Smernice 02/2021 o virtualnih glasovnih pomočnikih

Različica 2.0

Sprejete 7. julija 2021

Zgodovina različic

Različica 2.0	7. julij 2021	Sprejetje smernic po javnem posvetovanju
Različica 1.0	9. marec 2021	Sprejetje smernic za javno posvetovanje

POVZETEK

Virtualni glasovni pomočnik (VGP) je storitev, ki razume glasovne ukaze in jih po potrebi izvaja ali posreduje z drugimi informacijskimi sistemi. Virtualni glasovni pomočniki so trenutno na voljo na večini pametnih telefonov in tabličnih računalnikov, tradicionalnih računalnikih ter v zadnjem času tudi na samostojnih napravah, kot so pametni zvočniki.

VGP delujejo kot vmesnik med uporabniki in njihovimi računalniškimi napravami ter spletnimi storitvami, kot so iskalniki ali spletne trgovine. Zaradi svoje vloge imajo VGP dostop do ogromne količine osebnih podatkov, vključno z vsemi ukazi (na primer brskanjem po zgodovini iskanja) in odzivi (na primer sestanki na dnevnem redu) uporabnikov.

Veliko večino storitev VGP je zasnovalo le nekaj oblikovalcev VGP. Vendar lahko VGP sodelujejo z aplikacijami, ki so jih oblikovale tretje osebe (razvijalci aplikacij VGP), da zagotovijo bolj izpopolnjene ukaze.

Za pravilno delovanje VGP potrebuje terminalsko napravo z mikrofoni in zvočniki. Naprava shranjuje glasovne in druge podatke, ki jih trenutni VGP prenašajo v oddaljene strežnike VGP.

Upravljavci podatkov, ki zagotavljajo storitve VGP, in obdelovalci podatkov morajo zato upoštevati Splošno uredbo o varstvu podatkov[1] in Direktivo o zasebnosti in elektronskih komunikacijah[2].

Te smernice opredeljujejo nekatere najpomembnejše izzive v zvezi s skladnostjo in vsebujejo priporočila ustreznim deležnikom o tem, kako jih obravnavati.

Upravljavci podatkov, ki zagotavljajo storitve VGP prek terminalskih naprav brez zaslona, morajo uporabnike, ko ti vzpostavijo VGP ali prvič namestijo ali uporabljajo VGP, še vedno obveščati v skladu s Splošno uredbo o varstvu podatkov. Zato ponudnikom oziroma oblikovalcem in razvijalcem VGP priporočamo, da razvijejo glasovne vmesnike za lažje zagotavljanje obveznih informacij.

Trenutno se mora pri vseh VGP vsaj en uporabnik registrirati. V skladu z obveznostjo vgrajenega in privzetega varstva podatkov bi morali ponudniki oziroma oblikovalci in razvijalci VGP razmisliti, ali je nujno, da vsaka funkcija VGP potrebuje registriranega uporabnika.

Uporabniški račun, ki ga uporabljajo številni oblikovalci VGP, povezuje storitev VGP z drugimi storitvami, kot je elektronska pošta ali pretakanje videoposnetkov. Evropski odbor za varstvo podatkov meni, da bi se morali upravljavci podatkov vzdržati takih praks, saj te vključujejo uporabo obsežnih in zapletenih politik varovanja zasebnosti, ki niso skladne z načelom preglednosti po Splošni uredbi o varstvu podatkov.

Smernice obravnavajo štiri najpogostejše namene, za katere VGP obdelujejo osebne podatke, in sicer izvrševanje zahtev, izboljšanje modela strojnega učenja VGP, biometrična identifikacija in profiliranje prilagojenih vsebin ali oglaševanja.

[1] Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (v nadaljevanju: Splošna uredba o varstvu podatkov).

[2] Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah), kot je bila spremenjena z Direktivo 2006/24/ES in Direktivo 2009/136/ES (v nadaljevanju: Direktiva o zasebnosti in elektronskih komunikacijah).

Če se podatki VGP obdelujejo za izpolnitev zahtev uporabnika, tj. če je to nujno potrebno za zagotavljanje storitve, ki jo želi uporabnik, so upravljavci podatkov izvzeti iz zahteve po predhodni privolitvi v skladu s členom 5(3) Direktive o zasebnosti in elektronskih komunikacijah. Nasprotno pa bi bilo tako soglasje, kot se zahteva v členu 5(3) Direktive o zasebnosti in elektronskih komunikacijah, potrebno za shranjevanje ali pridobitev dostopa do informacij za kateri koli namen, ki ni izvršitev zahteve uporabnikov.

Nekatere storitve VGP hranijo osebne podatke, dokler njihovi uporabniki ne zahtevajo izbrisa. To ni v skladu z načelom omejitve shranjevanja. VGP ne bi smeli hraniti podatkov dlje, kot je potrebno za namene, za katere se osebni podatki obdelujejo.

Če upravljavec podatkov ugotovi (na primer med postopki pregleda kakovosti) nenamerno zbiranje osebnih podatkov, bi moral preveriti, ali obstaja veljavna pravna podlaga za posamezne namene obdelave takih podatkov. Sicer bi bilo treba nenamerno zbrane podatke izbrisati.

VGP lahko obdelujejo podatke več posameznikov, na katere se nanašajo osebni podatki. Ponudniki oziroma oblikovalci VGP bi zato morali uvesti mehanizme za nadzor dostopa, da bi zagotovili zaupnost, celovitost in razpoložljivost osebnih podatkov. Vendar nekateri tradicionalni mehanizmi za nadzor dostopa, kot so gesla, ne ustrezajo kontekstu VGP, saj bi jih bilo treba izgovarjati naglas. Smernice vsebujejo nekaj premislekov v zvezi s tem in oddelek, ki se nanaša posebej na obdelavo posebnih vrst podatkov za biometrično identifikacijo.

Ponudniki oziroma oblikovalci VGP bi morali upoštevati, da lahko pri snemanju glasu uporabnika posnetek vsebuje glasove ali podatke drugih posameznikov, kot je šum ozadja, in za storitev niso potrebni. Zato bi morali oblikovalci VGP, kadar je mogoče, premisliti o tehnologijah za filtriranje nepotrebnih podatkov in zagotavljanje, da se posname samo glas uporabnika.

Evropski odbor za varstvo podatkov pri ocenjevanju potrebe po oceni varstva podatkov meni, da je zelo verjetno, da storitve VGP spadajo v tiste kategorije in pogoje, za katere je treba opraviti oceno varstva podatkov.

Upravljavci podatkov, ki zagotavljajo storitve VGP, bi morali uporabnikom zagotoviti, da lahko uveljavljajo svoje pravice posameznikov, na katere se nanašajo osebni podatki, prek razumljivih glasovnih ukazov. Ponudniki oziroma oblikovalci VGP in razvijalci aplikacij bi morali ob koncu postopka uporabnike obvestiti, da so bile njihove pravice ustrezno upoštevane, in sicer glasovno ali s pisnim obvestilom na uporabnikov mobilni telefon ali račun ali na kateri koli drug način, ki ga je izbral uporabnik.

Kazalo

Evropski odbor za varstvo podatkov je –

ob upoštevanju člena 70(1)(j) in (1)(e) Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES,

ob upoštevanju Sporazuma EGP ter zlasti Priloge XI in Protokola 37 k Sporazumu EGP, kakor je bil spremenjen s Sklepom Skupnega odbora EGP št. 154/2018 z dne 6. julija 2018[3],

ob upoštevanju členov 12 in 22 svojega poslovnika –

SPREJEL NASLEDNJE SMERNICE:

1 SPLOŠNO

1. Novejši tehnološki napredek je močno povečal natančnost in priljubljenost virtualnih glasovnih pomočnikov (VGP). VGP so bili vgrajeni v pametne telefone, povezana vozila, pametne zvočnike in pametne televizorje ter druge naprave. S tem se je VGP omogočil dostop do zasebnih informacij, katerih nepravilno upravljanje bi lahko ogrozilo pravice posameznikov do varstva podatkov in zasebnosti. Zato so VGP in naprave, v katere so vgrajeni, pod drobnogledom različnih organov za varstvo podatkov.

2. Uporaba govorne interakcije ima številne prednosti, kot so njena naravnost, ki ne zahteva posebnega znanja uporabnikov, hitrost izvedbe ukaza in razširitev področja delovanja, ki omogoča hitrejši dostop do informacij. Vendar zanašanje na govor povzroča tudi težave pri pravilnem tolmačenju sporočila, ki izhajajo iz spremenljivosti zvočnega signala med različnimi govorci, akustičnega okolja, dvoumnosti jezika itd.

3. V praksi glavna motivacija za nakup opreme z VGP ostajata pretočnost ali poenostavitev nalog. To lahko na primer vključuje klicanje oziroma javljanje na klic, nastavitev merilnika časa itd., zlasti kadar uporabniki ne morejo uporabljati rok. Vodilna uporaba, ki jo promovirajo oblikovalci VGP, je avtomatizacija doma. S predlagano poenostavitvijo izvajanja nalog (prižiganje luči, uravnavanje ogrevanja, spuščanje rolet itd.) in njihovo centralizacijo z enim samim orodjem, ki ga je mogoče zlahka aktivirati na daljavo, govorimo o domačih posrednikih. Poleg osebne ali domače uporabe so lahko glasovni ukazi koristni v profesionalnih delovnih okoljih, v katerih je težko upravljati računalniška orodja in uporabljati pisne ukaze (na primer proizvodna dela).

4. Teoretično bi lahko bili glavni uporabniki glasovnega vmesnika invalidi ali osebe, ki so odvisne od pomoči, ki imajo težave z uporabo tradicionalnih vmesnikov. Virtualni glasovni pomočnik spodbuja vključenost, saj lahko nekaterim kategorijam uporabnikov, ki imajo težave s pisanjem, olajša dostop do informacij in računalniških virov tako, da ti uporabljajo glas.

5. Tudi na področju zdravja je veliko priložnosti za uporabo pogovornih agentov, glasovno ali ne. Med pandemijo covida-19 so se na primer vzpostavili različni boti za klic, ki so uporabnikom

[3] Sklicevanje na „države članice“ v tem dokumentu je treba razumeti kot sklicevanje na „države članice EGP“.

ponudili predhodno diagnozo. Dolgoročno se predvideva, da bi lahko na celoten postopek oskrbe pacientov vplivale interakcije med človekom in robotskim pomočnikom, in sicer ne le za dobro počutje in preventivo, temveč tudi za zdravljenje in podporo.

6. Trenutno je v uporabi več kot 3 milijarde pametnih telefonov in vsi imajo vgrajene VGP, večina od katerih je vključena privzeto. Tudi nekateri najbolj razširjeni operacijski sistemi v osebnih in prenosnih računalnikih imajo vgrajene VGP. Nedavna porast uporabe pametnih zvočnikov (leta 2019 je bilo prodanih 147 milijonov[4]) prinaša VGP v milijone domov in pisarn. Vendar sedanji modeli VGP privzeto ne ponujajo mehanizmov avtentikacije ali nadzora dostopa.

7. Namen tega dokumenta je zagotoviti smernice glede uporabe Splošne uredbe o varstvu podatkov na področju virtualnih glasovnih pomočnikov (VGP).

2 TEHNOLOŠKO OZADJE

2.1 Osnovne značilnosti virtualnih glasovnih pomočnikov (VGP)

8. VGP se lahko opredeli kot programska aplikacija, ki omogoča govorni dialog z uporabnikom v naravnem jeziku.

9. Naravni jezik ima semantiko, značilno za človeški jezik. Glede na značilnosti posameznega jezika in raznolikost besedišča se lahko isto navodilo oblikuje na več načinov, medtem ko se lahko nekateri ukazi zdijo podobni, vendar se nanašajo na dva različna predmeta. Za odpravo takih dvoumnosti se zato pogosto uporabljajo mehanizmi za sklepno analizo, na primer glede na to, kaj je bilo povedano prej, čas izreka navodila, kraj, interesi osebe itd.

10. VGP se lahko razdeli v module, ki omogočajo izvajanje različnih opravil: zajemanje in restitucija zvoka, samodejni prepis govora (napisan govor), avtomatska obdelava jezika, strategije dialoga, dostop do ontologij (podatkovni nizi in strukturirani koncepti, povezani s posamezno domeno) in zunanji viri znanja, ustvarjanje jezika, sinteza govora (glasovno prebrano besedilo) itd. Konkretno bi moral avtomatski pomočnik omogočiti interakcijo za izvedbo dejanj (na primer „prižgi radio“, „ugasni luč“) ali za dostop do informacij (na primer „Kakšno vreme bo jutri?“, „Ali vlak ob 7.43 vozi?“). Tako ima vlogo posrednika in organizatorja z namenom olajšati izvajanje nalog za uporabnika.

11. V praksi VGP ni pametni zvočnik, vendar je pametni zvočnik lahko opremljen z glasovnim pomočnikom. Običajno je, da ju ljudje zamenjujejo, vendar je drugi le fizična podoba prvega. VGP se lahko namesti v pametni telefon, pametni zvočnik, povezano uro, vozilo, gospodinjski aparat itd.

12. Organizacija osnovne obdelave podatkov lahko vključuje več vzorcev pretoka informacij. Izluščimo lahko tri glavne elemente:

    Fizični element: element strojne opreme, v katerega je vgrajen pomočnik (pametni telefon, zvočnik, pametna televizija itd.) in ki vsebuje mikrofone, zvočnike ter omrežne in računalniške zmogljivosti (raven razvitosti je odvisna od posameznega primera).

    Programska oprema: del, ki izvaja interakcijo med človekom in strojem v strogem pomenu besede in vključuje module za samodejno prepoznavanje govora, obdelavo naravnega jezika,

[4] Glej na primer sporočilo za javnost z dne 1. avgusta 2019, ki ga je pripravil hamburški organ za varstvo podatkov in informacije: https://datenschutz-hamburg.de/pressemitteilungen/2019/08/2019-08-01-google-assistant.

dialog in sintezo govora. To se lahko upravlja neposredno znotraj fizične opreme, vendar se v številnih primerih izvaja na daljavo.

Viri: zunanji podatki, kot so zbirke podatkov vsebin, ontologije ali poslovne aplikacije, ki zagotavljajo informacije (na primer „Koliko je ura na zahodni obali Združenih držav Amerike?“, „Preberi mojo elektronsko pošto“) ali omogočajo konkretno izvedbo želenega opravila (na primer „Povišaj temperaturo za 1,5 °C“).

13. VGP za razširitev svojih osnovnih funkcij omogočajo namestitev sestavnih delov ali aplikacij tretjih oseb. Sestavni deli posameznih VGP so lahko različno poimenovani, vsi pa vključujejo izmenjavo osebnih podatkov uporabnikov med oblikovalcem VGP in razvijalcem aplikacij.

14. Čeprav večina VGP glasovnih izrezkov ne posreduje razvijalcem aplikacij, ti akterji še vedno obdelujejo osebne podatke. Poleg tega razvijalec aplikacij pri nekaterih funkcijah iz nabora podatkov prejema namene in reže, ki lahko vključujejo občutljive informacije, kot so zdravstveni podatki.

2.2 Akterji v ekosistemu VGP

15. VGP lahko v celotni verigi izvrševanja vključuje veliko akterjev in posrednikov. V praksi je mogoče opredeliti do pet različnih akterjev. Glede na poslovne modele in tehnološke izbire pa lahko nekateri akterji prevzamejo več kombinacij vlog, na primer oblikovalec in integrator ali oblikovalec in razvijalec aplikacij:

    a. **ponudnik (ali oblikovalec) VGP** je odgovoren za razvoj VGP, zasnuje in opredeli možnosti ter privzete funkcije VGP, kot so načini aktivacije, izbira arhitekture, dostop do podatkov, upravljanje zapisov, specifikacije strojne opreme itd.;

    b. **razvijalec aplikacij VGP** ustvari aplikacije (kot pri mobilnih aplikacijah), ki omogočajo razširitev privzetih funkcij VGP. Pri tem je treba upoštevati omejitve za nadaljnje razvijanje, ki jih postavi oblikovalec;

    c. **integrator** je proizvajalec povezanih predmetov, ki jih želi opremiti z VGP. Upoštevati bi moral zahteve, ki jih je določil oblikovalec;

    d. **lastnik** je odgovoren za fizične prostore za sprejem ljudi (nastanitve, delovna okolja, vozila za najem itd.) in želi svojemu občinstvu zagotoviti VGP (po možnosti z namenskimi aplikacijami);

    e. **uporabnik** je končni člen v vrednostni verigi VGP, ki VGP lahko uporablja na različnih napravah (zvočnik, televizija, pametni telefon, ura itd.), odvisno od tega, kako in kje je bil VGP nameščen in vzpostavljen.

