Uvodno pojasnilo

Delovna skupina za varstvo podatkov iz člena 29 (Article 29 Working Party; WP29) je 5. in 6. aprila 2017 v Bruslju organizirala posvetovanje z zainteresiranimi deležniki (t.i. Fablab) na temo Splošne uredbe o varstvu osebnih podatkov (angl. GDPR). Namen posvetovanje je bil udeležencem omogočiti diskusijo s predstavniki evropske industrije, civilne družbe, akademiki in relevantnimi združenji glede določenih operativnih in praktičnih vprašanj v zvezi z implementacijo GDPR. ***Predsedstvo WP29 je pripravilo povzetke razprave[1],*** *pri Informacijskem pooblaščencu pa smo pripravili* ***neuradni prevod povzetkov*** *delavnice, kot sledi v nadaljevanju. Opozarjamo, da* ***povzetki razprave ne predstavljajo zavezujočih stališč Informacijskega pooblaščenca kakor tudi ne drugih nadzornih organov, temveč služijo zgolj kot opomnik oz. predstavitev odprtih vprašanj in razprave na posvetovanju.***

***

2017 GDPR Fablab delavnica - rezultati razprave

Splošna uredba o varstvu osebnih podatkov (angl. GDPR), objavljena maja 2016, se v državah članicah EU prične uporabljati maja 2018. Dosežen je **veliki mejnik**, za zaključek priprav na njeno uporabo pa je na voljo le **še približno eno leto**.

Zahvaljujoč podpori in sodelovanju zainteresiranih deležnikov je lahko Delovna skupina iz člena 29 (angl. WP29) **izdala številne smernice** (glede oseb pristojnih za varstvo osebnih podatkov – DPO, vodilnega organa in prenosljivosti podatkov), objavila pa je tudi smernice o oceni učinkov na varstvo osebnih podatkov (DPIA), ki so bile **v postopku javne razprave do 23. maja 2017**.

WP29 priznava pomen in vrednost odziva **različnih deležnikov na implementacijo GDPR** in je hvaležna za to plodno sodelovanje.

3. januarja 2017 je WP29 kot del svoje strategije za implementacijo GDPR do leta 2018 sprejela svoj **akcijski načrt za leto 2017**.

Akcijski načrt dopolnjuje prioritete iz leta 2016 (certificiranje, DPIA, administrativne globe, vzpostavitev Evropskega odbora za varstvo osebnih podatkov, itd.) in **zastavlja nove cilje in dokumente, ki bodo izdani v prihajajočem letu**.

Da bi se lahko **pripravili na pravočasno in ustrezno implementacijo GDPR**, je WP29 5. aprila 2017 v Bruslju organizirala drugo **Fablab delavnico** in tako omogočila udeležencem diskusijo s predstavniki evropske industrije, civilne družbe, akademiki in relevantnimi združenji glede določenih **operativnih in praktičnih vprašanj.**

[1] http://ec.europa.eu/newsroom/document.cfm?doc_id=44645

Fablab delavnice se je udeležilo več kot **90 predstavnikov**, vključno s **predstavniki nacionalnih organov za varstvo osebnih podatkov**: udeleženci so se osredotočili na **nekaj tematik, ki so bile kot prioriteta določene v akcijskem načrtu WP29.**

Cilj Fablab delavnice je bil prispevek k delu WP29 pri razvoju smernic glede:

A. kriterijev (tudi praktičnih) za **veljavno privolitev**,
B. **poročanja o kršitvah varstva osebnih podatkov** nadzornim organom in posameznikom,
C. kriterijev in pogojev za odločitve, ki temeljijo na **profiliranju.**

Delavnica o privolitvi

Moderatorji: Giovanni Buttarelli – Evropski nadzornik za varstvo osebnih podatkov (EDPS) in David Martin – višji pravni strokovnjak (BEUC)

I. Uvod

Udeleženci delavnice so razpravljali o konceptu privolitve, predvsem po 4. in 7. členu GDPR.

