

Usmernenia



Usmernenia 02/2021 o virtuálnych hlasových asistentoch

Verzia 2.0

Prijaté 7. júla 2021

História verzií

Verzia 2.0	7. júla 2021	Prijatie usmernení po verejnej konzultácii
Verzia 1.0	9. marca 2021	Prijatie usmernení na verejnú konzultáciu

ZHRNUTIE

Virtuálny hlasový asistent (VVA) je služba, ktorá rozumie hlasovým príkazom a plní ich alebo ich v prípade potreby sprostredkúva iným informačným systémom. VVA sú v súčasnosti k dispozícii vo väčšine smartfónov a tabletov, tradičných počítačov a v posledných rokoch dokonca aj v samostatných zariadeniach ako sú inteligentné reproduktory.

VVA fungujú ako rozhranie medzi používateľmi a ich počítačovými zariadeniami a online službami, ako sú vyhľadávače alebo internetové obchody. VVA majú vďaka svojej úlohe prístup k obrovskému množstvu osobných údajov vrátane príkazov všetkých používateľov (napr. história prezerania alebo vyhľadávania) a odpovedí (napr. plánované stretnutia).

Prevažnú väčšinu služieb VVA vytvorilo niekoľko tvorcov VVA. VVA však dokážu spolupracovať s aplikáciami, ktoré tretie strany (vývojári aplikácií VVA) naprogramovali na umožnenie používania sofistikovanejších príkazov.

Správne fungovanie VVA si vyžaduje koncové zariadenie vybavené mikrofónom a reproduktormi. Toto zariadenie ukladá hlasové a iné údaje, ktoré súčasní VVA zároveň prenášajú na vzdialené servery VVA.

Prevádzkovatelia, ktorí poskytujú služby VVA, a ich sprostredkovatelia musia preto zohľadniť nielen všeobecné nariadenie o ochrane údajov¹, ale aj smernicu o súde a elektronických komunikáciách².

V týchto usmerneniach sa identifikujú niektoré z najvýznamnejších problémov v oblasti dodržiavania predpisov a príslušným zainteresovaným stranám sa poskytujú odporúčania na ich riešenie.

Prevádzkovatelia, ktorí poskytujú služby VVA prostredníctvom koncových zariadení bez obrazovky, musia v súlade so všeobecným nariadením o ochrane údajov naďalej informovať používateľov pri nastavovaní VVA, alebo inštalácii či pri prvom použití aplikácie VVA. Poskytovateľom/tvorcom VVA a vývojárom preto odporúčame, aby na uľahčenie poskytovania povinných informácií vyvinuli hlasové rozhrania.

V súčasnosti všetci VVA vyžadujú, aby sa do služby zaregistroval aspoň jeden používateľ. Vzhľadom na povinnosť špecificky navrhutej a štandardnej ochrany údajov by poskytovatelia/tvorcovia a vývojári VVA mali zvážiť, či si každá z ich funkcií vyžaduje registrovaného používateľa.

Mnohí tvorcovia VVA využívajú používateľské konto, pomocou ktorého službu VVA spájajú s inými službami, ako sú, napríklad, e-mail alebo streamovanie videí. Európsky výbor pre ochranu údajov (EDPB) sa domnieva, že prevádzkovatelia by sa mali zdržať takýchto postupov, pretože si vyžadujú používanie zdĺhavých a komplexných politík ochrany osobných údajov, ktoré by neboli v súlade so zásadou transparentnosti podľa všeobecného nariadenia o ochrane údajov.

V týchto usmerneniach sa zohľadňujú štyri z najbežnejších účelov, na ktoré VVA spracúvajú osobné údaje: plnenie požiadaviek, zlepšovanie modelu strojového učenia VVA, biometrická identifikácia a profilovanie na účely personalizácie obsahu alebo reklamy.

¹ Nariadenie Európskeho parlamentu a Rady 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (ďalej len „všeobecné nariadenie o ochrane údajov“).

² Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúca sa spracúvania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súde a elektronických komunikáciách), zmenená smernicou 2006/24/ES a smernicou 2009/136/ES (ďalej len „smernica o súde a elektronických komunikáciách“).

Pokiaľ sa údaje VVA spracúvajú na účely plnenia požiadaviek používateľa, t. j. ak je to nevyhnutne potrebné na poskytovanie služby, ktorú požaduje používateľ, prevádzkovatelia sú oslobodení od požiadavky predchádzajúceho súhlasu podľa článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách. Naopak, súhlas podľa článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách, by bol potrebný na uchovávanie alebo získanie prístupu k informáciám na akýkoľvek iný účel, než je plnenie požiadaviek používateľov.

Niektoré služby VVA uchovávajú osobné údaje dovtedy, kým ich používatelia nepožiadajú o ich vymazanie. To nie je v súlade so zásadou minimalizácie uchovávania. VVA by mali údaje uchovávať len dovtedy, kým je to potrebné na účely, na ktoré sa osobné údaje spracúvajú.

Ak prevádzkovateľ zistí (napr. v rámci procesu kontroly kvality), že dochádza k náhodnému získaniu osobných údajov, mal by si overiť, či existuje platný právny základ pre každý účel spracúvania takýchto údajov. V opačnom prípade by sa náhodne získané údaje mali vymazať.