2.3 Opis po korakih

16. Da bi VGP izvedel dejanje ali dostopal do informacij, se izvede naslednje zaporedje opravil:

    1) VGP je nameščen v kosu opreme (pametni telefon, zvočnik, vozilo) in je v stanju pripravljenosti. Natančneje, nenehno posluša. Vendar dokler naprava za zaznavanje glasu ne zazna posebne fraze za aktivacijo, ne prenaša zvoka in razen zaznavanja besed za aktivacijo se ne izvaja noben drug postopek. V ta namen se uporabi medpomnilnik v dolžini nekaj sekund (za več podrobnosti glej naslednji oddelek);

2) uporabnik izgovori aktivacijsko frazo, VGP pa na lokalni ravni primerja zvočni signal z aktivacijsko frazo. Če se ujemata, VGP odpre kanal za poslušanje, zvočna vsebina pa se takoj prenese;

3) če se ukaz obdeluje na daljavo, se v številnih primerih na strežniku opravi drugo preverjanje izgovarjave ključnih besed, da se omejijo neželene aktivacije;

4) uporabnik izreče svojo zahtevo, ki se sprotno posreduje ponudniku VGP. Zaporedje izgovorjenih besed se nato samodejno prepiše (pretvorba govora v besedilo);

5) ukaz se interpretira s pomočjo tehnologij za obdelavo naravnega jezika (NLP). Razločijo se nameni sporočila in opredelijo se informacijske spremenljivke (reže). Upravljalnik dialoga nato določiti scenarij interakcije, ki je potrebna z uporabnikom, tako da zagotovi ustrezno shemo odzivanja;

6) če ukaz vključuje funkcionalnost, ki jo nudi aplikacija tretje osebe (spretnost, dejanje, bližnjica itd.), ponudnik VGP razvijalcu aplikacije pošlje namene in informacijske spremenljivke (reže) sporočila;

7) opredeli se odgovor, prilagojen zahtevi uporabnika – vsaj domnevno; pri čemer je odziv „Nimam odgovora na vaše vprašanje“ prilagojen odgovor v primeru, ko VGP ne more pravilno interpretirati izrečenega. Po potrebi se uporabljajo oddaljeni viri: javno dostopne podatkovne zbirke znanja (spletne enciklopedije itd.) ali z avtentikacijo (bančni račun, aplikacija za glasbo, račun stranke za spletni nakup itd.);

8) ustvari se odgovor in/ali se prepozna dejanje (zastrtje senčil, dvig temperature, predvajanje glasbenega posnetka, odgovarjanje na vprašanje itd.). Stavek se sintetizira (besedilo v govor) in/ali dejanje, ki ga je treba izvesti, se pošlje opremi v izvršitev;

9) VGP se vrne v stanje pripravljenosti.

Čeprav se večina obdelave v zvezi z govorom trenutno izvaja na oddaljenih strežnikih, nekateri ponudniki VGP razvijajo sisteme, ki bi lahko del te obdelave izvajali lokalno.[5]

2.4 Aktivacijske fraze

17. VGP se lahko uporablja samo, če je „buden“. To pomeni, da pomočnik preklopi na aktivni način poslušanja in tako od uporabnika prejema ukaze in zahteve. Čeprav se lahko ta budnost včasih doseže tudi s fizičnim dejanjem (na primer s pritiskom gumba, pritiskom na pametni zvočnik itd.), skoraj vsi VGP na trgu temeljijo na zaznavi aktivacijske fraze ali besede za prehod na aktivni način poslušanja (poznane tudi kot aktivacijska beseda ali sprožilna beseda oziroma vroča beseda).

18. Pomočnik pri tem uporablja mikrofon in majhne računalniške zmogljivosti, da ugotovi, ali je bila izgovorjena ključna beseda. Ta analiza, ki se izvaja neprekinjeno od trenutka, ko je VGP vklopljen, se izvaja izključno lokalno. Šele ko je ključna beseda prepoznana, so zvočni posnetki obdelani za interpretacijo in izvedbo ukaza, kar v številnih primerih pomeni, da se prek

[5] To je bilo na primer sporočeno tukaj: https://www.amazon.science/blog/alexas-new-speech-recognition-abilities-showcased-at-interspeech.

interneta pošljejo v oddaljene strežnike. Zaznavanje ključnih besed temelji na tehnikah strojnega učenja. Glavni izziv pri uporabi takih načinov je, da je zaznavanje verjetnostno. Tako sistem za vsako izgovorjeno besedo ali izraz izvede oceno zanesljivosti glede tega, ali je bila dejansko izgovorjena ključna beseda. Če se izkaže, da je ta ocena višja od vnaprej določene mejne vrednosti, se šteje, da je bila izgovorjena ključna beseda. Tak sistem torej ni brez napak: v nekaterih primerih se aktivacija ne zgodi, čeprav je bila izrečena ključna beseda (lažna zavrnitev), v drugih primerih pa se lahko aktivacija izvede, čeprav uporabnik ni izrekel ključne besede (napačno sprejetje).

19. V praksi je treba najti sprejemljiv kompromis med tema dvema vrstama napak, da se določi mejna vrednost. Ker pa se lahko zaradi napačnega zaznavanja ključne besede pošiljajo zvočni posnetki, je verjetno, da bo prišlo do nepričakovanega in neželenega prenosa podatkov. Zelo pogosto ponudniki VGP, ki izvajajo obdelavo na daljavo, za odkrivanje takih nepravilnosti uporabljajo dvosmerni mehanizem, in sicer je prva faza zaznave vgrajena lokalno v sami opremi, druga pa se izvede na oddaljenih strežnikih, kjer poteka naslednja faza obdelave podatkov. V tem primeru razvijalci običajno določijo razmeroma nizek prag, da bi izboljšali uporabniško izkušnjo in zagotovili, da je, ko uporabnik izreče ključno besedo, ta skoraj vedno prepoznana – tudi če to pomeni „čezmerno prepoznavanje“ – in nato izvedejo drugo fazo zaznave na strežniku, ki je bolj restriktivna.

2.5 Glasovni izrezki in strojno učenje

20. VGP se pri opravljanju najrazličnejših nalog (zaznavanje ključnih besed, samodejno prepoznavanje govora, obdelava naravnega jezika, sinteza govora itd.) opirajo na metode strojnega učenja, zato potrebujejo velike nabore podatkov, ki jih zbirajo, izbirajo, označujejo itd.

21. Prevelika ali premajhna zastopanost nekaterih statističnih značilnosti lahko vpliva na razvoj nalog, ki temeljijo na strojnem učenju, kar se nato kaže v izračunih in s tem v načinu delovanja. Kakovost podatkov ima tako kot njihova količina pomembno vlogo pri natančnosti in točnosti učnega procesa.

22. Da bi povečali kakovost VGP in izboljšali uporabljene metode strojnega učenja, želijo morda oblikovalci VGP imeti dostop do podatkov v zvezi z uporabo naprave v dejanskih razmerah, tj. glasovnih izrezkov, da bi si tako lahko prizadevali za izboljšanje.

23. Ne glede na to, ali je treba opredeliti podatkovno zbirko za učenje ali popraviti napake, nastale ob uporabi algoritma, je za učenje in usposabljanje sistemov umetne inteligence nujno človekovo posredovanje. Ta del dela, znan kot digitalna delovna sila, sproža vprašanja o delovnih pogojih in varnosti. V zvezi s tem so novičarski mediji poročali tudi o prenosih podatkov med oblikovalci in podizvajalci VGP, ki naj ne bi imeli potrebnih jamstev za varstvo zasebnosti.

3 ELEMENTI VARSTVA PODATKOV

3.1 Pravni okvir

24. Zadevni pravni okvir EU za VGP je najprej Splošna uredba o varstvu podatkov, saj obdelava osebnih podatkov spada med osrednje funkcije VGP. Poleg Splošne uredbe o varstvu podatkov

Direktiva o zasebnosti in elektronskih komunikacijah[6] določa poseben standard za vse akterje, ki želijo shraniti podatke ali pridobiti dostop do podatkov, shranjenih v terminalski opremi naročnika ali uporabnika v EGP.

25. V skladu z opredelitvijo „*terminalske opreme*“[7] so primeri terminalske opreme pametni telefoni, pametni televizorji in podobne naprave interneta stvari. Čeprav so VGP same po sebi storitve programske opreme, vedno delujejo prek fizične naprave, kot je pametni zvočnik ali pametna televizija. **VGP za dostop do teh fizičnih naprav, ki sestavljajo terminalsko opremo v smislu Direktive o zasebnosti in elektronskih komunikacijah, uporabljajo elektronska komunikacijska omrežja. Zato se vedno, kadar VGP shranjuje podatke ali dostopa do podatkov v fizični napravi, ki je z njim povezana, uporabljajo določbe člena 5(3) Direktive o zasebnosti in elektronskih komunikacijah**.[8]

26. Vsi postopki obdelave osebnih podatkov, ki sledijo zgoraj navedenim postopkom obdelave, vključno z obdelavo osebnih podatkov, pridobljenih z dostopom do podatkov na terminalski opremi, morajo prav tako imeti pravno podlago v skladu s členom 6 Splošne uredbe o varstvu podatkov, da so zakoniti.[9]

27. Ker bo moral upravljavec, ko zahteva privolitev za shranjevanje ali pridobitev dostopa do podatkov v skladu s členom 5(3) Direktive o zasebnosti in elektronskih komunikacijah, posameznika, na katerega se nanašajo osebni podatki, obvestiti o vseh namenih obdelave (v smislu „naknadne obdelave“), vključno s kakršno koli obdelavo na podlagi zgoraj navedenih postopkov, bo privolitev v skladu s členom 6 Splošne uredbe o varstvu podatkov na splošno najprimernejša pravna podlaga za naknadno obdelavo osebnih podatkov. Zato bo privolitev verjetno pravna podlaga za shranjevanje podatkov in pridobitev dostopa do podatkov, ki so že shranjeni, ter za obdelavo osebnih podatkov po zgoraj navedenih postopkih obdelave. Pri presoji skladnosti s členom 6 Splošne uredbe o varstvu podatkov bi bilo treba upoštevati, da obdelava kot celota vključuje posebne dejavnosti, za katere je zakonodajalec EU želel zagotoviti dodatno varstvo.[10] Poleg tega morajo upravljavci pri ugotavljanju ustrezne zakonite podlage upoštevati vpliv na pravice posameznikov, na katere se nanašajo osebni podatki, da se zagotovi spoštovanje načela pravičnosti.[11] Bistvo je, da se upravljavci ne morejo sklicevati

[6] Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah), kot je bila spremenjena z Direktivo 2006/24/ES in Direktivo 2009/136/ES (v nadaljevanju: Direktiva o zasebnosti in elektronskih komunikacijah).

[7] Člen 1 Direktive Komisije 2008/63/ES z dne 20. junija 2008 o konkurenci na trgih za telekomunikacijsko terminalsko opremo opredeljuje „*terminalsko opremo*“ kot „*(a) vso opremo, ki je neposredno ali posredno priključena na mrežni vmesnik javnega telekomunikacijskega omrežja za pošiljanje, obdelovanje ali sprejemanje informacij; v obeh primerih (neposredna ali posredna) se lahko priključitev izvede z žico, optičnim kablom ali elektromagnetno; priključitev je posredna, če je oprema nameščena med terminalom in javnim mrežnim vmesnikom; (b) […] tudi opremo satelitskih zemeljskih postaj*“.

[8] Glej odstavek 12 Smernic Evropskega odbora za varstvo podatkov 1/2020 za podobno utemeljitev v zvezi s povezanimi vozili (v nadaljevanju: Smernice Evropskega odbora za varstvo podatkov 1/2020). Glej tudi Mnenje Evropskega odbora za varstvo podatkov št. 5/2019 o medsebojnem vplivu Direktive o zasebnosti in elektronskih komunikacijah ter Splošne uredbe o varstvu podatkov, zlasti v zvezi s pristojnostmi, nalogami in pooblastili organov za varstvo podatkov.

Prav tam, odstavek 41.

[10] Mnenje št. 5/2019, odstavek 41.

[11] Evropski odbor za varstvo podatkov: Smernice 2/2019 o obdelavi osebnih podatkov na podlagi člena 6(1)(b) Splošne uredbe o varstvu podatkov v okviru zagotavljanja spletnih storitev posameznikom, na katere se nanašajo osebni podatki, različica 2.0, 8. oktober 2019, odstavek 1.

na člen 6 Splošne uredbe o varstvu podatkov, da bi znižali stopnjo dodatnega varstva iz člena 5(3) Direktive o zasebnosti in elektronskih komunikacijah.

28. Kot je prikazano v oddelku 2.3 (korak 2 in 3), trenutni VGP zahtevajo dostop do glasovnih podatkov, shranjenih na napravi VGP.[12] Zato se uporablja člen 5(3) Direktive o zasebnosti in elektronskih komunikacijah. Uporaba člena 5(3) Direktive o zasebnosti in elektronskih komunikacijah pomeni, da je za shranjevanje podatkov in dostop do podatkov, ki so že shranjeni v VGP, praviloma potrebno predhodno soglasje končnega uporabnika[13], vendar sta dovoljeni dve izjemi: prvič, izvajanje ali omogočanje prenosa sporočila prek elektronskega komunikacijskega omrežja ali, drugič, kar je nujno potrebno za zagotavljanje storitve informacijske družbe, ki jo naročnik ali uporabnik izrecno zahteva.

29. Druga izjema („kar je nujno potrebno za zagotavljanje storitve informacijske družbe, ki jo naročnik ali uporabnik izrecno zahteva“) bi ponudniku storitev VGP omogočila obdelavo podatkov uporabnikov za izvrševanje zahtev uporabnikov (glej odstavek 72 v oddelku 3.4.1) brez privolitve iz člena 5(3) Direktive o zasebnosti in elektronskih komunikacijah. Nasprotno pa bi bila taka **privolitev, kot jo zahteva člen 5(3) Direktive o zasebnosti in elektronskih komunikacijah, potrebna za** shranjevanje podatkov ali pridobitev dostopa do podatkov za **kateri koli namen, ki ni izvršitev zahteve uporabnikov** (na primer oblikovanje profilov uporabnikov). Upravljavci podatkov bi morali privolitev pripisati določenim uporabnikom. Zato bi morali upravljavci podatkov za izpolnitev zahtev uporabnikov obdelati samo podatke neregistriranih uporabnikov.

30. VGP lahko naključno posnamejo zvočne posnetke posameznikov, ki niso nameravali uporabljati storitve VGP. Prvič, deloma in odvisno od VGP se lahko aktivacijska fraza spremeni. Posamezniki, ki ne vedo za to spremembo, bi lahko nenamerno uporabili posodobljeno aktivacijsko frazo. Drugič, VGP lahko zazna aktivacijsko frazo po pomoti ali napačno. Zelo malo verjetno je, da bi se v primeru nenamerne aktivacije uporabljala katera od izjem iz člena 5(3) Direktive o zasebnosti in elektronskih komunikacijah. Poleg tega mora biti privolitev, kot je opredeljena v Splošni uredbi o varstvu podatkov, „nedvoumna izjava volje posameznika, na katerega se nanašajo osebni podatki“. Zato je zelo malo verjetno, da bi se nenamerna aktivacija lahko razlagala kot veljavna privolitev. Če upravljavci podatkov (na primer med samodejnim ali človeškim pregledom) ugotovijo, da je storitev VGP pomotoma obdelala osebne podatke, bi morali preveriti, ali obstaja veljavna pravna podlaga za vsak namen obdelave takih podatkov. Sicer bi bilo treba nenamerno zbrane podatke izbrisati.

31. Poleg tega je treba opozoriti, da so lahko osebni podatki, ki jih obdeluje VGP, zelo občutljivi. Osebni podatki se lahko nahajajo v njegovi vsebini (pomen govorjenega besedila) in metapodatkih (spol ali starost govorca itd.). Evropski odbor za varstvo podatkov opozarja, da so glasovni podatki sami po sebi biometrični osebni podatki.[14] Iz tega izhaja, da kadar se taki podatki obdelujejo za namene edinstvene identifikacije fizične osebe ali so sami po sebi osebni podatki posebne kategorije ali se določijo kot taki, mora obdelava takih podatkov imeti

[12] Možno je, da bodo prihodnje naprave z VGP sprejele paradigmo računalništva na robu in bodo lahko nekatere storitve zagotavljale lokalno. V takem primeru bo treba vnovič oceniti ustreznost uporabe Direktive o zasebnosti in elektronskih komunikacijah.

[13] Glej tudi smernice Evropskega odbora za varstvo podatkov 1/2020, odstavek 14.

[14] Člen 4(14) Splošne uredbe o varstvu podatkov biometrične podatke opredeljuje kot „osebne podatke, ki so rezultat posebne tehnične obdelave v zvezi s fizičnimi, fiziološkimi ali vedenjskimi značilnostmi posameznika, ki omogočajo ali potrjujejo edinstveno identifikacijo tega posameznika, kot so podobe obraza ali daktiloskopski podatki“.

veljavno pravno podlago v členu 6, spremljati pa jo mora odstopanje od člena 9 Splošne uredbe o varstvu podatkov (glej oddelek 3.7 v nadaljevanju).

3.2 Identifikacija obdelave podatkov in deležnikov

32. Glede na številne možnosti pomoči, ki jih VGP lahko zagotovi v toliko različnih okoljih v vsakdanjem življenju posameznika, na katerega se nanašajo osebni podatki[15], je treba opozoriti, da bi bilo treba skrbno premisliti o obdelavi osebnih podatkov, na katero lahko vplivajo tudi različni deležniki.