Razprava se je začela s pregledom sprememb, ki jih glede privolitve prinaša GDPR. **Splošen zaključek je bil, da ni toliko novosti kot je sledenja istim standardom**, da pa GDPR prinaša pomembne nove elemente.

Uporaba **privolitve kot pravne podlage bo pod podrobnejšim pregledom, še posebej pogoji za veljavno privolitev** v skladu z načelom odgovornosti (angl. accountability).

Trenutno je **privolitev ena od mogočih pravnih podlag** za varstvo osebnih podatkov.

V nekaterih primerih morda ni najprimernejša pravna podlaga za obdelavo osebnih podatkov. V odziv na to nekateri sektorji menijo, da jih uredba želi odvrniti od uporabe privolitve kot pravne podlage, drugi pa menijo, da je preveč poudarka na privolitvi, kar omejuje njihovo izbiro glede pravne podlage.

II. Poziv za nadzorne organe

- Pojasniti koncept **»informirane« privolitve** in kaj pomeni **»jasno pritrdilno dejanje«.**
- Obstaja splošna negotovost glede **obstoječih privolitev oziroma izjav glede privolitve.**
- Zahteva po jasnosti glede **načinov, kako upravljati s privolitvami za več kot en namen** (recital 32).
- Zahteva po pojasnilu, do katere mere bi morala biti privolitev podana za vsako posamezno dejanje obdelave ali za posamezen namen.
- **Otroci in obdelava za znanstvene namene** so bili izpostavljeni kot tematika, kjer so potrebne posebne smernice glede »posebnosti« privolitve.

- Smernice bi morale pojasniti situacije, ki vključujejo **skupne upravljavce** ali primere, kjer ena stranka zbira privolitve za račun druge. Kako upravljati s privolitvami (podajanje in umikanje privolitve) v takih primerih?
- Smernice so potrebne v zvezi s pomenom besedne zveze **»ki se jasno razlikuje«** v členu 7.2. Ali to pomeni, da je privolitev lahko pridobljena v okviru splošnih pogojev ali ne?
- Smernice so potrebne glede praktičnih načinov implementacije člena 7.4 – kako oceniti pogojenost in njen vpliv na veljavnost privolitve.
- **Kakšni so kriteriji prostovoljne, izrecne, informirane in nedvoumne privolitve? Kaj so novosti glede na dikcijo Direktive o varstvu osebnih podatkov?** Omenjeno je bilo, kako pomembno je imeti enotno razumevanje terminologije. Glavne novosti, »vidik jasnega razlikovanja« in koncept »neenake moči«. Potreba po razvezavi privolitve od splošnih pogojev. Poziv za jasno enako razumevanje vseh teh elementov.
- Potreba po granularnosti v smislu namenov in strank, ki jih zahteva po privolitvi zadeva.

III. Izpostavljeni pomisleki

Glede **čezmejnega toka podatkov** je bil izpostavljen pomislek o deljenju občutljivih osebnih podatkov, kadar **ni enakovrednega varovanja** osebnih podatkov.

Mladoletniki so prioriteta, vendar je moč odločanja na ravni držav članic EU in **preverjanje starosti mladoletnikov** problematično, enako tudi preverjanje privolitve starša ali skrbnika.

Glede **raziskav** so bila izpostavljena vprašanja o privolitvi v **sekundarno rabo podatkov za raziskovalne namene** in glede definicije informacijskih storitev, ki so običajno ponujene za plačilo in kako v ta okvir sodijo spletne storitve za paciente.

Udeleženci so izrazili pomisleke glede **umaknjene privolitve in posledic, če uporabnik noče podati privolitve**. Ali so »vzemi in pusti« situacije še vedno dovoljene in če so, pod kakšnimi pogoji? Kaj pomeni »brez škode« v praksi, ko je privolitev umaknjena?

Izpostavljena je bila potreba po **fleksibilnosti,** tudi glede tega, kako se bo tehnologija razvijala v prihodnosti. **Kreativnost in tehnološki napredek** morata biti v vidu med ustvarjanjem smernic. Privolitev ne bi smela voditi k »utrujenosti« uporabnikov.