VVA môžu spracúvať údaje viacerých dotknutých osôb. Poskytovatelia/tvorcovia VVA by preto mali zaviesť mechanizmy kontroly prístupu za zabezpečenie zachovania dôvernosti, integrity a dostupnosti osobných údajov. Niektoré tradičné mechanizmy kontroly prístupu, napríklad heslá, však nie sú v súvislosti s VVA vhodné, pretože by museli byť vyslovené nahlas. V usmerneniach sa v tejto súvislosti uvádzajú určité úvahy vrátane oddielu, ktorý sa týka spracúvania osobitných kategórií údajov na účely biometrickej identifikácie.

Poskytovatelia/tvorcovia VVA by mali vziať do úvahy, že pri získavaní hlasových záznamov používateľa môže záznam obsahovať hlas alebo údaje iných jednotlivcov, ako napríklad šum pozadia, ktorý nie je pre službu potrebný. Vždy, keď je to možné, by tvorcovia VVA preto mali zvážiť použitie technológií filtrovania nepotrebných údajov a zabezpečiť, aby sa zaznamenával len hlas používateľa.

Pri vyhodnocovaní potreby posúdenia vplyvu na ochranu údajov sa EDPB domnieva, že je veľmi pravdepodobné, že služby VVA spadajú do kategórií a medzi podmienky, ktoré si vyžadujú posúdenie vplyvu na ochranu údajov.

Prevádzkovatelia poskytujúci služby VVA by mali zabezpečiť, aby používatelia mohli uplatňovať svoje práva dotknutej osoby pomocou jednoduchých [easy-to-follow] hlasových príkazov. Poskytovatelia/tvorcovia VVA, ako aj vývojári aplikácií by mali na konci procesu informovať používateľov, že ich práva boli riadne zohľadnené, a to buď v hlasovej forme alebo zaslaním písomného oznámenia na mobilný telefón, používateľské konto alebo akýkoľvek iný prostriedok, ktorý si používateľ vybral.

Obsah

ZHRNUTIE	3
1 VŠEOBECNÉ INFORMÁCIE	7
2 TECHNOLOGICKÉ INFORMÁCIE	8
2.1 Základné charakteristiky virtuálnych hlasových asistentov	8
2.2 Účastníci ekosystému VVA	9
2.3 Opis jednotlivých krokov	9
2.4 Aktivačné výrazy	10
2.5 Hlasové úryvky a strojové učenie	11
3 PRVKY OCHRANY OSOBNÝCH ÚDAJOV	12
3.1 Právny rámec.....	12
3.2 Identifikácia spracúvania údajov a zainteresovaných strán	14
3.2.1 Spracúvanie osobných údajov	14
3.2.2 Spracúvanie prevádzkovateľmi a sprostredkovateľmi	16
3.3 Transparentnosť	17
3.4 Obmedzenie účelu a právny základ.....	21
3.4.1 Plnenie požiadaviek používateľov	22
3.4.2 Zlepšovanie VVA trénovaním systémov strojového učenia a manuálnou kontrolou hlasu a prepisov.....	23
3.4.3 Identifikácia používateľa (pomocou hlasových údajov)	24
3.4.4 Profilovanie používateľov na účely personalizácie obsahu alebo reklamy	24
3.5 Spracúvanie osobných údajov detí.....	26
3.6 Uchovávanie údajov	26
3.7 Bezpečnosť	28
3.8 Spracúvanie osobitných kategórií údajov	31
3.8.1 Všeobecné otázky pri spracúvaní osobitných kategórií údajov	31
3.8.2 Osobitné otázky pri spracúvaní biometrických údajov	31
3.9 Minimalizácia údajov.....	33
3.10 Zodpovednosť.....	33
3.11 Špecificky navrhnutá a štandardná ochrana údajov	34
4 Mechanizmy na uplatňovanie práv dotknutých osôb	35
4.1 Právo na prístup	35
4.2 Právo na opravu	36
4.3 Právo na výmaz.....	36
4.4 Právo na prenosnosť údajov.....	38

5	Príloha: Automatické rozpoznávanie reči, syntéza reči a spracúvanie prirodzeného jazyka	39
5.1	Automatické rozpoznávanie reči (ASR)	39
5.2	Spracovanie prirodzeného jazyka.....	39
5.3	Syntéza reči	40

Európsky výbor pre ochranu údajov

so zreteľom na článok 70 ods. 1 písm. j) a písm. e) nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (ďalej len „všeobecné nariadenie o ochrane údajov“),

so zreteľom na Dohodu o EHP, a najmä na jej prílohu XI a protokol 37, ktoré boli zmenené rozhodnutím Spoločného výboru EHP č. 154/2018 zo 6. júla 2018³,