3.2.1 Obdelava osebnih podatkov

33. Z vidika varstva osebnih podatkov je mogoče opaziti več konstant ne glede na vrsto VGP (tj. vrsta naprave, funkcije, storitve ali njihova kombinacija), ki jih lahko uporablja posameznik, na katerega se nanašajo osebni podatki. Te konstante so povezane s pluralnostjo osebnih podatkov, posamezniki, na katere se nanašajo osebni podatki, in zadevno obdelavo podatkov.

Pluralnost vrst osebnih podatkov

34. Opredelitev osebnih podatkov v skladu s členom 4(1) Splošne uredbe o varstvu podatkov vključuje širok nabor različnih podatkov in se v tehnološko nevtralnem okviru uporablja za katero koli informacijo v zvezi „*z določenim ali določljivim posameznikom*“[16]. Vsaka interakcija posameznika, na katerega se nanašajo osebni podatki, z VGP lahko spada na področje uporabe te opredelitve. Ko pride do interakcije, se lahko med celotnim delovanjem VGP obdelajo različni osebni podatki, kot je opisano v oddelku 2.4.

35. Od prvotne zahteve do ustreznega odgovora, dejanja ali nadaljnjega ukrepa (na primer priprava tedenskega opozorila) se bodo po prvem vnosu osebnih podatkov pridobivali nadaljnji osebni podatki. To vključuje primarne podatke (na primer podatke o računu, glasovne posnetke, zgodovino zahtevkov), podatke, zbrane z opazovanjem (na primer podatke o napravi v zvezi s posameznikom, na katerega se nanašajo osebni podatki, dnevnike dejavnosti, spletne dejavnosti), ter povzetke ali izpeljane podatke (na primer oblikovanje profilov uporabnikov). VGP uporabljajo govor za posredovanje med uporabniki in vsemi povezanimi storitvami (na primer iskalnikom, spletno trgovino ali storitvijo pretakanja glasbe), vendar imajo lahko VGP drugače kot drugi posredniki popoln dostop do vsebine zahtevkov in zato oblikovalcu VGP zagotavljajo širok nabor osebnih podatkov, odvisno od namenov obdelave.

36. Pluralnost osebnih podatkov, ki se obdelujejo pri uporabi VGP, se nanaša tudi na pluralnost kategorij osebnih podatkov, ki jim je treba nameniti pozornost (glej oddelek 3.7 v nadaljevanju). Evropski odbor za varstvo podatkov opozarja, da mora upravljavec pri obdelavi posebnih vrst podatkov[17] v skladu s členom 9 Splošne uredbe o varstvu podatkov opredeliti

[15] Primeri: doma, v vozilu, na ulici, na delovnem mestu ali v katerem koli drugem zasebnem, javnem ali poklicnem prostoru ali kombinaciji teh prostorov.

[16] Člen 4(1) Splošne uredbe o varstvu podatkov določa tudi, da je določljiv posameznik „*tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika*“.

[17] Člen 9(1) Splošne uredbe o varstvu podatkov določa, da so posebne vrste osebnih podatkov tiste, „*ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, in obdelava*

veljavno izjemo od prepovedi obdelave iz člena 9(1) in veljavno pravno podlago iz člena 6(1) z uporabo ustreznih sredstev, opredeljenih v členu 9(2). Izrecno soglasje je lahko eno od ustreznih odstopanj, kadar je privolitev pravna podlaga, na katero se sklicuje člen 6(1). V členu 9 je tudi (podrobno) navedeno, da lahko države članice uvedejo dodatne pogoje glede obdelave biometričnih ali drugih posebnih vrst podatkov.

Pluralnost posameznikov, na katere se nanašajo osebni podatki

37. Pri uporabi VGP se osebni podatki obdelujejo od prve interakcije z VGP. Za nekatere posameznike, na katere se nanašajo osebni podatki, to pomeni nakup VGP in/ali konfiguracijo uporabniškega računa (tj. registrirani uporabniki). Za druge posameznike, na katere se nanašajo osebni podatki, to pomeni prvo zavestno komunikacijo z VGP drugega posameznika, na katerega se nanašajo osebni podatki, ki je tega VGP kupil in/ali konfiguriral (tj. neregistrirani uporabniki). Potem je tu še tretja kategorija posameznikov, na katere se nanašajo osebni podatki, in sicer naključni uporabniki, registrirani ali ne, ki so nevede komunicirali z VGP (na primer so izgovorili ustrezno aktivacijsko frazo, ne da bi vedeli, da je VGP aktiven, ali so izgovorili druge besede, ki jih je VGP pomotoma prepoznal kot aktivacijsko frazo).

38. Izraz pluralnost posameznikov, na katere se nanašajo osebni podatki, pomeni tudi več uporabnikov enega VGP (na primer naprava, ki si jo delijo registrirani in neregistrirani uporabniki, sodelavci, družina, šola) in različne vrste uporabnikov glede na njihove značilnosti (na primer odrasla oseba, otrok, starejša oseba ali invalidna oseba). Čeprav lahko VGP omogoči lažjo interakcijo z digitalnim orodjem in nudi številne koristi nekaterim kategorijam posameznikov, na katere se nanašajo osebni podatki, je pomembno upoštevati posebnosti vsake kategorije posameznikov, na katere se nanašajo osebni podatki, in kontekst uporabe VGP.

Pluralnost obdelave podatkov

39. Tehnologije, ki se uporabljajo za delovanje VGP, vplivajo tudi na količino obdelanih podatkov in vrste obdelave. Bolj ko se uporabljajo storitve ali funkcije posameznega VGP in bolj ko je povezan z drugimi napravami ali storitvami tretjih oseb, večja je količina osebnih podatkov, ki se obdelujejo in spreminjajo namembnost. Posledica tega je raznolikost obdelave, ki se izvaja s samodejnimi načini, kot je opisano v oddelku 2. Poleg samodejnih načinov lahko posamezna obdelava vključuje tudi človeške vire. To velja na primer, kadar uporabljena tehnologija vključuje človekovo posredovanje, kot je pregled prepisa glasovnih sporočil v besedila, ali zagotavljanje opomb o osebnih podatkih, ki se lahko uporabijo za vključitev novih modelov v tehnologijo strojnega učenja. To velja tudi, kadar osebne podatke (na primer metapodatke) analizira človek, da bi izboljšal storitev VGP.

3.2.2 Obdelava s strani upravljavcev in obdelovalcev podatkov

40. Posamezniki, na katere se nanašajo osebni podatki, bi morali biti sposobni razumeti in prepoznati zadevne vloge ter imeti možnost, da vzpostavijo stik z vsakim posameznim deležnikom ali ukrepajo z njim, kot to zahteva Splošna uredba o varstvu podatkov. Porazdelitev vlog ne bi smela škoditi posameznikom, na katere se nanašajo osebni podatki, čeprav lahko gre za zapletene ali nedokončane razvoje dogodkov. Deležniki so za oceno svojih vlog napoteni

genetskih podatkov, biometričnih podatkov za namene edinstvene identifikacije posameznika, podatkov v zvezi z zdravjem ali podatkov v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo.“

na smernice Evropskega odbora za varstvo podatkov št. 7/2020 o pojmih upravljavca in obdelovalca v Splošni uredbi o varstvu podatkov.[18]

41. Kot je navedeno v odstavku 15, se lahko glavni deležniki opredelijo v okviru vloge ponudnika ali oblikovalca, razvijalca aplikacij, integratorja, lastnika ali kombinaciji teh vlog. Možni so različni scenariji, odvisno od tega, kdo počne kaj v poslovnem odnosu deležnikov, od zahteve uporabnika, osebnih podatkov, dejavnosti obdelave podatkov in njihovih namenov. Jasno bi morali določiti in obvestiti posameznike, na katere se nanašajo osebni podatki, o pogojih, pod katerimi bo vsak od njih deloval in izpolnjevati izhajajoče vloge upravljavcev, skupnih upravljavcev ali obdelovalcev, kot je določeno v Splošni uredbi o varstvu podatkov[19]. Vsak od njih lahko prevzame eno ali več vlog, saj so lahko enkratni upravljavec podatkov, skupni upravljavec podatkov ali obdelovalec podatkov za eno obdelavo podatkov, pri drugi obdelavi podatkov pa ima drugo vlogo.

42. Z vidika na visoki ravni lahko oblikovalec deluje kot upravljavec podatkov pri določanju namenov in sredstev obdelave, lahko pa posreduje kot obdelovalec podatkov, kadar obdeluje osebne podatke v imenu tretjih oseb, kot je razvijalec aplikacij. Uporabnik VGP bi bil zato podvržen več upravljavcem podatkov: razvijalcem in oblikovalcem aplikacij. Možno je tudi, da so oblikovalec, integrator in razvijalec združeni v en sam organ, ki deluje kot edinstven upravljavec podatkov. V vsakem primeru je treba kvalifikacije, ki se uporabljajo, določiti na podlagi analize za vsak primer posebej.

Primer 1:
Oblikovalec VGP podatke o uporabnikih obdeluje za številne namene, vključno za izboljšanje sposobnosti razumevanja glasu VGP in natančno odzivanje na ukaze. Čeprav lahko ta namen vodi do obdelave podatkov, ki izhajajo iz uporabe aplikacij tretjih oseb, obstaja samo en upravljavec podatkov, in sicer oblikovalec VGP, v imenu katerega in za namene katerega se izvaja obdelava.

Primer 2:
Banka svojim strankam ponuja aplikacijo, pri kateri lahko stranke za upravljanje svojih računov uporabljajo neposredno poizvedovanje prek VGP. V obdelavo osebnih podatkov sta vključena dva akterja: oblikovalec VGP in razvijalec bančne aplikacije. V predstavljenem scenariju je banka upravljavec podatkov za zagotavljanje storitve, saj določa namene in bistvena sredstva obdelave v zvezi z aplikacijo, ki omogočajo interakcijo s pomočnikom. Dejansko banka ponuja posebno aplikacijo, ki uporabniku (svoji stranki) omogoča, da svoje račune upravlja na daljavo. Poleg tega odloča o sredstvih obdelave z izbiro ustreznega obdelovalca, ki je oblikovalec VGP in ima lahko s svojim strokovnim znanjem pomembno vlogo pri določanju teh sredstev (lahko na primer upravlja razvojno

[18] Smernice Evropskega odbora za varstvo podatkov 07/2020 o pojmih upravljavca in obdelovalca v Splošni uredbi o varstvu podatkov, različica 2.0, sprejete 7. julija 2021 (v nadaljevanju: smernice 7/2020).

[19] Splošna uredba o varstvu podatkov, členi od 12 do 14, člen 26.

platformo, ki omogoča vključitev aplikacij tretjih oseb v VGP, s čimer določa okvir in pogoje, ki jih morajo upoštevati razvijalci aplikacij).

43. Treba je opozoriti, da lahko iste osebne podatke posameznika obdeluje več deležnikov, pri čemer posameznik, na katerega se nanašajo osebni podatki, morda ne pričakuje, da bodo v procesno verigo poleg ponudnika VGP vključene tudi druge strani. Kadar posameznik, na katerega se nanašajo osebni podatki, ukrepa pri ponudniku VGP v zvezi s svojimi osebnimi podatki (na primer uveljavljanje pravic posameznika, na katerega se nanašajo osebni podatki), to samodejno ne pomeni, da se bo ta ukrep uporabljal tudi za iste osebne podatke, ki jih obdeluje drug deležnik. Kadar so ti deležniki neodvisni upravljavci, je pomembno, da se posameznikom, na katere se nanašajo osebni podatki, pošlje jasno informativno obvestilo, v katerem so pojasnjene različne faze in akterji obdelave. Poleg tega bi bilo treba v primerih skupnega upravljanja jasno navesti, ali je vsak upravljavec pristojen za spoštovanje vseh pravic posameznika, na katerega se nanašajo osebni podatki, ali kateri upravljavec je pristojen za katero pravico.[20]

Primer 3:

V tem primeru želi oblikovalec VGP uporabiti podatke, zbrane in obdelane za storitev, ki jo zagotavlja banka, da bi izboljšala svoj sistem prepoznavanja glasu. Oblikovalec VGP, ki obdeluje podatke za lastne namene, bo imel status upravljavca za tako namensko obdelavo.

44. Ker je lahko v procesno verigo vključenih veliko deležnikov oziroma veliko zaposlenih, lahko pride do tveganih situacij, če niso vzpostavljeni ustrezni in zaščitni ukrepi. Zanje so odgovorni upravljavci, zato bi se morali osrediniti na varstvo osebnih podatkov, zlasti z izbiro ustreznih poslovnih partnerjev in obdelovalcev podatkov, uporabo načel privzete in vgrajene zasebnosti[21] ter izvajanjem ustreznih varnostnih in drugih orodij Splošne uredbe o varstvu podatkov, kot so revizije in pravni sporazumi (na primer člen 26 Splošne uredbe o varstvu podatkov za skupne upravljavce ali člen 28 Splošne uredbe o varstvu podatkov za obdelovalce).

45. Ekosistem VGP je zapleten sistem, pri katerem bi lahko številni akterji izmenjevali in obdelovali osebne podatke kot upravljavci ali obdelovalci podatkov. Zelo pomembno je pojasniti vlogo vsakega akterja pri vsaki obdelavi in upoštevati načelo najmanjšega obsega podatkov tudi v zvezi z izmenjavo podatkov.

46. Poleg tega bi morali biti upravljavci pozorni na prenose osebnih podatkov in zagotavljati zahtevano raven varstva v celotni verigi obdelave, zlasti kadar uporabljajo storitve izvajalcev s sedežem zunaj EGP.

3.3 Preglednost

47. Ker VGP obdelujejo osebne podatke (na primer glasove uporabnikov, lokacijo ali vsebino komunikacije), morajo izpolnjevati zahteve glede preglednosti iz Splošne uredbe o varstvu podatkov, kot so določene v členih 5(1)(a), 12 in 13 (pojasnjeno v uvodni izjavi 58). Upravljavci podatkov morajo uporabnike obvestiti o obdelavi njihovih osebnih podatkov v jedrnati, pregledni, razumljivi in lahko dostopni obliki.

[20] Smernice 7/2020, odst. 165.

[21] Glej Smernice Evropskega odbora za varstvo podatkov št. 4/2019 o členu 25, Vgrajeno in privzeto varstvo podatkov, različica 2.0, sprejete 20. oktobra 2020.

48. Če potrebne informacije niso zagotovljene, gre za kršitev obveznosti, ki lahko vpliva na zakonitost obdelave podatkov. Izpolnjevanje zahteve po preglednosti je nujno, saj služi kot nadzorni mehanizem nad obdelavo podatkov in uporabnikom omogoča uveljavljanje njihovih pravic. Ustrezno obveščanje uporabnikov o tem, kako se uporabljajo njihovi osebni podatki, upravljavcem podatkov otežuje zlorabo VGP za namene, ki močno presegajo pričakovanja uporabnikov. Patentirane tehnologije na primer poskušajo na podlagi glasu uporabnika ugotoviti njegovo zdravstveno stanje in čustvena stanja ter ustrezno prilagoditi ponujene storitve.

49. Izpolnjevanje zahtev glede preglednosti je lahko zlasti težavno za ponudnika storitev VGP ali kateri koli drug subjekt v vlogi upravljavca podatkov. Glede na posebno naravo VGP se upravljavci podatkov spopadajo z več ovirami pri izpolnjevanju zahtev Splošne uredbe o varstvu podatkov glede preglednosti:

- **več uporabnikov**: upravljavci podatkov bi morali obvestiti vse uporabnike (registrirane, neregistrirane in naključne uporabnike), ne le uporabnika, ki vzpostavi VGP;
- **zapletenost ekosistema**: kot je pojasnjeno v oddelku o tehnološkem ozadju, identitete in vloge tistih, ki obdelujejo osebne podatke pri uporabi VGP, uporabnikom še zdaleč niso znane;
- **posebnosti glasovnega vmesnika**: digitalni sistemi še niso primerni za zgolj glasovno interakcijo, kar dokazuje skoraj sistematična uporaba spremljevalnega zaslona. Vendar sta nujna prilagoditev na glasovni vmesnik in možnost jasnega ter pravilnega obveščanja uporabnika na ta način.

50. VGP lahko štejejo za naprave s končnim številom stanj, ki med običajnim delovanjem prehajajo skozi več stanj. Lokalno lahko zaznavajo morebitne aktivacijske fraze ali sodelujejo z oddaljenim strežnikom za razrešitev ukaza, vendar lahko glede na kontekst (na primer če obstaja šum okolja iz ozadja) ali uporabnika, ki se z njimi pogovarja (na primer lahko se pogovarjajo z določenim ali neznanim uporabnikom), prevzamejo še veliko drugih stanj. Žal se te situacije pojavljajo v velikem nesorazmerju informacij z uporabnikom, ki se le bežno zaveda, da naprava posluša, še manj pa se zaveda trenutnega stanja naprave.

