvoltatorii de aplicații trebuie să adopte, de asemenea, măsuri de prevenire a accesului neautorizat la datele cu caracter personal prin garantarea faptului că datele respective sunt protejate atât în timpul tranzitului, cât și în timpul stocării, dacă este cazul.

Aplicațiile mobile ar trebui să funcționeze în amplasamente specifice chiar în memoria dispozitivelor (*sandbox*[40]) cu scopul de a reduce consecințele aplicațiilor nocive/dăunătoare. În strânsă colaborare cu producătorul de SO și/sau magazinul de aplicații, dezvoltatorii de aplicații trebuie să utilizeze mecanismele disponibile care permit utilizatorilor să vadă ce tip de date sunt prelucrate de o anumită aplicație și să activeze sau să dezactiveze, în mod selectiv, autorizațiile. Ar trebui interzisă utilizarea funcționalităților ascunse.

Dezvoltatorii de aplicații trebuie să acorde atenția cuvenită metodelor lor de identificare și autentificare a utilizatorilor. Aceștia nu ar trebui să utilizeze identificatori persistenți (specifici anumitor dispozitive), ci identificatori cu entropie scăzută specifici aplicațiilor sau

[40] *Sandbox* este un mecanism de securitate pentru separarea programelor în curs de rulare.

identificatori temporari ai dispozitivului cu scopul de a evita urmărirea utilizatorilor de-a lungul timpului. Ar trebui avute în vedere mecanisme de autentificare care respectă confidențialitatea. În momentul autentificării utilizatorilor, dezvoltatorii de aplicații trebuie să acorde o atenție specială gestionării identificatorilor și parolelor utilizatorilor. Acestea din urmă trebuie stocate în stare criptată și în siguranță ca valoare *hash* securizată din punct de vedere criptografic. Punerea la dispoziția utilizatorilor a posibilității de testare a robusteții parolelor alese este, de asemenea, o tehnică utilă de încurajare a alegerii unor parole mai bune (verificare entropică). După caz (accesul la date sensibile, dar și la resurse contra cost), poate fi avută în vedere reautentificarea, care poate avea loc și prin intermediul unei game variate de factori și canale (de exemplu, codul de acces trimis prin SMS) și/sau utilizarea datelor de autentificare legate de utilizatorul final (în locul celor legate de dispozitiv). De asemenea, în momentul selectării identificatorilor de sesiune, ar trebui utilizate șiruri imprevizibile, eventual în combinație cu informații contextuale precum ora și data, dar și adresa IP sau date de geolocalizare.

De asemenea, dezvoltatorii de aplicații ar trebui să aibă în vedere cerințele prevăzute în Directiva asupra confidențialității și comunicațiilor electronice referitoare la încălcarea confidențialității datelor cu caracter personal și necesitatea de a informa în mod proactiv utilizatorii. Deși cerințele respective se aplică în prezent numai furnizorilor de servicii de comunicații electronice disponibile pentru public, se așteaptă ca obligația în cauză să fie extinsă la toți operatorii de date (și persoanele împuternicite de către operator) prin intermediul viitorului Regulament privind protecția datelor, care se bazează pe propunerile Comisiei (COM 2012/0011/COD). Acesta consolidează și mai mult necesitatea de a deține și de a evalua în permanență un „plan de securitate” detaliat care să acopere colectarea, stocarea și prelucrarea oricăror date cu caracter personal cu scopul de a se preveni comiterea unor astfel de încălcări și impunerea sancțiunilor pecuniare grave prevăzute în astfel de cazuri. Planul de securitate trebuie să asigure, printre altele, gestionarea vulnerabilității și furnizarea în timp util și în siguranță a unor corecturi fiabile.

Responsabilitatea dezvoltatorilor de aplicații pentru securitatea produselor lor nu încetează odată cu livrarea unei versiuni de lucru pe piață. La fel ca oricare alt produs software, aplicațiile pot prezenta defecte de securitate și vulnerabilități, dezvoltatorii de aplicații trebuind să conceapă remedii și corecturi adecvate și să le furnizeze acelor actori care le pot pune la dispoziția utilizatorilor sau care pot opera ei înșiși corecțiile.

Magazinele de aplicații

Magazinele de aplicații reprezintă un intermediar important între utilizatorii finali și dezvoltatorii de aplicații și ar trebui să includă o serie de verificări robuste și eficace privind aplicațiile înainte de a autoriza comercializarea lor. Acestea ar trebui să furnizeze informații cu privire la verificările efectuate în mod real și să includă informații despre tipul de verificări de conformitate pe care le efectuează în materie de protecție a datelor.

Deși această măsură nu este 100% eficace pentru eliminarea difuzării de aplicații dăunătoare, statisticile indică faptul că această practică reduce în mod semnificativ apariția de funcționalități dăunătoare în magazinele „oficiale” de aplicații[41]. Pentru a gestiona numărul

[41] *„Hey, You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets”*, Y Zhou et al., Simpozionul privind securitatea rețelelor și a sistemelor distribuite (Network and Distributed System Security Symposium – NDSS) din 2012.

mare de aplicații prezentate zilnic, în acest proces ar putea fi utilizate instrumentele automate de analiză disponibile și canalele de schimb de informații între experții în materie de securitate și profesioniștii din domeniul software, precum și procedurile și politicile eficace puse în aplicare pentru gestionarea problemelor constatate.

Pe lângă revizuirea aplicațiilor înainte de admiterea acestora în magazinele de aplicații, aplicațiile ar trebui să facă, de asemenea, obiectul unui mecanism de reputație publică. Utilizatorii ar trebui să clasifice aplicațiile nu doar în funcție de cât de „grozave" sunt, ci și pe baza funcționalităților acestora, în special cu privire la mecanismele de confidențialitate și securitate. De asemenea, mecanismele de reputație ar trebui proiectate astfel încât să prevină clasificările false. Mecanismele de calificative și de reputație pentru aplicații se pot dovedi eficace și pentru construirea încrederii reciproce între diverse entități, în special dacă schimbul de date trece printr-un lung lanț de terți.

