ARTIKLI 29 ALUSEL ASUTATUD ANDMEKAITSE TÖÖRÜHM

00461/13/ET
WP 202

Arvamus 02/2013 nutiseadmete rakenduste kohta

Vastu võetud 27. veebruaril 2013

Lühiülevaade

Nutiseadmete rakenduste poodides on iga levinud nutiseadme liigi jaoks saadaval sadu tuhandeid rakendusi. On teada, et poodidesse lisandub iga päev üle 1 600 uue rakenduse. Teadaolevalt laadib keskmine nutitelefoni kasutaja alla 37 rakendust. Rakendusi pakutakse lõppkasutajale väikese tasu eest või tasuta ning kasutajate arv võib ulatuda mõnest inimesest mitme miljonini.

Rakendused suudavad koguda seadmest suures mahus andmeid (nt andmed, mida kasutaja seadmes hoiab, ja eri andurite, sh asukohaandurite andmed) ning töödelda neid lõppkasutajale uute ja innovatiivsete teenuste pakkumiseks. Samas on neidsamu andmeid võimalik edasi töödelda – üldjuhul lisatulu saamiseks lõppkasutaja teadmata või tema jaoks soovimatul viisil.

Rakenduste arendajad, kes andmekaitsenõudeid ei tunne, võivad nutiseadmete kasutajate eraelu ja mainet olulisel määral ohustada. Andmekaitseriskidest ohustavad lõppkasutajaid eelkõige läbipaistvuse puudumine ja teadmatus rakenduse võimalikest töötlemisviisidest ning lõppkasutajate sisulise nõusoleku puudumine enne töötlemist. Puudulikud turvameetmed, ilmne soov koguda võimalikult palju andmeid ja isikuandmete kogumise hägusad eesmärgid suurendavad praeguses rakenduste keskkonnas riske veelgi.

Suur andmekaitserisk tuleneb ka rakenduste arendamise valdkonnas tegutsevate arvukate osalejate killustatusest. Nende hulka kuuluvad rakenduste arendajad; rakenduste omanikud; rakenduste poed; operatsioonisüsteemi ja seadmete tootjad ning muud kolmandad isikud, kes võivad osaleda nutiseadmetest pärit isikuandmete kogumisel ja töötlemisel, nagu analüütikud ja reklaamiandjad. Enamik käesolevas arvamuses esitatud järeldusi ja soovitusi on mõeldud rakenduste arendajatele (sest nemad saavad töötlemise või teabe esitamise konkreetset viisi rakenduses kõige rohkem mõjutada), kuid sageli peavad nad eraelu puutumatuse ja andmekaitse kõrgeimate standardite saavutamiseks tegema rakenduste vallas koostööd teiste osalejatega. See on eriti oluline turvalisuse seisukohast, sest mitmest osalejast koosnev kett on ainult nii tugev, kui seda on keti nõrgim lüli.

Suur osa nutitelefonides kättesaadavatest andmeliikidest on isikuandmed. Asjaomase õigusraamistiku moodustab andmekaitsedirektiiv koos eraelu puutumatuse ja elektroonilise side direktiiviga, milles käsitletakse kasutajate eraelu osaks olevate mobiilseadmete kaitset. Kõnealuseid eeskirju kohaldatakse kõikidele ELi kasutajatele mõeldud rakenduste suhtes, olenemata rakenduste arendaja või rakenduste poe asukohast.

Käesolevas arvamuses selgitab töörühm nutiseadmete rakenduste arendamisel, levitamisel ja kasutamisel isikuandmete töötlemise suhtes kohaldatavat õigusraamistikku, keskendudes nõusoleku küsimise nõudele, eesmärgi piiramise ja minimaalsete andmete kogumise põhimõttele, vajadusele võtta piisavaid turvameetmeid, kohustusele lõppkasutajaid nõuetekohaselt teavitada, nende õigustele, andmete säilitamise mõistlikele ajavahemikele ning eelkõige lastelt ja laste kohta kogutud andmete õiglasele töötlemisele.

Sisukord

1. Sissejuhatus

Rakendused on tarkvararakendused, mis on sageli kavandatud konkreetseks otstarbeks ja mõeldud teatavatele nutiseadmetele, nagu nutitelefonid, tahvelarvutid ja internetiühendusega telerid. Need süstematiseerivad teabe seadme konkreetsete omaduste jaoks sobival viisil ning suhtlevad tihedalt seadmete riistvara ja operatsioonisüsteemi funktsioonidega.

Nutiseadmete rakenduste poodides on iga levinud nutiseadme liigi jaoks saadaval sadu tuhandeid rakendusi. Rakendused on mõeldud väga erinevaks otstarbeks, muu hulgas veebi lehitsemiseks, suhtlemiseks (e-post, telefoni- ja internetisõnumid), meelelahutuseks (mängud, filmid/videod ja muusika), sotsiaalmeedia, pangandus- ja asukohapõhiste teenuste jaoks. On teada, et poodidesse lisandub iga päev üle 1 600 uue rakenduse[1]. Keskmine nutitelefoni kasutaja laadib alla 37 rakendust[2]. Rakendusi pakutakse lõppkasutajale väikese tasu eest või tasuta ning kasutajate arv võib ulatuda mõnest inimesest mitme miljonini.

Operatsioonisüsteem hõlmab ka nutiseadme põhiteenuste jaoks olulisi tarkvara- või andmestruktuure, näiteks nutitelefoni aadressiraamatut. Operatsioonisüsteem võimaldab teha need komponendid rakendustele kättesaadavaks rakenduste programmeerimise liideste kaudu. Liidesed võimaldavad juurdepääsu nutiseadmetes leiduvatele arvukatele anduritele. Sellised andurid hõlmavad järgmist: güroskoop, digitaalne kompass ja kiirendusmõõtur kiiruse ja liikumissuuna määramiseks; esi- ja tagakaamera videote ja fotode tegemiseks ning mikrofon heli salvestamiseks. Samuti võivad nutiseadmetesse olla paigaldatud lähedusandurid[3]. Nutiseadmeid võib ühendada ka mitmete võrguliideste kaudu, sealhulgas wifi, Bluetooth, lähiväljaside või Ethernet. Lõpuks võib õige asukoha määrata ka geograafilise asukoha kindlaksmääramise teenuse abil (nagu on kirjeldatud artikli 29 alusel asutatud andmekaitse töörühma arvamuses 13/2011 nutiseadmetes kasutatava asukoha kindlaksmääramise teenuse kohta[4]). Eri seadmetes ja operatsioonisüsteemides kogutakse andurite abil eri liiki andmeid erineva täpsusastme ja sagedusega.

Rakenduste programmeerimise liidese abil on rakenduste arendajatel võimalik selliseid andmeid järjepidevalt koguda, kasutada ning üles kirjutada kontaktandmeid, saata e-kirju, lühisõnumeid või sotsiaalvõrgustike sõnumeid, lugeda/muuta/kustutada SD-kaardi sisu, salvestada helifaile, kasutada kaamerat ja tutvuda salvestatud piltidega, tuvastada telefoni staatust ja andmeid, muuta süsteemi üldisi seadistusi ning vältida telefoni ooterežiimi

---

[1] ConceivablyTechi aruanne, 19. august 2012, kättesaadav aadressil www.conceivablytech.com/10283/business/apple-app-store-to-reach-1mapps-this-year-sort-of . Tsiteeritud väljaandes: Kamala D. Harris, Attorney General California Department of Justice, „Privacy on the go, Recommendations for the mobile ecosystem", jaanuar 2013, http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf .

[2] ABI Researchi maailmaprognoos 2012. aastaks, http://www.abiresearch.com/press/smartphone-users-worldwide-will-download-37-apps-o.

[3] Andur, mis suudab tuvastada füüsilise objekti kohalolu ilma füüsilise kontaktita. Vt: http://www.w3.org/TR/2012/WD-proximity-20121206/.

[4] Vt artikli 29 alusel asutatud andmekaitse töörühma arvamust 13/2011 nutiseadmetes kasutatava asukoha kindlaksmääramise teenuse kohta (mai 2011), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_et.pdf .

minekut. Samuti võivad rakenduste programmeerimise liidesed anda ühe või mitme kordumatu tunnuse abil teavet seadme enda või muude allalaaditud rakenduste kohta. Neidsamu andmeallikaid on võimalik edasi töödelda: üldjuhul lisatulu saamiseks lõppkasutajale teadmata või tema jaoks soovimatul viisil.

Käesoleva arvamuse eesmärk on selgitada nutiseadmete rakenduste levitamisel ja kasutamisel isikuandmete töötlemise suhtes kohaldatavat õigusraamistikku ning arutleda edasise töötlemise üle, mis võib toimuda väljaspool rakendust, nagu kogutud andmete kasutamine profiilide koostamiseks ja kasutajateni jõudmiseks. Arvamuses analüüsitakse peamisi andmekaitseriske, kirjeldatakse asjaomaseid osalejaid ja tuuakse esile erinevad seadusjärgsed kohustused. Osalejate hulka kuuluvad rakenduste arendajad; rakenduste omanikud; rakenduste poed; seadmete ja operatsioonisüsteemide tootjad ning muud kolmandad isikud, kes võivad osaleda nutiseadmetest pärit isikuandmete kogumisel ja töötlemisel, nagu analüütikud ja reklaamiandjad.

Arvamus keskendub nõusoleku küsimise nõudele, eesmärgi piiramise ja minimaalsete andmete kogumise põhimõttele, vajadusele võtta piisavaid turvameetmeid, kohustusele lõppkasutajaid nõuetekohaselt teavitada, nende õigustele, andmete säilitamise mõistlikele tähtaegadele ning eelkõige lastelt ja laste kohta kogutud andmete õiglasele töötlemisele.

Kohaldamisalasse kuuluvad paljud eri liiki nutiseadmed, kuid eelkõige mobiilsetele nutiseadmetele mõeldud rakendused.

2. Andmekaitseriskid

Tihe seotus operatsioonisüsteemiga võimaldab rakendustel tutvuda palju suurema andmehulgaga kui traditsiooniline veebilehitseja[5]. Rakendused suudavad koguda seadmest suures mahus andmeid (asukohaandmed, kasutaja poolt seadmes hoitavad andmed ja eri andurite andmed) ning neid töödelda lõppkasutajale uute ja innovatiivsete teenuste pakkumiseks.

Suur andmekaitserisk tuleneb ka rakenduste arendamise valdkonnas tegutsevate arvukate osalejate killustatusest. Andmeühiku saab seadmest töötlemiseks edastada reaalajas teisele poole maakera või kopeerida seda kolmandate isikute vahel. Mõned populaarseimad rakendused on välja arendanud suured tehnoloogiaettevõtted, kuid paljusid teisi kavandavad väikesed idufirmad. Üksainus programmeerija, kellel on idee ja vähene või olematu eelnev programmeerimisoskus, võib jõuda lühikese ajaga kogu maailma kasutajateni. Rakenduste arendajad, kes andmekaitsenõudeid ei tunne, võivad nutiseadmete kasutajate eraelu ja mainet olulisel määral ohustada. Samal ajal arenevad kiiresti kolmandate isikute pakutavad teenused, näiteks reklaam, ning kui rakenduste arendaja need läbimõtlematult rakendusse integreerib, võivad need avalikustada märkimisväärse hulga isikuandmeid.

Andmekaitseriskidest ohustavad lõppkasutajaid eelkõige läbipaistvuse puudumine ja teadmatus rakenduse võimalikest töötlemisviisidest ning lõppkasutajate sisulise nõusoleku

[5] Ehkki tänu veebimängude arendajatele laieneb ka lauaarvutite veebilehitsejate juurdepääs lõppkasutajate seadmete andurite andmetele.

puudumine enne töötlemist. Puudulikud turvameetmed, ilmne soov koguda võimalikult palju andmeid ja isikuandmete kogumise hägusad eesmärgid suurendavad praeguses rakenduste valdkonnas riske veelgi. Paljusid neist riskidest on uurinud ja käsitlenud juba teised rahvusvahelised reguleerivad asutused, nagu USA föderaalne kaubanduskomisjon, Kanada eraelu puutumatuse kaitse amet ja California õigusameti peaprokurör[6].

- Andmekaitse peamine risk on läbipaistvuse puudumine. Rakenduste arendajad peavad tagama, et operatsioonisüsteemi loojate ja rakenduste poodide pakutavatest võimalustest lähtudes oleks lõppkasutajale vajalikul hetkel kättesaadav põhjalik teave. Ent kõik rakenduste arendajad ei kasuta neid võimalusi piisaval määral, sest paljudel rakendustel puudub eraelu puutumatuse poliitika või nad ei teavita võimalikke kasutajaid arusaadavalt, mis liiki isikuandmeid rakendus võib töödelda ja millistel eesmärkidel. Läbipaistvuse puudumine ei ole ainult tasuta rakenduste või kogenematute arendajate rakenduste probleem, sest hiljutine uuring näitas, et 150 populaarsemast rakendusest vaid 61,3 %-l on olemas eraelu puutumatuse poliitika[7].

- Läbipaistvuse puudumine on tihedalt seotud vaba ja teadliku nõusoleku puudumisega. Pärast rakenduse allalaadimist piirdub nõusolek sageli vaid „linnukesega" kastis, mis näitab, et lõppkasutaja nõustub kasutustingimustega, ning keeldumisvõimalust isegi ei pakuta. Üleilmse mobiilsideoperaatorite ühenduse (GSMA) 2011. aasta septembris läbiviidud uuringu kohaselt soovib rakenduste kasutajatest 92 % üksikasjalikumat valikut[8].

- Puudulikud turvameetmed võivad viia (tundlike) isikuandmete lubamatu töötlemiseni, näiteks kui rakenduste arendaja kogutud isikuandmeid väärkasutatakse või kui isikuandmed rakendusest välja lekivad.