51. Zelo priporočljivo je, da oblikovalci in razvijalci VGP sprejmejo ustrezne ukrepe za odpravljanje teh nesorazmerij, da bi delovanje VGP postalo bolj interaktivno. Uporabnike bi bilo treba obvestiti o stanju, v katerem je naprava v nekem trenutku. Tako večjo preglednost je mogoče doseči tako, da postane dialog med človekom in strojem bolj interaktiven (na primer naprava lahko na neki način potrdi sprejem glasovnega ukaza) ali pa da se stanje naprave sporoča s posebnimi signali. V zvezi s tem je mogoče preučiti številne možnosti, od uporabe posebnih glasovnih zaznamkov in vizualnih ikon ali luči do uporabe prikazovalnikov na napravi.

52. Ta vprašanja so zlasti pomembna glede na pluralnost uporabnikov in prisotnost ranljivih skupin posameznikov, kot so otroci, starejši ljudje ali uporabniki z avdiovizualnimi motnjami.

53. Iz teh vprašanj sta razvidni dve pomembni vprašanji: kateri je najbolj izvedljiv način obveščanja uporabnikov in kdaj je primeren čas za njihovo obveščanje? Ta vprašanja bi bilo treba dodatno preučiti v dveh različnih situacijah, odvisno od tega, ali ima VGP samo enega uporabnika (kot je osebni pametni telefon) ali potencialno več uporabnikov (na primer naprava za pametni dom). Z uporabo tehnologije VGP bi lahko prišlo tudi do neskladja teh dveh osnovnih nastavitev, na primer kadar ima uporabnik osebni pametni telefon in ga poveže z

avtomobilom. VGP pametnega telefona, za katerega se lahko razumno pričakuje, da ga bo uporabljal samo dani uporabnik, je zdaj „razširjen“ na druge v avtomobilu.

54. Trenutno so vsi VGP povezani z uporabniškim računom in/ali so vzpostavljeni z aplikacijo, ki tak račun zahteva. Obravnavati bi bilo treba vprašanje, kako bi lahko upravljavci podatkov te uporabnike obveščali o politiki varovanja zasebnosti pri vzpostavljanju VGP, kot je opisano v smernicah Delovne skupine iz člena 29 o preglednosti. Aplikacije bi morale v spletni trgovini vsebovati potrebne informacije, ki so na voljo pred prenosom[22]. Tako so informacije na voljo čim prej, najpozneje pa ob pridobivanju osebnih podatkov. Nekateri ponudniki VGP v privzeto nastavitev VGP vključijo aplikacije tretjih oseb, tako da lahko te aplikacije z uporabo posebnih aktivacijskih fraz izvajajo tiste aplikacije. VGP, ki uporabljajo to strategijo uvajanja aplikacij tretjih oseb, bi morala zagotoviti, da uporabniki dobijo potrebne informacije tudi o obdelavi, ki jo izvajajo tretje osebe.

55. Vendar številni oblikovalci VGP zahtevajo uporabniške račune VGP, ki združujejo storitev VGP s številnimi drugimi storitvami, med katerimi so elektronska pošta, pretakanje videovsebin ali nakupi. Če se oblikovalec VGP odloči, da račun poveže z več različnimi storitvami, to zahteva zelo dolge in zapletene pravilnike varovanja zasebnosti. Dolžina in zapletenost takih pravilnikov o zasebnosti močno ovirata uresničevanje načela preglednosti.

> Primer 4:
>
> Oblikovalec VGP od uporabnikov zahteva, da imajo za dostop do storitve VGP uporabniški račun. Ta uporabniški račun ni specifičen za storitev VGP in se lahko uporablja za druge storitve, ki jih nudi oblikovalec VGP, kot so elektronska pošta, shranjevanje v oblaku in družbeni mediji. Uporabniki morajo za ustvarjanje računa prebrati in sprejeti 30 strani dolg pravilnik o varstvu osebnih podatkov. Pravilnik vključuje informacije o obdelavi osebnih podatkov s strani vseh storitev, ki bi lahko bile povezane z računom.
>
> Informacije, ki jih je zagotovil oblikovalec VGP, v tem primeru ne bi smele šteti za jedrnate, poleg tega njihova zapletenost zmanjšuje zahtevano preglednost. Zato oblikovalec VGP ne bi izpolnjeval zahtev glede preglednosti iz členov 12 in 13 Splošne uredbe o varstvu podatkov.

56. Čeprav se zahtevane informacije najpogosteje posredujejo v pisni obliki, Splošna uredba o varstvu podatkov dovoljuje tudi „druga sredstva“. V uvodni izjavi 58 je izrecno navedeno, da se informacije lahko predložijo v elektronski obliki, na primer na spletnem mestu. Poleg tega bi bilo treba pri izbiri ustreznega načina obveščanja posameznikov, na katere se nanašajo osebni podatki, upoštevati posebne okoliščine, kot je način, kako upravljavec podatkov in posameznik, na katerega se nanašajo osebni podatki, tudi sicer medsebojno komunicirata.[23] Možnost za naprave brez zaslona bi lahko bila, da se zagotovi povezava, ki je lahko razumljiva, bodisi neposredno bodisi v elektronski pošti. Kot primer za informacije bi lahko služile že obstoječe rešitve, na primer prakse klicnih centrov, ki obveščajo kličočega o snemanju telefonskega klica in ga usmerjajo v svoj pravilnik varovanja zasebnosti. Omejitve VGP brez zaslona upravljavca podatkov ne odvezujejo od zagotavljanja potrebnih informacij v skladu s Splošno uredbo o varstvu podatkov pri vzpostavitvi VGP ali namestitvi ali uporabi aplikacije

[22] Smernice o preglednosti na podlagi Uredbe 2016/679, WP260 rev. 01, ki jih je potrdil Evropski odbor za varstvo podatkov (v nadaljevanju: smernice DS29 o preglednosti), odstavek 11.

[23] Smernice DS29 o preglednosti, odstavek 19.

VGP. Ponudniki in razvijalci VGP bi morali razviti glasovne vmesnike za lažje zagotavljanje obveznih informacij.

57. VGP bi lahko bila zelo zanimiva možnost za uporabnike z oslabljenim vidom, saj zagotavljajo alternativen način za interakcijo s storitvami IT, ki se običajno opirajo na vizualne informacije. V skladu s členom 12(1) Splošne uredbe o varstvu podatkov se potrebne informacije lahko predložijo ustno izključno na zahtevo posameznika, na katerega se nanašajo osebni podatki, ne pa kot privzet način podajanja informacij. Vendar bi bili zaradi omejitev VGP brez zaslona potrebni načini za samodejno glasovno podajanje informacij, ki bi jih lahko dopolnjevale pisne informacije. Upravljavci podatkov bi morali pri uporabi zvoka za obveščanje posameznikov, na katere se nanašajo osebni podatki, zagotoviti, da se potrebne informacije podajo na jedrnat in jasen način. Poleg tega bi bilo treba posameznikom, na katere se nanašajo osebni podatki, omogočiti večkratno poslušanje[24].

58. Sprejemanje ustreznih ukrepov za skladnost z zahtevami glede preglednosti iz Splošne uredbe o varstvu podatkov je bolj zapleteno, kadar VGP uporablja več uporabnikov, ki niso lastniki naprave. Oblikovalci VGP morajo premisliti o tem, kako neregistrirane in naključne uporabnike ustrezno obvestiti o obdelavi njihovih osebnih podatkov. Kadar je pravna podlaga za obdelavo podatkov uporabnikov privolitev, morajo biti uporabniki ustrezno obveščeni, da je privolitev veljavna.[25]

59. Za zagotovitev skladnosti s Splošno uredbo o varstvu podatkov bi morali upravljavci podatkov najti način za obveščanje ne le registriranih uporabnikov, temveč tudi neregistriranih in naključnih uporabnikov VGP. Te uporabnike je treba čim prej obvestiti, **najpozneje pa v času** obdelave. V praksi bo ta pogoj še posebej težko izpolniti.

60. Nekatere poslovne posebnosti prav tako ne bi smele škoditi posameznikom, na katere se nanašajo osebni podatki. Ker so številni deležniki globalna podjetja ali so dobro poznani po posebnih poslovnih dejavnostih (na primer telekomunikacije, e-trgovanje, informacijske tehnologije, spletne dejavnosti), bi moral biti njihov način zagotavljanja storitve VGP jasen. Posamezniki, na katere se nanašajo osebni podatki, bi morali na podlagi ustreznih informacij razumeti, ali bo njihova uporaba VGP povezana z drugimi dejavnostmi obdelave, ki jih upravlja ponudnik storitev VGP (na primer telekomunikacije, e-trgovanje, informacijske tehnologije ali spletne dejavnosti), razen strogo za VGP.

> Primer 5:
>
> Oblikovalec VGP, ki zagotavlja tudi platformo družbenih medijev in iskalnik, za uporabo svojega pomočnika od uporabnika zahteva, da svoj uporabniški račun poveže s pomočnikom. S povezovanjem uporabniškega računa z uporabo VGP lahko oblikovalec izboljša profil svojih uporabnikov z uporabo pomočnika, nameščenimi aplikacijami (ali zmožnostmi), oddanimi naročili itd. Zato so interakcije s pomočniki nov vir informacij, povezan z uporabnikom. Oblikovalec VGP bi moral uporabnikom zagotoviti jasne informacije o tem, kako se bodo njihovi podatki obdelovali za vsako storitev, in o možnostih nadzora, ki uporabniku omogočajo, da izbere, ali se bodo podatki uporabili za profiliranje ali ne.

Priporočila

[24] Smernice DS29 o preglednosti, odstavek 21.

[25] Glej člen 4(11) Splošne uredbe o varstvu podatkov.

61. Kadar so uporabniki obveščeni o obdelavi osebnih podatkov VGP s pravilnikom o zasebnosti uporabniškega računa in je račun povezan z drugimi neodvisnimi storitvami (na primer elektronsko pošto ali spletnimi nakupi), Evropski odbor za varstvo podatkov priporoča, da ima pravilnik o varstvu zasebnosti jasno ločen oddelek v zvezi z obdelavo osebnih podatkov VGP.

62. Informacije, namenjene uporabniku, bi morale vsebovati natančne podatke o zbiranju in obdelavi, ki se izvajata. Glasovni vzorec vsebuje nekatere metainformacije (na primer raven stresa govorca), vendar ni samodejno jasno, ali se taka analiza izvaja. Bistveno je, da upravljavci zagotavljajo pregledne informacije o tem, katere posebne vidike surovih podatkov obdelujejo.

63. Vedno bi moralo biti tudi razvidno, v katerem stanju je VGP. Uporabniki bi morali imeti možnost v vsakem trenutku izvedeti, ali VGP „posluša“ glasove v svojem internem dosegu in zlasti, ali pretaka informacije v zaledni del. Te informacije bi morale biti dostopne tudi invalidom z barvno slepoto (daltonizem), gluhim (anakuzija) itd. Posebno skrb bi bilo treba nameniti temu, da bi se VGP lahko uporabljali tudi brez očesnega stika z napravo. Zato bi morale biti vse povratne informacije za uporabnike, vključno s spremembami stanja, na voljo najmanj v vizualni in zvočni obliki.

64. Posebno pozornost bi bila potrebna, če naprave omogočajo dodajanje funkcij tretje oseb („aplikacije“ za VGP). Uporabniku so lahko na voljo nekatere splošne informacije, kadar dodajajo take funkcije (glede na to, da jih izbere uporabnik), med običajno uporabo naprave pa so lahko meje med različnimi vključenimi upravljavci veliko manj jasne, tj. uporabnik morda ni dovolj obveščen o tem, kako in kdo jih obdeluje (in v kakšnem obsegu) pri posamezni poizvedbi.

65. V skladu s členom 12 Splošne uredbe o varstvu podatkov bi morale biti vse informacije o obdelavi na podlagi podatkov, zbranih in pridobljenih z obdelavo posnetih glasov, na voljo tudi uporabnikom.

66. Upravljavci VGP bi morali zagotoviti preglednost informacij, ki jih VGP lahko pridobi o svoji okolici, kot so med drugim druge osebe v prostoru, glasba, ki se predvaja v ozadju, kakršna koli obdelava glasu iz medicinskih ali tržnih razlogov, hišne živali itd.

3.4 Omejitev namena in pravna podlaga

67. Obravnava glasovnih zahtev s strani VGP ima jasen namen, tj. izvršitev zahteve. Vendar pogosto obstajajo dodatni nameni, ki niso tako očitni, kot je izboljšanje sposobnosti razumevanja naravnega jezika VGP, pri čemer se model VGP nadgrajuje s tehnikami strojnega učenja. Med najpogostejšimi nameni obdelave osebnih podatkov VGP so:

- izvrševanje zahtev uporabnikov;
- izboljšanje VGP z nadgradnjo modela strojnega učenja ter človeškim pregledom in označevanjem glasovnih prepisov;
- identifikacija uporabnika (uporaba glasovnih podatkov);
- oblikovanje profilov uporabnikov za prilagojenost vsebin ali oglasov.

68. VGP zaradi svoje vloge posrednikov in načina zasnove obdelujejo veliko različnih osebnih in neosebnih podatkov. To omogoča obdelavo osebnih podatkov za številne namene, ki presegajo odzivanje na zahteve uporabnikov in bi lahko bili popolnoma neopaženi. Z analizo podatkov, zbranih prek VGP, je mogoče poznati ali izluščiti zanimanja uporabnikov, njihove urnike, poti vožnje ali navade. S tem bi se lahko osebni podatki obdelovali v nepredvidene

namene (na primer analiza razpoloženja ali ocena zdravstvenega stanja[26]), kar bi bilo daleč od tega, kar bi uporabnik lahko upravičeno pričakoval.

69. Upravljavci podatkov morajo jasno opredeliti svoj(-e) namen(-e) v zvezi z okoliščinami, v katerih se VGP uporablja, tako da jih posamezniki, na katere se nanašajo osebni podatki, jasno razumejo (na primer predstavitev namenov v kategorijah). V skladu s členom 5(1) Splošne uredbe o varstvu podatkov je treba osebne podatke zbirati za določene, izrecne in zakonite namene ter se ne smejo nadalje obdelovati na način, ki ni združljiv s temi nameni.

3.4.1 Izvrševanje zahtev uporabnikov

70. VGP se v glavnem uporablja tako, da se izrečejo glasovni ukazi, ki jih mora izvršiti VGP ali povezana aplikacija ali storitev (na primer storitev pretakanja glasbe, storitev kartiranja ali elektronska ključavnica). Zato se lahko obdelajo podatki, kot so glas uporabnika in morebitni drugi podatki (na primer položaj uporabnika, ko želi informacije o poti do določenega kraja).

> Primer 6:
>
> Potnik v pametnem avtomobilu z vgrajenim VGP izreče zahtevo za pot do najbližje bencinske postaje. VGP obdela glas uporabnika, da bi razumel ukaz, in položaj avtomobila, da najde pot, ter jo pošlje pametnemu sestavnemu delu, da jo prikaže na zaslonu avtomobila.

71. Če obdelava glasovnih ukazov vključuje shranjevanje ali dostop do podatkov, shranjenih na terminalskih napravah končnega uporabnika, je treba upoštevati člen 5(3) Direktive o zasebnosti in elektronskih komunikacijah. Člen 5(3) vključuje splošno načelo, da je za tako shranjevanje ali dostop potrebno predhodno soglasje končnega uporabnika, določa pa tudi izjemo od zahteve po privolitvi, kadar je to „nujno potrebno za zagotovitev storitve informacijske družbe, ki jo naročnik ali uporabnik izrecno zahtevata“. Če se glasovni podatki obdelujejo za izvršitev zahtev uporabnika, so izvzeti iz zahteve po predhodni privolitvi.

72. Kot je bilo že navedeno, morajo imeti vsi postopki obdelave osebnih podatkov, ki sledijo shranjevanju podatkov na terminalski napravi končnih uporabnikov ali dostopu do njih, pravno podlago v skladu s členom 6 Splošne uredbe o varstvu podatkov, da so zakoniti.

73. V VGP potekata dva zaporedna postopka obdelave. Kot je navedeno zgoraj, prva zahteva dostop do VGP (zato morajo biti izpolnjeni pogoji iz člena 5(3) Direktive o zasebnosti in elektronskih komunikacijah). Za ta drugi korak se poleg pogojev iz člena 5(3) Direktive o zasebnosti in elektronskih komunikacijah zahteva tudi pravna podlaga v skladu s členom 6 Splošne uredbe o varstvu podatkov.

74. Kadar se posameznik odloči za uporabo VGP, to na splošno pomeni, da mora kot začetni uporabnik najprej registrirati račun za aktiviranje VGP. Povedano drugače, to se nanaša na pogodbeno razmerje[27] med registriranim uporabnikom in upravljavcem VGP. Glede na vsebino in temeljni cilj te pogodbe je njen glavni namen uporaba VGP za izpolnitev uporabnikove zahteve za pomoč.

[26] Eoghan Furey, Juanita Blue, “Alexa, Emotion, Privacy and GDPR”, Conference paper, Human Computer Interaction Conference, julij 2018.