so zreteľom na článok 12 a článok 22 svojho rokovacieho poriadku,

PRIJAL TIETO USMERNENIA

1 VŠEOBECNÉ INFORMÁCIE

1. Vďaka súčasnému technologickému pokroku sa výrazne zvýšila presnosť a popularita virtuálnych hlasových asistentov (ďalej iba „VVA“). Služby VVA sú zabudované do smartfónov, prepojených vozidiel, inteligentných reproduktorov a inteligentných televízorov. Touto integráciou VVA získali prístup k informáciám intímnej povahy, ktoré by v prípade, že nebudú riadne spravované, mohli poškodiť práva jednotlivcov na ochranu údajov a súkromia. V dôsledku toho sú VVA a zariadenia, do ktorých boli zabudované, predmetom kontroly zo strany rôznych orgánov pre ochranu osobných údajov.
2. Používanie interakcií na základe hovorenej reči má niekoľko výhod, ako napríklad: prirodzenosť interakcie, ktorá si od používateľov nevyžaduje, aby sa niečo ďalšie učili, rýchlosť vykonania príkazu a rozšírenie oblasti činnosti, čo môže umožniť rýchlejší prístup k informáciám. Pri spoliehaní sa na rečový prejav však vznikajú ťažkosti pri správnom výklade správy: premenlivosť zvukového signálu medzi rôznymi rečníkmi, akustické prostredie, nejednoznačnosť jazyka atď.
3. Hlavnou motiváciou na používanie VVA ostáva v praxi aj naďalej plynulosť alebo zjednodušenie úloh. Môže to zahŕňať, napríklad, uskutočnenie/prijatie hovoru, nastavenie časovača atď., najmä ak používatelia nemôžu práve využívať ruky. Automatizácia domácností je hlavnou oblasťou využitia, pre ktorú tvorcovia VVA vytvorili. Tým, že navrhujú zjednodušiť vykonávanie úloh (zapínanie svetla, nastavovanie vykurovania, spúšťanie žalúzií atď.) a centralizovať ich do jedného nástroja, ktorý sa dá ľahko aktivovať na diaľku, je ich možné považovať za pomocníkov pri uľahčovaní fungovania domácnosti [domestic facilitator]. Okrem použitia na osobné účely alebo v domácnosti môžu byť hlasové príkazy zaujímavé aj v pracovnom prostredí, kde je ťažké manipulovať s počítačovými zariadeniami a používať písomné príkazy (napr. práca vo výrobe).
4. Teoreticky by najväčší úžitok z hlasového rozhrania mohli mať osoby so zdravotným postihnutím alebo osoby odkázané na starostlivosť, pre ktoré je používanie tradičných rozhraní problematické. Virtuálny hlasový asistent môže uľahčiť prístup k informáciám a počítačovým

³ Odkazy na „členské štáty“ uvedené v tomto dokumente by sa mali chápať ako odkazy na „členské štáty EHP“.

zdrojom, a tým podporiť inkluzívne myslenie, keďže použitie hlasu umožní prekonať ťažkosti spojené s písaným slovom, ktorým môžu čeliť určité skupiny používateľov.

5. Nakoniec, aj zdravie je oblasťou, v ktorej existuje mnoho možností na využitie konverzačných pomôcok, či už hlasových alebo iných. Napríklad, počas pandémie COVID-19 sa využívali rôzne tzv. callboty (formy automatických telefonických asistentov), ktorí volajúcim používateľom poskytovali predbežnú diagnostiku. Predpokladá sa, že z dlhodobého hľadiska by interakcia medzi človekom a asistentom mohla ovplyvniť celý proces starostlivosti o pacienta: nielen z hľadiska dobrých životných podmienok a prevencie, ale aj z hľadiska liečby a podpory.
6. V súčasnosti existujú viac ako 3 miliardy smartfónov a všetky majú zabudované VVA, pričom vo väčšine z nich je VVA v štandardnom nastavení zapnuté. V niektorých z najrozšírenejších operačných systémov v osobných počítačoch a laptopoch sú VVA takisto zabudované. Vďaka najnovšiemu nárastu počtu inteligentných reproduktorov (147 miliónov bolo predaných v roku 2019⁴) prichádzajú VVA do miliónov domácností a kancelárií. Súčasná riešenia VVA však v štandardnom nastavení neponúkajú mechanizmy autentifikácie ani kontroly prístupu.
7. Cieľom tohto dokumentu je poskytnúť usmernenie k uplatňovaniu všeobecného nariadenia o ochrane údajov v kontexte VVA.

2 TECHNOLOGICKÉ INFORMÁCIE

2.1 Základné charakteristiky virtuálnych hlasových asistentov

8. VVA možno definovať ako softvérovú aplikáciu, ktorá umožňuje viesť hovorený dialóg s používateľom v prirodzenom jazyku.
9. Prirodzený jazyk má sémantiku, ktorá je pre ľudský jazyk špecifická. V závislosti od charakteristík jazyka a rozmanitosti jeho slovnej zásoby možno ten istý pokyn vyjadriť viacerými spôsobmi, pričom niektoré príkazy sa môžu zdať podobné, ale týkajú sa dvoch rôznych vecí. Na vyriešenie týchto nejednoznačností sa potom často používajú inferenčné mechanizmy, napríklad, v závislosti od toho, čo už bolo povedané, od času vydania pokynu, miesta, záujmov osoby atď.
10. VVA možno rozdeliť na moduly, ktoré umožňujú vykonávať rôzne úlohy: zaznamenávanie a reštitúcia zvuku, automatický prepis reči (prevod reči na text), automatické spracovanie jazyka, stratégie dialógu, prístup k ontológiám (súbory údajov a štruktúrované koncepcie súvisiace s danou oblasťou) a externé zdroje znalostí, generovanie jazyka, hlasová syntéza (prevod textu na reči) atď. Asistent by konkrétne mal umožňovať interakciu na účel vykonania činnosti (napr. „zapni rádio“, „vypni svetlo“) alebo prístupu k informáciám (napr. „aké bude počasie zajtra?“, „pôjde vlak o 7.43?“). Zohráva teda úlohu sprostredkovateľa [intermediary] a organizátora, ktorý má uľahčiť plnenie úloh používateľa.
11. V praxi VVA nie je inteligentný reproduktor, ale inteligentný reproduktor môže byť vybavený hlasovým asistentom. Je bežné si ich zamieňať, v praxi je však inteligentný reproduktor vlastne fyzickým stelesnením VVA. VVA môže byť použitý v smartfóne, inteligentnom reproduktore, prepojených hodinkách, prepojenom vozidle, domácom spotrebiči atď.