- Teine andmekaitserisk on seotud eesmärgi piiramise põhimõtte eiramisega (teadmatusest või tahtlikult): selle põhimõtte kohaselt võib isikuandmeid koguda ja töödelda ainult konkreetsetel ja õiguspärastel eesmärkidel. Rakenduste kaudu kogutud

---

6 Vt muu hulgas USA föderaalse kaubanduskomisjoni aruannet „Mobiilirakenduste pakkujate avaldused eraeluliste andmete kogumise kohta, usalduse loomine läbipaistvuse kaudu", veebruar 2013, http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf, föderaalse kaubanduskomisjoni aruanne „Mobiilirakendused lastele: praegused avaldused eraeluliste andmete kogumise kohta on ebarahuldavad", veebruar 2012, http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf, ja järelaruanne „Mobiilirakendused lastele: avaldused eraeluliste andmete kogumise kohta ei vasta ootustele", detsember 2012, http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf, Kanada eraelu puutumatuse kaitse amet, „Võimaluse kasutamine: eraelu kaitsega seotud head tavad mobiilirakenduste arendamisel", oktoober 2012, http://www.priv.gc.ca/information/pub/gd_app_201210_e.pdf, Kamala D. Harris, Attorney General California Department of Justice, „Privacy on the go, Recommendations for the mobile ecosystem", jaanuar 2013, http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf .

7 FPF (Future of Privacy Forum, eraelu puutumatust käsitleva foorumi) mobiilirakenduste uuring, juuni 2012, http://www.futureofprivacy.org/wp-content/uploads/Mobile-Apps-Study-June-2012.pdf.

8 „[Kasutajatest] 89 % arvab, et on oluline teada, kui rakendus jagab nende isikuandmeid, koos võimalusega seda funktsiooni välja või sisse lülitada." Allikas: „User perspectives on mobile privacy", september 2011, http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/futuresightuserperspectivesonuserprivacy.pdf.

isikuandmeid võidakse laialdaselt levitada mitmetele kolmandatele isikutele määramatutel ja hägusatel eesmärkidel, näiteks „turu-uuringute" eesmärgil. Samamoodi eiratakse muret tekitaval moel minimaalsete andmete kogumise põhimõtet. Hiljutised uuringud on näidanud, et paljud rakendused koguvad nutitelefonidest hulgaliselt andmeid, ilma et see oleks konkreetselt seotud rakenduse ilmsete funktsioonidega[9].

3 Andmekaitse põhimõtted

3.1 Kohaldatav õigus

ELi asjaomane õigusraamistik on andmekaitsedirektiiv (95/46/EÜ). Seda kohaldatakse kõikidel juhtudel, kui nutiseadmete rakenduste kasutamine hõlmab üksikisikute isikuandmete töötlemist. Kohaldatava õiguse kindlaks tegemiseks on kõigepealt oluline välja selgitada eri sidusrühmade roll: kohaldatava õigusega seoses on eriti oluline selgitada välja mobiilirakenduste kaudu toimuva andmetöötluse eest vastutav(ad) töötleja(d). Töötleja tuvastamine on ELi andmekaitseõiguse kohaldamise puhul otsustav, ehkki mitte ainus kriteerium. Andmekaitsedirektiivi artikli 4 lõike 1 punkti a kohaselt kohaldatakse isikuandmete mis tahes töötlemise suhtes liikmesriigi siseriiklikku õigust, kui töötlemine toimub selle liikmesriigi territooriumil paikneva vastutava töötleja „asutuse tegevuse raames". Andmekaitsedirektiivi artikli 4 lõike 1 punkti c kohaselt kohaldatakse liikmesriigi siseriiklikku õigust ka juhtudel, kui vastutav töötleja *ei ole registreeritud* ühenduse territooriumil ja kasutab vahendeid, mis paiknevad kõnealuse liikmesriigi territooriumil. Kuna ilma vahendita kasutajalt kogutud ja teda käsitlevaid isikuandmeid töödelda ei saa, siis seda kriteeriumi tavaliselt täidetakse[10]. Kuid see on asjakohane vaid siis, kui vastutav töötleja ei ole ELis registreeritud.

Seega iga kord, kui rakenduste arendamise, levitamise ja käitamisega seotud isik on vastutav töötleja, vastutab see isik üksi või koos teistega kõikide andmekaitsedirektiivis sätestatud nõuete täitmise eest. Mobiilirakendustega tegelevate isikute rolli väljaselgitamist analüüsitakse täpsemalt allpool punktis 3.3.

Lisaks andmekaitsedirektiivile kehtestatakse eraelu puutumatust ja elektroonilist sidet käsitleva direktiiviga (2002/58/EÜ, mida on muudetud direktiiviga 2009/136/EÜ) eristandardid kõikidele isikutele üle maailma, kes soovivad Euroopa Majanduspiirkonna (EMP) kasutajate seadmetes salvestatud teavet säilitada või sellega tutvuda.

Eraelu puutumatust ja elektroonilist sidet käsitleva direktiivi artikli 5 lõikega 3 nähakse ette, et *teabe salvestamine või juurdepääs abonendi või kasutaja lõppseadmesse salvestatud teabele on lubatud ainult tingimusel, et asjaomasele abonendile või kasutajale esitatakse direktiivi 95/46/EÜ kohaselt selge ja arusaadav teave muu hulgas andmete töötlemise eesmärgi kohta.*

---

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

[10] Kui rakendus edastab isikuandmeid vastutavatele töötlejatele. Kriteeriumi ei pruugita täita, kui andmeid töödeldakse ainult kohapeal, seadmes endas.

Ehkki paljud direktiivi sätted kehtivad vaid ühenduse üldkasutatavate elektrooniliste sideteenuste osutajatele ja üldkasutatavate elektrooniliste sidevõrkude pakkujatele, kehtib artikli 5 lõige 3 kõikidele üksustele, kes edastavad nutiseadmetele teavet või loevad sealt teavet. See kehtib olenemata üksuse laadist (st avaliku või erasektori üksus, üksikprogrammeerija või suurettevõtja või vastutav töötleja, andmetöötleja või kolmas isik). Artikli 5 lõikes 3 sätestatud nõusoleku küsimise nõue kehtib mis tahes teabe kohta, olenemata salvestatava või kasutatava teabe laadist. Reguleerimisala ei piirdu isikuandmetega; teabena võib käsitleda mis tahes liiki andmeid, mida seadmes salvestatakse.

Eraelu puutumatust ja elektroonilist sidet käsitleva direktiivi artikli 5 lõikes 3 sätestatud nõusoleku küsimise nõue kehtib *ühenduses* pakutavatele teenustele, see tähendab, kõikidele Euroopa Majanduspiirkonna elanikele teenusepakkuja asukohast olenemata. On oluline, et rakenduste arendajad teaksid, et mõlemad direktiivid on kohustuslikud õigusaktid ning et üksikisiku õigusi ei saa edasi anda ega nendest lepinguga loobuda. See tähendab, et Euroopa eraelu puutumatust käsitlevaid õigusnorme ei saa välistada ühepoolse avalduse ega kokkuleppe alusel[11].

3.2 Rakendustes töödeldavad isikuandmed

Paljud nutiseadmetes salvestatavatest või genereeritavatest andmeliikidest on isikuandmed. Eraelu puutumatust ja elektroonilist sidet käsitleva direktiivi põhjenduse 24 kohaselt:

> „*Elektrooniliste sidevõrkude kasutajate lõppseadmed ja sellistes seadmetes säilitatav teave moodustavad osa kasutajate eraelust, mida tuleb kaitsta inimõiguste ja põhivabaduste kaitse Euroopa konventsiooni kohaselt*."

Tegemist on isikuandmetega, olenemata sellest, kas need käsitlevad isikut, keda vastutaval töötlejal on võimalik kas otseselt (näiteks nime järgi) või kaudselt tuvastada, või kolmandat isikut. Need võivad käsitleda seadme omanikku või muud isikut, näiteks aadressiraamatus registreeritud sõprade kontaktandmeid[12]. Andmeid on võimalik koguda ja töödelda seadmes või (pärast edastamist) mujal rakenduste arendajate või kolmandate isikute infrastruktuuris välise rakenduste programmeerimise liidesega ühenduse kaudu reaalajas ilma lõppkasutaja teadmata.

Sellised isikuandmed, mis võivad kasutajate ja teiste inimeste eraelu märkimisväärselt mõjutada, on näiteks järgmised:

- asukoht;
- kontaktandmed;
- seadme ja kliendi kordumatud kasutajatunnused (nagu IMEI,[13] IMSI,[14] UDID[15] ja mobiiltelefoni number);

---

[11] Näiteks väited, nagu kehtiks ainult EMP-välise jurisdiktsiooni õigus.

[12] Andmeid on võimalik i) genereerida automaatselt seadme operatsioonisüsteemis ja/või seadmete tootja või asjaomase mobiiltelefoniteenuse pakkuja eelnevalt määratletud funktsioonide abil (nt geograafilise asukoha andmed, võrguseadistused, IP-aadress); ii) genereerida kasutaja rakenduste abil (kontaktandmete loetelud; märkmed, fotod); iii) genereerida rakendustes (nt külastatud veebilehtede loetelu).

[13] Rahvusvaheline mobiilside terminalseadme **tunnus**.

[14] Rahvusvaheline mobiilside **tunnus**.

- andmesubjekti andmed;
- telefoni andmed (st telefoni nimi[16]);
- krediitkaardi ja makseandmed;
- telefonikõnede logid, lühi- ja kiirsõnumid;
- külastatud veebilehtede loetelu;
- e-post;
- infoühiskonna teenuste autentimise mandaadid (eelkõige sotsiaalfunktsioonidega teenused);
- pildid ja videod;
- biomeetria (nt näotuvastus ja sõrmejäljemallid).

3.3 Andmetöötluses osalevad isikud

Rakenduste arendamisel, levitamisel ja käitamisel osaleb mitmeid eri isikuid ning igaühel neist võivad olla erinevad andmekaitsekohustused.

Eristada võib nelja peamist isikut. Need on järgmised: i) rakenduste arendajad (sealhulgas rakenduste omanikud),[17] operatsioonisüsteemi ja seadmete tootjad;[18] iii) rakenduste poed (rakenduse levitaja) ning lõpuks iv) muud isikuandmete töötlemises osalevad isikud. Mõnel juhul on isikutel ühised andmekaitsekohustused, eelkõige juhul, kui sama üksus tegeleb mitme etapiga, näiteks kui operatsioonisüsteemi tootja haldab ka rakenduste poodi.

Ka lõppkasutajad peavad täitma oma rolli ning nõuetekohaselt vastutama oma mobiilseadmete kaudu isikuandmete genereerimise ja salvestamise eest. Kui selline töötlemine teenib üksnes isiklikke või koduseid eesmärke, siis andmekaitsedirektiivi (artikli 3 lõiget 2) ei kohaldata ning ametlikud andmekaitsekohustused kasutaja suhtes ei kehti. Kui aga kasutajad otsustavad andmeid rakenduse kaudu jagada, näiteks avalikustades teavet sotsiaalvõrgustiku rakenduse kaudu määramata arvule inimestele,[19] töötlevad nad teavet koduse kasutuse erandi tingimustest suuremas mahus[20].

3.3.1 Rakenduste arendajad

Rakenduste arendajad loovad rakendusi ja/või teevad need lõppkasutajatele kättesaadavaks. Kõnealune kategooria hõlmab era- ja avaliku sektori organisatsioone, kes tellivad rakenduste arendamise teistelt, ning rakendusi tootvaid ja turustavaid ettevõtteid ja üksikisikuid. Nad kavandavad ja/või toodavad nutitelefonides kasutatavat tarkvara ning otsustavad seega, millises ulatuses kasutab rakendus kas seadmes asuvaid ja/või eemal asuvate arvutisüsteemide

---

15 Seadme kordumatu **identifitseerimistunnus**.

16 Inimesed kasutavad telefonis sageli oma pärisnime, nt John Doe' iPhone.

17 Töörühm kasutab ühist terminit „rakenduste tootjad", kuid rõhutab, et mõiste ei piirdu rakenduste programmeerijate või tehniliste arendajatega, vaid hõlmab rakenduste omanikke, see tähendab ettevõtteid ja organisatsioone, kes tellivad rakenduste arendamise ja määravad nende eesmärgid.

18 Mõnel juhul on operatsioonisüsteemi ja seadmete tootja sama, samal ajal kui muudel juhtudel on seadmete tootja ja operatsioonisüsteemi tarnija erinevad ettevõtted.

19 Vt Euroopa Kohtu kohtuasju, kohtuasi C-101/01 kriminaalasi Bodil Lindqvisti süüdistuses, 6. novembri 2003. aasta otsus, ja kohtuasi C-73/07 Tietosuojavaltuutettu *vs*. Satakunnan Markkinapörssi Oy ja SatamediaOy, 16. detsembri 2008. aasta otsus.

20 Vt artikli 29 alusel asutatud andmekaitse töörühma arvamust 5/2009 Interneti suhtlusvõrkude kohta (juuni 2009), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_et.pdf.

vahendusel (rakenduste arendajate või kolmandate isikute arvutisüsteemid) kasutatavaid eri liiki isikuandmeid ning töötleb neid. Sel määral, mil rakenduste arendaja määrab kindlaks nutiseadmetes salvestatud isikuandmete töötlemise eesmärgi ja vahendid, on ta vastutav töötleja andmekaitsedirektiivi artikli 2 punkti d tähenduses. Sellisel juhul peab ta täitma kõiki andmekaitsedirektiivi sätteid. Põhisätteid on selgitatud käesoleva arvamuse punktides 3.4–3.10.

Isegi kui kasutaja suhtes kehtib koduse kasutuse erand, vastutab rakenduste arendaja siiski vastutava töötlejana, kui ta töötleb andmeid enda eesmärkidel. See on asjakohane näiteks juhul, kui rakendus nõuab teenuse osutamiseks (kiirsõnumid, telefoni- ja videokõned) võimalust tutvuda kogu aadressiraamatuga.