[27] Če je *„pogodba veljavna v skladu z veljavnim nacionalnim pogodbenim pravom“*, izvleček iz Smernic št. 2/2019 o obdelavi osebnih podatkov na podlagi člena 6(1)(b) Splošne uredbe o varstvu podatkov v okviru zagotavljanja spletnih storitev posameznikom, na katere se nanašajo osebni podatki (v nadaljevanju: Smernice 2/2019), točka 26.

75. Vsaka obdelava osebnih podatkov, ki je potrebna za izvršitev uporabnikove zahteve, se lahko opira na pravno podlago za izvajanje pogodbe[28]. Taka obdelava vključuje zlasti zajetje uporabnikove glasovne zahteve, prepis te zahteve v besedilo, njeno razlago, informacije, izmenjane z viri znanja za pripravo odgovora, in nato prepis v glasovni končni odgovor, s čimer se konča uporabnikova zahteva.

76. Izvajanje pogodbe je lahko pravna podlaga za obdelavo osebnih podatkov s pomočjo strojnega učenja, kadar je to potrebno za zagotavljanje storitve. Obdelava osebnih podatkov z uporabo strojnega učenja za druge namene, ki niso potrebni, kot je izboljšanje storitev, se ne bi smela opirati na to pravno podlago.

77. Navsezadnje se ne sme zamenjevati pravnih podlag za izvajanje pogodbe in privolitev na podlagi Splošne uredbe o varstvu podatkov. Soglasje, dano za sklenitev pogodbe, tj. strinjanje s pogodbo, je del veljavnosti te pogodbe in se ne nanaša na poseben pomen privolitve v skladu s Splošno uredbo o varstvu podatkov[29].

78. Pri uporabi VGP predhodna konfiguracija uporabniškega računa v VGP ni potrebna, privolitev pa bi lahko bila možna pravna podlaga.

3.4.2 Izboljšanje VGP z usposabljanjem sistemov strojnega učenja in ročnim pregledom glasovnega sporočila in prepisov

79. Človeški govor ima zelo veliko naglasov in različic. Vse VGP delujejo tudi zunaj okvira, vendar se lahko njihova učinkovitost izboljša, če se prilagodijo posebnim značilnostim govora uporabnikov. Kot je navedeno v oddelku 2.6, ta postopek prilagajanja temelji na metodah strojnega učenja in je sestavljen iz dveh procesov: dodajanja novih podatkov v nabor podatkov za usposabljanje VGP, zbranih od njegovih uporabnikov, in človeškim pregledom podatkov, obdelanih za izvršitev dela zahtev.

> Primer 7:
>
> Uporabnik VGP mora trikrat ponoviti isti glasovni ukaz, ker ga VGP ne razume. Trije glasovni ukazi in z njimi povezani prepisi se pošljejo pregledovalcem, ki pregledajo in popravijo prepise. Glasovni ukazi in pregledani prepisi se dodajo v nabor podatkov za usposabljanje VGP, da se izboljša njegovo delovanje.

80. Dejavnosti obdelave v tem primeru ne bi smele šteti za (nujno) „*potrebne za izvajanje pogodbe*“ v smislu člena 6(1)(b) Splošne uredbe o varstvu podatkov, zato je zanje potrebna druga pravna podlaga iz člena 6 Splošne uredbe o varstvu podatkov. Glavni razlog za to je, da so VGP že funkcionalni, ko jih uporabnik vzame iz embalaže, in že delujejo, kot je (nujno) potrebno za izpolnitev pogodbe. Evropski odbor za varstvo podatkov meni, da člen 6(1)(b) na splošno ne bi bil ustrezna zakonita podlaga za obdelavo za namene izboljšanja storitve ali razvoja novih funkcij v okviru obstoječe storitve. V večini primerov uporabnik sklene pogodbo zaradi uporabe obstoječe storitve. Čeprav je lahko možnost izboljšav in sprememb storitve redno vključena v pogodbene določbe, take obdelave običajno ni mogoče šteti za objektivno potrebno za izpolnjevanje pogodbe z uporabnikom.

[28] V skladu s Smernicami 2/2019, v katerih je tudi navedeno, da se Mnenje št. 6/2014 še naprej upošteva za člen 6(1)(b) in Splošna uredba o varstvu podatkov (glej zlasti strani 11, 16, 17, 18 in 55 v Mnenju št. 6/2014).
[29] Glej Smernice 2/2019, točke 18, 19, 20, 21 in 27.

3.4.3 Identifikacija uporabnika[30] (uporaba glasovnih podatkov)

81. Uporaba glasovnih podatkov za identifikacijo uporabnika pomeni obdelavo biometričnih podatkov, kot je opredeljena v členu 4(14) Splošne uredbe o varstvu podatkov. Zato bo moral upravljavec podatkov poleg opredelitve pravne podlage v skladu s členom 6 Splošne uredbe o varstvu podatkov opredeliti izjemo v skladu z njenim členom 9.[31]

82. Med izjemami, navedenimi v členu 9 Splošne uredbe o varstvu podatkov, se za ta posebni namen dozdevno uporablja samo izrecna privolitev posameznikov, na katere se nanašajo osebni podatki.

83. Ker pa ta namen zahteva uporabo posebne pravne ureditve iz člena 9 Splošne uredbe o varstvu podatkov, sledijo dodatne podrobnosti v oddelku 3.8, ki se nanaša na obdelavo posebnih vrst podatkov.

3.4.4 Oblikovanje profilov uporabnikov za prilagojenost vsebin ali oglasov

84. Kot je navedeno zgoraj, imajo VGP dostop do vsebine vseh glasovnih ukazov, tudi če so namenjeni storitvam, ki jih zagotavljajo tretje osebe. Ta dostop bi oblikovalcu VGP omogočil izdelavo zelo natančnih uporabniških profilov, ki bi se lahko uporabljali za omogočanje prilagojenih storitev ali oglasov.

> Primer 8:
>
> Vsakič, ko uporabnik VGP opravi internetno iskanje, VGP doda oznake za teme, ki so zanimive za uporabniški profil. Rezultati vsakega novega iskanja se ob upoštevanju teh oznak prikažejo uporabniku v vrstnem redu.
>
> Primer 9:
>
> Vsakič, ko uporabnik VGP opravi spletni nakup v e-trgovini, VGP shrani zapis naročila za nakup. Ponudnik VGP tretjim osebam omogoča, da ciljno usmerjene oglase usmerijo na uporabnika VGP na podlagi preteklih nakupov.

85. Prilagojenost vsebine je lahko (vendar ne vedno) sestavni in pričakovani element VGP. To, ali se taka obdelava lahko šteje za neločljiv vidik storitve VGP, je odvisno od narave opravljene storitve, pričakovanj povprečnega posameznika, na katerega se nanašajo osebni podatki, in sicer ne le glede pogojev storitve, temveč tudi glede načina, kako se storitev promovira uporabnikom, in ali se lahko storitev opravi brez prilagoditve.[32]

---

[30] Tehnično je treba pojem identifikacije razlikovati od preverjanja (avtentikacija). Identifikacija je iskanje in primerjava „eden proti mnogim“ (1 : N) ter načeloma potrebuje zbirko podatkov, v kateri je navedenih več posameznikov. Pri obdelavi za namene preverjanja pa gre za primerjavo ena proti ena (1 : 1) in se uporablja za preverjanje in potrditev z biometrično primerjavo, ali je posameznik ista oseba kot oseba, od katere izvirajo biometrični podatki. Po podatkih Evropskega odbora za varstvo podatkov se VGP na trgu opirajo izključno na uporabo tehnologij za identifikacijo govorcev.

[31] Po Splošni uredbi o varstvu podatkov zgolj narava podatkov ne zadostuje vedno za ugotovitev, ali ti štejejo za posebne vrste podatkov, saj podatki pri obdelavi *„fotografij […] spadajo v opredelitev biometričnih podatkov le, kadar so obdelane s posebnimi tehničnimi sredstvi, ki omogočajo edinstveno identifikacijo ali avtentikacijo posameznika.*“ (uvodna izjava 51). Enako razlogovanje velja za glas.

[32] Glej tudi Smernice 2/2019, odstavek 57.

86. Kadar se prilagoditev izvede v okviru pogodbenega razmerja in kot del storitve, ki jo izrecno zahteva končni uporabnik (in je obdelava omejena na to, kar je nujno potrebno za zagotavljanje te storitve), lahko taka obdelava temelji na členu 6(1)(b) Splošne uredbe o varstvu podatkov.

87. Če obdelava ni nujno *„potrebna za izvajanje pogodbe*" v smislu člena 6(1)(b) Splošne uredbe o varstvu podatkov, mora ponudnik VGP načeloma pridobiti privolitev posameznika, na katerega se nanašajo osebni podatki. Ker bo privolitev namreč na podlagi člena 5(3) Direktive o zasebnosti in elektronskih komunikacijah potrebna za shranjevanje podatkov ali pridobitev dostopa do njih (glej točke od 28 do 29 zgoraj), bo privolitev na podlagi člena 6(1)(a) Splošne uredbe o varstvu podatkov načeloma tudi ustrezna pravna podlaga za obdelavo osebnih podatkov, ki sledi navedenim dejanjem, saj bi lahko sklicevanje na legitimni interes v nekaterih primerih ogrozilo dodatno raven varstva iz člena 5(3) Direktive o zasebnosti in elektronskih komunikacijah.

88. Glede oblikovanja profilov uporabnikov za oglaševanje je treba opozoriti, da ta namen nikoli ne šteje za storitev, ki jo izrecno zahteva končni uporabnik. Zato bi bilo treba v primeru obdelave v ta namen sistematično zbirati privolitve uporabnikov.

Priporočila

89. Uporabnike bi bilo treba obvestiti o namenu obdelave osebnih podatkov, ta namen pa bi moral biti v skladu z njihovimi pričakovanji glede naprave, ki so jo kupili. V primeru VGP je jasno, da je ta namen – z vidika uporabnika – obdelava uporabnikovega glasu izključno za razlago njegove izrečene poizvedbe in zagotavljanje smiselnih odgovorov (ne glede na to, ali gre za odgovore na poizvedbo ali druge odzive, kot je daljinsko upravljanje stikala).

90. Kadar obdelava osebnih podatkov temelji na privolitvi, bi morala biti taka privolitev *„dana za ‚enega ali več določenih namenov' in da ima posameznik, na katerega se nanašajo osebni podatki, izbiro v zvezi z vsakim od njih*". Poleg tega *„mora upravljavec, ki želi pridobiti privolitev za različne namene, zagotoviti ločene možnosti privolitve za vsak namen, da uporabnikom omogoči, da dajo konkretno privolitev za določene namene."*[33] Uporabniki bi na primer morali imeti možnost, da ločeno privolijo v ročno pregledovanje in označevanje glasovnih prepisov ali uporabo svojih glasovnih podatkov za identifikacijo oziroma avtentikacijo uporabnika (glej oddelek 3.7).

3.5 Obdelava podatkov otrok

91. Tudi otroci lahko komunicirajo z VGP ali ustvarijo lastne profile, povezane s profili odraslih. Nekateri VGP so vgrajeni v naprave, ki so posebej namenjene otrokom.

92. Kadar je pravna podlaga za obdelavo izvajanje pogodbe, so pogoji za obdelavo podatkov otrok odvisni od nacionalnega pogodbenega prava.

93. Kadar je pravna podlaga za obdelavo privolitev in v skladu s členom 8(1) Splošne uredbe o varstvu podatkov je obdelava podatkov otrok zakonita le,*„kadar ima otrok vsaj 16 let*. *Kadar je otrok mlajši od 16 let, je takšna obdelava zakonita le, če in kolikor takšno privolitev da ali odobri nosilec starševske odgovornosti za otroka.*" Zato bi bilo treba v primerih, ko je privolitev pravna podlaga, za skladnost s Splošno uredbo o varstvu podatkov od staršev ali skrbnikov

[33] Glej Smernice Evropskega odbora za varstvo podatkov št. 05/2020 o privolitvi na podlagi Uredbe 2016/679, sprejete 4. maja 2020, oddelek 3.2.

pridobiti izrecno dovoljenje za zbiranje, obdelavo in shranjevanje podatkov otrok (glas, dobesedni zapisi itd.).

94. Starševski nadzor je deloma na voljo, vendar v sedanji obliki ni uporabniku prijazen (na primer treba se je prijaviti v novo storitev) ali ima omejene zmogljivosti. Upravljavci podatkov bi morali vlagati v razvoj sredstev za starše ali skrbnike za nadzor nad uporabo VGP s strani otrok.

3.6 Hramba podatkov

95. VGP obdelujejo in ustvarjajo veliko različnih osebnih podatkov, kot so glas, prepisi glasov, metapodatki ali sistemski dnevniki. Te vrste podatkov bi se lahko obdelovale za najrazličnejše namene, kot so zagotavljanje storitve, izboljšanje obdelave naravnega jezika, prilagoditev ali znanstvene raziskave. V skladu z načelom omejitve shranjevanja podatkov iz Splošne uredbe o varstvu podatkov bi morali VGP podatke hraniti le toliko časa, kolikor je potrebno za namene, za katere se osebni podatki obdelujejo. Zato bi morala biti obdobja hrambe podatkov vezana na različne namene obdelave. Ponudniki storitev VGP ali tretje osebe, ki zagotavljajo storitve prek VGP, bi morali oceniti najdaljše obdobje hrambe za vsak sklop in namen podatkov.

96. Z načelom omejitve shranjevanja podatkov je tesno povezano načelo najmanjšega obsega podatkov. Upravljavci podatkov morajo omejiti obdobje hrambe podatkov, vendar tudi vrsto in količino podatkov.

97. Upravljavci podatkov bi si morali med drugim postaviti naslednja vprašanja: Ali je treba shraniti vse glasovne posnetke ali vse prepise, da se doseže namen X? Ali je treba po shranitvi zapisa shraniti tudi glasovne podatke? Če je odgovor da, za kakšen namen? Kako dolgo so glasovni podatki ali podatki zapisa potrebni za posamezen namen? V odgovoru na ta in druga podobna vprašanja bodo opredeljena obdobja hrambe, ki bi morala biti zajeta v informacijah, ki so na voljo posameznikom, na katere se nanašajo osebni podatki.

98. Nekateri VGP privzeto shranjujejo osebne podatke, kot so glasovni izrezki ali prepisi, za nedoločen čas, hkrati pa uporabnikom zagotavljajo sredstva za brisanje takih podatkov. Hramba osebnih podatkov za nedoločen čas je v nasprotju z načelom omejitve hrambe. Zagotavljanje sredstev posameznikom, na katere se nanašajo osebni podatki, za izbris njihovih osebnih podatkov ne pomeni, da upravljavec podatkov ni odgovoren za opredelitev in izvrševanje politike hrambe podatkov.

99. Pri zasnovi VGP je treba upoštevati, da morajo uporabniki imeti nadzor, da lahko izbrišejo svoje osebne podatke v svojih napravah in v vseh sistemih oddaljenega shranjevanja. Tak nadzor je lahko potreben za reševanje različnih vrst zahtevkov uporabnikov, na primer zahteve za izbris ali preklic predhodno dane privolitve. Pri zasnovi nekaterih VGP ta zahteva ni bila upoštevana.[34]

100. Kot v drugih kontekstih bodo upravljavci podatkov morda morali hraniti osebne podatke kot dokaz o storitvi, ki se zagotavlja uporabniku za izpolnitev pravne obveznosti. Upravljavec podatkov lahko na tej podlagi hrani osebne podatke. Vendar bi morali podatki ostati hranjeni v najmanjšem obsegu, ki je potreben za izpolnitev take pravne obveznosti, in za najkrajše mogoče obdobje. Seveda se podatki, ki se hranijo zaradi izpolnjevanja pravne obveznosti, ne

[34] Glej Amazonov dopis z dne 28. junija 2019 v odgovor senatorju ZDA Christopherju Coonsu: https://www.coons.senate.gov/imo/media/doc/Amazon%20Senator%20Coons__Response%20Letter__6.28.19[3].pdf.

bi smeli uporabljati za druge namene brez pravne podlage v skladu s členom 6 Splošne uredbe o varstvu podatkov.

> Primer 10:
>
> Uporabnik kupi televizor v storitvi e-trgovine, pri čemer uporabi glasovni ukaz za VGP. Tudi če uporabnik pozneje zahteva izbris svojih podatkov, bi lahko ponudnik ali razvijalec VGP še vedno hranil nekatere podatke na podlagi svoje pravne obveznosti, določene z davčnim predpisom, da hrani dokaze o nakupu. Vendar podatki, shranjeni za ta namen, ne bi smeli presegati najmanjšega obsega, potrebnega za izpolnitev pravne obveznosti, in jih brez pravne podlage v skladu s členom 6 Splošne uredbe o varstvu podatkov ne bi bilo mogoče obdelovati za noben drug namen.