Magazinele de aplicații pun deseori în aplicare o metodă de dezinstalare la distanță a aplicațiilor dăunătoare sau nesigure. În cazul în care nu este proiectat în mod corespunzător, acest mecanism ar putea răpi utilizatorilor posibilitatea de a exercita un control mai strict asupra datelor lor. Pentru a respecta viața privată, metodele alese de magazinele de aplicații pentru dezinstalarea la distanță a aplicațiilor ar trebui să se bazeze, așadar, pe informarea și consimțământul utilizatorului. Mai mult, dintr-un punct de vedere mai practic, ar trebui puse la dispoziția utilizatorilor canale de răspuns („feedback") pentru raportarea problemelor de securitate ale aplicațiilor lor și pentru transmiterea unor comentarii cu privire la eficacitatea eventualelor proceduri de eliminare la distanță.

La fel ca dezvoltatorii de aplicații, magazinele de aplicații ar trebui să cunoască viitoarele obligații de notificare a oricărei încălcări a datelor cu caracter personal și să conlucreze îndeaproape cu dezvoltatorii de aplicații pentru prevenirea unor astfel de încălcări.

Producătorii de SO și de dispozitive

Producătorii de SO și de dispozitive sunt, de asemenea, actori importanți în procesul de definire a standardelor minime și a celor mai bune practici în rândul dezvoltatorilor de aplicații, nu doar în ceea ce privește securitatea software-ului și a API subiacente, ci și în ceea ce privește instrumentele, orientările și materialul de referință pe care le pun la dispoziție. Producătorii de SO și de dispozitive ar trebui să pună la dispoziție algoritme de criptare puternice și bine cunoscute și să permită lungimi de cheie adecvate. De asemenea, aceștia ar trebui să pună la dispoziția dezvoltatorilor de aplicații mecanisme puternice și sigure de autentificare (de exemplu, utilizarea certificatelor semnate de autorități de certificare de încredere pentru verificarea autorizării unei resurse la distanță). Nu ar mai fi necesar, astfel, ca dezvoltatorii de aplicații să dezvolte mecanisme de autentificare dedicate. În practică, acestea sunt rareori puse în aplicare, putând reprezenta o vulnerabilitate gravă[42].

[42] S-a evidențiat recent că lipsa unor indicatori vizuali de securitate pentru utilizarea protocoalelor securizate (SSL/TLS) și utilizarea necorespunzătoare a protocoalelor securizate (SSL/TLS) pot fi exploatate pentru lansarea de atacuri „om la mijloc" (MITM – *Man-in-the-Middle*). Conform studiilor recente, baza cumulativă instalată a aplicațiilor, care prezintă vulnerabilități confirmate la atacurile MITM, include câteva milioane de utilizatori. Bernd Freisleben și Matthew Smith, „*Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security"*, cea de-a 19-a Conferință ACM privind securitatea computerelor și a comunicațiilor (ACM CCS 2012).

Accesul la datele cu caracter personal și prelucrarea acestora de către aplicații ar trebui gestionate prin clase și metode integrate în API care să ofere verificările și garanțiile corespunzătoare. Producătorii de SO și de dispozitive ar trebui să se asigure că metodele și funcțiile care permit accesul la datele cu caracter personal includ caracteristici menite să asigure funcționarea unui sistem de cereri de consimțământ detaliat. În mod similar, ar trebui adoptate măsuri de excludere sau de limitare a accesului la datele cu caracter personal prin utilizarea funcțiilor la nivel inferior sau a altor mijloace care pot eluda controalele și garanțiile integrate în API.

De asemenea, producătorii de SO și de dispozitive trebuie să dezvolte în cadrul dispozitivelor piste clare de audit, astfel încât utilizatorii să poată vedea în mod clar care aplicații au accesat date de pe dispozitivele lor.

Toate părțile trebuie să reacționeze rapid și în timp util la vulnerabilitățile în materie de securitate, astfel încât utilizatorii finali să nu fie expuși în mod inutil la defectele de securitate. Din păcate, anumiți producători de SO și de dispozitive (și operatori de telecomunicații, atunci când distribuie dispozitive de marcă) nu reușesc să ofere asistență pe termen lung pentru versiuni ale SO, lăsându-i pe utilizatori neprotejați împotriva unor vulnerabilități de securitate binecunoscute. Producătorii de SO și de dispozitive, împreună cu dezvoltatorii de aplicații, trebuie să furnizeze în prealabil utilizatorilor finali informații privind durata de timp pe parcursul căreia se pot aștepta la actualizări periodice de securitate. De asemenea, aceștia ar trebui să îi informeze cât mai curând posibil pe utilizatori în cazul în care o anumită problemă de securitate necesită o actualizare pentru a fi corectată.

Terții

Caracteristicile și considerațiile de mai sus în materie de securitate trebuie aplicate, de asemenea, de către terți în momentul în care colectează și prelucrează date cu caracter personal în scopuri proprii, în special agenții de publicitate și furnizorii de instrumente analitice. În această categorie intră transmisia sigură și stocarea criptată de identificatori unici ai dispozitivelor și ai utilizatorilor de aplicații, precum și a altor date cu caracter personal.