Rakenduste arendaja kohustused on märgatavalt väiksemad, kui isikuandmeid ei töödelda ja/või ei tehta väljaspool seadet kättesaadavaks või kui rakenduste arendaja on võtnud asjakohaseid tehnilisi ja korralduslikke meetmeid tagamaks, et andmed muudetakse enne seadmest edastamist pöördumatult anonüümseks ning kogutakse konkreetselt sellesse seadmesse.

Igal juhul, kui rakenduste arendaja saab seadmes salvestatud teabega tutvuda, kohaldatakse ka eraelu puutumatust ja elektroonilist sidet käsitlevat direktiivi ning rakenduste arendaja peab täitma direktiivi artikli 5 lõikes 3 sätestatud nõusoleku küsimise kohustust.

Kui rakenduste arendaja on tellinud osa andmete tegelikust töötlemisest või kogu andmetöötluse kolmandalt isikult ja kõnealune kolmas isik täidab volitatud töötleja ülesandeid, peab rakenduste arendaja täitma kõiki volitatud töötleja kasutamisega seotud kohustusi. See hõlmab ka pilveteenuse osutaja kasutamist (nt andmete väliseks salvestamiseks)[21].

Kui rakenduste arendaja võimaldab kolmandatel isikutel kasutajaandmetega tutvuda (näiteks reklaamivõrgustik tutvub seadme geograafilise asukoha andmetega käitumispõhise reklaami edastamiseks), peab ta kasutama asjakohaseid vahendeid ELi õigusraamistikust tulenevate kohaldatavate nõuete täitmiseks. Kui kolmas isik saab tutvuda seadmes salvestatud andmetega, kohaldatakse eraelu puutumatust ja elektroonilist sidet käsitleva direktiivi artikli 5 lõikes 3 sätestatud teadliku nõusoleku küsimise kohustust. Veel enam, kui kolmas isik töötleb isikuandmeid enda eesmärkidel, võib ta olla koos rakenduse kasutajaga vastutav töötleja ning peab seetõttu järgima eesmärgi piiramise põhimõtet ja turvakohustusi[22] töötlemise selles osas, mille puhul tema määrab eesmärgi ja vahendid. Et rakenduste arendajate ja kolmandate isikute vahel võib olla eri liiki – nii ärilisi kui ka tehnilisi – kokkuleppeid, tuleb iga poole asjaomane vastutus määrata kindlaks iga juhtumi puhul eraldi, võttes arvesse asjaomase töötlemise konkreetseid asjaolusid.

---

[21] Vt artikli 29 alusel asutatud andmekaitse töörühma arvamust 5/2012 pilveandmetöötluse kohta (juuli 2012), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

[22] Vt artikli 29 alusel asutatud andmekaitse töörühma arvamust 2/2010 käitumispõhise internetireklaami kohta (juuni 2010), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf ja töörühma arvamust 1/2010 mõistete „vastutav töötleja" ja „volitatud töötleja" kohta (veebruar 2010), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.

Rakenduste arendaja võib kasutada kolmanda isiku teeke tavapärase funktsionaalsusega tarkvara abil, näiteks sotsiaalvõrgustikes mängitavate mängude platvormi teek. Rakenduste arendaja peab tagama, et kasutajad on teadlikud sellistes teekides toimuvast mis tahes andmetöötlusest ja et sellistel juhtudel vastab andmete töötlemine ELi õigusraamistikule, sealhulgas küsitakse asjakohastel puhkudel kasutaja nõusolekut. Selles mõttes peavad rakenduste arendajad vältima kasutaja eest varjatud funktsioonide kasutamist.

3.3.2 Operatsioonisüsteemi ja seadmete tootjad

Ka operatsioonisüsteemi ja seadmete tootjat tuleks lugeda vastutavaks töötlejaks (ja asjakohastel puhkudel ühistöötlejateks) mis tahes isikuandmete töötlemisel enda eesmärkidel, nagu seadme ladus töötamine, turvalisus jms. See hõlmab kasutaja genereeritud andmeid (nt kasutaja andmeid registreerimisel), seadme poolt automaatselt genereeritud andmeid (nt kui seadmel on asukohapõhine „kojuhelistamise" funktsioon) või operatsioonisüsteemi või seadmete tootja poolt rakenduste paigaldamise või kasutamise tulemusena töödeldavaid isikuandmeid. Kui operatsioonisüsteemi või seadmete tootja pakub lisafunktsioone, nagu varundamis- või asukoha määramise funktsioon, on tema ka selle tarvis töödeldud isikuandmete vastutav töötleja.

Rakendused, mis nõuavad geograafilise asukoha määramist, peavad kasutama operatsioonisüsteemi asukoha määramise teenuseid. Kui rakendus kasutab geograafilise asukoha määramist, võib operatsioonisüsteem koguda isikuandmeid geograafilise asukoha teabe edastamiseks rakendusele ning võib ühtlasi kaaluda andmete kasutamist oma asukoha määramise teenuste parandamiseks. Viimasel juhul on operatsioonisüsteem vastutav töötleja.

Operatsioonisüsteemi ja seadmete tootja vastutavad ka rakenduste programmeerimise liidese eest, mis võimaldab nutiseadmes asuvatel rakendustel isikuandmeid töödelda. Rakenduste arendaja saab tutvuda nende funktsioonidega, mille operatsioonisüsteemi ja seadmete tootjad teevad rakenduse programmeerimise liidese kaudu kättesaadavaks. Et operatsioonisüsteemi ja seadmete tootja määravad isikuandmetega tutvumise vahendid (ja ulatuse), peavad nad tagama, et rakenduste arendajal on piisavalt üksikasjalikud kontrollivolitused, et tutvuda võimaldataks ainult rakenduse toimimiseks vajalike andmetega. Operatsioonisüsteemi ja seadmete tootja peaksid samuti tagama, et juurdepääsu on võimalik lihtsal ja tõhusal viisil lõpetada.

„Lõimitud eraelukaitse" kontseptsioon on oluline põhimõte, millele viidatakse kaudselt juba andmekaitsedirektiivis[23] ja mis koos eraelu kaitsvate vaikesätetega tuleb selgemalt esile eraelu puutumatust ja elektroonilist sidet käsitlevas direktiivis[24]. Sellega nõutakse, et seadme või rakenduse tootjad võtaksid andmekaitset arvesse juba alates seadme või rakenduse kavandamise algusest. Lõimitud eraelukaitset nõutakse raadio- ja telekommunikatsioonivõrgu lõppseadmete direktiivi sätetes sõnaselgelt telekommunikatsiooniseadmete väljatöötamisel[25].

---

[23] Vt põhjendust 46 ja artiklit 17.

[24] Vt artikli 14 lõiget 3.

[25] Direktiiv 1999/5/EÜ, 9. märts 1999, raadioseadmete ja telekommunikatsioonivõrgu lõppseadmete ning nende nõuetekohasuse vastastikuse tunnustamise kohta. EÜT, L 91/10, 7.4.1999. Artikli 3 lõike 3 punktis c

Seepärast on operatsioonisüsteemi ja seadmete tootjatel koos rakenduste poodidega oluline ülesanne tagada rakenduste kasutajate isikuandmete ja eraelu puutumatuse kaitse. See hõlmab asjakohaste mehhanismide kättesaadavust lõppkasutajate teavitamiseks ja harimiseks selles valdkonnas, mida rakendused suudavad teha ja milliste andmetega tutvuda, samuti rakenduste kasutajatele asjakohaste seadistuste tagamist töötlemisparameetrite muutmiseks[26].

3.3.3 Rakenduste poed

Kõikidel populaarsematel nutiseadmete liikidel on oma rakenduste pood ja sageli on konkreetne operatsioonisüsteem konkreetse rakenduste poega tihedalt seotud. Rakenduste poed töötlevad sageli rakenduste eest tehtud ettemakseid ja võivad toetada ka rakenduse kaudu ostmist ning nõuavad seepärast kasutajate nime, aadressi ja finantsandmete registreerimist. Kõnealuseid (otseselt) tuvastatavad andmeid võidakse siduda ostu- ja kasutaja käitumist käsitlevate andmetega ning seadmest loetud või selles genereeritud andmetega (näiteks kordumatud tunnused). Selliste isikuandmete töötlemisel on rakenduste poed tõenäoliselt vastutavad töötlejad, sealhulgas juhul, kui nad edastavad sellise teabe uuesti rakenduste arendajatele. Kui rakenduste pood töötleb lõppkasutaja rakenduste allalaadimiste või kasutusajalugu või sarnast loetelu varem allalaaditud rakenduste taastamiseks, on ta samuti sel eesmärgil töödeldud isikuandmete vastutav töötleja.

Rakenduste pood registreerib sisselogimise mandaadid ja andmed varem ostetud rakenduste kohta. Samuti palub ta kasutajal sisestada krediitkaardi numbri, mis salvestatakse kasutaja kontole. Nende toimingute puhul on rakenduste pood vastutav töötleja. Seevastu võib selguda, et veebisaidid, kus lubatakse rakendus seadmesse paigaldamiseks alla laadida ilma autentimiseta, ei töötle isikuandmeid.

Rakenduste poodidel on oluline roll rakenduste arendajate esitatud nõuetekohase teabe vahendamisel rakenduse, sealhulgas rakenduses töödeldavate andmete liigi ja töötlemise eesmärgi kohta. Rakenduste poed saavad tagada kõnealuste eeskirjade täitmise oma kasutuspoliitika kaudu (mis põhineb eel- või järelkontrollil). Koostöös operatsioonisüsteemi tootjaga võib rakenduste pood välja töötada raamistiku, milles rakenduste arendajad saavad edastada järjepidevat ja sisukat teavet (näiteks sümboleid, mis näitavad teatavat liiki juurdepääsu andurite andmetele) ja kus teave esitatakse rakenduste poe kataloogis nähtaval kohal.

3.3.4 Kolmandad isikud

Rakenduste kasutamisel kogutud andmete töötlemisega on seotud mitmed erinevad kolmandad isikud.

Näiteks paljude tasuta rakenduste eest tasutakse reklaamidega, mis võivad (kuid ei pruugi) olla seotud kontekstiga või personaliseeritud ning mille edastamist võimaldavad

---

sätestatakse, et Euroopa Komisjon võib otsustada, et lõppkasutajate seadmed peavad olema valmistatud sel viisil, et need sisaldavad kasutajate ja abonentide isikuandmete ja eraelu puutumatuse kaitse tagatisi.

[26] Töörühm tervitab selles suhtes föderaalse kaubanduskomisjoni soovitusi eespool viites 6 osutatud aruandes „Mobiilirakenduste pakkujate avaldused", näiteks leheküljel 15: „(…) platvormidel on hea võimalus teha rakenduste kaudu järjepidevalt avaldusi ja neid julgustatakse avaldusi tegema. Vastavalt seminari käigus laekunud märkustele võiksid nad kaaluda kõnealuste avalduste tegemist eri aegadel ."

jälgimisfunktsioonid, näiteks küpsised või muu seadmetuvastus. Reklaam võib hõlmata rakenduses leiduvat reklaamiriba, rakenduse väliseid reklaame, mida edastatakse veebilehitseja seadistusi muutes või ikoonide suunamisega mobiilsele töölauale või rakenduse sisu personaliseeritud esituse kaudu (nt sponsitud otsingutulemused).

Rakendustesse suunavad reklaame üldjuhul reklaamivõrgustikud või muud sarnased vahendajad, kelleks võib olla operatsioonisüsteemi tootja või rakenduste pood või nendega seotud üksus. Nagu on viidatud artikli 29 alusel asutatud andmekaitse töörühma arvamuses 2/2010,[27] hõlmab internetireklaam sageli isikuandmete töötlemist vastavalt andmekaitsedirektiivi artiklis 2 sätestatule ja töörühma tõlgendusele[28].

Muud kolmandad isikud on näiteks analüüsiteenuste pakkujad ja sideteenuste pakkujad. Analüüsiteenuste pakkujad võimaldavad rakenduste arendajatel saada ülevaade oma rakenduste kasutamisest, populaarsusest ja kasutusmugavusest. Ka sideteenuste pakkujad[29] võivad etendada paljude seadmete vaikeseadistuste ja turvavärskenduste määramisel olulist rolli ning võivad töödelda rakenduste kasutamist käsitlevaid andmeid. Nende teostataval kohandamisel (individualiseerimisel) võivad olla tagajärjed võimalikele tehnilistele ja funktsionaalsetele meetmetele, mida kasutaja saab oma isikuandmete kaitsmiseks võtta.

Rakenduste arendajatega võrreldes võivad kolmandad isikud mängida kaht erinevat rolli: esiteks teha rakenduse omaniku jaoks toiminguid, näiteks esitada rakenduses analüüsiandmeid. Sel juhul – kui nad tegutsevad üksnes rakenduste arendaja nimel ega töötle andmeid enda eesmärkidel ega edasta andmeid teistele arendajatele – tegutsevad nad tõenäoliselt volitatud töötlejana.

Teiseks on nende ülesanne koguda rakendustest teavet lisateenuste pakkumiseks: edastada analüüsiandmeid (rakenduste populaarsus, personaliseeritud soovitus) laiemalt või vältida sama reklaami kuvamist samale kasutajale. Kui kolmandad isikud töötlevad isikuandmeid enda eesmärkidel, tegutsevad nad vastutava töötlejana ja peavad seepärast täitma kõiki andmekaitsedirektiivi[30] kohaldatavaid sätteid. Käitumispõhise reklaami puhul peab vastutav töötleja saama kasutaja kehtiva nõusoleku isikuandmete kogumiseks ja töötlemiseks, mis hõlmab näiteks isikuandmete analüüsi ja ühendamist ning profiilide koostamist ja/või kasutamist. Nagu artikli 29 alusel asutatud andmekaitse töörühm on selgitanud oma arvamuses 2/2012 käitumispõhise internetireklaami kohta, on sellist nõusolekut kõige lihtsam hankida eelneva nõusoleku mehhanismi abil.

---

[27] Artikli 29 alusel asutatud andmekaitse töörühma arvamus 2/2010 käitumispõhise internetireklaami kohta (juuni 2010), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_et.pdf.