Privolitev je od vseh pravnih podlag najtežje dokazovati.

IV. Druga posebna vprašanja

- Ali lahko posamezniki privolijo v nekatere uporabnike osebnih podatkov in ne v druge?
- Kako pridobiti in dokazati **ustno privolitev?**
- Kaj v primeru **pogojne privolitve** (pojasnila so potrebna pri členu 7.4)?
- Ali je lahko pogojna privolitev veljavna pri obdelavi občutljivih osebnih podatkov v kontekstu izvajanja storitve kot je zavarovanje?

- Kaj če obdelava temelji na privolitvi in je posameznik **privolitev umaknil,** pa obstaja **druga pravna podlaga za obdelavo osebnih podatkov** (to je bilo izpostavljeno kot nepoštena praksa)?
- Kaj pa glede učinkov umika privolitve in zagotovil, da bodo podatki izbrisani?
- Ali je lahko privolitev dana za **nedoločen čas** ali je treba privolitev vedno **obnavljati?**
- Ali bi morala biti izvedena **analiza posameznih primerov?**
- **Kakšne informacije** morajo biti dane posamezniku? Kako dobro morajo biti obveščeni prejemniki (povezava s členom 13)?
- Kaj pa privolitev za dejanja obdelave in ko je ta ponovno uporabljena za druga dejanja?
- Kaj je jasna **»izjava«**, jasno pritrdilno dejanje, je klik na določen link ali nadaljevanje uporabe storitve dovolj?
- **Povezava člena 35 o oceni učinka na zasebnost (DPIA) in določb o privolitvi.** Ali je potrebno, v primeru DPIA zaznanega posebnega tveganja (npr. da bodo storitev uporabljali mladoletniki), posebno skrb posvetiti zahtevam za privolitev in upravljanju s privolitvami?
- Ali so ustrezne **»priporočene nastavitve«**, ki še vedno zahtevajo pritrdilno dejanje uporabnika, da potrdi izbiro?
- Kakšen je pomen **»jasnega razlikovanja«** od drugih zadev? Ali se nanaša samo na »izbiro« ali na »obvestilo in izbiro«?

Delavnica o poročanju kršitev varstva osebnih podatkov

Moderatorji: Wilbert Tomesen – podpredsednik in član nizozemskega organa za varstvo osebnih podatkov in Gwendal Le Grand – vodja za tehnologijo in inovacije – francoski organ za varstvo osebnih podatkov – CNIL

I. Uvod

Udeleženci delavnice so razpravljali o vprašanjih poročanja o kršitvah varstva osebnih podatkov po členih 33 in 34 GDPR.

Na poročanje o kršitvah bi morali gledati kot na orodje za **večanje odgovornosti** (angl. accountability).

Udeleženci so izrazili željo, da bi dobili neko vrsto **poročila** o vseh poročanjih kršitev (anonimiziranih), da bi dobili pregled nad **dogajanjem po sektorjih (in sprejetih ukrepih)** in se lahko učili iz izkušenj drugih.

Udeleženci so prav tako zahtevali konzultacijo s strokovnjaki s področja IT pri oblikovanju smernic.

V zaključku so udeleženci menili, da bi bilo koristno imeti smernice glede uskladitve zahtev GDPR z zahtevami drugih instrumentov, kot je NIS direktiva (Direktiva o varnosti omrežij in informacijskih sistemov).