101. Kot je navedeno v oddelku 2, se zmogljivost prepoznavanja glasu VGP izboljšuje z nadgradnjo sistemov strojnega učenja s podatki uporabnikov. Če uporabniki ne privolijo v uporabo svojih podatkov za ta namen ali tako privolitev umaknejo, njihovih podatkov ni mogoče zakonito uporabiti za nadgradnjo drugih modelov in bi jih moral upravljavec podatkov izbrisati, če ne obstaja namen, ki bi upravičeval nadaljnjo hrambo. Vendar obstajajo dokazi, da pri nekaterih modelih strojnega učenja obstaja tveganje za vnovično identifikacijo.[35]

102. Upravljavci in obdelovalci podatkov bi morali uporabljati modele, ki ne omejujejo njihove zmožnosti, da ustavijo obdelavo, če posameznik prekliče svojo privolitev, prav tako pa ne bi smeli uporabljati modelov, ki omejujejo njihovo zmožnost za olajšanje pravic posameznikov, na katere se nanašajo osebni podatki. Upravljavci in obdelovalci bi morali izvajati blažilne ukrepe za zmanjšanje tveganja vnovične identifikacije na sprejemljivo mejno vrednost.

103. Če uporabnik prekliče svojo privolitev, se podatki, zbrani od uporabnika, ne morejo več uporabljati za nadaljnjo nadgradnjo modela. Vendar modela, ki je bil predhodno usposobljen za uporabo teh podatkov, ni treba izbrisati. Evropski odbor za varstvo podatkov kljub vsemu poudarja, da obstajajo dokazi, da lahko pri nekaterih modelih strojnega učenja pride do razkritja osebnih podatkov. Več študij je zlasti pokazalo, da se lahko izvedejo rekonstrukcija in napadi z motnjami podatkovnih sklopov, kar napadalcem omogoča, da pridobijo informacije o posameznikih.[36] Upravljavci in obdelovalci podatkov bi zato morali izvajati blažilne ukrepe za zmanjšanje tveganja vnovične identifikacije na sprejemljivo mejno vrednost, da bi zagotovili, da uporabljajo modele, ki ne vsebujejo osebnih podatkov.

104. Na posameznike, na katere se nanašajo osebni podatki, se ne bi smelo vplivati tako, da privolijo v hrambo njihovih podatkov za nedoločen čas. Brisanje shranjenih glasovnih podatkov ali prepisov lahko vpliva na učinkovitost storitve, vendar bi bilo treba tak vpliv uporabnikom pojasniti jasno in merljivo. Ponudniki storitev VGP bi se morali izogibati podajanju splošnih izjav o poslabšanju storitve, če se izbrišejo osebni podatki.

105. Anonimizacija zvočnih posnetkov je posebej zahtevna, saj je mogoče uporabnike identificirati z vsebino sporočila in značilnostmi glasu. Kljub temu se izvajajo nekatere raziskave[37] o

[35] Veale Michael, Binns Reuben in Edwards Lilian 2018 „Algorithms that remember: model inversion attacks and data protection law“ Phil. Trans. R. Soc. A.37620180083, doi: 10.1098/rsta.2018.0083

[36] N. Carlini idr., “Extracting Training Tata form Lare Language Models”, december 2020.

[37] Glej na primer VoicePrivacy (https://www.voiceprivacychallenge.org), pobudo za razvoj rešitev za varstvo zasebnosti za govorno tehnologijo.
Glej tudi odprtokodna orodja za anonimizacijo glasov, ki so bila razvita v okviru raziskovalnega in inovacijskega projekta COMPRISE v okviru programa Obzorje 2020: https://gitlab.inria.fr/comprise/voice_transformation.

tehnikah, ki bi lahko omogočile odstranjevanje situacijskih informacij, kot je šum ozadja, in anonimiziranje glasu.

Priporočila

106. Z vidika uporabnika je glavni namen obdelave njegovih podatkov poizvedovanje in prejemanje odzivov in/ali sprožitev dejanj, kot so igranje glasbe ali vklop ali izklop luči. Po odgovoru na poizvedbo ali izvršitvi ukaza bi bilo treba osebne podatke izbrisati, razen če ima oblikovalec ali razvijalec VGP veljavno pravno podlago za njihovo hrambo za določen namen.

107. Preden se šteje, da je anonimizacija sredstvo za izpolnitev načela omejitve shranjevanja podatkov, bi morali ponudniki in razvijalci VGP preveriti, ali postopek anonimizacije povzroči neprepoznavnost glasu.

108. Privzete konfiguracije bi morale te zahteve odražati tako, da bi privzeto shranjevale najmanjši možen obseg uporabniških informacij. Če so te možnosti vsebovane kot del čarovnika za nastavitev, bi se to moralo odražati v privzeti nastavitvi, vse možnosti pa bi morale biti predstavljene kot enakovredne in brez vizualne diskriminacije.

109. Kadar ponudnik ali razvijalec VGP med postopkom pregleda zazna zapis, ki izvira iz aktivacije, do katere je prišlo pomotoma, je treba zapis in vse povezane podatke takoj izbrisati ter se ne smejo uporabiti za noben namen.

3.7 Varnost

110. Za varno obdelavo osebnih podatkov bi morali VGP varovati njihovo zaupnost, celovitost in razpoložljivost. Poleg tveganj, ki izhajajo iz elementov ekosistema VGP, uporaba glasu kot komunikacijskega sredstva ustvarja nov sklop varnostnih tveganj.

111. VGP so večuporabniški. Omogočajo lahko več kot enega registriranega uporabnika in vsakdo v njihovi okolici lahko izdaja ukaze ter uporablja njihove storitve. Vsaka storitev VGP, ki zahteva zaupnost, bo vključevala mehanizem za nadzor dostopa in avtentikacijo uporabnika. Brez nadzora dostopa bi lahko vsi, ki lahko VGP izdajajo glasovne ukaze, dostopali do osebnih podatkov uporabnikov, jih spremenili ali izbrisali (na primer zaprosili za prejeta sporočila, naslov uporabnika ali koledarske dogodke). Fizična bližina VGP za izdajanje glasovnih ukazov ni nujna, saj je VGP mogoče manipulirati, na primer prek oddajanja signalov[38] (na primer radijski ali televizijski signali). Nekaterih znanih metod za oddaljeno izdajanje ukazov VGP, kot so laserski[39] ali ultrazvočni (neslišni) valovi[40], s človeškimi čuti niti ni mogoče zaznati.

112. Avtentikacija uporabnika lahko temelji na enem ali več od naslednjih dejavnikov: nekaj, kar uporabnik ve (na primer geslo), nekaj, kar ima (na primer pametna kartica), ali njegova individualna značilnost (na primer glasovni vzorec). Podrobnejši pregled teh dejavnikov avtentikacije v okviru VGP kaže naslednje:

    - avtentikacija z uporabo nečesa, kar uporabnik ve, je problematična. Tajnost, ki bi uporabnikom omogočila, da izkažejo svojo identiteto, je treba izgovoriti na glas, s čimer se razkrije komur koli v okolici. Komunikacijski kanal VGP je okoliški zrak, vrsta kanala, ki ga

[38] X. Yuan idr., „All Your Alexa Are Belong to Us: A Remote Voice Control Attack against Echo“ 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dabi, Združeni arabski emirati, 2018, str. 1–6, doi: 10.1109/GLOCOM.2018.8647762.

[39] Glej na primer https://lightcommands.com.

[40] Glej na primer https://surfingattack.github.io.

ni mogoče dodatno zavarovati na način, kot je to mogoče pri tradicionalnih kanalih (na primer z omejitvijo dostopa do kanala ali šifriranjem njegove vsebine);

- za avtentikacijo z uporabo nečesa, kar uporabnik ima, bi morali ponudniki storitev VGP za dokazovanje identitete uporabnika ustvariti, razširjati in upravljati posebne „žetone“;
- avtentikacija z uporabo nečesa, kar je značilno za uporabnika samega, pomeni uporabo biometričnih podatkov za namene edinstvene identifikacije fizične osebe (glej oddelek 3.7 spodaj).

113. Uporabniški računi VGP so povezani z napravami, v katerih se opravlja storitev. Za upravljanje drugih storitev se pogosto uporablja isti račun, kot se uporablja za upravljanje VGP. Lastniki mobilnega telefona Android in zvočnika Google Home lahko na primer svoj Googlov račun povežejo z obema napravama, kar večinoma tudi naredijo. Večina VGP ne zahtevajo ali omogočajo mehanizma za identifikacijo ali avtentikacijo, če ima naprava, ki zagotavlja storitev VGP, samo en uporabniški račun.

114. Če je z napravo povezanih več uporabniških računov, nekateri VGP ponujajo neobvezni osnovni nadzor dostopa v obliki številke PIN brez prave avtentikacije uporabnika. Nekateri drugi VGP imajo možnost, da kot mehanizem identifikacije uporabijo prepoznavanje glasovnih vzorcev.

115. Čeprav identifikacija ali avtentikacija uporabnika nista vedno potrebni za dostop do vseh storitev VGP, za nekatere zagotovo sta. Brez mehanizma identifikacije ali avtentikacije lahko vsakdo dostopa do podatkov drugih uporabnikov in jih po želji spremeni ali izbriše. Vsaka oseba v bližini pametnega zvočnika bi lahko na primer izbrisala sezname predvajanja drugih uporabnikov iz storitve pretakanja glasbe, ukaze iz zgodovine ukazov ali stike s seznama stikov.

116. Večina VGP v celoti zaupa svojim lokalnim omrežjem. Vsaka ogrožena naprava v istem omrežju bi lahko spremenila nastavitve pametnega zvočnika ali omogočila namestitev zlonamerne programske opreme ali povezala lažne aplikacije/spretnosti brez uporabnikovega vedenja ali soglasja.[41]

117. VGP so tako kot vsaka druga programska oprema izpostavljeni ranljivosti. Vendar bi lahko zaradi koncentracije na trgu VGP[42] vsaka taka ranljivost vplivala na milijone uporabnikov VGP. Če VGP deluje v skladu s sedanjo zasnovo, storitvi oblaka za prepoznavanje govora ne pošlje nobenih informacij, dokler ne zazna aktivacijskega izraza. Vendar bi lahko zaradi ranljivosti programske opreme napadalec zaobšel nastavitve in varnostne ukrepe VGP. Tako bi lahko na primer pridobil kopijo vseh podatkov, poslanih v oblak VGP, in jih posredoval strežniku, ki ga nadzoruje napadalec.

118. Podatki, ki jih VGP zakonito obdelujejo ali pridobivajo, omogočajo oblikovanje precej točnega profila njihovih uporabnikov, saj VGP pozna ali lahko na podlagi sklepanja prepozna lokacijo, odnose in zanimanja svojih uporabnikov. VGP so čedalje bolj prisotni v domovih in pametnih telefonih. Ta pojav povečuje tveganje za množični nadzor in množično profiliranje. Zato bi

[41] Glej na primer Deepak Kumar idr., *Skill Squatting Attacks on Amazon Alexa*, USENIX Security Symposium, avgust 2018, https://www.usenix.org/conference/usenixsecurity18/presentation/kumar.
Security Research Labs, *Smart Spies: Alexa and Google Home expose users to vishing and* eavesdropping, November 2019, https://srlabs.de/bites/smart-spies.

[42] Na trgu VGP je trenutno manj kot dvanajst ponudnikov storitev.

morali biti varnostni ukrepi za varstvo podatkov med tranzitom in v mirovanju ter v napravah in v oblaku kos tem tveganjem.

119. Čedalje večja uporaba VGP v povezavi z neustrezno uravnoteženimi pravicami do dostopa s strani organov kazenskega pregona bi lahko povzročila odvračilni učinek, ki bi ogrozil temeljne pravice, kot je svoboda govora.

120. Organi kazenskega pregona v EU[43] in zunaj EU[44] so že izrazili zanimanje za dostop do glasovnih izrezkov, ki so jih posneli VGP. Dostop do podatkov, ki jih VGP obdelujejo ali pridobivajo v EU, bi moral biti skladen z veljavnim okvirom EU za ureditev varstva podatkov in zasebnosti. Če nekatere države članice razmišljajo o sprejetju posebne zakonodaje, ki omejuje temeljni pravici do zasebnosti in varstva podatkov, bi morale biti take omejitve vedno skladne z zahtevo iz člena 23 Splošne uredbe o varstvu podatkov[45].

121. Med VGP je običajno, da zvočne posnetke in povezane podatke za izboljšanje kakovosti storitev VGP pregleda človek. Zaradi občutljive narave podatkov, ki jih obdelujejo ti pregledovalci, in dejstva, da se ta postopek pogosto odda obdelovalcu, ki je podizvajalec, je zelo pomembno, da se uvedejo ustrezni varnostni ukrepi.

Priporočila

122. Oblikovalci in razvijalci aplikacij VGP bi morali uporabnikom zagotoviti varne in najsodobnejše postopke avtentikacije.

123. Pregledovalci morajo vedno prejeti le nujno potrebne in psevdonimizirane podatke. Pravni sporazumi, ki urejajo pregled, bi morali izrecno prepovedati vsako obdelavo, ki bi lahko privedla do identifikacije posameznika, na katerega se nanašajo osebni podatki.

124. Če VGP omogoča klice v sili, bi bilo treba zagotoviti čas[46] neprekinjene razpoložljivosti VGP.

3.8 Obdelava posebnih vrst podatkov

125. Kot je bilo navedeno, imajo VGP dostop do intimnih informacij, ki jih je mogoče zaščititi v skladu s členom 9 Splošne uredbe o varstvu podatkov (glej oddelek 3.7.1), kot so biometrični podatki (glej oddelek 3.7.2). Zato morajo oblikovalci in razvijalci VGP natančno opredeliti, v katerih primerih obdelava vključuje posebne vrste podatkov.

3.8.1 Splošni vidiki pri obdelavi posebnih vrst podatkov

126. VGP lahko obdelujejo posebne vrste podatkov v različnih okoliščinah:

- kot del lastnih storitev VGP, na primer pri upravljanju zdravniških obiskov na koledarjih uporabnikov;
- kadar ponudniki VGP delujejo kot vmesnik za storitve tretjih oseb, obdelajo vsebino ukazov. Ponudniki VGP bi lahko glede na vrsto storitve, ki jo zahteva uporabnik, obdelali

[43] Glej na primer https://www.ft.com/content/ad765972-87a2-11e9-a028-86cea8523dc2.
[44] Glej na primer https://cdt.org/insights/alexa-is-law-enforcement-listening.
[45] Glej tudi Smernice Evropskega odbora za varstvo podatkov št. 10/2020 o omejitvah na podlagi člena 23 Splošne uredbe o varstvu podatkov.
[46] Čas, ko lahko naprava ali storitev delujeta brez nadzora, ne da bi prišlo do zrušitve ali bi ju bilo treba vnovič zagnati iz skrbniških ali vzdrževalnih namenov.

posebne kategorije podatkov. Eden od primerov je, ko uporabnica da ukaz VGP, naj uporabi aplikacijo tretje strani, s katero spremlja svojo ovulacijo;[47]

- kadar se glasovni podatki uporabljajo za namene edinstvene identifikacije uporabnika, kot je prikazano spodaj.

3.8.2 Splošni premisleki pri obdelavi biometričnih podatkov

127. Nekateri VGP imajo zmožnost edinstvene identifikacije svojih uporabnikov zgolj na podlagi njihovega glasu. Ta proces se imenuje prepoznavanje glasovnega modela. VGP med registracijsko fazo prepoznavanja glasu obdela glas uporabnika, da ustvari glasovni model (ali glasovni odtis). VGP lahko med vsakdanjo uporabo izračuna glasovni model katerega koli uporabnika in ga primerja z registriranimi modeli, da edinstveno identificira uporabnika, ki je izvedel ukaz.

> Primer 11:
>
> Skupina uporabnikov je v VGP vzpostavila možnost uporabe prepoznavanja modela govora. Nato vsak od njih registrira svoj glasovni model.
>
> Eden od uporabnikov pozneje zahteva dostop VGP do sestankov na njegovem dnevnem redu. Ker je za dostop do dnevnega reda potrebna identifikacija uporabnika, VGP ekstrahira model iz glasu zahteve, izračuna njegov glasovni model in preveri, ali se ujema z registriranim uporabnikom in ali ima ta uporabnik dostop do dnevnega reda.

128. V zgornjem primeru prepoznavanje uporabnikovega glasu na podlagi glasovnega modela pomeni obdelavo posebnih vrst osebnih podatkov v smislu člena 9 Splošne uredbe o varstvu podatkov (obdelava biometričnih podatkov za namene edinstvene identifikacije posameznika).[48] Za obdelavo biometričnih podatkov za namene identifikacije uporabnika, kot se zahteva v zgornjem primeru, bo potrebna izrecna privolitev zadevnih posameznikov, na katere se nanašajo osebni podatki (člen 9(2)(a) Splošne uredbe o varstvu podatkov). Zato morajo upravljavci podatkov pri pridobivanju privolitve uporabnikov izpolnjevati pogoje iz člena 7 in upoštevati pojasnilo v uvodni izjavi (32) Splošne uredbe o varstvu podatkov ter ponuditi alternativno metodo identifikacije biometričnim podatkom glede na prostovoljnost privolitve.