[28] Vt ka isikuandmete kontseptsiooni tõlgendust töörühma arvamuses 4/2007 isikuandmete mõiste kohta (juuni 2007), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_et.pdf.

[29] Sideteenuste pakkujad peavad täitma ka valdkonnapõhiseid andmekaitsekohustusi, mis jäävad käesoleva arvamuse reguleerimisalast välja.

[30] Artikli 29 alusel asutatud andmekaitse töörühma arvamus 2/2010, lk 10–11.

Ettevõte pakub rakenduste omanikele ja reklaamiandjatele rakenduste arendaja poolt rakendustesse integreeritud jälgimisvahendeid, kasutades mõõdikuid. Seepärast on võimalik ettevõtte jälgimisvahendeid paigaldada paljudesse rakendustesse ja seadmetesse. Üks teenuseid on teavitada rakenduste arendajaid kordumatute tunnuste kogumise tulemusena sellest, milliseid muid rakendusi kasutaja kasutab. Ettevõte määratleb oma vahendite funktsioonid (st jälgimismehhanismid) ja eesmärgid enne, kui pakub neid rakenduste arendajatele, reklaamiandjatele ja teistele, ning tegutseb seetõttu vastutava töötlejana.

Kui kolmandad isikud tutvuvad nutiseadmetes asuva teabega või salvestavad seda, peavad nad täitma eraelu puutumatust ja elektroonilist sidet käsitleva direktiivi artikli 5 lõikes 3 sätestatud nõusoleku küsimise nõuet.

Sellega seoses on oluline märkida, et nutiseadmetes on kasutajate võimalused paigaldada isikuandmete töötlemist jälgivat tarkvara (mis on tavaline lauaarvuti veebikeskkonnas) üldiselt piiratud. HTTP-küpsiste asemel kasutavad kolmandad isikud kasutajate (kasutajarühmade) tuvastamiseks ja neile suunatud teenuste, sealhulgas reklaamide pakkumiseks sageli kordumatuid tunnuseid. Kuna kasutajad ei saa suurt osa neist tunnustest (nagu IMEI, IMSI, MSISDN[31] ja operatsioonisüsteemi lisatud spetsiifilised kordumatud seadmetunnused) ise kustutada ega muuta, on neil kolmandatel isikutel võimalus töödelda suurt hulka isikuandmeid nii, et lõppkasutajal ei ole võimalik seda jälgida.

3.4 Õiguslik alus

Isikuandmete töötlemiseks on vaja õiguslikku alust vastavalt andmekaitsedirektiivi artiklis 7 esitatud loetelule. Artiklis 7 eristatakse andmetöötluseks kuus õiguslikku alust: andmesubjekti antud ühemõtteline nõusolek; vajadus täita andmesubjektiga sõlmitud lepingut; andmesubjekti eluliste huvide kaitse, vajadus täita seadusjärgset kohustust; (avaliku sektori asutuste) üldiste huvidega seotud ülesande täitmine ja õigustatud (äri)huvide elluviimise vajadus.

Teabe salvestamise või nutiseadmes juba salvestatud teabe kasutamise puhul kehtestatakse eraelu puutumatust ja elektroonilist sidet käsitleva direktiivi artikli 5 lõikega 3 (st nõusoleku küsimine seadmesse teabe edastamiseks ja sealt väljavõtete tegemiseks) õigusliku aluse suhtes üksikasjalikumad piirangud, mida võib arvesse võtta.

3.4.1 Enne paigaldamist ja isikuandmete töötlemist antav nõusolek

Rakenduste puhul kasutatakse õigusliku alusena peamiselt nõusolekut. Rakenduse paigaldamisel edastatakse lõppkasutaja seadmesse teavet. Ühtlasi tutvuvad paljud rakendused seadmesse salvestatud andmete, aadressiraamatu kontaktandmete, piltide, videote ja muude isiklike dokumentidega. Eraelu puutumatust ja elektroonilist sidet käsitleva direktiivi artikli 5 lõikega 3 nõutakse kõikidel sellistel juhtudel nõusoleku küsimist kasutajalt, kellele on enne teabe seadmesse edastamist või sellest väljavõtete tegemist antud selget ja põhjalikku teavet.

On oluline märkida erinevust nõusoleku vahel, mida nõutakse seadmesse teabe edastamiseks ja seadmest teabe lugemiseks, ja nõusoleku vahel, mida on vaja õigusliku aluse tagamiseks eri

[31] Mobiilijaama integreeritud teenusega digitaalvõrk.

liiki isikuandmete töötlemisel. Ehkki mõlemad nõusoleku küsimise nõuded kehtivad üheaegselt, kumbki erineval õiguslikul alusel, kohaldatakse mõlema suhtes tingimust, et nõusolek peab olema vabatahtlik, konkreetne ja teadlik (nagu on määratletud andmekaitsedirektiivi artikli 2 punktis h). Seepärast võib need kaht liiki nõusolekud praktikas ühendada kas paigaldamise ajal või enne, kui rakendus hakkab seadmest isikuandmeid koguma –, tingimusel et kasutajale teatatakse ühemõtteliselt, millega ta nõustub.

Paljud rakenduste poed pakuvad rakenduste arendajatele võimalust teavitada lõppkasutajaid enne paigaldamist rakenduse põhiomadustest ja nõuda kasutajalt enne rakenduse allalaadimist ja paigaldamist positiivset kinnitust (st paigaldamise nupu klõpsamist). Ehkki selline tegevus võib mõnel juhul artikli 5 lõikes 3 sätestatud nõusoleku küsimise nõude täita, ei anna see tõenäoliselt piisavalt teavet, et lugeda see kehtivaks nõusolekuks isikuandmete töötlemiseks. Küsimust on varem arutanud artikli 29 alusel asutatud andmekaitse töörühm oma arvamuses 15/2011 nõusoleku määratluse kohta[32].

Nutiseadmete puhul tähendab „vabatahtlik", et kasutajal peab olema võimalus oma isikuandmete töötlemisega nõustuda või sellest keelduda. Seega, kui rakendusel on vaja isikuandmeid töödelda, peab olema kasutajal valikuvõimalus sellega nõustuda või sellest keelduda. Kasutajale ei tohiks paigaldamise lõpuleviimiseks kuvada ekraanil ainuüksi varianti „Jah, nõustun". Tuleb kuvada ka variant „Keeldun" või mingi muu võimalus, et paigaldamine peatada.

„Teadlik" tähendab, et andmesubjekti käsutuses peab olema mõistliku otsustuse tegemiseks vajalik teave[33]. Ebaselguse vältimiseks tuleb selline teave teha kättesaadavaks enne isikuandmete töötlemist. See hõlmab andmetöötlust, mis võib toimuda näiteks paigaldamise ajal, silumise või jälgimise jaoks. Sellise teabe sisu ja vormi käsitletakse põhjalikumalt käesoleva arvamuse punktis 3.7.

„Konkreetne" tähendab, et tahteavaldus peab olema seotud konkreetse andmeühiku töötlemise või andmetöötluse piiratud liigiga. Seepärast ei saa lihtsalt paigaldamise nupul klõpsamist lugeda isikuandmete töötlemise kehtivaks nõusolekuks, sest nõusolekuks ei või olla üldsõnaline luba. Mõnel juhul on kasutajatel võimalus anda üksikasjalik nõusolek, kui nõusolekut küsitakse iga andmeliigi kohta, millega rakendus kavatseb tutvuda[34]. Sellise lähenemisega täidetakse kaks olulist õiguslikku nõuet: esiteks teavitatakse kasutajat nõuetekohaselt teenuse olulistest kriteeriumidest ja teiseks küsitakse konkreetselt iga

---

[32] Artikli 29 alusel asutatud andmekaitse töörühma arvamus 15/2011 nõusoleku määratluse kohta (juuli 2011), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_et.pdf.

[33] Samas, lk 19.

[34] Üksikasjalik nõusolek tähendab, et inimesed saavad täpselt (konkreetselt) määrata, milliseid rakenduse pakutavaid isikuandmete töötlemise funktsioone nad soovivad aktiveerida.

kriteeriumi kohta nõusolekut[35]. Kui rakenduste arendaja palub kasutajatel nõustuda mahukate tingimustega ja/või eraelu puutumatuse poliitikaga, ei ole tegu konkreetse nõusolekuga[36].

Konkreetsus on seotud ka reklaamiandjate ja muude kolmandate isikute tegevusega kasutajate käitumise jälgimisel. Operatsioonisüsteemide ja rakenduste pakutavad vaikeseadistused peavad jälgimise välistama ning võimaldama kasutajatel anda seda liiki andmetöötluseks konkreetne nõusolek. Kolmandad isikud ei tohi kõnealustest vaikeseadistustest mööda hiilida, nagu praegu veebilehitsejates kasutatavate jälgimisvastaste mehhanismide puhul sageli tehakse.

Konkreetse nõusoleku näide

Rakendus annab teavet lähikonnas asuvate restoranide kohta. Paigaldamiseks peab rakenduste arendaja küsima nõusolekut. Geograafilise asukoha andmetega tutvumiseks peab rakenduste arendaja küsima nõusolekut eraldi, nt paigaldamise ajal või enne geograafilise asukoha andmetega tutvumist. „Konkreetne" tähendab, et nõusolek peab piirduma konkreetse eesmärgiga anda kasutajale soovitusi lähikonnas asuvate restoranide kohta. Seepärast võib seadmes asuvate asukohaandmetega tutvuda vaid siis, kui kasutaja kasutab rakendust sellel eesmärgil. Kasutaja nõusolek geograafilise asukoha andmete töötlemiseks ei luba rakendusel seadmest asukohaandmeid pidevalt koguda. Selline edasine töötlemine nõuaks lisateavet ja eraldi nõustumist.

Samamoodi selleks, et võimaldada siderakendusel tutvuda kasutaja kontaktide nimekirjaga, peab kasutaja saama välja valida kontaktid, kellega ta tahab suhelda, selle asemel et võimaldada tutvumist kogu aadressiraamatuga (sealhulgas nende inimeste kontaktandmetega, kes teenust ei kasuta ja kes ei saa olla endaga seotud andmete töötlemisega nõustunud).

Siiski on oluline märkida, et isegi kui nõusolek vastab eespool kirjeldatud kolmele kriteeriumile, ei anna see õigust ebaõiglaseks ja ebaseaduslikuks töötlemiseks. Kui andmete töötlemine ületab otstarbe piire ja/või on ebaproportsionaalne, ei ole rakenduste arendajal isegi kasutaja nõustumise korral andmete töötlemiseks kehtivat õiguslikku alust ja suure tõenäosusega rikub ta andmekaitsedirektiivi.

Otstarbe piire ületava ja ebaseadusliku andmetöötluse näide

Äratuskella rakendus sisaldab valikulist funktsiooni, mille kaudu kasutaja saab alarmi häälkäsklusega vaigistada või tellida selle korduse. Kõnealuses näites annab nõusolek õiguse salvestada andmeid vaid alarmsignaali ajal. Mis tahes jälgimist või salvestamist või heli alarmi vaikimise ajal loetakse suure tõenäosusega otstarbe piire ületavaks ja ebaseaduslikuks.

---

[35] Vajadust sellise üksikasjaliku nõusoleku järele kinnitatakse sõnaselgelt ka föderaalse kaubanduskomisjoni viimases aruandes (viide 6 eespool), lk 15–16: „platvormid peaksid kaaluma täpselt ajastatud avalduste tegemist ja küsima konkreetset nõusolekut muu sisu kogumiseks, mida paljud tarbijad peaksid paljudel juhtudel tundlikuks, nagu fotod, kontaktandmed, kalendrikirjed või audio- või videosisu salvestamine."

[36] Samas, lk 34–35: „Üldine nõusolek, kus ei näidata ära töötlemise eesmärki, millega andmesubjekt nõustub, ei vasta sellele nõudele. See tähendab, et töötlemise eesmärki ei tule lisada üldsätetesse, vaid see tuleb esitada eraldi nõustumisklauslina."

Seadmesse vaikimisi (enne seadme jõudmist lõppkasutaja omandusse) paigaldatud rakenduste või muu operatsioonisüsteemi-poolse töötlemise puhul, kus õigusliku alusena kasutatakse nõusolekut, peavad vastutavad töötlejad hoolikalt uurima, kas nõusolek tõepoolest kehtib. Paljudel juhtudel tuleks kaaluda eraldi nõusolekumehhanismi kasutuselevõttu, näiteks rakenduse esmakordsel käitamisel, et anda vastutavale töötlejale piisav võimalus lõppkasutajat täielikult teavitada. Kui tegemist on andmekaitsedirektiivi artiklis 8 määratletud andmete eriliikidega, peab nõusolek olema sõnaselge.

Samuti on oluline anda kasutajatele võimalus oma nõusolek lihtsal ja tõhusal viisil tagasi võtta. Seda käsitletakse põhjalikumalt käesoleva arvamuse punktis 3.8.

3.4.2 Andmetöötluse õiguslik alus rakenduse kasutamise ajal

Nagu eespool selgitatud, on nõusolek õiguslik alus, mida rakenduste arendaja vajab teabe õiguspäraseks lugemiseks ja/või kirjutamiseks ja seega isikuandmete töötlemiseks. Järgmises etapis, rakenduse kasutamise ajal võib rakenduse kasutaja tugineda muud liiki andmetöötluse puhul muudele õiguslikele alustele – kui see ei hõlma tundlike isikuandmete töötlemist.

Selline õiguslik alus – vastavalt andmekaitsedirektiivi artikli 7 punktidele b ja f – võib olla vajalik andmesubjektiga sõlmitud lepingu täitmiseks või õigustatud (äri)huvide elluviimiseks.

Kõnealust õiguslikku alust saab kasutada ainult konkreetse kasutaja mittetundlike isikuandmete töötlemisel ning sellele võib tugineda üksnes sel määral, kui teatav andmetöötlus on soovitud teenuse osutamiseks rangelt vajalik, või artikli 7 punkti f puhul vaid juhul, kui selliseid huve ei kaalu üles andmesubjekti põhiõiguste ja -vabadustega seotud huvid.