Udeleženci pričakujejo **več fleksibilnosti pri vsebini poročanja o kršitvah.**

II. Poziv/pričakovanja za nadzorne organe

- Obstaja dilema, kako izpolniti zahteve po poročanju in se izogniti slabemu vplivu na ugled.
- Postopek za vodilni organ (ki mora biti obveščen).
- Pojasnilo glede poročanja o kršitvah varovanja podatkov.
- Ne izbris določenih elementov ampak **dodatek: glede informacij o možnosti, da bi izpostavili pogodbenega obdelovalca, ki je odgovoren za kršitev.**
- Zahtevali so tudi možnost, da opravijo **nepopolno poročanje.**
- Povezano tveganje.
- Nujno je definirati kršitev varstva osebnih podatkov.
- <u>O čem poročati?</u>
- Vsebina/izpostavljanje obdelave, ki je odgovorna za kršitev varstva osebnih podatkov, neposredno posameznikom. Težavnost pri povezovanju dogodkov (dodati informacije poročilu nadzornemu organu).
- Enoten obrazec za poročanje, preveden v različne jezike.
- Vsebina: ne vseh tehničnih podrobnosti kršitve/nekatere informacije niso uporabne.
- Kdo mora biti obveščen?
- <u>Kdaj?</u>
- Kdaj se zaveš kršitve varstva osebnih podatkov? Eskaliranje postopka včasih ne obstaja. Pomembno je vedeti, **kdaj začne 72 urni rok teči**. Povezava med poročanjem in določbami glede zavarovanja osebnih podatkov.
- Morda ne moreš poročati o vsem, kar zahteva zakonodaja/morda lahko dodaš več informacij šele kasneje: **kaj pa nepopolna poročanja.**
- Potrdilo nadzornega organa, da je prejel poročilo o kršitvi.
- Poudarjeno je bilo, da je v realnosti potreben čas, da kršitev varstva osebnih podatkov razumeš. Rok 72 ur bi moral začeti teči od takrat, ko razumemo, kakšna je kršitev in ne od takrat, ko se je zavemo.

III. Izpostavljeni pomisleki

Udeleženci so mnenja, da je termin »kršitev varstva osebnih podatkov« pogosto **podcenjen**. To **ne pomeni le kršitve zaupnosti podatkov**. Prosijo za pojasnilo glede tega v smernicah.

Izpostavljeno je bilo vprašanje, **kateri nadzorni organ obvestiti** v primeru različnih posameznikov v različnih državah članicah EU. Kaj če je poročanje o kršitvi prepovedano zaradi teka kazenskega postopka?

Udeleženci so zahtevali smernice glede **72 urnega roka in še posebej o točki, kdaj začne ta rok teči.**

Udeleženci so menili, da bi nadzorni organ moral imeti za namen poročanja vzpostavljen **varen kanal.**

Vpliv na ugled.

Poročanje posameznikom: ne le, da imamo v uvidu število posameznikov, pač pa moramo imeti **smernice glede resnosti kršitve/orodja, ki omogočajo oceno resnosti kršitve.**

Splošne smernice za mala in srednja podjetja: dobre prakse glede poročanja s kontaktnimi točkami znotraj podjetja.

Udeleženci so mnenja, da **ne bi smelo biti več poročil različnim organom.**

IV. Druga posebna vprašanja

- Poročanje posameznikom in zahteva, da se **informacije podajo v jasnem jeziku.**
- Uporaba **obstoječih kanalov**/pošiljanje jasnega in le temu namenjenega poročila o kršitvi.
- **Dobre prakse** v sektorjih.
- Obrazložitev, če **presežeš 72 urni rok.**
- Telekomunikacijski operaterji imajo **drugačne roke za poročanje**.
- Visoka raven zaupnosti.
- Forenziki/pravniki/strokovnjaki za medije se ukvarjajo s tem.
- Več podrobnosti o tem, kako **upravljavec zazna kršitev in kdaj.**
- **Načini poročanja?** E-pošta/telefon, itd. Upravljavci bi morali glede kršitve poslati namensko sporočilo in ne vključiti informacij o kršitvi v druge komunikacije.
- **Nesorazmeren trud za obveščanje posameznikov**. O tem ni zaključka, upravljavec mora imeti evidenco kršitev varstva osebnih podatkov.
- Določbe GDPR in povezave z drugo EU zakonodajo/koristna bi bila pojasnila glede enotne organizacije poročanja.