3.7 Informare

3.7.1 Obligația de informare și conținutul necesar

În conformitate cu articolul 10 din Directiva privind protecția datelor, fiecare persoană vizată are dreptul să cunoască identitatea operatorului de date care îi prelucrează datele cu caracter personal. În plus, în contextul aplicațiilor, utilizatorul final are dreptul să cunoască tipul de date cu caracter personal care sunt prelucrate și în ce scopuri urmează să fie prelucrate datele respective. În cazul în care datele cu caracter personal ale utilizatorului sunt colectate de la alți actori din ecosistemul de aplicații (astfel cum se descrie în secțiunea 3.3 din prezentul aviz), utilizatorul final are totuși dreptul, în conformitate cu articolul 11 din Directiva privind protecția datelor, să fie informat cu privire la o astfel de prelucrare în aceeași manieră descrisă anterior. Prin urmare, în cazul prelucrării datelor cu caracter personal, operatorii de date relevanți trebuie să comunice potențialilor utilizatori cel puțin următoarele informații:

- identitatea și datele de contact ale acestora;
- categoriile precise de date cu caracter personal care urmează să fie colectate și prelucrate de către dezvoltatorul de aplicații;
- scopurile precise ale prelucrării;

— eventuala transmitere a datelor respective către terți;
— modul în care utilizatorii își pot exercita drepturile în cazul retragerii consimțământului și al ștergerii datelor.

Disponibilitatea acestor informații cu privire la prelucrarea datelor cu caracter personal este esențială pentru obținerea consimțământului utilizatorului. Consimțământul este valabil numai dacă persoana vizată a fost informată în prealabil cu privire la elementele-cheie ale prelucrării datelor sale. Furnizarea informațiilor respective numai după ce aplicația a început să prelucreze date cu caracter personal (adeseori în cursul instalării aplicației) nu este considerată suficientă, nefiind valabilă din punct de vedere juridic. În acord cu raportul serviciilor FTC, grupul de lucru subliniază necesitatea furnizării de informații în momentul oportun pentru consumatori, chiar înainte de colectarea informațiilor respective de către aplicații. Precizarea datelor care sunt prelucrate este deosebit de importantă având în vedere accesul larg de care beneficiază în general aplicațiile la senzorii și structurile de date din dispozitiv, acces care în majoritatea cazurilor nu este evident în mod intuitiv. Furnizarea de informații corespunzătoare are, de asemenea, o importanță vitală atunci când aplicația prelucrează categorii speciale de date cu caracter personal, de exemplu, cu privire la starea de sănătate, convingerile politice, orientarea sexuală etc. În fine, dezvoltatorul de aplicații ar trebui să facă o diferență clară între informațiile obligatorii și informațiile opționale, iar sistemul ar trebui să permită utilizatorului să refuze accesul la informațiile opționale prin intermediul opțiunilor standard care respectă confidențialitatea.

În ceea ce privește identitatea operatorului de date, utilizatorii trebuie să știe cine răspunde din punct de vedere juridic pentru prelucrarea datelor lor cu caracter personal și modul în care poate fi contactat operatorul de date. În caz contrar, aceștia nu își pot exercita drepturile, cum ar fi dreptul de a accesa (la distanță) datele stocate care îi privesc. Din cauza naturii fragmentate a mediului aplicațiilor, este esențial ca fiecare aplicație să dețină un singur punct de contact, asumându-și responsabilitatea pentru toate prelucrările de date care au loc prin intermediul aplicației. Nu trebuie să se lase în sarcina utilizatorului final să cerceteze relațiile dintre dezvoltatorul unei aplicații și alte părți care prelucrează date cu caracter personal prin intermediul aplicației respective.

În ceea ce privește scopul (scopurile), utilizatorii finali trebuie să fie informați în mod corespunzător cu privire la natura datelor colectate care îi privesc și la scopul în care acestea sunt colectate. De asemenea, utilizatorilor ar trebuie să li se comunice, într-un limbaj clar și simplu, faptul că datele respective ar putea fi reutilizate de alte părți și, în acest caz, scopurile acestei reutilizări. Scopuri elastice precum „inovarea de produse” nu sunt adecvate pentru informarea utilizatorilor. Trebuie să se precizeze în mod clar dacă utilizatorilor li se va solicita consimțământul cu privire la împărtășirea datelor cu terții în scopuri publicitare și/sau analitice. Magazinele de aplicații dețin responsabilitatea importantă de a se asigura că informațiile respective sunt disponibile și ușor de accesat pentru fiecare aplicație în parte.

O altă responsabilitate importantă pe care o au magazinele de aplicații este aceea de a asigura furnizarea de informații corespunzătoare. Se recomandă insistent utilizarea de simboluri vizuale sau pictograme care să indice utilizările de date, astfel încât utilizatorii să fie conștienți de tipurile de prelucrare a datelor care au loc.

Pe lângă scopul minim de informare, menționat mai sus și necesar pentru obținerea consimțământului din partea utilizatorului de aplicații, și în vederea unei prelucrări echitabile

a datelor cu caracter personal, grupul de lucru recomandă insistent ca operatorii de date să furnizeze utilizatorilor și informații cu privire la:

— considerentele de proporționalitate privind tipurile de date colectate sau accesate pe dispozitiv;
— perioadele de păstrare a datelor;
— măsurile de securitate aplicate de către operatorul de date.

De asemenea, grupul de lucru recomandă ca dezvoltatorii de aplicații să precizeze în politica lor de confidențialitate destinată utilizatorilor europeni în ce mod aplicația respectă legislația europeană în materie de protecție a datelor, inclusiv posibilele transferuri de date cu caracter personal din Europa spre SUA, de exemplu, precum și dacă și în ce mod aplicația respectă, într-un astfel de caz, cadrul „sferei de siguranță”.

3.7.2 Forma informațiilor

Domeniul esențial al informațiilor referitoare la prelucrarea datelor trebuie să fie comunicat utilizatorilor înainte de instalarea aplicației, prin intermediul magazinului de aplicații. În al doilea rând, informațiile relevante referitoare la prelucrarea datelor trebuie să fie accesibile și din interiorul aplicației, după instalare.

În calitate de cooperatori de date, alături de dezvoltatorii de aplicații, în materie de informații, magazinele de aplicații trebuie să se asigure că fiecare aplicație furnizează informații esențiale cu privire la prelucrarea datelor cu caracter personal. Acestea trebuie să verifice hiperlinkurile pentru a include pagini cu informații privind confidențialitatea și pentru a elimina aplicațiile care prezintă linkuri defecte sau care conțin informații inaccesibile referitoare la prelucrarea datelor.