Lepingulise õigusliku aluse näide

Kasutaja annab nõusoleku paigaldada mobiilpanganduse rakendus. Maksekorralduse taotluse täitmiseks ei pea pank küsima kasutajalt eraldi nõusolekut tema nime ja kontonumbri avalikustamiseks makse saajale. Nende andmete avaldamine on selle konkreetse kasutajaga sõlmitud lepingu täitmiseks rangelt vajalik ja seepärast on pangal olemas andmekaitsedirektiivi artikli 7 punktile b vastav õiguslik alus. Sama põhjendus kehtib siderakenduste puhul: kui pangad edastavad esmavajaliku teabe, nagu konto nime, e-posti aadressi või telefoninumbri teisele inimesele, kellega kasutaja soovib suhelda, on andmete avaldamine lepingu täitmiseks ilmselgelt vajalik.

3.5 Eesmärgi piiramine ja minimaalsete andmete kogumine

Andmekaitsedirektiivi aluspõhimõtted on eesmärgi piiramine ja minimaalsete andmete kogumine. Eesmärgi piiramine võimaldab kasutajatel teha läbimõeldud otsus usaldada oma isikuandmed partnerile, kui nad teavad, kuidas nende andmeid kasutatakse, ning saavad oma andmete kasutuseesmärkide mõistmiseks tugineda piirava eesmärgi kirjeldusele. Seepärast peavad andmetöötluse eesmärgid olema hoolikalt määratletud ja arusaadavad keskmisele kasutajale, kellel ei ole õiguslikke või tehnilisi eriteadmisi.

Samal ajal nõuab eesmärgi piiramise põhimõte, et rakenduste arendajatel oleks enne kasutajatelt isikuandmete kogumise alustamist oma ärimudelist hea ülevaade. Isikuandmeid võib töödelda ainult õiglasel ja seaduslikul eesmärgil (andmekaitsedirektiivi artikli 6 lõige 1) ning need eesmärgid tuleb määratleda enne andmetöötlusega alustamist.

Eesmärgi piiramise põhimõte välistab töötlemise peamiste tingimuste järsu muutmise.

Näiteks kui rakenduse algne eesmärk on võimaldada kasutajatel üksteisele e-kirju saata, kuid arendaja otsustab oma ärimudelit muuta ja ühendab oma kasutajate e-posti aadressid teise rakenduse kasutajate telefoninumbritega. Asjaomased vastutavad töötlejad peaksid sel juhul küsima eelnevalt kõikidelt kasutajatelt eraldi ühemõttelist nõusolekut nende andmete töötlemiseks uuel eesmärgil.

Eesmärgi piiramine on tihedalt seotud minimaalsete andmete kogumise põhimõttega. Tarbetu ja potentsiaalselt ebaseadusliku andmetöötluse vältimiseks peavad rakenduste arendajad hoolikalt kaaluma, millised andmed on soovitud funktsiooni pakkumiseks rangelt vajalikud.

Rakendused võivad saada juurdepääsu seadme paljudele funktsioonidele ja seetõttu on neil võimalus teha paljusid asju, näiteks saata varjatud lühisõnum, tutvuda piltide ja kogu aadressiraamatuga. Paljud rakenduste poed toetavad (pool)automaatset ajakohastamist, mille puhul rakenduste arendaja saab lisada uued funktsioonid ja teha need kättesaadavaks lõppkasutaja vähesel sekkumisel või ilma selleta.

Töörühm rõhutab siinkohal, et rakenduste kaudu kasutaja andmetega tutvuvad kolmandad isikud peavad järgima eesmärgi piiramise ja minimaalsete andmete kogumise põhimõtet. Seadme kordumatuid ja sageli muutumatuid tunnuseid ei tohiks kasutada huvipõhise reklaami ja/või analüüside jaoks, sest kasutajad ei saa oma nõusolekut tühistada. Rakenduste arendajad peaksid välistama funktsioonide laienemise ja mitte kolima andmetöötlust rakenduse ühest versioonist teise, ilma et teavitaksid sellest nõuetekohaselt lõppkasutajaid ning pakuksid neile võimalust töötlemisest või kogu teenusest loobuda. Samuti tuleks kasutajatele pakkuda tehnilisi vahendeid avaldatud eesmärkide kontrollimiseks, võimaldades neil tutvuda teabega rakendusest väljuva liikluse mahu kohta ja võrrelda seda kasutajate algatatud liikluse mahuga.

Minimaalsete andmete kogumise ja eesmärgi piiramise põhimõtte järgimise tagamisel on peamised mehhanismid teavitamine ja kasutajatepoolne kontroll.

See, et rakenduste programmeerimise liidese kaudu on võimalik tutvuda seadmes asuvate alusandmetega, annab operatsioonisüsteemi ja seadmete tootjatele ning rakenduste poodidele võimaluse kohaldada erieeskirju ja pakkuda lõppkasutajatele asjakohast teavet. Näiteks peaksid operatsioonisüsteemi ja seadmete tootjad pakkuma rakenduse programmeerimise liidest, mis sisaldab täpseid kontrollimehhanisme andmeliikide eristamiseks ja selle tagamiseks, et rakenduste arendajad saavad taotleda võimalust tutvuda ainult andmetega, mis on nende rakenduse (seaduslike) funktsioonide jaoks rangelt vajalikud. Sel juhul on võimalik rakenduste arendaja taotletud andmeliike rakenduste poes selgesti kuvada ja kasutajat enne paigaldamist teavitada.

Sellega seoses tuginetakse seadmes salvestatud andmetega tutvumise jälgimisel järgmistele eri mehhanismidele:

a. operatsioonisüsteemi ja seadmete tootjad ning rakenduste poed määratlevad **eeskirjad**, mida kohaldatakse rakenduste suunamisel nende rakenduste poodi: rakenduste arendajad peavad kõnealuseid eeskirju järgima või riskima sellega, et nende rakendused ei ole asjaomastes poodides saadaval[37];
b. operatsioonisüsteemide **rakenduste programmeerimise liidestes** määratletakse standardsed meetodid andmetega tutvumiseks telefonis, millele on rakendustel juurdepääs. Samuti mõjutavad nad andmete kogumist serveri poolel;
c. **eelkontroll** – enne rakenduse paigaldamist toimuv kontroll[38];
d. **järelkontroll** – kontroll, mis toimub pärast rakenduse paigaldamist.

3.6 Turvalisus

Andmekaitsedirektiivi artikli 17 kohaselt peavad vastutavad ja volitatud töötlejad võtma töödeldavate isikuandmete kaitseks vajalikke tehnilisi ja korralduslikke meetmeid. Selle tulemusena peavad kõik punktis 3.3 määratletud osalejad võtma vastavalt oma ülesandele ja vastutusele meetmeid.

Turvalisuskohustuse täitmisel on kaks eesmärki. See võimaldab kasutajatel oma andmeid hoolikamalt jälgida ja suurendada usaldust nende üksuste vastu, kes kasutajate andmetega tegelikult tegelevad.

Oma vastutava töötleja asjaomaste turvalisuskohustuste täitmiseks peavad rakenduste arendajad, rakenduste poed, operatsioonisüsteemi ja seadmete tootjad ning kolmandad isikud arvesse võtma lõimitud eraelukaitse ja eraelu kaitsvate vaikesätete põhimõtet. See nõuab praeguste ja tulevaste andmekaitseriskide pidevat hindamist ning tõhusate leevendusmeetmete, sealhulgas minimaalsete andmete kogumise meetmete võtmist ja hindamist.

Rakenduste arendajad

Operatsioonisüsteemi ja seadmete tootjad ning sõltumatud kolmandad isikud, näiteks Euroopa Võrgu- ja Infoturbeamet (ENISA) on avaldanud mobiilirakenduste turvalisuse kohta palju üldsusele kättesaadavaid suuniseid[39].

Rakenduste arenduse kõikide parimate tavade läbivaatamine jääb väljapoole käesoleva arvamuse reguleerimisala; siiski kasutab töörühm võimalust vaadata läbi need tavad, mis võivad avaldada tõsist mõju rakenduste kasutajate põhiõigustele.

Enne rakenduse kavandamist on oluline otsustada, kuhu hakata andmeid salvestama. Mõnel juhul salvestatakse kasutaja andmed seadmesse, kuid rakenduste arendajad võivad kasutada

---

[37] Häkitud seadmed võimaldavad paigaldada rakendusi väljaspool ametlikke poode; Androidi seadmed võimaldavad rakendusi paigaldada ka muudest allikatest.
[38] Kehtib eelkõige eelpaigaldatud rakenduste puhul.
[39] ENISA „Nutitelefonide turvalise arendamise suunis”: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/smartphone-secure-development-guidelines.

ka klient-serveri arhitektuuri. See tähendab, et isikuandmed edastatakse või kopeeritakse serveriteenuse pakkuja süsteemidesse. Andmete salvestamisel ja töötlemisel seadmes saavad lõppkasutajad andmeid täpsemalt jälgida: näiteks andmete töötlemiseks antud nõusoleku tagasivõtmise korral on neil võimalik andmed kustutada. Andmete turvalisest salvestamisest eemal asuvas allikas võib aga olla abi andmete taastamisel, kui seade kaob või varastatakse. Võimalikud on ka vahepealsed meetodid.

Rakenduste arendajad peavad määratlema tarkvara arendamise ja levitamise selge poliitika. Ka operatsioonisüsteemi ja seadmete tootjatel on ülesanne edendada rakendustes isikuandmete turvalist töötlemist; seda käsitletakse lähemalt allpool. Teiseks peavad rakenduste arendajad ja rakenduste poed kavandama ja looma turvalisust soodustava keskkonna, mis sisaldab vahendeid pahavaraliste rakenduste leviku tõkestamiseks ja võimaldab iga rakendust kergesti paigaldada/eemaldada.

Head tavad, mida on võimalik rakenduse kavandamise käigus kasutusele võtta, hõlmavad koodiridade vähendamist ja lihtsustamist ning kontrollimeetmeid, et välistada andmete tahtmatu edastamine või ohustamine. Lisaks tuleks puhvri ületäitumise või injektsiooniga seotud rünnete vältimiseks kontrollida kõigi sisendite õigsust. Teised nimetamist väärivad turvamehhanismid hõlmavad piisavaid turvaaukude lappimise strateegiaid ning süsteemi turvalisuse regulaarset, sõltumatut auditit. Lisaks peaksid rakenduse kavandamise kriteeriumid hõlmama vähima vaikimisi eelisõiguse põhimõtet, mille alusel rakendustel võimaldatakse tutvuda vaid nende andmetega, mida nad funktsiooni kasutajale kättesaadavaks tegemiseks ka tegelikult vajavad. Samuti peaksid rakenduste arendajad ja rakenduste poed kasutajaid hoiatama ja julgustama neid kõnealuseid hea kavandamise tavasid täiendama, lisades sinna kasutajate tõhusaid tavasid, nagu kõige viimaste versioonide kasutamine rakendustes ja meeldetuletus kasutada eri teenuste puhul erinevaid salasõnu.

Rakenduse kavandamise etapis peavad rakenduste arendajad võtma ka meetmeid isikuandmete lubamatu kasutamise vältimiseks, tagades, et andmed on asjakohastel puhkudel kaitstud nii edastamise kui ka salvestamise ajal.

Pahavara / pahavaraliste rakenduste tagajärgede leevendamiseks peaksid mobiilirakendused töötama seadmete mälus konkreetses kohas (nn liivakastis[40]). Rakenduste arendajad peavad tihedas koostöös operatsioonisüsteemi tootja ja/või rakenduse poega kasutama kättesaadavaid mehhanisme, mis võimaldavad kasutajatel näha, millised rakendused milliseid andmeid töötlevad, ning andmetega tutvumist valikuliselt lubama ja keelama. Varjatud funktsioonide kasutamist ei tohiks lubada.

Rakenduste arendajad peavad hoolikalt läbi mõtlema, milliseid meetodeid kasutajate tuvastamiseks ja autentimiseks kasutada. Nad ei tohiks kasutada püsivaid (seadmega seotud) tunnuseid, vaid selle asemel madala entroopiaga ja rakendusega seotud või ajutisi seadmetunnuseid, et kasutajaid ei oleks võimalik ajas jälgida. Kaaluda tuleks eraelu puutumatust toetavate autentimismehhanismide kasutuselevõttu. Kasutajate autentimisel peavad rakenduste arendajad suhtuma erilise hoolikusega kasutajatunnuste ja salasõnade haldamisse. Viimased tuleb salvestada krüpteerituna ja turvaliselt, võtmega krüptograafilise

[40] „Liivakast" on kindlaksmääratud reeglitega turvamehhanism, mis eraldab töötavaid programme.

räsiväärtusena. Üks kasulik võimalus paremate salasõnade kasutuselevõtu soodustamiseks on võimaldada kasutajatel oma salasõna keerukust testida (entroopia kontroll). Asjakohastel puhkudel (juurdepääs tundlikele andmetele, kuid ka juurdepääs tasulistele vahenditele) võib ette näha korduva autentimise ka eri viisil ja eri kanalite kaudu (nt SMSiga saadetav juurdepääsukood) ja/või lõppkasutajaga (mitte seadmega) seotud autentimisandmete kasutamise teel. Samuti tuleks seansitunnuste valimisel kasutada ennustamatuid stringe, võimaluse korral koos taustateabega, nagu kuupäev ja kellaaeg, aga ka IP-aadress või geograafilise asukoha andmed.