Delavnica o profiliranju

Moderatorji: Giuseppe Busia – generalni sekretar – italijanski organ za varstvo osebnih podatkov in Carl Wiper- vodja skupine – organ za varstvo osebnih podatkov iz Velike Britanije

I. Uvod

Udeleženci delavnice so razpravljali o vprašanjih glede profiliranja in avtomatiziranega odločanja po določbah 4. in 22. člena GDPR.

Glavne točke razprave so bile osredotočene na:

- Človeški vpliv v procesu odločanja.
- Transparentnost.
- Pošteno obdelavo: etično odločanje/organizacijsko odločanje.

- Logiko sprejemanja odločitev/količina podrobnosti, ki so podane posameznikom.
- Poslovna zaupnost in poslovne skrivnosti: namen profiliranja je pomemben/kakšen je vpliv: razumevanje kriterijev.
- Iskanje ravnovesja in spodbujanje zaupanja.
- Osredotočenost na cilje.

II. Poziv za nadzorne organe

Člen 22 – avtomatizirano odločanje

- Ni jasne razmejitve med avtomatiziranim odločanjem in odločanjem s **človeško intervencijo. Lahko je oboje,** ali gre za popolnoma avtomatizirano odločanje ali odločanje, ki vključuje človeško intervencijo, mora biti odločeno od primera do primera. V smernicah je potrebna jasnost.
- Pri finančnih storitvah obstajajo mednarodne smernice, ki so lahko relevantne, na primer glede predpogodbenih ocen glede preventive pred zlorabami.
- Kako lahko algoritem predstavimo potrošniku, da bo zanj imelo smisel? Upravljavci morajo razumeti katere informacije o algoritmih morajo podati posameznikom, da bo zanje obdelava smiselna.
- Upravljavci potrebujejo pojasnila glede posebnih situacij, ki jih predvideva člen 22(1).
- Termina »pravni učinki« in »nanj znatno vpliva« potrebujeta interpretacijo. Znatno vpliva je v povezavi s tveganji; nanaša se na tveganje in škodo. Ni le vprašanje ali je učinek pozitiven ali negativen. Vprašanje je, ali vpliva na pravice in svoboščine, npr. na pravico do svobode izražanja? Če je temu tako, potem gre za znaten vpliv.
- Posameznik ima po 21. členu pravico do ugovora profiliranju; ali ima posameznik tudi pravico do ugovora po 22(3). členu?
- Obstaja razlika med profiliranjem, kot ga definira 4. člen in avtomatiziranim odločanjem glede na 22. člen. Smernice o tem vprašanju so potrebne.

Ali bi morale obstajati omejitve glede podatkov, ki so lahko uporabljeni?

- Ali bi morali biti določeni tipi podatkov izključeni? Če je posameznik soglašal, potem se občutljivi podatki lahko obdelujejo.
  - **GDPR usklajuje pravila**. Države članice lahko določijo dodatne pogoje za določene podatke, vendar **ne morejo pod nivo GDPR.** GDPR postavlja mejo. Podatki, ki zbujajo etična vprašanja niso nujno izključeni. Vendar pa lahko upravljavci izključijo določene rabe podatkov.
  - Naj to velja za vse sektorje? Profiliranje bi lahko bilo izključeno **za določne namene.**
- Kaj pa posredna diskriminacija za zakonit namen?