Grupul de lucru recomandă ca informațiile referitoare la prelucrarea datelor cu caracter personal să fie, de asemenea, disponibile și ușor de localizat, cum ar fi în magazinul de aplicații și, de preferat, pe site-urile obișnuite ale dezvoltatorului de aplicații responsabil de aplicația respectivă. Este inacceptabil ca utilizatorii să fie puși în situația în care să trebuiască să caute pe internet informații referitoare la politicile de prelucrare a datelor în loc să fie informați în mod direct de către dezvoltatorul de aplicații sau de către un alt operator de date.

Fiecare aplicație ar trebui cel puțin să dețină o politică de confidențialitate ușor de citit, de înțeles și de accesat, în care să fie incluse toate informațiile menționate anterior. Numeroase aplicații nu îndeplinesc această cerință minimă în materie de transparență. Conform studiului FPF din iunie 2012, 56 % dintre aplicațiile contra cost și aproximativ 30 % dintre aplicațiile gratuite nu dețin o politică de confidențialitate.

Aplicațiile care nu prelucrează date cu caracter personal sau care nu au fost proiectate în acest scop ar trebui să precizeze în mod clar acest lucru în politica lor de confidențialitate.

Bineînțeles, există anumite limite cu privire la cantitatea de informații care pot fi prezentate pe un ecran de mici dimensiuni, însă acest lucru nu reprezintă o scuză pentru informarea necorespunzătoare a utilizatorilor finali. Există mai multe strategii la care se poate recurge pentru a se asigura că utilizatorii au cunoștință de elementele esențiale ale serviciului. Grupul de lucru consideră că utilizarea notificărilor în diferite etape, astfel cum sunt prezentate în

detaliu în Avizul nr. 10/2004 al GL29[43], este benefică atunci când înștiințarea prealabilă a utilizatorului conține informațiile minime prevăzute de cadrul juridic al UE și când sunt disponibile informații suplimentare prin intermediul linkurilor către întreaga politică de confidențialitate. Informațiile ar trebui să fie prezentate direct pe ecran și să fie ușor de accesat și foarte ușor de parcurs. Pe lângă informațiile cuprinzătoare adecvate pentru ecranele de mici dimensiuni ale dispozitivelor mobile, utilizatorilor trebuie să le fie puse la dispoziție linkuri spre informații mai detaliate, de exemplu, informații cuprinse în politica de confidențialitate, modul în care aplicația utilizează datele cu caracter personal, identitatea operatorului de date și situația în care un utilizator își poate exercita drepturile.

O astfel de abordare poate fi combinată cu utilizarea de pictograme, imagini, înregistrări video și audio, și poate recurge la notificări contextuale în timp real în momentul în care aplicația accesează carnetul de adrese sau fotografiile[44]. Pictogramele trebuie să fie adecvate, și anume să fie clare, explicite și neechivoce. În mod clar, producătorul de SO deține o responsabilitate comună importantă în ceea ce privește facilitarea utilizării unor astfel de pictograme.

În fapt, dezvoltatorii de aplicații excelează în programarea și proiectarea de interfețe complexe pentru ecranele de mici dimensiuni, iar grupul de lucru lansează industriei un apel de a-și utiliza talentul creativ pentru oferirea unor soluții mai inovatoare de informare eficace a utilizatorilor pe dispozitivele mobile. Pentru a garanta faptul că informațiile sunt într-adevăr înțelese de către utilizatori care nu dețin cunoștințe tehnice sau juridice, grupul de lucru (în acord cu raportul serviciilor FTC) recomandă insistent testarea de către consumatori a strategiilor de informare alese[45].

3.8 Drepturile persoanei vizate

În conformitate cu articolele 12 și 14 din Directiva privind protecția datelor, dezvoltatorii de aplicații și alți operatori de date din ecosistemul de aplicații mobile trebuie să permită utilizatorilor de aplicații să își exercite drepturile de acces, de rectificare, de ștergere și de obiecție în ceea ce privește prelucrarea datelor. În cazul în care un utilizator își exercită dreptul de acces, operatorul de date trebuie să pună la dispoziția acestuia informații referitoare la datele care sunt prelucrate și la sursa datelor respective. În cazul în care ia decizii automatizate pe baza datelor compilate, operatorul de date trebuie să informeze, de asemenea, utilizatorul cu privire la raționamentul din spatele deciziilor respective. Acest lucru ar putea fi valabil în cazul în care se evaluează performanța sau conduita utilizatorilor, de exemplu, pe baza datelor financiare sau referitoare la sănătate sau pe baza altor date de profil. La solicitarea utilizatorului, operatorul datelor din aplicație trebuie să permită, în egală măsură, rectificarea, ștergerea sau blocarea datelor cu caracter personal în cazul în care acestea sunt incomplete, inexacte sau prelucrate în mod ilegal.

Pentru ca utilizatorii să își poată exercita controlul asupra prelucrării datelor lor cu caracter personal, aplicațiile trebuie să își informeze în mod clar și vizibil utilizatorii cu privire la existența acestor mecanisme de acces și de corecție. Grupul de lucru pentru protecția persoanelor în ceea ce privește prelucrarea datelor cu caracter personal instituit în temeiul

[43] Avizul nr. 10/2004 al GL29 privind dispoziții mai armonizate în domeniul informațiilor (iulie 2004): http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_en.pdf

[44] De exemplu, pictograma de avertizare pentru prelucrarea datelor de geolocalizare utilizată pe iPhone.