Rakenduste arendajad peaksid ühtlasi arvesse võtma eraelu puutumatust ja elektroonilist sidet käsitlevas direktiivis sätestatud nõudeid isikuandmete rikkumise ja kasutajate eelteavitamise kohta. Ehkki kõnealuseid nõudeid kohaldatakse praegu ainult üldkasutatavate elektrooniliste sideteenuste osutajate suhtes, laiendatakse kohustust eeldatavasti vastavalt komisjoni ettepanekutele (COM 2012/0011/COD) tulevase isikuandmete kaitse määrusega kõikidele vastutavatele ja volitatud töötlejatele. See suurendab veelgi vajadust põhjaliku kõikide isikuandmete kogumist, salvestamist ja töötlemist käsitleva turvakava ning selle järjepideva hindamise järele, et vältida selliseid rikkumisi ja sellistel juhtudel ette nähtud suurte rahatrahvide tasumist. Turvakavas tuleb muu hulgas ette näha nõrkade kohtade kõrvaldamine ning usaldusväärsete veaparanduste õigeaegne ja turvaline kasutuselevõtt.

Rakenduste arendajate vastutus oma toodete turvalisuse eest ei lõpe töötava versiooni turuletoomisega. Nagu kõikides tarkvaratoodetes, võib ka rakendustes esineda turvavigu ja nõrku kohti ning rakenduste arendajad peavad arendama nende jaoks parandusi või paiku ning edastama need osalejatele, kes saavad need teha kasutajatele kättesaadavaks, või teevad seda ise.

Rakenduste poed

Rakenduste poed on lõppkasutajate ja rakenduste arendajate oluline vahendaja, kus rakendusi tuleks enne turule lubamist mitu korda hoolikalt ja tõhusalt kontrollida. Poed peaksid andma teavet oma tegelike kontrollimehhanismide kohta ning lisama andmekaitsekontrolli liiki käsitleva teabe.

Ehkki see meede ei ole pahavaraliste rakenduste leviku vältimisel 100 % tõhus, näitab statistika, et asjaomane tava vähendab märkimisväärselt pahavaraliste funktsioonide levikut nn ametlikes rakenduste poodides[41]. Selleks et iga päev esitataks kontrolliks arvukalt rakendusi, võiks protsessis olla kasu automaatsetest analüüsivahenditest, samuti teabevahetuskanalite loomisest turva- ja tarkvaraekspertide jaoks ning ilmnenud probleemide lahendamise tõhusast korrast ja strateegiast.

Lisaks rakenduste läbivaatamisele enne rakenduste poodi lubamist tuleks üldsusel lasta ka neid hinnata. Kasutajad ei peaks rakendusi hindama üksnes nende „laheduse", vaid ka funktsioonide alusel, pöörates erilist tähelepanu eraelu puutumatusele ja turvamehhanismidele. Samuti tuleks välja arendada võltshinnangute välistamise mehhanismid. Rakenduste hindamise mehhanismid võivad osutuda tõhusaks ka usalduse

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

suurendamisel eri üksuste vahel, eelkõige kui andmevahetus toimub mitme kolmanda isiku kaudu.

Rakenduste poed on pahatahtlike või ebaturvaliste rakenduste eemaldamiseks kasutanud distantsmeetodit. Kui selline mehhanism ei ole nõuetekohaselt kavandatud, võib see takistada kasutajatel oma andmeid hoolikamalt jälgida. Seepärast peaks rakenduste poe eraelu puutumatust toetav ja rakenduste distantsilt eemaldamiseks mõeldud vahend toimima teabe ja kasutajate nõusoleku alusel. Veelgi enam, praktilisemast seisukohast tuleks kasutajate käsutusse anda tagasisidekanalid, mille kaudu saab teatada rakenduste turvaprobleemidest ja distantsilt eemaldamise tõhususest.

Nii nagu rakenduste arendajad, peaksid ka rakenduste poed olema teadlikud kohustusest isikuandmete rikkumisest edaspidi teatada ning tegema rakenduste arendajatega selliste rikkumiste vältimiseks tõhusat koostööd.

Operatsioonisüsteemi ja seadmete tootjad

Operatsioonisüsteemi ja seadmete tootjad on rakenduste arendajate seas olulised osalejad ka miinimumstandardite ja parimate tavade määratlemisel mitte ainult kasutatava tarkvara ja rakenduste programmeerimise liideste turvalisuse, vaid ka pakutavate vahendite, suuniste ja abimaterjali alal. Operatsioonisüsteemi ja seadmete tootjad peaksid tegema kättesaadavaks tugevad ja tuntud krüpteerimisalgoritmid ning toetama võtmete asjakohast pikkust. Samuti peaksid nad rakenduste arendajatele kättesaadavaks tegema tugevad ja turvalised autentimismehhanismid (nt sertifikaatide kasutamine, millel usaldusväärsed sertifitseerimisasutused kinnitavad eemalasuva arvutisüsteemi autoriseerimist oma allkirjaga). Tänu sellele ei oleks rakenduste arendajatel vaja välja töötada ka firmaomaseid autentimismehhanisme. Praktikas rakendatakse seda sageli puudulikult ja see võib endast kujutada tõsist nõrkust[42].

Isikuandmetega tutvumist ja nende töötlemist rakendustes tuleks hallata rakenduste programmeerimise liidestesse integreeritud klasside ja meetodite abil, mis tagavad asjakohase kontrolli ja tagatised. Operatsioonisüsteemi ja seadmete tootjad peaksid tagama, et isikuandmetega tutvumist võimaldavad meetodid ja funktsioonid hõlmavad ka üksikasjaliku nõusoleku küsimiseks mõeldud funktsioone. Samamoodi tuleks võtta meetmeid isikuandmetega tutvumise välistamiseks või piiramiseks, kui kasutatakse madala tasemega funktsioone või muid vahendeid, millega võidakse rakenduste programmeerimise liidestesse integreeritud kontrollimeetmetest ja tagatistest mööda hiilida.

Operatsioonisüsteemi ja seadmete tootjad peavad seadmete jaoks välja töötama ka selged kontrolljäljed, et lõppkasutajatele oleks selgesti näha, millised rakendused on nende seadmetes olevate isikuandmetega tutvunud.

---

[42] Hiljuti toodi välja, et visuaalsete viidete puudumist SSL/TLS kasutamisel ja SSL/TLS ebapiisavat kasutamist võidakse ära kasutada vahendaja kaudu toimuvates rünnetes. Hiljutise uuringu kohaselt on rünnete suhtes haavatavate rakenduste koondandmebaasis mitut miljonit kasutajat. „Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security", Bernd Freisleben ja Matthew Smith, ACMi 19. arvuti- ja telekommunikatsioonitehnoloogia turvalisuse konverents (ACM CCS 2012).

Et turvavead lõppkasutajaid tarbetult ei ohustaks, peavad kõik osalejad turvaprobleemidele kiiresti reageerima. Kahjuks ei paku mõned operatsioonisüsteemi ja seadmete tootjad (ja telekommunikatsioonivõrgu operaatorid individualiseeritud seadmete turustamisel) operatsioonisüsteemi versioonidele pikaajalist tuge, jättes kasutajad levinud turvaprobleemide ees kaitseta. Operatsioonisüsteemi ja seadmete tootjad ning rakenduste arendajad peavad andma lõppkasutajatele eelteavet regulaarsete turvauuenduste paigaldamise intervalli kohta. Samuti peaksid nad teavitama kasutajaid võimalikult kiiresti, kui turvaprobleemi lahendamiseks on vaja tarkvara ajakohastada.

Kolmandad isikud
Eespool kirjeldatud turvafunktsioone ja kaalutlusi tuleb kohaldada ka kolmandate isikute (eelkõige reklaamiandjate ja analüüsiteenuste pakkujate) suhtes, kui nad koguvad ja töötlevad isikuandmeid oma eesmärkidel. See hõlmab seadme ja rakenduse kasutajate kordumatu tunnuse ja muude isikuandmete turvalist edastamist ja krüpteeritud salvestamist.

3.7 Teave

3.7.1 Teavitamiskohustus ja nõutav sisu
Andmekaitsedirektiivi artikli 10 kohaselt on igal andmesubjektil õigus teada tema isikuandmeid töötleva vastutava töötleja andmeid. Rakenduste puhul on lõppkasutajal lisaks õigus teada, mis liiki isikuandmeid töödeldakse ja mis eesmärgil andmeid kavatsetakse kasutada. Kui kasutaja isikuandmeid kogutakse teistelt rakenduste valdkonnas osalejatelt (nagu on kirjeldatud käesoleva arvamuse punktis 3.3), on lõppkasutajal vastavalt andmekaitsedirektiivi artiklile 11 sellegipoolest õigus saada andmete sellise töötlemise kohta kirjeldatud viisil teavet. Seepärast peab asjaomane vastutav töötleja isikuandmete töötlemisel teavitama potentsiaalseid kasutajaid vähemalt järgmisest:

- kes ta on (nimi ja kontaktandmed),
- rakenduste arendaja kogutavate ja töödeldavate isikuandmete täpsed kategooriad,
- miks (millistel konkreetsetel eesmärkidel) ta andmeid töötleb,
- kas andmeid avaldatakse kolmandatele isikutele,
- kuidas kasutajad võivad teostada oma õigusi nõusoleku tagasivõtmiseks ja andmete kustutamiseks).

Kõnealuse isikuandmete töötlemist käsitleva teabe kättesaadavus on kasutajalt andmete töötlemiseks nõusoleku saamisel otsustava tähtsusega. Nõusolek kehtib vaid siis, kui isikut on kõigepealt teavitatud andmete töötlemise peamistest kriteeriumidest. Sellise teabe esitamist alles pärast isikuandmete töötlemise alustamist rakenduses (mis sageli algab paigaldamise ajal) ei loeta piisavaks ja see on õiguslikult kehtetu. Kooskõlas föderaalse kaubanduskomisjoni aruandega rõhutab töörühm vajadust teavitada tarbijaid olulisel ajahetkel, vahetult enne sellise teabe kogumist rakendustes. Eriti oluline on täpsustada, milliseid andmeid kogutakse, arvestades rakenduste üldist laialdast juurdepääsu seadme anduritele ja andmestruktuuridele, kusjuures selline juurdepääs ei ole paljudel juhtudel automaatselt ilmselge. Samuti on väga oluline teabe piisavus, kui rakendus töötleb isikuandmete eriliike, nt tervislikku seisundit, poliitilisi uskumusi, seksuaalset sättumust jms käsitlevaid andmeid. Kokkuvõttes peaks rakenduste arendaja eristama selgesti kohustuslikku ja valikulist teavet ning süsteem peaks võimaldama kasutajal keelata valikulise teabega tutvumise, kasutades selleks eraelu puutumatust toetavaid vaikimisi valikuid.

Seoses volitatud töötleja isikuga peavad kasutajad teadma, kes nende isikuandmete töötlemise eest õiguslikult vastutab ja kuidas sellise töötlejaga ühendust saada. Vastasel juhul ei saa nad teostada oma õigusi, nagu õigus nende kohta (distantsilt) salvestatud teabega tutvuda. Rakenduste valdkonna killustatuse tõttu on väga oluline, et igal rakendusel oleks ühtne kontaktpunkt, mis vastutab kogu rakenduse kaudu toimuva andmetöötluse eest. Rakenduste arendajate ja teiste rakenduse kaudu isikuandmeid töötlevate isikute suhete väljaselgitamist ei tohi teha lõppkasutaja ülesandeks.

Eesmärgiga (eesmärkidega) seoses tuleb kasutajaid nõuetekohaselt teavitada, milliseid andmeid nende kohta kogutakse ja miks. Samuti tuleb kasutajatele selges ja lihtsas keeles teatada, kas andmeid võivad kasutada teised isikud, ning kui jah, siis millistel eesmärkidel. Hägusad eesmärgid, näiteks tooteinnovatsioon, ei ole kasutajate teavitamiseks piisavad. Tuleks selgelt välja öelda, kui kasutajatelt küsitakse nõusolekut andmete jagamiseks kolmandate isikutega reklaami ja/või analüüside jaoks. Rakenduste poodide oluline ülesanne on tagada, et selline teave on igale rakendusele kättesaadav ja sellega on lihtne tutvuda.

Rakenduste poodide oluline ülesanne on tagada asjakohane teave. Kasutajate teavitamiseks andmetöötluse liikidest on ülimalt soovitatav kasutada andmekasutust kirjeldavaid visuaalseid tähiseid või ikoone.

Lisaks eespool esitatud minimaalsele teabele, mis on vajalik rakenduse kasutaja nõusoleku küsimiseks, soovitab töörühm isikuandmete õiglase töötlemise tagamiseks anda vastutavatel töötlejatel kasutajatele ka järgmist teavet:

– proportsionaalsusega seotud kaalutlused andmeliikide puhul, mida seadme kaudu kogutakse või millega tutvutakse,
– andmete säilitamise aeg,
– turvameetmed, mida vastutav töötleja kasutab.

Samuti soovitab töörühm rakenduste arendajatel lisada oma Euroopa kasutajatele mõeldud eraelu puutumatuse poliitikasse ka teave selle kohta, kuidas rakendus vastab Euroopa andmekaitseõigusele, sealhulgas isikuandmete võimalik edastamine Euroopast näiteks USAsse, ning kas ja kuidas vastab rakendus sel juhul programmi Safe Harbori raamistikule.

3.7.2 Teabevorm

Esmatähtis teave andmetöötluse kohta peab olema kasutajatele kättesaadav rakenduste poe kaudu enne rakenduse paigaldamist. Teiseks peab andmete töötlemist käsitlev asjakohane teave olema pärast paigaldamist kättesaadav ka rakenduses endas.

Et rakenduste poed on koos rakenduste arendajatega teabe ühistöötlejad, peavad poed tagama, et esmatähtis teave isikuandmete töötlemise kohta esitatakse igas rakenduses. Nad peaksid kontrollima eraelu puutumatust käsitlevatele lehtedele suunavaid hüperlinke ning eemaldama rakendused, mis sisaldavad andmete töötlemise kohta vigaseid linke või muul moel kättesaamatuks jäävat teavet.

Töörühm soovitab teha isikuandmete töötlemist käsitleva teabe kättesaadavaks ja kergesti leitavaks ka rakenduste poes ning eelistatavalt rakenduse eest vastutava arendaja tavalisel veebisaidil. On vastuvõetamatu panna kasutajad olukorda, kus nad peavad ise veebist rakenduse andmetöötluspoliitika kohta teavet otsima, selle asemel et saada rakenduse arendaja või muu vastutava töötleja käest otse teavet.