Transparentnost informacij in pravice dostopa

- Pojasniti končno rabo profiliranja je lahko težavno. Kako naj upravljavci zagotovijo pravo mero podrobnosti?
- Upravljavci potrebujejo pojasnilo glede termina »smiselne informacije«: ali to pomeni informacije o algoritmu?
- Obstaja meja, kako transparentni so upravljavci lahko:
  - Ali je transparentnost mogoče doseči le preko izjav o zasebnosti in pravnih izjav, ali vključuje tudi izobraževanje posameznikov?
  - Nadzorni organi za varstvo osebnih podatkov bi morali biti realistični in razumeti, da so določbe glede zagotavljanja transparentnosti lahko breme za upravljavce.
  - Kakšen je namen transparentnosti? Ali je to pritisk na podjetja, da bi bila bolj odgovorna (angl. accountable)?
  - Kakšna je vloga pooblaščene osebe za varstvo osebnih podatkov (DPO) glede transparentnosti?
  - Vloga DPO je pomembna: upravljavci morajo biti transparentni tudi do nadzornih organov za varstvo osebnih podatkov, še posebej, ker posamezniki morda niso sposobni razumeti kompleksnosti obdelave.
- Namen transparentnosti je omogočiti ljudem, da izvajajo svoje pravice.
- Transparentnost je prav tako pomembna za zagotavljanje, da podjetja varujejo temeljne pravice – npr. ali uporabljajo nezakonite podatke? Javnost mora vedeti, kadar obstajajo kršitve.
- Upravljavci morajo biti z možni razumeti algoritme, ki jih uporabljajo in biti zmožni podati pojasnila o njih. Vendar pa na točki, ko bi morali podati transparentne informacije, ki jih zahtevata člena 13 in 14, morda še ne vejo, kaj bo rezultat profiliranja.

III. Izpostavljeni pomisleki

Otroci: V zvezi z otroci je bil izpostavljen etični vidik. Kako naj upravljavci vedno, ali je oseba otrok ali ne? To je težavno vprašanje zaradi razlik v nacionalnih praksah starostnih meja. Smernice naj se izognejo posebnim vprašanjem glede preverjanja starosti.

Namen profiliranja: Profiliranje se izvaja z dvema namenoma: sledenje vedenju posameznikov, ali razumevanje problema in iskanje odgovora; npr. razumeti, kateri zaposleni bodo najverjetneje zapustili podjetje ali odkriti vzorce določene bolezni.

Profiliranje je povezano z umetno inteligenco in strojnim učenjem: Včasih naprave sprejemajo boljše odločitve kot ljudje.

Točnost: Potreba po točnosti je različna v različnih sektorjih. Podjetja lahko izvajajo profiliranje zaradi profitabilnosti, vendar profitabilnost ne zahteva vedno točnosti. Profiliranje se ne tiče le profitabilnosti.

Vidik posameznikov: Z njihove perspektive ni pomembno, kako je profiliranje izvedeno. Posamezniki bi morali imeti dostop do sklepanja, ki ga upravljavec opravi na podlagi njihovih podatkov.

Posameznik mora imeti pravico, da izve zaključke, ki so o njem sprejeti in pravico da temu ugovarja, npr. v primeru zavarovalnega tveganja.

Organizacijska odgovornost (angl. accountability in responsibility): Smernice bi morale podjetja spodbuditi k razmisleku, kaj morajo storiti. Ni enotnih rešitev za vse. Profiliranje je v različnih sektorjih industrije različno. Sektorske smernice bi bile koristne.

Profiliranje je oblika obdelave osebnih podatkov, zato veljajo temeljna načela (omejitev nabora osebnih podatkov, itd.). Obstaja veliko oblik profiliranja.

IV. Druga posebna vprašanja

- Ali ocenjevanje (angl. scoring) spada pod profiliranje?
- Kako realno je, da za avtomatizirano odločanje obstaja podlaga v zakonu?
- Ali človeška intervencija pred ali po procesu pomeni, da odločitev ni sprejeta avtomatizirano?
- Kaj če je profiliranje izvedeno s strani druge stranke?
- Sistemi za prepoznavo obraza so primer avtomatiziranega odločanja. Posamezniki lahko ugovarjajo in izvejo, zakaj jim je bil dostop zavrnjen.
- Upravljavci so odgovorni, da pojasnijo kako in zakaj profilirajo. Kako lahko pojasnijo kompleksnost profiliranja?
- Med inovacijo in regulacijo za varovaje interesov posameznikov je ravnovesje, tudi inovacija lahko prinaša prednosti za posameznike.
- Profiliranje se lahko sprevrže v prazni up.
- Ali klasifikacija tudi pomeni profiliranje? Definicija v GDPR je široka. Mišljeno je, da vključuje klasificiranje.