⁴ Pozri napríklad tlačovú správu hamburského orgánu pre ochranu osobných údajov a informácie z 1. augusta 2019: <https://datenschutz-hamburg.de/pressemitteilungen/2019/08/2019-08-01-google-assistant>.

12. Organizácia základného spracúvania údajov môže zahŕňať viaceré vzorce informačných tokov. Je možné vymedziť tri hlavné entity:

Fyzická časť: hardvérové zariadenie, v ktorom je asistent zabudovaný (smartfón, reproduktor, inteligentná televízia atď.) a ktorého súčasťou sú mikrofóny, reproduktory a sieťové a výpočtové kapacity (na vyššej alebo nižšej úrovni v závislosti od konkrétneho prípadu).

Softvérová časť: časť, ktorá realizuje interakciu medzi človekom a strojom, a ktorá zahŕňa moduly automatického rozpoznávania reči, spracovania prirodzeného jazyka, dialógu a syntézy reči. Je možné ju ovládať priamo v rámci fyzického zariadenia, ale v mnohých prípadoch funguje na diaľku.

Zdroje: externé údaje, ako sú databázy s obsahom, ontológie alebo obchodné aplikácie, ktoré poskytujú informácie (napr. „koľko je hodín na západnom pobreží Spojených štátov“, „prečítaj moje e-maily“) alebo umožňujú, aby sa požadované činnosti vykonali konkrétnym spôsobom (napr. „zvýš teplotu o 1,5°C“).

13. VVA umožňujú inštaláciu komponentov alebo aplikácií tretích strán, ktoré rozširujú ich základné funkcie. Pri každom VVA sa komponenty pomenúvajú inak, ale všetky zahŕňajú výmenu osobných údajov používateľov medzi tvorcom VVA a vývojárom aplikácií.
14. Hoci väčšina VVA nezdiera hlasový úryvok s vývojármi aplikácií, tieto subjekty stále spracúvajú osobné údaje. Okrem toho v závislosti od povahy poskytovanej funkcie, vývojár aplikácií získava informácie o zámeroch a časových úsekoch, ktoré by mohli zahŕňať citlivé informácie, ako sú údaje týkajúce sa zdravia.

2.2 Účastníci ekosystému VVA

15. VVA môže v rámci vykonávacieho reťazca zahŕňať veľký počet účastníkov a sprostredkovateľov [intermediaries]. V praxi možno identifikovať až päť rôznych účastníkov. V závislosti od obchodných modelov a technologických možností však niektorí účastníci môžu prevziať viaceré kombinácie úloh, napríklad tvorca a integrátor alebo tvorca a vývojár aplikácie:
 - a. **Poskytovateľ (alebo tvorca) VVA:** zodpovedný za vývoj VVA, návrhy a vymedzenie jeho možností a predvolených funkcií: spôsoby aktivácie, výber architektúry, prístup k údajom, správa záznamov, špecifikácie hardvéru atď.
 - b. **Vývojár aplikácií VVA:** ako v prípade mobilných aplikácií, vytvára aplikácie rozširujúce štandardné funkcie VVA. Pri vývoji rešpektuje vývojárske obmedzenia, ktoré stanovil tvorca.
 - c. **Integrátor:** výrobca prepojených zariadení, ktorý tieto zariadenia chce vybaviť VVA. Mal by rešpektovať požiadavky vymedzené tvorcom.
 - d. **Majiteľ:** zodpovedný za fyzické priestory pre ľudí (ubytovanie, pracovné prostredie, prenájom vozidiel atď.) chce svojej klientele poskytnúť VVA (prípadne spolu so špecializovanými aplikáciami).
 - e. **Používateľ:** konečný článok v hodnotovom reťazci VVA, ktorý môže VVA používať na rôznych zariadeniach (reproduktor, televízny prijímač, smartfón, hodinky atď.) v závislosti od toho, ako a kde bol VVA inštalovaný a nastavený.