Vähimal juhul iga rakendus peaks sisaldama kergesti loetavat, arusaadavat ja hõlpsasti kättesaadavat eraelu puutumatuse poliitikat, mis hõlmab kogu eespool nimetatud teavet. Paljude rakenduste puhul ei ole see läbipaistvuse miinimumnõue täidetud. FPF (eraelu puutumatust käsitleva foorumi) 2012. aasta juuni uuringu kohaselt ei ole 56 %-l tasulistest ja ligi 30 %-l tasuta rakendustest eraelu puutumatuse poliitikat.
Kui rakendused ei töötle isikuandmeid ega ole nende töötlemiseks mõeldud, tuleks seda eraelu puutumatuse poliitikas selgesti öelda.

Muidugi on teabe hulk, mida väikesel ekraanil esitada saab, piiratud, kuid sellega ei saa välja vabandada lõppkasutajate ebapiisavat teavitamist. Kasutajate teavitamiseks teenuse põhikriteeriumidest on võimalik kasutada mitut eri strateegiat. Töörühm näeb kasu mitmekihiliste teadete kasutamises, mida töörühm on lähemalt kirjeldanud arvamuses 10/2004[43] ja mille puhul algne teade kasutajale sisaldab ELi õigusraamistikus nõutud minimaalset teavet ja täiendav teave on kättesaadav linkide kaudu, mis suunavad eraelu puutumatuse täismahus esitatud poliitika juurde. Teave tuleks esitada otse ekraanil, hõlpsasti kättesaadavas ja kergesti märgatavas vormis. Mobiilseadmete väikesele ekraanile sobiva ülevaatliku teabe kõrval peab kasutajatel olema võimalus liikuda näiteks eraelu puutumatuse poliitikas sisalduvate pikemate selgituste juurde, kuidas rakenduses isikuandmeid kasutatakse, kes on vastutav töötleja ja kus saab kasutaja oma õigusi teostada.

Kõnealuse lähenemisviisi raames saab kasutada ikoone, pilte, video- ja audiosalvestisi ning kasutajat kontekstipõhiselt reaalajas teavitada, kui rakendus tutvub aadressiraamatu või fotodega[44]. Ikoonid peavad väljendama sisu, st olema selged, enesestmõistetavad ja ühemõttelised. Kahtlemata kannab operatsioonisüsteemi tootja selliste ikoonide kasutamise hõlbustamise eest olulist ühisvastutust.

Tegelikult oskavad rakenduste arendajad väikesele ekraanile mõeldud keerulisi liideseid suurepäraselt programmeerida ja kavandada ning töörühm kutsub arendajaid üles kasutama seda loomingulist oskust innovatiivsemate lahenduste loomiseks, et kasutajaid mobiilseadmete kaudu tõhusalt teavitada. Tagamaks, et tehnilise või õigustaustata kasutajad teabest tõepoolest aru saavad, soovitab töörühm tungivalt (kooskõlas föderaalse kaubanduskomisjoni aruandega) korraldada valitud teabestrateegiate tarbijauuring[45].

3.8 Andmesubjekti õigused

Andmekaitsedirektiivi artiklite 12 ja 14 kohaselt peavad rakenduste arendajad ja teised mobiilirakenduste valdkonna vastutavad töötlejad võimaldama rakenduste kasutajatel teostada oma õigust andmetega tutvuda, neid parandada, kustutada ja esitada andmetöötlemise suhtes vastuväiteid. Kui kasutaja teostab andmetega tutvumise õigust, peab vastutav töötleja andma kasutajale teavet töödeldavate andmete ja nende allika kohta. Kui vastutav töötleja teeb kogutud andmete põhjal automatiseeritud otsuseid, peab ta teavitama kasutajat ka nende otsuste loogikast. Selline olukord võib tekkida kasutajate tööviljakuse või käitumise

---

[43] Artikli 29 alusel asutatud andmekaitse töörühma arvamus 10/2004 teabesätete suurema ühtlustatuse kohta (juuli 2004), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_et.pdf.

[44] Näiteks iPhone'ides kasutatav hoiatusikoon geograafilise asukoha andmete töötlemise kohta.

[45] Föderaalse kaubanduskomisjoni aruanne, viide 6 eespool, lk 16.

hindamisel näiteks finants- või terviseandmete või muude profiiliandmete alusel. Kasutaja taotlusel peab rakenduse andmete töötleja võimaldama isikuandmeid parandada, kustutada või sulgeda, kui need on ebatäielikud või ebaõiged või neid töödeldakse ebaseaduslikult.

Et kasutajad saaksid oma isikuandmete töötlemist jälgida, tuleb rakendustes kasutajaid nende tutvumis- ja parandusmehhanismide olemasolust selgesti ja nähtavalt teavitada. Artikli 29 alusel asutatud andmekaitse töörühm soovitab kavandada ja rakendada lihtsaid, kuid turvalisi veebipõhised juurdepääsuvahendeid. Juurdepääsuvahendid peaksid olema eelistatavalt kättesaadavad iga rakenduse sees või lingina veebifunktsiooni juurde, kus kasutajad saavad kohe tutvuda kõikide neid puudutavate töödeldavate andmetega ja nende vajalike selgitustega. Sarnaseid algatusi on kasutanud internetiteenuste pakkujad, näiteks mitmesugused andmete ülevaadet pakkuvad keskkonnad ja muud juurdepääsumehhanismid.

Lihtne veebipõhine juurdepääs on eriti oluline rakenduste puhul, mis töötlevad mahukaid kasutajaprofiile, nagu võrgundus-, sotsiaal- ja sõnumirakendused või rakendused, mis töötlevad tundlikke või finantsandmeid. Vältimaks andmete lekkimist kolmandatele isikutele, tuleks juurdepääs anda loomulikult alles pärast andmesubjekti isiku tuvastamist. Kuid isiku tuvastamise kohustus ei tohiks kaasa tuua täiendavat, otstarbe piire ületavat isikuandmete kogumist andmesubjekti kohta. Paljudel juhtudel piisaks isiku (täieliku) tuvastamise asemel autentimisest.

Lisaks tuleks kasutajatel alati võimaldada oma nõusolek lihtsal ja mittekoormaval viisil tagasi võtta. Andmesubjekt võib andmetöötluseks antud nõusoleku tagasi võtta mitmel eri viisil ja mitmel eri põhjusel. Nõusoleku peaks eelistatavalt saama tagasi võtta eespool nimetatud kergesti kättesaadavate mehhanismide abil. Kasutajatel peab olema võimalus rakendused eemaldada ja sellega koos kõrvaldada kõik isikuandmed ka vastutava(te) andmetöötleja(te) serveritest. Et kasutajatel oleks võimalik lasta rakenduste arendajal oma andmed kustutada, on operatsioonisüsteemi tootjal oluline roll anda rakenduste arendajale märku, kui kasutaja rakenduse eemaldab. Sellise märguande võib edastada rakenduse programmeerimise liidese kaudu. Põhimõtteliselt ei ole rakenduste arendajal pärast seda, kui kasutaja on rakenduse eemaldanud, õiguslikku alust selle kasutajaga seotud isikuandmete töötlemist jätkata ning seepärast peab ta kõik andmed kustutama. Rakenduste arendaja, kes soovib teatud andmed alles hoida – näiteks rakenduse ennistamise hõlbustamiseks – peab eemaldamise käigus küsima kasutajalt määratletud säilitamise lisaperioodiks eraldi nõusolekut. Ainsaks erandiks sellest reeglist võivad olla seadusjärgsed kohustused säilitada konkreetsetel eesmärkidel osa andmeid, näiteks finantstehingutega seotud finantskohustuste andmed[46].

[46] Töörühm tuletab kõikidele infoühiskonna teenuste pakkujatele, näiteks rakenduste pakkujatele, meelde, et Euroopa andmete säilitamise kohustust (direktiiv 2006/24/EÜ) ei kohaldata nende suhtes ja seepärast ei saa seda kasutada õigusliku alusena rakenduse kasutajaid käsitlevate andmete töötlemise jätkamiseks pärast rakenduse kustutamist. Töörühm kasutab siinkohal võimalust rõhutada andmete edastamise riskantsust, mis nõuab erilisi ettevaatlusabinõusid ja tagatisi – nagu on näidatud artikli 29 alusel asutatud töörühma aruandes andmete säilitamist käsitleva direktiivi jõustamise kohta (WP172), kus kõiki asjaomaseid sidusrühmi kutsuti üles võtma asjakohaseid turvameetmeid.

3.9 Säilitamise periood

Rakenduste arendajad peavad arutama rakenduse abil kogutud andmete säilitamist ja sellega kaasnevaid andmekaitseriske. Konkreetne periood oleneb rakenduse eesmärgist ja andmete asjakohasusest lõppkasutaja jaoks. Näiteks kalendri, päeviku või fotojagamisrakenduse puhul otsustab säilitamise aja üle lõppkasutaja, samal ajal kui navigeerimisrakenduse puhul võib piisata vaid kümne viimati külastatud asukoha säilitamisest. Samuti peaksid rakenduste arendajad pöörama tähelepanu nende kasutajate andmetele, kes ei ole rakendust pikemat aega kasutanud. Need kasutajad on oma mobiilseadme kaotanud või selle välja vahetanud, ilma et oleksid algsest seadmest kõiki rakendusi eemaldanud. Rakenduste arendajad peaksid seepärast eelnevalt määratlema, kui pikalt peab rakendus seisma kasutamata, et konto loetaks aegunuks, ja tagama kasutaja teavitamise sellisest ajakavast. Sellise perioodi lõppemisel peaks vastutav töötleja kasutajat teavitama ja andma talle võimaluse isikuandmed kustutada. Kui kasutaja teatele ei vasta, tuleks kasutaja isikuandmed ja rakenduse kasutus muuta pöördumatult anonüümseks või kustutada. Meeldetuletusperiood oleneb rakenduse eesmärgist ja andmete säilitamise kohast. Kui tegemist on seadmes endas säilitatavate andmetega, näiteks mängus saadud suure punktisummaga, võib andmeid alles hoida senikaua, kui rakendus on seadmesse paigaldatud. Kui tegemist on andmetega, mida kasutatakse vaid kord aastas, näiteks teave suusakuurordi kohta, võiks meeldetuletamise periood olla 15 kuud.

3.10 Lapsed

Lapsed kasutavad rakendusi kas isiklikes või jagatud seadmetes (nt vanematele või õdedele-vendadele kuuluvates seadmetes või haridusasutustes) aktiivselt ning lastele mõeldud rakenduste turg on ilmselgelt suur ja mitmepalgeline. Kuid samal ajal on lastel keeruline või võimatu mõista nende andmete mahtu ja tundlikkust, millega rakendused võivad tutvuda, või andmete kolmandate isikutega jagamise ulatust reklaamide edastamiseks ning neil on selle kohta vähe teadmisi.

Töörühm on käsitlenud laste andmete töötlemist põhjalikult arvamuses 2/2009 laste isikuandmete kaitse kohta ning käsitleb selles osas ainult mitmeid rakendustega seotud riske ja soovitusi[47].

Rakenduste arendajad ja teised vastutavad töötlejad peaksid pöörama tähelepanu siseriiklikes õigusaktides laste või alaealiste määratlemise vanusepiirile, kui rakenduse puhul on andmete seadusliku töötlemise eeltingimuseks lapsevanema nõusolek andmete töötlemiseks[48].

Kui alaealiselt saab seaduslikult nõusolekut küsida ja rakendus on mõeldud lastele või alaealistele, peaks vastutav töötleja pöörama tähelepanu sellele, et alaealisel võib olla andmete töötlemist käsitlevast teabest raske aru saada ja puudu võib jääda tähelepanelikkusest. Pidades silmas, et lapsed ja alaealised on üldiselt haavatavad, ning lähtudes isikuandmete õiglase ja seadusliku töötlemise nõudest, peaksid lastega tegelevad vastutavad töötlejad järgima

---

[47] WP 160, arvamus 2/2009 laste isikuandmete kaitse kohta (Üldised suunised ja erijuhtum koolide puhul) (11. veebruar 2009), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_et.pdf.

[48] ELi liikmesriikides ulatub vanusepiir 12–18 eluaastani.

minimaalsete andmete kogumise ja eesmärgi piiramise põhimõtet veelgi rangemalt. Täpsemalt ei tohiks vastutavad töötlejad laste andmeid töödelda ei otse ega kaudselt käitumispõhise reklaami tarbeks, sest see on väljaspool lapse arusaamist ja seetõttu ületab seadusliku töötlemise piire.

Töörühm jagab muret, mida föderaalne kaubanduskomisjon väljendas oma aruandes lastele mõeldud mobiilirakenduste kohta[49].

Rakenduste arendajad peaksid esitama asjaomase teabe koostöös rakenduste poodide ning operatsioonisüsteemi ja seadmete tootjatega lihtsal viisil ja eakohases sõnastuses. Samuti peaksid vastutavad töötlejad konkreetselt hoiduma lapseealise kasutaja vanemate või perekonnaliikmetega seotud andmete kogumisest (näiteks finantsteave või info teabe eriliikide kohta, nagu terviseteave).

4 Järeldused ja soovitused

Suur osa nutitelefonides kättesaadavatest andmeliikidest on isikuandmed. Neid käsitletakse andmekaitsedirektiivis ning eraelu puutumatust ja elektroonilist sidet käsitleva direktiivi artikli 5 lõikes 3 sätestatud nõusoleku küsimise erinõudes. Kõnealuseid eeskirju kohaldatakse kõikidele ELi kasutajatele mõeldud rakenduste suhtes, olenemata rakenduste arendaja või rakenduste poe asukohast.