[45] Pagina 16 din raportul serviciilor FTC, menționat la nota de subsol nr. 6 de mai sus, p. 16.

articolului 29 recomandă proiectarea și implementarea unor instrumente de acces online simple, dar sigure. Instrumentele de acces ar trebui, de preferință, să fie disponibile în cadrul fiecărei aplicații în parte sau prin furnizarea unui link către o caracteristică online unde utilizatorii pot obține acces instantaneu la toate datele lor cu caracter personal care sunt prelucrate și la explicațiile necesare. Inițiative similare au fost adoptate de către furnizorii de servicii online, precum diferite tablouri de bord sau alte mecanisme de acces.

Necesitatea unui acces online facil este cu precădere importantă în cazul aplicațiilor care prelucrează profiluri de utilizator bogate, cum ar fi conectarea în rețea, aplicațiile sociale și de mesagerie sau aplicațiile care prelucrează date sensibile sau financiare. Bineînțeles, accesul ar trebui acordat numai dacă a fost stabilită identitatea persoanei vizate cu scopul de a se preveni scurgerile de date către terți. Această obligație de verificare a identității corecte nu ar trebui să conducă însă la o colectare suplimentară și excesivă de date cu caracter personal cu privire la persoana vizată. În numeroase cazuri, autentificarea poate fi suficientă în locul identificării (complete).

În plus, utilizatorii ar trebui să dispună întotdeauna de posibilitatea de a-și retrage consimțământul într-o manieră simplă și nu foarte solicitantă. O persoană vizată își poate retrage consimțământul cu privire la prelucrarea datelor în diferite moduri și din diferite motive. De preferință, opțiunea de retragere a consimțământului ar trebui să fie disponibilă prin intermediul mecanismelor ușor de accesat menționate mai sus. Trebuie să fie existe posibilitatea de dezinstalare a aplicațiilor și, astfel, de ștergere a tuturor datelor cu caracter personal și din serverele operatorului (operatorilor) de date. Pentru a permite ștergerea datelor utilizatorilor de către dezvoltatorul de aplicații, este important ca producătorul de SO să transmită un semnal dezvoltatorului de aplicații după ce un utilizator a dezinstalat o aplicație. Un astfel de semnal poate fi transmis prin intermediul API. În principiu, după ce utilizatorul a dezinstalat aplicația, dezvoltatorul de aplicații nu mai deține niciun temei juridic pentru a continua prelucrarea datelor cu caracter personal referitoare la utilizatorul respectiv și, prin urmare, trebuie să șteargă toate datele respective. Un dezvoltator de aplicații care dorește să păstreze anumite date, de exemplu, cu scopul de a facilita reinstalarea aplicației, trebuie să solicite separat consimțământul utilizatorului pe parcursul procesului de dezinstalare a aplicației, precum și acordul acestuia pentru stabilirea unei perioade de păstrare suplimentare. Singura excepție de la această regulă este posibila existență a unor obligații juridice de păstrare a anumitor date în scopuri specifice, de exemplu, obligații fiscale referitoare la tranzacții financiare[46].

3.9 Perioadele de păstrare a datelor

Dezvoltatorii de aplicații trebuie să țină seama de păstrarea datelor colectate prin intermediul aplicației și de riscurile pe care aceasta le implică în materie de protecție a datelor. Duratele de timp specifice vor depinde de scopul aplicației și de relevanța datelor pentru utilizatorul final. De exemplu, în cazul unei aplicații de calendar, de jurnal sau de publicare a fotografiilor perioada de păstrare ar fi controlată de utilizatorul final, în timp ce pentru o aplicație de

[46] Grupul de lucru reamintește tuturor serviciilor societății informaționale, cum ar fi aplicațiile, că obligația europeană de păstrare a datelor (Directiva 2006/24/CE) nu se aplică în cazul lor și că, prin urmare, aceasta nu poate fi invocată drept temei juridic pentru continuarea prelucrării datelor utilizatorilor de aplicații după ce aceștia au șters aplicația în cauză. Grupul de lucru dorește să evidențieze pe această cale natura extrem de riscantă a traficului de date, care necesită precauții și garanții speciale *per* se – astfel cum se subliniază în raportul GL29 privind punerea în aplicare a Directivei privind păstrarea datelor (WP172), în care tuturor părților interesate relevante li s-a solicitat să adopte măsurile de securitate corespunzătoare.

navigare ar fi suficientă stocarea doar a ultimelor 10 locuri vizitate recent. Dezvoltatorii de aplicații ar trebui să țină seama și de datele utilizatorilor care nu au utilizat aplicația pentru o perioadă de timp îndelungată. Este posibil ca acești utilizatori să își fi pierdut dispozitivul mobil sau să fi trecut la un alt dispozitiv fără să dezinstaleze în mod activ toate aplicațiile de pe dispozitivul inițial. Prin urmare, dezvoltatorii de aplicații ar trebui să definească în prealabil o perioadă de timp de inactivitate după scurgerea căreia contul este considerat expirat și să se asigure că utilizatorul este informat cu privire la perioada respectivă. La expirarea perioadei de timp în cauză, operatorul de date ar trebui să avertizeze utilizatorul și să îi ofere posibilitatea de a-și recupera datele cu caracter personal. În cazul în care utilizatorul nu răspunde la atenționare, datele sale cu caracter personal și utilizarea aplicației ar trebui anonimizate în mod ireversibil sau șterse. Perioada de atenționare depinde de scopul aplicației și de locul în care sunt stocate datele. Dacă aceasta privește datele stocate în dispozitiv, de exemplu, un scor mare la un joc, datele pot fi păstrate atât timp cât aplicația este instalată. Dacă ea privește date care sunt utilizate doar o dată pe an, cum ar fi informații privind o stațiune de schi, perioada de atenționare poate fi de 15 luni.