2.3 Opis jednotlivých krokov

16. Aby VVA mohol realizovať činnosti alebo získať prístup k informáciám, vykoná viacero úloh:

- 1) VVA zabudovaný v zariadení (smartfón, reproduktor, vozidlo) je v pohotovostnom režime. Lepšie povedané, neustále počúva. Kým však nezaznamená konkrétny aktivačný výraz, zariadenie prijímajúce hlas žiadny zvuk nevysiela a nevykonáva žiadnu inú operáciu okrem detekcie aktivačného výrazu. Na tento účel slúži vyrovnávacia pamäť na niekoľko sekúnd (podrobnejšie informácie sú uvedené v nasledujúcom oddiele).
- 2) Používateľ vysloví aktivačný výraz a VVA tento zvuk lokálne porovná s aktivačným výrazom. Ak sa zistí zhoda, VVA otvorí kanál na počúvanie a zvukový obsah okamžite odošle.
- 3) V mnohých prípadoch, ak sa príkaz spracúva na diaľku, na serveri sa vykoná druhá kontrola výslovnosti kľúčového slova, aby sa obmedzili nechcené aktivácie.
- 4) Používateľ vysloví požiadavku, ktorá sa priebežne odosiela poskytovateľovi VVA. Sekvencia hovorenej reči sa potom automaticky prepisuje (prevod reči na text).
- 5) Pomocou technológií spracovania prirodzeného jazyka sa príkaz interpretuje. Z príkazu sa extrahujú príslušné zámery správy a identifikujú sa informačné premenné (časové úseky). Následne sa použije správca dialógov na určenie scenára interakcie, ktorý má s používateľom prebehnúť, a to poskytnutím vhodnej štruktúry reakcie.
- 6) Ak príkaz zahŕňa funkciu poskytovanú aplikáciou tretej strany (zručnosť, činnosť, skratka atď.), poskytovateľ VVA zašle vývojárovi aplikácií zámery a informačné premenné (časové úseky) zo správy.
- 7) Identifikuje sa odpoveď prispôbena požiadavke používateľa – prinajmenšom sa prispôsobí odpoveď „Neviem odpovedať na vašu otázku“ v prípade, že VVA nebol schopný požiadavku správne interpretovať. V prípade potreby sa využívajú vzdialené zdroje: verejne prístupné znalostné databázy (online encyklopédia atď.) alebo autentifikácia (bankový účet, hudobná aplikácia, zákaznícky účet na online nakupovanie atď.) a informačné premenné (časové úseky) sa vyplnia získanými vedomosťami.
- 8) Vytvorí sa veta na odpoveď a/alebo sa identifikuje úkon (spustenie žalúzií, zvýšenie teploty, prehranie hudby, zodpovedanie otázky atď.). Veta sa syntetizuje (prevod textu na reč) a/alebo sa úkon, ktorý sa má vykonať, odošle do zariadenia a je vykonaný.
- 9) VVA sa vráti do pohotovostného režimu.

Je potrebné pripomenúť, že zatiaľ čo väčšina spracúvania v súvislosti s hlasom sa v súčasnosti vykonáva na vzdialených serveroch, niektorí poskytovatelia VVA vyvíjajú systémy, ktoré by mohli časť tohto spracúvania vykonávať lokálne.⁵

2.4 Aktivačné výrazy

17. Pred použitím musí byť VVA „aktivovaný“. Znamená to, že asistent sa prepne do režimu aktívneho počúvania, aby mohol prijímať pokyny a príkazy od používateľa. Hoci túto aktiváciu možno niekedy vykonať aj fyzickým úkonom (napr. stlačením tlačidla, stlačením inteligentného reproduktora atď.), takmer všetky VVA na trhu fungujú na princípe detekcie aktivačného

⁵ Viac informácií o tejto téme nájdete napríklad tu: <https://www.amazon.science/blog/alexa-new-speech-recognition-abilities-showcased-at-interspeech>

výrazu alebo slova, na základe ktorého prechádzajú do režimu aktívneho počúvania (známe aj ako aktivačné slovo alebo prebúdzacie slovo / tzv. „hot word“).

18. Asistent sa pritom spolieha na použitie mikrofónu a základných výpočtových schopností, aby zistil, či bolo vyslovené aktivačné slovo. Táto analýza, ktorá sa vykonáva nepretržite od chvíle, keď sa VVA zapne, sa vykonáva výlučne lokálne. Až po rozpoznaní aktivačného slova sa zvukové záznamy spracúvajú na účely interpretácie a plnenia príkazu, čo v mnohých prípadoch znamená ich odosielanie cez internet na vzdialené servery. Detekcia aktivačných slov je založená na technikách strojového učenia. Hlavnou výzvou pri používaní takýchto metód je, že detekcia vychádza z pravdepodobnosti. Pri každom vyslovenom slove alebo výraze tak systém poskytne skóre dôveryhodnosti, či bolo aktivačné slovo skutočne vyslovené. Ak toto skóre je vyššie ako určitá prednastavená prahová hodnota, zachytený zvuk sa považuje za aktivačné slovo. Takýto systém však nie je bezchybný: v niektorých prípadoch sa aktivácia nemusí zistiť, aj keď bolo aktivačné slovo vyslovené (nesprávne odmietnutie) a v iných prípadoch sa aktivácia môže zachytiť aj napriek tomu, že používateľ nevyslovil kľúčové slovo (nesprávna akceptácia).
19. V praxi by sa mal nájsť prijateľný kompromis medzi týmito dvoma typmi chýb a na jeho základe stanoviť prahová hodnota. Keďže však v dôsledku nesprávnej detekcie aktivačného slova môže dôjsť k odoslaniu zvukových záznamov, vzniká tu pravdepodobnosť neočakávaných a nežiaducich poskytnutí údajov. Poskytovatelia VVA, ktorí uplatňujú vzdialené spracúvanie údajov, veľmi často používajú na túto detekciu dvojstupňový mechanizmus: prvá kontrola sa vykonáva lokálne na úrovni zariadenia a druhá na vzdialených serveroch, kde prebieha ďalšie spracúvanie údajov. V tomto prípade vývojári zvyčajne nastavujú pomerne nízku prahovú hodnotu, aby zlepšili skúsenosť používateľa a zabezpečili, že keď používateľ aktivačné slovo vysloví, bude takmer vždy rozpoznané – hoci by to malo znamenať jeho „nadmernú detekciu“ – a potom vykonajú druhú, reštriktívnejšiu kontrolu detekcie na serveri.