Rakenduste valdkonna killustatus, arvukad tehnilised võimalused mobiilseadmetes salvestatud või genereeritud andmetega tutvumiseks ning arendajate vähene õigusalane teadlikkus toovad rakenduste kasutajatele kaasa hulga tõsiseid andmekaitseriske. Riskid ulatuvad läbipaistvuse ja teadlikkuse puudumisest rakenduste kasutajate seas puudulike turvameetmete, nõusoleku küsimise kehtetute mehhanismide, maksimaalsete andmete kogumise ja andmete töötlemise eesmärkide hägususeni.

Rakenduste arenduse, levitamise ja tehniliste võimalustega tegelevate eri isikute andmekaitsekohustused kattuvad. Enamik järeldusi ja soovitusi on mõeldud rakenduste arendajatele (sest nemad saavad töötlemise täpset viisi või teabe rakenduses esitamist kõige enam mõjutada), kuid sageli peavad nad eraelu puutumatuse ja andmekaitse kõrgeimate standardite saavutamiseks tegema rakenduste valdkonnas koostööd teiste isikutega, nagu operatsioonisüsteemi ja seadmete tootjad, rakenduste poed ja kolmandad isikud, näiteks analüüsiteenuste pakkujad ja reklaamiandjate võrgustikud.

Rakenduste arendajad peavad

- tundma kasutajatelt pärit ja kasutajaid käsitlevate andmete töötlemisel oma vastutava töötleja kohustusi ja neid täitma;

---

[49] Föderaalse kaubanduskomisjoni aruanne lastele mõeldud mobiilirakenduste kohta: praegused avaldused eraeluliste andmete kogumise kohta on ebarahuldavad (veebruar 2012), http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf. „Samal ajal kui töötajad leidsid sadade eri arendajate loodud väga erinevaid lastele mõeldud rakendusi, avastasid töötajad rakenduste müügikohtades väga vähe (kui üldse) teavet andmete kogumise ja jagamise põhimõtete kohta nendes rakendustes.”

- lepingulistes suhetes volitatud töötlejatega (sh isikuandmete kogumise ja töötlemise tellimisel arendajatelt, programmeerijatelt ja näiteks pilveteenuste pakkujatelt) teadma ja täitma oma vastutava töötleja kohustusi;
- küsima nõusolekut enne, kui rakendus hakkab andmetest väljavõtteid tegema või neid seadmesse salvestama, st enne rakenduse paigaldamist. Selline nõusolek peab olema vabatahtlik, konkreetne ja teadlik;
- küsima üksikasjalikku nõusolekut iga andmeliigi kohta, millega rakendus tutvub: vähemalt asukoha, kontaktandmete, seadme kordumatu tunnuse, andmesubjekti nime, telefoni andmete, krediitkaardi- ja makseandmete, telefoni ja SMSide, külastatud veebilehtede loetelu, e-posti aadressi, sotsiaalvõrgustike mandaatide ja biomeetria kategooria kohta;
- mõistma, et nõusolek ei seadusta otstarbe piire ületavat ega ebaproportsionaalset andmetöötlust;
- esitama enne rakenduse paigaldamist andmetöötluse hoolikalt määratletud ja põhjalikud eesmärgid ning mitte muutma eesmärke ilma nõusolekut uuendamata; esitama põhjaliku teabe, kui andmeid kasutatakse kolmandate isikute eesmärkide jaoks, nagu reklaam või analüüsiteenuste pakkumine;
- võimaldama kasutajatel oma nõusolek tagasi võtta ja rakendus eemaldada ning asjakohastel puhkudel andmed kustutada;
- järgima minimaalsete andmete kogumise põhimõtet ja koguma ainult neid andmeid, mis on soovitud funktsioonide pakkumiseks hädavajalikud;
- võtma vajalikke korralduslikke ja tehnilisi meetmeid töödeldavate isikuandmete kaitse tagamiseks rakenduse kavandamise ja rakendamise kõikides etappides (lõimitud eraelukaitse), nagu on määratletud käesoleva arvamuse punktis 3.6;
- looma rakenduse kasutajatele ühtse kontaktpunkti;
- esitama kergesti loetava, arusaadava ja hõlpsasti kättesaadava eraelu puutumatuse poliitika, milles teavitatakse kasutajaid vähemalt järgmisest:
  - kes nad on (nimi ja kontaktandmed);
  - isikuandmete täpsed kategooriad, mida rakendus tahab koguda ja töödelda;
  - miks (millistel konkreetsetel eesmärkidel) on andmete töötlemine vajalik;
  - kas andmeid avaldatakse kolmandatele isikutele (mitte ainult üldkirjeldus, vaid nende isikute konkreetne kirjeldus, kellele andmeid avalikustatakse);
  - millised õigused on kasutajatel nõusoleku tagasivõtmiseks ja andmete kustutamiseks;
- võimaldama rakenduse kasutajatel teostada oma õigust andmetega tutvuda, neid parandada ja kustutada ning esitada andmetöötlusele vastuväiteid ja teavitada kasutajaid nende mehhanismide olemasolust;
- määratlema rakendusega kogutud andmete mõistliku säilitamisperioodi ja eelnevalt määratlema, kui pikalt peab rakendus seisma kasutamata, et konto loetaks aegunuks;
- lastele mõeldud rakenduste puhul: pöörama tähelepanu siseriiklikes õigusaktides laste või alaealiste määratlemise vanusepiirile, valima kõige piiravama andmetöötlusmeetodi, järgides täielikult minimaalsete andmete kogumise ja eesmärgi piiramise põhimõtet, hoiduma laste andmete töötlemisest käitumispõhise reklaami otseseks või kaudseks edastamiseks ning hoiduma laste kaudu andmete kogumisest nende sugulaste ja/või sõprade kohta.

Töörühm soovitab rakenduste arendajatel

- uurida asjaomaseid suunised, pöörates tähelepanu konkreetsetele turvariskidele ja -meetmetele;
- ennetavalt teavitada kasutajaid isikuandmetega seotud nõuete rikkumisest eraelu puutumatust ja elektroonilist sidet käsitleva direktiivi tähenduses;
- teavitada kasutajaid proportsionaalsusega seotud kaalutlustest seoses andmeliikidega, mida rakenduste arendaja seadmest kogub või millega tutvub, andmete säilitamise tähtajast ja kohaldatavatest turvameetmetest;
- arendada välja vahendeid, mis võimaldavad kasutajatel ettemääratud säilitamise perioodi asemel valida oma isikuandmete säilitamiseks sobiva pikkusega periood vastavalt oma konkreetsetele eelistustele ja taustale;
- lisada oma eraelu puutumatuse poliitikasse Euroopa kasutajatele mõeldud teavet;
- arendada ja rakendada kasutajate jaoks lihtsaid, kuid turvalisi veebipõhise juurdepääsu vahendeid, kogumata täiendavalt isikuandmeid, mis ületavad selle otstarbe piire;
- kasutada koos operatsioonisüsteemi ja seadmete tootjate ning rakenduste poodidega oma loovust innovatiivsete lahenduste väljatöötamiseks, et anda mobiilseadmete kasutajatele piisavalt teavet, näiteks mitmekihiliste teadete süsteemi kaudu, kus kasutatakse sisu kirjeldavaid ikoone.

Rakenduste poed peavad

- tundma kasutajatelt pärit ja kasutajaid käsitlevate andmete töötlemisel oma vastutava töötleja kohustusi ja neid täitma;
- jõustama rakenduste arendaja kohustuse anda teavet, sealhulgas andmeliikide kohta, millega rakendus saab tutvuda, ja teavet eesmärkide kohta, samuti selle kohta, kas andmeid jagatakse kolmandate isikutega;
- pöörama erilist tähelepanu lastele mõeldud rakendustele, et pakkuda kaitset nende andmete ebaseadusliku töötlemise eest, ning eelkõige täitma kohustust esitada asjaomane teave lihtsal viisil ja eakohases sõnastuses;
- esitama üksikasjalikku teavet rakenduste tegeliku kontrollimise kohta nende levitamise eesmärgil esitamisel, sealhulgas eraelu ja andmekaitseküsimuste hindamise kontroll.

Töörühm soovitab rakenduste poodidel

- töötada koostöös operatsioonisüsteemi tootjaga välja kasutajatele mõeldud kontrollivahendid, nagu seadmes asuvad ja seal genereeritud andmetega tutvumist kujutavad sümbolid;
- lasta üldsusel kõiki rakendusi hinnata;
- rakendada eraelu kaitset toetav rakenduste distantsilt eemaldamise mehhanism;
- anda kasutajate käsutusse tagasisidekanalid, mille kaudu saab teatada eraelu puutumatuse ja/või turvaprobleemidest;
- teha rakenduste arendajatega koostööd, et teavitada kasutajaid varakult isikuandmete nõuete rikkumisest;
- hoiatada rakenduste arendajaid enne rakenduse Euroopasse levitamist Euroopa õiguse iseärasustest, näiteks nõusoleku küsimise nõudest ja nõuetest isikuandmete edastamisel kolmandatesse riikidesse.

Operatsioonisüsteemi ja seadmete tootjad peavad

- ajakohastama oma rakenduste programmeerimise ja kasutajaliidesed, et võimaldada kasutajatele piisavat kontrolli kehtiva nõusoleku andmiseks rakendustes töödeldavate andmete kohta;
- rakendama oma operatsioonisüsteemis nõusoleku kogumise mehhanisme rakenduse esmakäivitamisel või siis, kui rakendus püüab esimest korda tutvuda andmeliikidega, mis avaldavad eraelule märkimisväärset mõju;
- rakendama kasutaja salajase jälgimise vältimiseks lõimitud eraelukaitse põhimõtet;
- tagama töötlemise turvalisuse;
- tagama eelpaigaldatud rakenduste (vaikeseadistuste) vastavuse Euroopa andmekaitseõigusele;
- andma andmete, andurite ja teenuste kohta üksikasjalikku teavet tagamaks, et rakenduste arendaja saab tutvuda ainult oma rakenduse jaoks vajalike andmetega;
- tagama kasutajasõbralikud ja tõhusad vahendid vältimaks jälgimist reklaamiandjate ja mis tahes kolmandate isikute poolt. Vaikeseadistused peavad jälgimise välistama;
- tagama asjakohaste mehhanismide kättesaadavuse lõppkasutaja teavitamiseks ja harimiseks selles valdkonnas, mida rakendused suudavad teha ja milliste andmetega tutvuda;
- tagama, et iga andmeliigiga tutvumine kajastub kasutajale mõeldud teabes enne rakenduse paigaldamist: esitatud liigid peavad olema selged ja arusaadavad;
- looma turvalisust soodustava keskkonna, mis sisaldab vahendeid pahavaraliste rakenduste leviku tõkestamiseks ja võimaldab iga rakendust kergesti paigaldada/eemaldada.

Töörühm soovitab operatsioonisüsteemi ja seadmete tootjatel

- võimaldada kasutajatel rakendusi eemaldada ja anda rakenduste arendajale (näiteks rakenduse programmeerimise liidese kaudu) märku asjaomaste kasutajaandmete kustutamiseks;
- pakkuda pidevalt turvauuendusi ja soodustada nende regulaarset ajakohastamist;
- tagada, et isikuandmetega tutvumist võimaldavate meetodite ja funktsioonide hulka kuuluvad üksikasjaliku nõusoleku küsimise juurutamisele suunatud funktsioonid;
- aidata aktiivselt töötada välja ja soodustada ikoonide kasutamist, mis hoiatavad kasutajaid andmete eri kasutusviiside eest rakendustes;
- töötada seadmete jaoks välja selged kontrolljäljed, et lõppkasutajad saaksid selgesti näha, millised rakendused on nende seadmetes olevate isikuandmetega tutvunud, samuti väljuva liikluse mahtu rakenduse kohta võrdluses kasutajate algatatud liiklusega.

Kolmandad isikud peavad

- tundma kasutajaid käsitlevate andmete töötlemisel oma vastutava töötleja kohustusi ja neid täitma;
- täitma mobiilseadmetest andmete lugemisel ja andmete sinna kirjutamisel eraelu puutumatust ja elektroonilist sidet käsitleva direktiivi artikli 5 lõikes 3 määratud nõusoleku küsimise kohustust koostöös rakenduste arendajate ja/või rakenduste poodidega, kes teavitavad kasutajat andmete töötlemise eesmärkidest;
- mitte hiilima mööda ühestki jälgimise vältimiseks kavandatud mehhanismist, nagu praegu sageli juhtub veebilehitsejates kasutatavate jälgimisvastaste mehhanismide puhul;

- sideteenuste osutajad peavad individualiseeritud seadmete turustamisel tagama kasutajate kehtiva nõusoleku kogumise eelpaigaldatud rakenduste kohta ning täitma asjaomaseid kohustusi seadme ja operatsioonisüsteemi teatavate funktsioonide määratlemisele kaasaaitamisel, nt kasutaja juurdepääsu piiramisel seadmete ja operatsioonisüsteemi tootja teatavatele konfigureerimisparameetritele või (turva- ja funktsionaalsete) veaparanduste filtreerimisel;
- reklaamiandjad peavad konkreetselt vältima reklaamide edastamist väljaspool rakendust. Näiteks reklaamide edastamine veebilehitseja seadistuste muutmise või ikoonide mobiilsele töölauale suunamise teel; hoiduma seadme või abonendi kordumatute tunnuste kasutamisest jälgimise otstarbel;
- hoiduma laste andmete töötlemisest otseselt või kaudselt käitumispõhise reklaami edastamiseks, kohaldama asjakohaseid turvameetmeid. See hõlmab seadme ja rakenduse kasutaja kordumatu tunnuse ja muude isikuandmete turvalist edastamist ja krüpteeritud salvestamist.

Töörühm soovitab kolmandatel isikutel

- arendada ja rakendada kasutajate jaoks lihtsaid, kuid turvalisi veebipõhise juurdepääsu vahendeid, kogumata täiendavalt isikuandmeid, mis ületavad selle otstarbe piire;
- koguda ja töödelda vaid andmeid, mis haakuvad kasutaja andmete esitamise kontekstiga.