129. Pri uporabi glasovnih podatkov za biometrično identifikacijo ali avtentikacijo morajo upravljavci podatkov zagotoviti preglednost glede tega, kje se uporablja biometrična identifikacija ter kako se zvočni odtisi (biometrični modeli) shranjujejo in širijo po napravah. Za izpolnitev te zahteve po preglednosti Evropski odbor za varstvo podatkov priporoča, da se odgovori na naslednja vprašanja:

- Ali aktiviranje identifikacije glasu na eni napravi samodejno aktivira to funkcijo na vseh drugih napravah, ki delujejo z istim računom?
- Ali se aktivacija identifikacije zvoka prek infrastrukture krmilnika VGP širi na naprave, ki so v lasti drugih uporabnikov?
- Kje se ustvarjajo, shranjujejo in primerjajo biometrični modeli?

[47] Glej na primer aplikacijo, ki je na voljo na: https://www.amazon.com/Ethan-Fan-Ovulation-Period-Tracker/dp/B07CRLSHKY.

- Ali so biometrični modeli dostopni ponudnikom VGP, razvijalcem ali drugim osebam?

130. Ko registrirani uporabnik nastavi VGP za identifikacijo glasu uporabnikov, se z namenom edinstvene identifikacije obdelajo tudi glasovi neregistriranih in nenačrtovanih uporabnikov.

131. Dejansko odkrivanje glasu pravega govorca vključuje tudi primerjavo glasu drugih ljudi v bližini glasovnega pomočnika. Povedano drugače, funkcija prepoznavanja govorcev, ki se uporablja v glasovnih pomočnikih, lahko zahteva snemanje glasovne biometrije ljudi, ki živijo v istem gospodinjstvu, da bi lahko prepoznala glasovne značilnosti tistih oseb, ki želijo, da se njihov glas prepozna. Tako lahko biometrična identifikacija tudi za osebe, ki niso obveščene, opravi biometrično obdelavo, tako da registrira njihov model in ga primerja z modelom uporabnika, ki želi biti prepoznan.

132. Da bi preprečili tako zbiranje biometričnih podatkov brez vednosti posameznikov, na katere se nanašajo osebni podatki, hkrati pa bi pomočniku omogočili, da ga prepozna, bi bilo treba dati prednost rešitvam, ki temeljijo samo na podatkih uporabnika. Konkretno to pomeni, da se biometrično prepoznavanje aktivira samo ob vsaki uporabi na pobudo uporabnika in ne s stalno analizo glasov, ki jih sliši pomočnik. Za prisotne osebe bi se lahko na primer določila posebna ključna beseda ali vprašanje, da bi pridobili njihovo privolitev za sprožitev biometrične obdelave. Uporabnik lahko na primer reče „identifikacija“ ali pomočnik vpraša, „ali želite biti identificirani“, in počaka na pozitiven odgovor za aktivacijo obdelave biometričnih podatkov.

Primer 12:
Če želi uporabnik vzpostaviti biometrično avtentikacijo za dostop do nekaterih zaščitenih podatkov, kot je njegov bančni račun, lahko glasovni pomočnik sproži preverjanje govorca, ko ta zažene aplikacijo, in tako preveri njegovo identiteto.

Priporočila

133. Glasovni modeli bi morali biti ustvarjeni, shranjeni in primerjani izključno na lokalni napravi in ne v oddaljenih strežnikih.

134. Zaradi občutljivosti zvočnih odtisov bi bilo treba dosledno uporabljati standarde, kot je ISO/IEC 24745, in tehnike za zaščito biometričnih modelov[49].

135. Če VGP uporablja glasovno biometrično identifikacijo, bi morali ponudniki VGP:

- zagotoviti, da je identifikacija dovolj natančna, da lahko zanesljivo poveže osebne podatke s pravimi posamezniki, na katere se nanašajo osebni podatki;
- zagotoviti, da je natančnost enaka za vse skupine uporabnikov, in sicer s preverjanjem, da ni bistvene pristranskosti do različnih demografskih skupin.

3.9 Najmanjši obseg podatkov

[49] Glej na primer
Jain, Anil in Nandakumar, Karthik in Nagar, Abhishek. (2008). “*Biometric Template Security*”. EURASIP Journal on Advances in Signal Processing. 2008. 10.1155/2008/579416.
S. K. Jami, S. R. Chalamala in A. K. Jindal, "*Biometric Template Protection Through Adversarial Learning*" *2019 IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas (NV, ZDA), 2019, str. 1–6, doi: 10.1109/ICCE.2019.8661905.

136. Upravljavci bi morali čim bolj zmanjšati količino podatkov, ki se zbirajo neposredno ali posredno ter pridobijo z obdelavo in analizo, na primer ne izvajajo analize glasu uporabnika ali drugih zvočnih informacij, da bi pridobili informacije o njegovem duševnem stanju, morebitnih boleznih ali življenjskih okoliščinah.

137. Uvesti bi morali privzete nastavitve, ki omejujejo zbiranje in/ali obdelavo podatkov na najmanjšo potrebno količino, ki je nujna za opravljanje storitve.

138. Glede na lokacijo, kontekst uporabe in občutljivost mikrofona bi VGP lahko zbiral glasovne podatke tretjih oseb kot del šuma ozadja pri zbiranju glasu uporabnikov. Tudi če šum ozadja ne vključuje glasovnih podatkov, lahko še vedno vključuje podatke o razmerah, ki bi se lahko obdelali za pridobitev informacij o posamezniku (na primer lokacija).

Priporočila

139. Oblikovalci VGP bi morali premisliti o tehnologijah za brisanje šuma ozadja, da bi preprečili zapisovanje in obdelavo glasov iz ozadja in situacijskih informacij.

3.10 Odgovornost

140. Za vsako obdelavo, ki temelji na privolitvi, morajo biti upravljavci v skladu s členom 7(1) Splošne uredbe o varstvu podatkov sposobni dokazati privolitev posameznikov, na katere se nanašajo osebni podatki. Glasovni podatki se lahko uporabijo za odgovornost (na primer za dokazovanje privolitve). Obveznost hrambe takih glasovnih podatkov bi nato določale zahteve glede odgovornosti iz ustrezne posebne zakonodaje.

141. Evropski odbor za varstvo podatkov je pri ocenjevanju potrebe po oceni učinka v zvezi z varstvom podatkov določil merila[50], ki jih morajo organi za varstvo podatkov uporabiti pri oblikovanju seznamov dejanj obdelave, za katere je obvezna ocena učinka v zvezi z varstvom podatkov, in navedel primere obdelave, za katere je verjetno, da bo zanje potrebna ocena učinka v zvezi z varstvom podatkov. Zelo verjetno je, da storitve VGP spadajo v kategorije in pogoje, za katere je bila ugotovljena potreba po oceni učinka v zvezi z varstvom podatkov. Pri tem je treba upoštevati, ali lahko naprava opazuje, spremlja ali nadzoruje posameznike, na katere se nanašajo osebni podatki, ali izvaja obsežno sistematično spremljanje v skladu s členom 35(3)(c), ali se uporablja „nova tehnologija“ ali obdelujejo občutljivi podatki in podatki v zvezi z ranljivimi posamezniki, na katere se nanašajo osebni podatki.

142. V skladu s členom 30 Splošne uredbe o varstvu podatkov je treba dokumentirati vse dejavnosti zbiranja in obdelave podatkov. To pomeni vso obdelavo, ki vključuje glasovne podatke.

Priporočila

143. Če je treba za obveščanje uporabnikov v skladu s členom 13 uporabljati glasovna sporočila, bi morali upravljavci podatkov taka sporočila objaviti na svojem spletnem mestu, da so dostopna uporabnikom in organom za varstvo podatkov.

3.11 Vgrajeno in privzeto varstvo podatkov

144. Ponudniki in razvijalci VGP bi morali premisliti o nujnosti registracije uporabnika za vsako od funkcij. Čeprav je jasno, da se mora za upravljanje dnevnega reda ali imenika uporabnik

[50] Smernice Delovne skupine iz člena 29 glede ocene učinka v zvezi z varstvom podatkov, DS 248 rev. 01, ki jih je potrdil Evropski odbor za varstvo podatkov.

registrirati, ni tako jasno, zakaj je potrebna registracija za opravljanje telefonskega klica ali internetnega iskanja v VGP.

145. Storitve, za katere ni potrebna identifikacija uporabnika, ne bi smele privzeto povezati nobenega od identificiranih uporabnikov VGP z ukazi. VGP s privzeto in uporabniku prijazno zasebnostjo in varstvom podatkov naj bi obdelal podatke uporabnikov samo za izvrševanje njihovih zahtev in naj ne bi shranjeval niti glasovnih podatkov niti registra izvršenih ukazov.

146. Na nekaterih napravah se lahko izvaja samo en VGP, druge pa ponujajo možnost izbire med različnimi VGP. Ponudniki VGP bi morali razviti panožne standarde, ki bi omogočali prenosljivost podatkov v skladu s členom 20 Splošne uredbe o varstvu podatkov.

147. Nekateri ponudniki VGP so trdili, da njihovi VGP ne bi mogli izbrisati vseh podatkov uporabnikov, tudi če bi to zahteval posameznik, na katerega se nanašajo osebni podatki. V skladu s členom 17 Splošne uredbe o varstvu podatkov bi morali ponudniki VGP zagotoviti, da se lahko vsi uporabniški podatki izbrišejo na zahtevo uporabnika.

4 MEHANIZMI ZA UVELJAVLJANJE PRAVIC POSAMEZNIKOV, NA KATERE SE NANAŠAJO OSEBNI PODATKI

148. V skladu s Splošno uredbo o varstvu podatkov morajo upravljavci podatkov, ki zagotavljajo storitve VGP, vsem registriranim in neregistriranim uporabnikom omogočiti uveljavljanje pravic posameznikov, na katere se nanašajo osebni podatki.

149. Ponudniki in razvijalci VGP bi morali posameznikom, na katere se nanašajo osebni podatki, olajšati nadzor nad njihovimi podatki v celotnem obdobju obdelave ter zlasti olajšati njihovo pravico do dostopa, popravka, izbrisa, pravico do omejitve obdelave in, odvisno od pravne podlage obdelave, njihovo pravico do prenosljivosti podatkov ter pravico do ugovora.

150. Upravljavec podatkov bi moral zagotoviti informacije o pravicah posameznika, na katerega se nanašajo osebni podatki, v trenutku, ko posameznik, na katerega se nanašajo osebni podatki, preklopi na VGP, najpozneje pa ob obdelavi glasovne zahteve prvega uporabnika.

151. Glede na to, da je glavno sredstvo interakcije z VGP glas, bi morali oblikovalci VGP zagotoviti, da lahko uporabniki, registrirani ali ne, uveljavljajo kakršne koli pravice posameznika, na katerega se nanašajo osebni podatki, in sicer s preprostim sledenjem glasovnim ukazom. Oblikovalci VGP in razvijalci aplikacij, če so del zadevne rešitve, bi morali ob koncu postopka izvedbe uporabnika obvestiti, da so bile njegove pravice ustrezno upoštevane, in sicer glasovno ali s pisnim obvestilom na uporabnikov mobilni telefon, račun ali katero koli drugo sredstvo, ki ga je izbral uporabnik.

152. Zlasti oblikovalci in razvijalci aplikacij VVA bi morali vzpostaviti posebna orodja, ki zagotavljajo uspešen in učinkovit način uveljavljanja teh pravic. Zato bi morali za svoje naprave predlagati način uveljavljanja pravic posameznikov, na katere se nanašajo osebni podatki, tako da posamezniku, na katerega se nanašajo osebni podatki, zagotavljajo samopostrežna orodja v okviru sistema za upravljanje profilov[51]. To bi lahko olajšalo učinkovito in pravočasno

[51] Sistem upravljanja profilov se razume kot prostor v sistemu VGP, kjer lahko uporabniki kadar koli shranijo svoje nastavitve, nastavijo spremembe in preprosto spremenijo nastavitve zasebnosti.

obravnavanje pravic posameznika, na katerega se nanašajo osebni podatki, ter upravljavcu podatkov omogočilo, da mehanizem identifikacije vključi v samopostrežno orodje.

153. Kar zadeva uveljavljanje pravic posameznikov, na katere se nanašajo osebni podatki, v primeru več uporabnikov, kadar uporabnik, ki je registriran ali ne, uveljavlja eno od svojih pravic, bi moral to storiti brez poseganja v katere koli druge pravice uporabnikov. Vsi uporabniki, registrirani in neregistrirani, lahko uveljavljajo svoje pravice, dokler upravljavec podatkov še vedno obdeluje podatke. Upravljavec podatkov bi moral vzpostaviti postopek, ki zagotavlja uveljavljanje pravic posameznikov, na katere se nanašajo osebni podatki.

4.1 Pravica do dostopa

154. V skladu s členom 12(1) Splošne uredbe o varstvu podatkov bi bilo treba sporočila iz člena 15 zagotoviti v pisni obliki ali z drugimi sredstvi, vključno, kjer je ustrezno z elektronskimi sredstvi. Glede dostopa do osebnih podatkov, ki se obdelujejo, člen 15(3) določa, da kadar posameznik, na katerega se nanašajo osebni podatki, zahtevo predloži z elektronskimi sredstvi, in če posameznik, na katerega se nanašajo osebni podatki, ne zahteva drugače, se informacije zagotovijo v elektronski obliki, ki je splošno uporabljana. Elektronska oblika, ki je splošno uporabljana, bi morala temeljiti na razumnih pričakovanjih posameznikov, na katere se nanašajo osebni podatki, in ne na obliki, ki jo upravljavec podatkov uporablja pri svojem vsakodnevnem delovanju. Posameznik, na katerega se nanašajo osebni podatki, ne bi smel biti zavezan k nakupu posebne programske ali strojne opreme, da bi pridobil dostop do informacij.

155. Upravljavci podatkov bi zato morali na zahtevo posamezniku, na katerega se nanašajo osebni podatki, poslati kopijo osebnih podatkov in zlasti zvočnih podatkov (vključno z zvočnimi posnetki in prepisi), in sicer v splošni berljivi obliki.

156. Pri odločanju o vrsti oblike, ki bi jo bilo treba zagotoviti v skladu s členom 15, mora upravljavec podatkov upoštevati, da bi morala oblika omogočati predstavitev informacij na razumljiv in lahko dostopen način. Upravljavci podatkov bi morali informacije prilagoditi tudi posebnemu položaju posameznika, na katerega se nanašajo osebni podatki in ki je vložil zahtevo.

> Primer 13:
>
> Upravljavec podatkov, ki zagotavlja storitev VGP, od uporabnika prejme zahtevi za dostop in za prenosljivost podatkov. Upravljavec podatkov se odloči, da bo informacije v skladu s členoma 15 in 20 zagotovil v datoteki PDF. V takem primeru se ne bi smelo šteti, da upravljavec podatkov obe zahtevi obravnava pravilno. Datoteka PDF tehnično izpolnjuje obveznosti upravljavca podatkov iz člena 15, vendar ne izpolnjuje obveznosti upravljavca podatkov iz člena 20.[52]
>
> Opozoriti je treba, da zgolj sklicevanje uporabnikov na zgodovino njihovih interakcij z glasovnim asistentom dozdevno ne omogoča, da bi upravljavec podatkov izpolnil vse svoje obveznosti na podlagi pravice do dostopa, saj so dostopni podatki običajno le del informacij, ki se obdelujejo v okviru zagotavljanja storitve.

157. Pravica do dostopa se ne bi smela uporabljati za izpodbijanje načela zmanjševanja količine podatkov in njihove hrambe.

4.2 Pravica do popravka

[52] Smernice DS29 o pravici do prenosljivosti podatkov, ki jih je potrdil Evropski odbor za varstvo podatkov, str. 18.

158. Da bi olajšali popravek podatkov, bi morali imeti uporabniki, registrirani ali ne, možnost, da kadar koli glasovno upravljajo in posodabljajo svoje podatke neposredno iz naprave VGP, kot je opisano zgoraj. Poleg tega bi bilo treba v napravi ali aplikaciji uvesti samopostrežno orodje, s katerim bi lahko preprosto popravili svoje osebne podatke. Uporabniki bi morali biti o posodobitvi obveščeni v glasovni ali pisni obliki.

159. Splošneje, pravica do popravka velja za vsa mnenja in sklepne analize[53] upravljavca podatkov, vključno z oblikovanjem profilov, in bi morala upoštevati, da je velika večina podatkov zelo subjektivna.[54]

4.3 Pravica do izbrisa

160. Registrirani ali neregistrirani uporabniki bi morali imeti možnost, da kadar koli z glasovnim ukazom iz naprave VGP ali samopostrežnega orodja, vključenega v katero koli napravo, povezano z VGP, izbrišejo podatke, ki se nanašajo nanje. Glede tega lahko posameznik, na katerega se nanašajo osebni podatki, osebne podatke izbriše tako preprosto, kot so bili predloženi. Zaradi spremljajočih težav pri anonimizaciji glasovnih podatkov in velike raznolikosti osebnih podatkov, ki se zbirajo od posameznika, na katerega se nanašajo osebni podatki, ter opažajo in sklepajo o njem[55], bi bilo v tem okviru pravico do izbrisa težko nadomestiti z anonimizacijo naborov osebnih podatkov. Ker je Splošna uredba o varstvu podatkov tehnološko nevtralna in se tehnologija hitro razvija, vendarle ni izključeno, da se bo pravica do izbrisa lahko uveljavila z anonimizacijo.