2.5 Hlasové úryvky a strojové učenie

20. VVA využívajú metódy strojového učenia na vykonávanie širokého spektra úloh (detekcia aktivačného slova, automatické rozpoznávanie reči, spracovanie prirodzeného jazyka, syntéza reči atď.), čo si vyžaduje zhromažďovanie, výber, označovanie atď. veľkých súborov údajov.
21. Nadmerné alebo nedostatočné zastúpenie určitých štatistických charakteristík môže ovplyvniť vývoj úloh založených na strojovom učení a následne sa premietnuť do príslušných výpočtov, a teda aj do spôsobu ich fungovania. Kvalita údajov, rovnako ako ich kvantita, preto zohráva významnú úlohu pri precízności a správności procesu strojového učenia.
22. Tvorcovia VVA by mohli mať záujem o prístup k údajom týkajúcim sa používania zariadenia v reálnych podmienkach, t. j. k hlasovým úryvkom, aby mohli zvýšiť kvalitu VVA a zlepšiť používané metódy strojového učenia.
23. Či už je to určenie databázy, na základe ktorej má učenie prebiehať, alebo oprava chýb pri spúšťaní algoritmu, učenie a tréning systémov umelej inteligencie si nevyhnutne vyžadujú zásah človeka. Táto časť práce, známa ako digitálna práca [digital labor], vyvoláva otázky o pracovných podmienkach a bezpečnosti. Spravodajské médiá v tejto súvislosti informovali aj o prenosoch údajov medzi tvorcami VVA a subdodávateľmi, ktoré prebehli údajne bez potrebných záruk ochrany súkromia.

3 PRVKY OCHRANY OSOBNÝCH ÚDAJOV

3.1 Právny rámec

24. Príslušným právnym rámcom Európskej únie pre VVA je v prvom rade všeobecné nariadenie o ochrane údajov, keďže spracúvanie osobných údajov je súčasťou základnej funkcie VVA. Okrem všeobecného nariadenia o ochrane údajov sa v smernici o súkromí a elektronických komunikáciách⁶ stanovuje osobitná norma pre všetky subjekty, ktoré chcú uchovávať informácie uložené v koncovom zariadení účastníka alebo používateľa v rámci EHP alebo k nim pristupovať.
25. V súlade s vymedzením pojmu „*koncové zariadenie*“⁷ sú príkladmi koncových zariadení smartfóny, inteligentné televízne prijímače a podobné zariadenia internetu vecí. Hoci VVA ako také sú softvérovými službami, vždy fungujú prostredníctvom fyzického zariadenia, ako je inteligentný reproduktor alebo inteligentná televízia. **VVA využívajú elektronické komunikačné siete na prístup k týmto fyzickým zariadeniam, ktoré predstavujú „koncové zariadenie“ v zmysle smernice o súkromí a elektronických komunikáciách. V dôsledku toho sa ustanovenia článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách uplatňujú vždy, keď VVA uchováva alebo sprístupňuje informácie v pripojenom fyzickom zariadení.**⁸
26. Všetky spracovateľské operácie osobných údajov vyplývajúce z uvedených spracovateľských operácií vrátane spracúvania osobných údajov získaných prístupom k informáciám v koncovom zariadení musia mať právny základ aj podľa článku 6 všeobecného nariadenia o ochrane údajov, aby boli zákonné.⁹
27. Keďže prevádzkovateľ bude musieť pri získavaní súhlasu s uložením informácií alebo získaním prístupu k nim podľa článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách informovať dotknutú osobu o všetkých účeloch spracúvania (t. j. o „následnom spracúvaní“) [subsequent processing] – vrátane akéhokoľvek spracúvania po uvedených operáciách – súhlas podľa článku 6 všeobecného nariadenia o ochrane údajov bude vo všeobecnosti najvhodnejším právnym základom na pokrytie následného spracúvania osobných údajov. Súhlas preto pravdepodobne bude predstavovať právny základ tak pre uchovávanie informácií a získanie prístupu k už uloženým informáciám, ako aj pre spracúvanie osobných údajov na základe uvedených spracovateľských operácií. Pri posudzovaní súladu s článkom 6 všeobecného nariadenia o ochrane údajov by sa malo zohľadniť, že spracúvanie ako celok

⁶ Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúca sa spracúvania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách), zmenená smernicou 2006/24/ES a smernicou 2009/136/ES (ďalej len „smernica o súkromí a elektronických komunikáciách“).