3.10 Copiii

Copiii sunt utilizatori avizi de aplicații, instalate fie pe propriile dispozitive, fie pe cele pe care le împart cu alții (de exemplu, dispozitive care aparțin părinților, fraților sau unei instituții de învățământ), existând în mod evident o piață extinsă și diversificată de aplicații destinate copiilor. În același timp, copiii nu înțeleg/cunosc sau înțeleg/cunosc într-o mică măsură amploarea și gradul de sensibilitate al datelor la care pot avea acces aplicațiile sau amploarea procesului de partajare a datelor cu terții în scopuri publicitare.

Grupul de lucru s-a ocupat în detaliu de problema prelucrării datelor copiilor în Avizul nr. 2/2009 privind protecția datelor cu caracter personal ale copiilor, abordând în prezenta secțiune doar o serie de riscuri și de recomandări specifice aplicațiilor[47].

Dezvoltatorii de aplicații și alți operatori de date ar trebui să acorde atenția cuvenită limitei de vârstă care definește statutul de copil sau de minor în legislația națională, atunci când consimțământul părinților în legătură cu prelucrarea datelor este o condiție prealabilă pentru prelucrarea legală a datelor de către aplicații[48].

În cazul în care consimțământul respectiv poate fi obținut în mod legal din partea unui minor, iar aplicația urmează să fie utilizată de către un copil sau un minor, operatorul de date ar trebui să ia în considerare posibila capacitate redusă de înțelegere și de atenție a minorului cu privire la informații despre prelucrarea de date. Din cauza vulnerabilității lor generale și având în vedere faptul că datele cu caracter personal trebuie prelucrate în mod echitabil și legal, operatorii de date care vizează copiii ar trebui să respecte cu o și mai mare strictețe principiile minimizării datelor și limitării scopului. În mod specific, operatorii de date ar trebui să nu prelucreze, în mod direct sau indirect, datele copiilor în scopuri de publicitate

[47] WP 160, Avizul nr. 2/2009 privind protecția datelor cu caracter personal ale copiilor (Orientări generale și cazul special al școlilor) (11 februarie 2009): http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_ro.pdf

[48] În statele membre ale UE, limita de vârstă variază între 12 și 18 de ani.

comportamentală, întrucât acest lucru nu ar intra în sfera de înțelegere a unui copil și ar depăși, așadar, limitele unei prelucrări legale.

Grupul de lucru împărtășește preocupările exprimate de Comisia Federală pentru Comerț (FTC) în raportul serviciilor sale privind aplicațiile mobile destinate copiilor[49].

Dezvoltatorii de aplicații, în colaborare cu magazinele de aplicații și cu producătorii de SO și de dispozitive, ar trebui să prezinte informațiile relevante într-o manieră simplă și într-un limbaj adecvat vârstei copiilor. De asemenea, operatorii de date ar trebui să se abțină, în mod specific, de la colectarea de date referitoare la părinți sau la membrii familiei utilizatorului copil, cum ar fi informații financiare sau informații din categorii speciale de informații precum datele medicale.

4 Concluzii și recomandări

Numeroase tipuri de date disponibile pe un dispozitiv mobil inteligent sunt date cu caracter personal. Cadrul juridic relevant este reprezentat de Directiva privind protecția datelor, în combinație cu cerința privind obținerea consimțământului specific, prevăzută la articolul 5 alineatul (3) din Directiva asupra confidențialității și comunicațiilor electronice. Normele respective se aplică tuturor aplicațiilor destinate utilizatorilor de aplicații de pe teritoriul UE, indiferent de amplasarea dezvoltatorului sau a magazinului de aplicații.

Natura fragmentată a ecosistemului de aplicații, gama variată de posibilități tehnice de accesare a datelor stocate în dispozitivele mobile sau generate de acestea și lipsa cunoștințelor juridice în rândul dezvoltatorilor ocazionează o serie de riscuri grave cu privire la protecția datelor pentru utilizatorii de aplicații. Riscurile variază de la lipsa de transparență și lipsa de cunoștințe în rândul utilizatorilor de aplicații la măsuri insuficiente de securitate, mecanisme neconforme de obținere a consimțământului, o tendință de maximizare a datelor și elasticitatea scopurilor în care sunt prelucrate datele.

Există o suprapunere a responsabilităților care revin, în materie de protecție a datelor, diferitelor părți implicate în dezvoltarea, distribuția și capacitățile tehnice ale aplicațiilor. Majoritatea concluziilor și a recomandărilor se adresează dezvoltatorilor de aplicații (dat fiind că aceștia dețin cel mai mare control asupra manierei precise în care are loc prelucrarea sau în care sunt prezentate informațiile în cadrul aplicației), însă, de cele mai multe ori, pentru ca aceștia să atingă cele mai ridicate standarde în materie de confidențialitate și de protecție a datelor, trebuie să existe o colaborare cu alte părți din ecosistemul de aplicații, cum ar fi producătorii de SO și de dispozitive, magazinele de aplicații și terții precum furnizorii de instrumente analitice și rețelele de publicitate.

[49] Raportul serviciilor FTC intitulat „Mobile Apps for Kids: Current Privacy Disclosures are Disappointing" (februarie 2012): http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf. „*Personalul nostru a întâlnit o varietate de aplicații destinate copiilor create de sute de dezvoltatori diferiți în raport cu un număr limitat sau chiar inexistent de informații pe piețele de aplicații cu privire la colectarea datelor și practicile de împărtășire a aplicațiilor în cauză.* "