161. V nekaterih primerih je brez zaslona drugega ponudnika ali možnosti prikaza shranjenih podatkov (na primer mobilna aplikacija ali tablica) težko dobiti predogled zabeleženih sledi, da bi ocenili ustreznost predlogov. Nadzorno ploščo (ali aplikacijo), ki je za lažjo uporabo splošno dostopna uporabnikom, je treba opremiti z glasovnim pomočnikom, da se izbriše zgodovina izrečenih zahtev in da se orodje prilagodi potrebam uporabnika.[56]

162. Za vsako obdelavo podatkov in zlasti kadar registrirani posamezniki, na katere se nanašajo osebni podatki, privolijo v zvočne posnetke, ki jih ponudnik prepisuje in uporablja za izboljšanje svojih storitev, bi morali imeti ponudniki VGP možnost, da na zahtevo uporabnika izbrišejo prvotni zvočni posnetek in vse povezane prepise osebnih podatkov.

163. Upravljavec podatkov bi moral zagotoviti, da po uveljavljanju pravice do izbrisa ne bo več prišlo do obdelave. Glede prejšnjih ukrepov je treba upoštevati, da lahko pravico do izbrisa omejijo nekatere pravne in tehnične omejitve.

> Primer 14:
>
> Če je uporabnik pred zahtevo za izbris prek svojega VGP opravil spletni nakup, lahko ponudnik VGP izbriše glasovni zapis v zvezi s spletnim nakupom in zagotovi, da se v prihodnosti ne bo več uporabljal. Nakup bo še vedno izveden, prav tako tudi glasovni nalog ali pisni prepis, ki ga

[53] Dejstvo, da mnenja in sklepne analize lahko štejejo za osebne podatke, je potrdilo Sodišče Evropske unije, ki je ugotovilo, da izraz „katera koli informacija“ v opredelitvi pojma osebnih podatkov vključuje informacije, „tako objektivne kot subjektivne v obliki mnenj ali presoj, če se te ‚nanašajo‘ na zadevno osebo“ – Zadeva C-434/16, *Peter Nowak proti Data Protection Commissioner* ECLI:EU:C:2017:994 [34].

[54] Getting Data Subject Rights Right, A submission to the EDPB form data protection academics, november 2019.

[55] Delovna skupina iz člena 29, Mnenje št. 5/2014 o anonimizacijskih tehnikah, sprejeto 10. aprila 2014.

[56] "Assistants vocaux et enceintes connectées, l’impact de la voix sur l’offre et les usages culturels et médias", francoski "Conseil Supérieur de l’Audiovisuel", maj 2019.

obdela spletno mesto e-trgovine (v tem primeru izvzetje temelji na pravni obveznosti spletnega mesta e-trgovine).

Podobno velja, če je uporabnik pred zahtevo za izbris na svoj seznam predvajanja dodal določeno skladbo prek svojega VGP, pri čemer bodo lahko ponudniki VGP izbrisali glasovno zahtevo, ne pa tudi preteklih posledic take zahteve (izbris ne bo vplival na uporabnikov seznam predvajanja).

164. Na podlagi tega bi morali upravljavci podatkov, če se isti osebni podatki obdelujejo za različne namene obdelave, zahteve za izbris razlagati kot jasen signal za ustavitev obdelave podatkov za vse namene, ki niso pravno izvzeti.

V skladu s pogoji iz člena 21(1) Splošne uredbe o varstvu podatkov podatki, ki se obdelujejo na podlagi zakonitih interesov ponudnikov VGP, ne bi smeli biti izjema od pravice do izbrisa, zlasti ker posamezniki, na katere se nanašajo osebni podatki, ne pričakujejo nadaljnje obdelave svojih osebnih podatkov.

4.4 Pravica do prenosljivosti podatkov

165. Obdelava podatkov, ki jo izvajajo ponudniki VGP, spada na področje uporabe prenosljivosti podatkov, saj postopki obdelave večinoma temeljijo na privolitvi posameznika, na katerega se nanašajo osebni podatki, (v skladu s členom 6(1)(a) ali v skladu s členom 9(2)(a) v zvezi s posebnimi vrstami osebnih podatkov) ali na pogodbi, katere pogodbena stranka je posameznik, na katerega se nanašajo osebni podatki, v skladu s členom 6(1)(b).

166. V praksi bi morala pravica do prenosljivosti podatkov olajšati zamenjavo med različnimi ponudniki VGP. VGP delujejo v digitalnem okolju, zlasti če je glas posameznika, na katerega se nanašajo osebni podatki, zapisan v aplikaciji ali platformi, in bi bilo treba zagotoviti pravico do prenosljivosti podatkov za vse osebne podatke, ki jih posreduje posameznik, na katerega se nanašajo osebni podatki. Poleg tega bi moral upravljavec podatkov uporabnikom v obliki samopostrežnega orodja omogočiti neposreden dostop do njihovih osebnih podatkov v njihovem uporabniškem področju. Uporabniki bi morali imeti možnost, da to pravico uveljavijo tudi z glasovnim ukazom.

167. Ponudniki VGP in razvijalci bi morali posameznikom, na katere se nanašajo osebni podatki, zagotoviti obsežen nadzor nad osebnimi podatki v zvezi z njimi, da bi jim omogočili prenos osebnih podatkov od enega ponudnika VGP k drugemu. Posamezniki, na katere se nanašajo osebni podatki, bi zato morali prejeti svoje osebne podatke, ki so jih zagotovili upravljavcu podatkov, v strukturirani, splošno uporabljani in strojno berljivi obliki ter s sredstvi[57], ki

[57] Za ponazoritev glej obrazložitev Delovne skupine iz člena 29 v Smernicah o pravici do prenosljivosti podatkov, ki jih je potrdil Evropski odbor za varstvo podatkov, str. 16:
„Na tehnični ravni bi morali upravljavci podatkov proučiti in oceniti dva različna in dopolnjujoča se načina za dajanje prenosljivih podatkov na voljo posameznikom, na katere se nanašajo osebni podatki, ali drugim upravljavcem podatkov:
– neposreden prenos celotnega nabora prenosljivih podatkov (ali več izvlečkov delov splošnega nabora podatkov);
– avtomatizirano orodje, ki omogoča pridobivanje relevantnih podatkov.
Upravljavci podatkov morda dajejo prednost drugemu načinu, in sicer v primerih, ki vključujejo kompleksne in velike nabore podatkov, saj omogoča pridobitev katerega koli dela nabora podatkov, ki je glede na zahtevo posameznika, na katerega se nanašajo osebni podatki, relevanten zanj, lahko prispeva k zmanjšanju tveganja in potencialno omogoča uporabo mehanizmov za sinhronizacijo podatkov (na primer v smislu redne komunikacije med upravljavci podatkov). Morda je boljši način za zagotovitev skladnosti za ‚novega' upravljavca podatkov in

upoštevajo zahteve za prenosljivost podatkov (kot so orodja za prenos podatkov in vmesniki za aplikacijsko programiranje)[58]. Kot je navedeno v Smernicah o pravici do prenosljivosti podatkov, bi moral upravljavec podatkov v primeru obsežnega ali zapletenega zbiranja osebnih podatkov zagotoviti pregled *„v jedrnati, pregledni, razumljivi in lahko dostopni obliki ter jasnem in preprostem jeziku“* (glej člen 12(1) Splošne uredbe o varstvu podatkov), tako da bi posamezniki, na katere se nanašajo osebni podatki, morali imeti vedno jasne informacije o tem, katere podatke je treba prenesti ali posredovati drugemu upravljavcu podatkov v zvezi z določenim namenom. Posameznikom, na katere se nanašajo osebni podatki, bi bilo treba na primer omogočiti uporabo programske opreme, ki omogoča preprosto opredelitev, prepoznavanje in obdelavo posebnih podatkov.

168. Ta pravica bi morala uporabniku omogočiti, da za svojo osebno uporabo pridobi zlasti podatke, ki jih je sporočil prek svojega glasu (na primer zgodovina glasovnih interakcij) in v okviru ustvarjanja uporabniškega računa (na primer ime in priimek).

169. Za polno uporabo te pravice posameznikov, na katere se nanašajo osebni podatki, v okviru enotnega digitalnega trga bi morali oblikovalci VGP in razvijalci aplikacij zlasti razviti skupne strojno berljive oblike, ki bodo olajšale interoperabilnost oblik podatkov med sistemi VGP[59], vključno s standardnimi oblikami za glasovne podatke. Tehnologije bi morale biti strukturirane tako, da bi novi upravljavec zlahka in v celoti uporabljal osebne podatke, vključno z glasovnimi podatki.[60]

170. Glede oblike bi morali ponudniki VGP zagotoviti osebne podatke v običajno uporabljanih odprtih formatih (na primer mp3, wav, csv, gsm itd.) skupaj z ustreznimi metapodatki, ki se uporabljajo za natančen opis pomena izmenjanih informacij.[61]

5 PRILOGA: SAMODEJNO PREPOZNAVANJE GOVORA, SINTEZA GOVORA IN OBDELAVA NARAVNEGA JEZIKA

171. Po teoretičnih temeljih obdelave signalov, zlasti podatkov, Clauda Shannona in teorij vzorčenja, je samodejna obdelava govora postala temeljna sestavina tehničnih znanosti. Na stičišču fizike (akustika, širjenje valov), uporabne matematike (modeliranje, statistika), računalništva (algoritmi, učne tehnike) in humanističnih znanosti (prepoznavanje, sklepanje) je bila obdelava govora hitro razdeljena na številne študijske predmete: identifikacija in preverjanje govorcev, samodejno prepoznavanje govora, sinteza govora, zaznavanje čustev

bi pomenil dobro prakso pri zmanjševanju tveganja glede zasebnosti, kar zadeva prvotnega upravljavca podatkov.“

[58] V zvezi s tem: Smernice Delovne skupine iz člena 29 o pravici do prenosljivosti podatkov, ki jih je potrdil Evropski odbor za varstvo podatkov, str. 1.

[59] V zvezi s tem: uvodna izjava (68) Smernic Delovne skupine iz člena 29 o pravici do prenosljivosti podatkov, ki jih je potrdil Evropski odbor za varstvo podatkov, str. 17.

[60] *„V zvezi s tem uvodna izjava 68 upravljavce podatkov spodbuja, naj razvijejo interoperabilne oblike, ki omogočajo prenosljivost podatkov, vendar to ne pomeni obveznosti za upravljavce, da morajo uvesti ali vzdrževati sisteme za obdelavo, ki so tehnično združljivi. Vendar pa v skladu s Splošno uredbo o varstvu podatkov upravljavci ne smejo ustvarjati ovir za posredovanje.“* – Smernice Delovne skupine iz člena 29 o pravici do prenosljivosti podatkov, ki jih je potrdil Evropski odbor za varstvo podatkov, str. 5.

[61] Evropski odbor za varstvo podatkov močno spodbuja sodelovanje med deležniki in trgovinskimi združenji iz panoge za sodelovanje pri skupnem sklopu interoperabilnih standardov in oblik, da se izpolnijo zahteve glede pravice do prenosljivosti podatkov.

itd. V zadnjih petnajstih letih je disciplina kot celota zelo napredovala, k čemur so pripomogli različni dejavniki: izboljšane metode, znatno povečanje računalniških zmogljivosti in večja količina razpoložljivih podatkov.

5.1 Samodejno prepoznavanje govora

172. Samodejno prepoznavanje govora (imenovano tudi pretvorba govora v besedilo) je vključevalo tri različne faze, katerih cilj je bil: 1. z uporabo akustičnega modela določiti, kateri fonemi so bili izrečeni; 2. s fonetičnim slovarjem določiti, katere besede so bile navedene; 3. prepisati zaporedje besed (stavek), za katere je verjetno, da so bile izrečene z uporabo jezikovnega modela. Danes z napredkom, ki ga omogoča poglobljeno učenje (tehnika strojnega učenja), številni sistemi zagotavljajo celovito samodejno prepoznavanje govora. S tem ni več potrebe po zapletenem usposabljanju treh različnih modelov, hkrati pa se zagotovi večja uspešnost v smislu rezultatov in časa obdelave. Skoraj vsi glavni digitalni akterji zdaj ponujajo lastne izvedbe samodejnega prepoznavanja govora, ki jih lahko preprosto uporabljajo sistemi API, vendar obstajajo tudi odprtokodni sistemi (na primer DeepSpeech[62] ali Kaldi[63]).

5.2 Obdelava naravnega jezika

173. Obdelava naravnega jezika je večdisciplinarno področje, ki vključuje jezikoslovje, računalništvo in umetno inteligenco, njen cilj pa je ustvariti orodja za obdelavo naravnega jezika za različne aplikacije. Področja raziskav in uporabe so številna: sintaktična analiza, strojno prevajanje, samodejno ustvarjanje in povzemanje besedil, preverjanje črkovanja, sistemi za odgovarjanje na vprašanja, besedilno rudarjenje, prepoznavanje imenovanih subjektov, analiza razpoloženja itd. Konkretno je cilj obdelave naravnega jezika računalnikom omogočiti branje, razumevanje in izpeljavo pomena iz človeških jezikov. Razvoj aplikacij obdelave naravnega jezika je izziv, saj računalniška orodja običajno zahtevajo, da ljudje z njimi komunicirajo v programskem jeziku, ki je formalen, pomensko natančen, nedvoumen in zelo strukturiran. Človeški govor pa ni vedno natančen. Pogosto je dvoumen, jezikovna struktura pa je lahko odvisna od številnih zapletenih spremenljivk, vključno s slengom, regionalnimi narečji in družbenim kontekstom.

174. Glavni tehniki, ki se uporabljata za obdelavo naravnega jezika, sta sintaksa in semantična analiza. Sintaksa je razporeditev besed v povedi, da dobijo slovnični pomen. Pri obdelavi naravnega jezika se sintaksa uporablja za oceno pomena jezika na podlagi slovničnih pravil. Uporabljene tehnike sintakse vključujejo razčlenjevanje (gramatična analiza stavka), segmentacijo besed (s katero se velik del besedila deli na enote), lomljenje povedi (ki postavlja meje stavkov v velika besedila), morfološko segmentacijo (s katero se besede delijo v skupine) in krnjenje (ki besedam odreže končnice, da jih skrči na njihov koren). Semantika vključuje uporabo in pomen besed. Pri obdelavi naravnega jezika se uporabljajo algoritmi za razumevanje pomena in strukture stavkov. Tehnike, ki se pri obdelavi naravnega jezika uporabljajo v zvezi s semantiko, vključujejo razdvoumljanje večpomenskih besed (izpelje pomen besede na podlagi sobesedila), prepoznavanje imenovanih entitet (določa besede, ki jih je mogoče razvrstiti v skupine) in ustvarjanje naravnega jezika (določi semantiko besed). Prejšnji pristopi k obdelavi naravnega jezika so vključevali pristope, ki temeljijo na pravilih, pri katerih so bili preprosti algoritmi strojnega učenja naučeni, katere besede in fraze je treba iskati v besedilu, in so se ob pojavu teh fraz odzvali na določen način, sedanji pristopi k obdelavi

[62] https://github.com/mozilla/DeepSpeech
[63] https://github.com/kaldi-asr/kaldi

naravnega jezika pa temeljijo na globokem učenju, vrsti umetne inteligence, ki preučuje in uporablja vzorce v podatkih za izboljšanje razumevanja programa.

5.3 Sinteza govora

175. Sinteza govora je umetna produkcija človeškega govora. Sinteza govora se izvaja predvsem s povezovanjem glasovnih enot, ki so shranjene v podatkovni zbirki. Ta tehnika pomeni, da se med vsemi posnetki igralca, ki so bili pred tem prepisani v foneme, zloge in besede, izberejo zvočne kode, ki ustrezajo besedam, za katere želimo, da jih izgovori VGP, in da se jih eno za drugo združi v razumljiv stavek z naravnim dikcijo. Namesto tega lahko sintetizator govora vključuje model vokalnega trakta in drugih značilnosti človeškega glasu, da se parametri glasu, kot so intonacija, ritem in barva glasu, oblikujejo z generativnimi statističnimi modeli (kot so WaveNet[64], Tacotron[65] ali DeepVoice[66]) in ustvari popolnoma sintetični izhodni glas.

[64] Aäron van den Oord et Sander Dieleman, *WaveNet: A generative model for raw audio*, blog Deepmind, september 2016, https://deepmind.com/blog/article/wavenet-generative-model-raw-audio.

[65] Yuxuan Wang, *Expressive Speech Synthesis with Tacotron*, blog Google AI, marec 2018, https://ai.googleblog.com/2018/03/expressive-speech-synthesis-with.html.

[66] *Deep Voice 3: 2000-Speaker Neural Text-to-Speech*, blog Baidu Research, oktober 2017, http://research.baidu.com/Blog/index-view?id=91.