⁷ V článku 1 smernice Komisie 2008/63/ES z 20. júna 2008 o hospodárskej súťaži na trhoch s koncovými telekomunikačnými zariadeniami sa „*koncové zariadenie*“ vymedzuje ako „a) zariadenie priamo alebo nepriamo pripojené k rozhraniu verejnej telekomunikačnej siete na vysielanie, spracovanie alebo prijatie informácií; v oboch prípadoch (priamom alebo nepriamom) pripojenie môže byť urobené vodičom, optickým vláknom alebo elektromagneticky; pripojenie je nepriame, ak je zariadenie umiestnené medzi terminál a rozhranie verejnej siete; b) pozemnú družicovú stanicu“;

⁸ Pre podobné odôvodnenie týkajúce sa prepojených vozidiel pozri bod 12 usmernení EDPB 1/2020 (ďalej len „usmernenia EDPB 1/2020“). Pozri tiež EDPB, stanovisko 5/2019 týkajúce sa vzájomného pôsobenia medzi smernicou o súkromí a elektronických komunikáciách a všeobecným nariadením o ochrane údajov, najmä pokiaľ ide o príslušnosť, úlohy a právomoci orgánov pre ochranu osobných údajov.

⁹ Tamže, bod 41.

zahŕňa osobitné činnosti, v prípade ktorých sa zákonodarca EÚ snažil poskytnúť dodatočnú ochranu.¹⁰ Okrem toho prevádzkovatelia musia pri určovaní vhodného právneho základu zohľadniť vplyv na práva dotknutých osôb, aby sa dodržala zásada spravodlivosti.¹¹ Podstatné je, že prevádzkovatelia sa nemôžu odvolávať na článok 6 všeobecného nariadenia o ochrane údajov s cieľom znížiť dodatočnú ochranu stanovenú v článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách.

28. Ako sa uvádza v oddiele 2.3 (kroky 2 a 3), v súčasnosti si VVA vyžadujú prístup k hlasovým údajom [voice data], ktoré uchováva zariadenie VVA.¹² Preto sa uplatňuje článok 5 ods. 3 smernice o súkromí a elektronických komunikáciách. Uplatniteľnosť článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách znamená, že uchovávanie informácií, ako aj prístup k informáciám, ktoré už sú uložené vo VVA, si spravidla vyžaduje predchádzajúci súhlas koncového používateľa¹³, ale sú tu možné dve výnimky: po prvé vykonávanie alebo uľahčovanie prenosu [transmission] komunikácie cez elektronickú komunikačnú sieť, alebo po druhé, ak je to nevyhnutne potrebné na zabezpečenie služby informačnej spoločnosti, ktorú výslovne požaduje účastník alebo užívateľ.
29. Druhá výnimka („nevyhnutne potrebné na zabezpečenie služby informačnej spoločnosti, ktorú výslovne požaduje účastník alebo užívateľ“) by umožnila poskytovateľovi služieb VVA spracúvať údaje používateľov na účely plnenia požiadaviek používateľov (pozri odsek 72 v oddiele 3.4.1) bez súhlasu uvedeného v článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách. Naopak, **súhlas podľa článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách, by bol potrebný na uchovávanie informácií alebo získanie prístupu k informáciám na akýkoľvek iný účel, než je plnenie požiadaviek používateľov** (napr. profilovanie používateľov). Prevádzkovatelia by museli priradiť súhlas konkrétnym používateľom. Prevádzkovatelia by preto mali spracúvať údaje neregistrovaných používateľov, len aby mohli vykonávať ich požiadavky.
30. VVA môžu náhodne zachytiť zvuky osôb, ktoré nemali v úmysle používať službu VVA. Po prvé, do určitej miery a v závislosti od VVA sa aktivačný výraz môže meniť. Osoby, ktoré o tejto zmene nevedia, by mohli omylom použiť nový aktivačný výraz. Po druhé, k detekcii aktivačného výrazu môže dôjsť chybné alebo omylom. Je veľmi nepravdepodobné, že by sa v prípade náhodnej aktivácie uplatňovala niektorá z výnimiek uvedených v článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách. Súhlas podľa všeobecného nariadenia o ochrane údajov musí byť okrem toho „jednoznačným prejavom vôle dotknutej osoby“. Je preto veľmi nepravdepodobné, že by sa náhodná aktivácia mohla interpretovať ako platný súhlas. Ak prevádzkovatelia zistia (napr. na základe automatickej kontroly alebo kontroly ľuďmi), že služba VVA náhodne spracúvala osobné údaje, mali by overiť, či pre každý účel spracúvania takýchto údajov existuje platný právny základ. V opačnom prípade by sa náhodne získané údaje mali vymazať.

¹⁰ Stanovisko 5/2019, bod 41.

¹¹ EDPB – Usmernenia 2/2019 o spracúvaní osobných údajov podľa článku 6 ods. 1 písm. b) všeobecného nariadenia o ochrane údajov v súvislosti s poskytovaním on-line služieb dotknutým osobám, verzia 2.0, 8. októbra 2019, bod 1.