Dezvoltatorii de aplicații trebuie

- să își cunoască și să își respecte obligațiile în calitate de operatori de date atunci când prelucrează date de la și despre utilizatori;
- să își cunoască și să își respecte obligațiile în calitate de operatori de date atunci când încheie contracte cu persoanele împuternicite de către operator, de exemplu, în cazul în care externalizează colectarea și prelucrarea datelor cu caracter personal către dezvoltatori, programatori sau către furnizorii de stocare dematerializată („cloud”);
- să solicite consimțământul utilizatorilor înainte ca aplicația să înceapă extragerea sau plasarea de informații pe dispozitiv, și anume înainte de instalarea aplicației. Consimțământul respectiv trebuie să fie liber, specific și informat;
- să solicite consimțământul detaliat al utilizatorilor pentru fiecare tip de date care urmează să fie accesate de către aplicație, cel puțin pentru următoarele categorii: poziția exactă, contacte, identificator unic al dispozitivului, identitatea persoanei vizate, identitatea telefonului, cartea de credit și datele privind plățile, telefonie și SMS, istoricul navigărilor, e-mail, date de identificare pentru rețelele sociale și date biometrice;
- să fie conștienți de faptul că consimțământul nu autorizează prelucrarea excesivă sau disproporțională a datelor;
- să comunice scopurile prelucrării datelor într-un mod clar și cuprinzător înainte de instalarea aplicației și să nu modifice scopurile respective fără reînnoirea consimțământului; să furnizeze informații cuprinzătoare în cazul în care datele urmează să fie utilizate de terți, de exemplu în scopuri de publicitate sau analiză;
- să permită utilizatorilor să își revoce consimțământul și să dezinstaleze aplicația, precum și să șteargă datele, dacă este cazul;
- să respecte principiul minimizării datelor și să colecteze numai datele care sunt strict necesare pentru executarea funcționalității dorite;
- să adopte măsurile organizaționale și tehnice necesare pentru a garanta protecția datelor cu caracter personal pe care le prelucrează în toate etapele proiectării și implementării aplicației (luarea în considerare a vieții private începând cu momentul conceperii), astfel cum se prevede în secțiunea 3.6 din prezentul aviz;
- să furnizeze un singur punct de contact pentru utilizatorii aplicației;
- să propună o politică de confidențialitate ușor de citit, de înțeles și de accesat prin care utilizatorilor să le fie comunicate cel puțin următoarele informații:
  - identitatea și datele de contact;
  - categoriile precise de date cu caracter personal pe care aplicația urmează să le colecteze și să le prelucreze;
  - scopurile precise ale prelucrării;
  - eventuala transmitere a datelor respective către terți (nu doar o descriere generală, ci informații detaliate despre persoanele cărora le vor fi transmise datele);
  - drepturile utilizatorilor în legătură cu retragerea consimțământului și ștergerea datelor;
- să permită utilizatorilor de aplicații să își exercite drepturile de acces, de rectificare, de ștergere și de obiecție cu privire la prelucrarea datelor și să îi informeze cu privire la existența mecanismelor respective;
- să definească o perioadă rezonabilă de păstrare a datelor colectate prin intermediul aplicației și să definească în prealabil o perioadă de inactivitate după scurgerea căreia contul este considerat expirat;
- în ceea ce privește aplicațiile destinate copiilor: să acorde atenția cuvenită limitei de vârstă care definește statutul de copil sau de minor în legislația națională, să aleagă abordarea cea mai restrictivă în materie de prelucrare a datelor care să respecte în totalitate principiile minimizării datelor și limitării scopului, să se abțină de la prelucrarea, directă sau indirectă, a datelor copiilor în scopuri de publicitate comportamentală, precum și de la

colectarea de date referitoare la rudele și/sau prietenii copiilor prin intermediul acestora din urmă.

Grupul de lucru recomandă dezvoltatorilor de aplicații

- să consulte orientările relevante referitoare la riscurile și măsurile specifice în materie de securitate;
- să informeze în mod proactiv utilizatorii cu privire la încălcările referitoare la datele lor cu caracter personal, în conformitate cu cerințele prevăzute de Directiva asupra confidențialității și comunicațiilor electronice;
- să informeze utilizatorii cu privire la considerentele de proporționalitate pentru tipurile de date colectate sau accesate pe dispozitiv, perioadele de păstrare a datelor și măsurile de securitate aplicate;
- să dezvolte instrumente care să permită utilizatorilor să personalizeze perioadele de păstrare a datelor lor cu caracter personal mai degrabă în funcție de preferințele și contextele specifice ale acestora, mai degrabă decât să ofere perioade predefinite de păstrare a datelor respective;
- să includă în politica lor de confidențialitate informații special concepute pentru utilizatorii europeni;
- să dezvolte și să implementeze instrumente de acces online simple, dar sigure pentru utilizatori, fără să colecteze în exces date suplimentare cu caracter personal;
- împreună cu producătorii de SO și de dispozitive și magazinele de aplicații, să își utilizeze talentul creativ pentru a dezvolta soluții inovatoare pentru informarea corespunzătoare a utilizatorilor pe dispozitivele mobile, de exemplu, prin intermediul unui sistem de notificări informaționale în etape, combinate cu pictograme adecvate.

Magazinele de aplicații trebuie

- să își cunoască și să își respecte obligațiile în calitate de operatori de date atunci când prelucrează date de la și despre utilizatori;
- să asigure respectarea obligației de informare care revine dezvoltatorului de aplicații, mai ales în ceea ce privește tipurile de date pe care aplicația le poate accesa și scopurile acestei accesări, precum și eventuala transmitere a datelor către terți;
- să acorde o atenție specială aplicațiilor destinate copiilor cu scopul de a-i proteja împotriva prelucrării ilegale a datelor lor caracter personal și, în special, să asigure respectarea obligației de prezentare a informațiilor relevante într-o manieră simplă și într-un limbaj adecvat vârstei copiilor;
- să furnizeze informații detaliate despre verificările realizate efectiv în momentul prezentării aplicației, inclusiv despre cele menite să evalueze aspecte ale confidențialității și ale protecției datelor.

Grupul de lucru recomandă magazinelor de aplicații

- să dezvolte, în colaborare cu producătorul de SO, instrumente de control pentru utilizatori, cum ar fi simboluri care să reprezinte accesul la datele din dispozitivul mobil și la datele generate de acesta;
- să supună toate aplicațiile unui mecanism de reputație publică;
- să introducă un mecanism de dezinstalare la distanță a aplicației care să respecte viața privată;
- să pună la dispoziția utilizatorilor canale de răspuns („feedback") pentru raportarea problemelor în materie de confidențialitate și/sau securitate;
- să colaboreze cu dezvoltatorii de aplicații în scopul de a informa în mod proactiv utilizatorii cu privire la încălcările referitoare la datele lor cu caracter personal;
- să avertizeze dezvoltatorii de aplicații cu privire la caracteristicile dreptului european înainte de prezentarea aplicației în Europa, de exemplu, în legătură cu cerința de obținere a consimțământului și în cazul transferurilor de date cu caracter personal către țările care nu fac parte din UE.

Producătorii de SO și de dispozitive trebuie

- să își actualizeze API și să stocheze normele și interfețele cu utilizatorul cu scopul de a oferi utilizatorilor un control suficient pentru exercitarea unui consimțământ valabil în ceea ce privește prelucrarea datelor de către aplicații;
- să pună în aplicare mecanisme de obținere a consimțământului în cadrul SO la prima lansare a aplicației sau prima dată când aplicația încearcă să acceseze una dintre categoriile de date cu impact semnificativ asupra vieții private;
- să aplice principiile privind luarea în considerare a vieții private începând cu momentul conceperii și luarea în considerare a vieții private în setările standard cu scopul de a preveni monitorizarea în secret a utilizatorului;
- să garanteze securitatea prelucrării datelor;
- să se asigure că aplicațiile preinstalate (setările standard ale acestora) respectă dreptul european în domeniul protecției datelor;
- să ofere un acces detaliat la date, senzori și servicii cu scopul de a asigura că dezvoltatorul de aplicații poate accesa numai datele care sunt necesare pentru aplicația sa;
- să pună la dispoziție mijloace ușor de utilizat și eficace pentru a evita monitorizarea utilizatorilor de către agenții de publicitate și de către alți terți. Setările standard trebuie să fie concepute astfel încât să se evite orice monitorizare a utilizatorilor;
- să asigure că sunt disponibile mecanisme corespunzătoare de informare și educare a utilizatorilor finali cu privire la funcționalitatea aplicațiilor și la datele pe care le pot accesa;
- să asigure că fiecare acces la o categorie de date se reflectă în informațiile furnizate utilizatorului înainte de instalarea aplicației: categoriile prezentate trebuie să fie clare și cuprinzătoare;
- să instaureze un mediu propice securității, cu instrumente de prevenire a extinderii aplicațiilor dăunătoare și cu scopul de a permite instalarea/dezinstalarea cu ușurință a fiecărei funcționalități în parte.

Grupul de lucru recomandă producătorilor de SO și de dispozitive

- să permită utilizatorilor să dezinstaleze aplicațiile și să transmită dezvoltatorului de aplicații un semnal (de exemplu, prin intermediul API) pentru a permite ștergerea datelor relevante ale utilizatorului;
- să ofere și să faciliteze în mod sistematic actualizări de securitate periodice;

- să asigure că metodele și funcțiile care permit accesul la datele cu caracter personal includ caracteristici care permit introducerea unui sistem de cereri de consimțământ detaliat;
- să contribuie în mod activ la dezvoltarea și facilitarea de pictograme prin care utilizatorii sunt avertizați cu privire la diferite utilizări ale datelor de către aplicații;
- să dezvolte piste clare de audit în cadrul dispozitivelor astfel încât utilizatorii finali să vadă în mod clar care aplicații au accesat date cu caracter personal pe dispozitivele lor, precum și volumul traficului de ieșire pe aplicație în raport cu traficul inițiat de utilizatori.

Terții trebuie

- să își cunoască și să își respecte obligațiile în calitate de operatori de date atunci când prelucrează date de la și despre utilizatori;
- să respecte cerința de obținere a consimțământului, prevăzută la articolul 5 alineatul (3) din Directiva asupra confidențialității și comunicațiilor electronice, în momentul în care citesc sau scriu date pe dispozitivele mobile, în colaborare cu dezvoltatorii de aplicații și/sau magazinele de aplicații care informează în principiu utilizatorii cu privire la scopul prelucrării datelor lor cu caracter personal;
- să nu eludeze mecanismele proiectate pentru evitarea urmăririi, astfel cum se întâmplă adesea cu mecanismele „Nu urmări” (*Do Not Track*) integrate în browsere;
- atunci când sunt furnizori de servicii de comunicații și distribuie dispozitive de marcă, să se asigure că utilizatorii și-au exprimat consimțământul valabil cu privire la aplicațiile preinstalate și să își asume responsabilitățile relevante în cazul în care contribuie la determinarea anumitor caracteristici ale dispozitivului și ale SO, de exemplu, în cazul limitării accesului utilizatorilor la anumiți parametri de configurare sau al filtrării corecturilor (de securitate și funcționale) furnizate de către producătorii de dispozitive și de SO;
- atunci când sunt agenți de publicitate, să evite în mod specific propunerea de reclame în afara contextului aplicației, de exemplu propunerea de reclame prin modificarea setărilor browserului sau plasarea de pictograme pe ecranul dispozitivului mobil, și să se abțină de la utilizarea identificatorilor unici ai dispozitivelor sau ai abonaților în scopul urmăririi;
- să se abțină de la prelucrarea, directă sau indirectă, a datelor copiilor în scopuri de publicitate comportamentală și să aplice măsuri corespunzătoare de securitate. Aceasta include transmisia în siguranță și stocarea criptată a identificatorilor unici ai dispozitivelor și ai utilizatorilor de aplicații, precum și a altor date cu caracter personal.

Grupul de lucru recomandă terților

- să dezvolte și să implementeze instrumente de acces online simple, dar sigure pentru utilizatori, fără să colecteze în exces date suplimentare cu caracter personal;
- să colecteze și să prelucreze numai datele relevante pentru contextul în care utilizatorul furnizează aceste date.