¹² Je možné, že v budúcnosti zariadenia VVA budú fungovať na paradigme edge computing a budú schopné poskytovať niektoré služby lokálne. V takom prípade bude potrebné prehodnotiť uplatniteľnosť smernice o súkromí a elektronických komunikáciách.

¹³ Pozri aj usmernenia EDPB 1/2020, bod 14.

31. Okrem toho treba poznamenať, že osobné údaje spracúvané VVA môžu byť veľmi citlivej povahy. Môže to byť osobné údaje z hľadiska obsahu (čo znamená hovorený text), ako aj z hľadiska metaúdajov (pohlavie alebo vek hovoriaceho atď.). EDPB pripomína, že hlasové údaje sú vo svojej podstate biometrické osobné údaje.¹⁴ Preto, ak sa takéto údaje spracúvajú na účely individuálnej identifikácie fyzickej osoby alebo ak sú vo svojej podstate osobnými údajmi osobitnej kategórie alebo ak boli ako také určené, spracúvanie musí mať platný právny základ podľa článku 6 a musí byť sprevádzané výnimkou z článku 9 všeobecného nariadenia o ochrane údajov (pozri oddiel 3.7 ďalej).

3.2 Identifikácia spracúvania údajov a zainteresovaných strán

32. Vzhľadom na početné možnosti pomoci, ktorú VVA môže poskytovať v rôznych prostrediach každodenného života dotknutej osoby¹⁵, treba poznamenať, že by sa malo starostlivo zvážiť spracúvanie osobných údajov, na ktoré môžu mať vplyv rôzne zainteresované strany.

3.2.1 Spracúvanie osobných údajov

33. Z hľadiska ochrany osobných údajov možno bez ohľadu na typ VVA (t. j. typ zariadenia, funkcie, služby alebo ich kombináciu), ktorý dotknutá osoba používa, opísať niekoľko konštantných prvkov. Tieto konštantné prvky sa týkajú plurality osobných údajov, dotknutých osôb a spracúvania údajov.

Pluralita typov osobných údajov

34. Vymedzenie pojmu osobných údajov podľa článku 4 ods. 1 všeobecného nariadenia o ochrane údajov zahŕňa širokú škálu rôznych údajov a uplatňuje sa v technologicky neutrálnom kontexte na akékoľvek informácie, ktoré sa týkajú „*identifikovanej alebo identifikovateľnej fyzickej osoby*“.¹⁶ Akákoľvek interakcia dotknutej osoby s VVA môže patriť do rozsahu pôsobnosti tohto vymedzenia. V priebehu interakcie sa počas prevádzky VVA môže spracúvať široký rozsah osobných údajov, ako sa uvádza v oddiele 2.4.
35. Od prvotnej požiadavky až po súvisiacu odpoveď, činnosť alebo následný úkon (napr. nastavenie týždenného upozornenia) sa preto na základe prvého vstupu osobných údajov generujú následné osobné údaje. Ide o primárne údaje (napr. údaje o konte, hlasové záznamy, história žiadostí), pozorované údaje [observed data] (napr. údaje zo zariadenia, ktoré sa týkajú dotknutej osoby, záznamy o činnostiach, online činnosti), ako aj odvodené údaje [inferred or derived data] (napr. profilovanie používateľov). VVA používajú reč na sprostredkovanie medzi používateľmi a všetkými prepojenými službami (napr. vyhľadávačom, internetovým obchodom alebo službou streamovania hudby), ale na rozdiel od iných sprostredkovateľov môžu mať VVA

¹⁴ V článku 4 ods. 14 všeobecného nariadenia o ochrane údajov sa „biometrické údaje“ vymedzujú ako „osobné údaje, ktoré sú výsledkom osobitného technického spracúvania, ktoré sa týka fyzických, fyziologických alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby, ako napríklad vyobrazenia tváre alebo daktyloskopické údaje“.

¹⁵ Napríklad: doma, vo vozidle, na ulici, v práci alebo v akýchkoľvek iných súkromných, verejných alebo pracovných priestoroch alebo v kombinácii týchto priestorov.

¹⁶ V článku 4 ods. 1 všeobecného nariadenia o ochrane údajov sa taktiež stanovuje, že „*identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby*“.

úplný prístup k obsahu požiadaviek a následne poskytovať tvorcom VVA širokú škálu osobných údajov v závislosti od účelu spracúvania.

36. Pri pluralite osobných údajov spracúvaných pri používaní VVA, by sa pozornosť mala venovať aj pluralite kategórií osobných údajov (pozri oddiel 3.7). EDPB pripomína, že ak sa spracúvajú osobitné kategórie údajov¹⁷, v článku 9 všeobecného nariadenia o ochrane údajov sa vyžaduje, aby prevádzkovateľ určil platnú výnimku zo zákazu spracúvania podľa článku 9 ods. 1 a platný právny základ podľa článku 6 ods. 1 s použitím primeraných prostriedkov uvedených v článku 9 ods. 2. Výslovný súhlas môže byť jednou z vhodných výnimiek, ak je právnym základom súhlas podľa článku 6 ods. 1. V článku 9 sa tiež (podrobne) uvádza, že členské štáty môžu zaviesť ďalšie podmienky spracúvania biometrických údajov alebo údajov z iných osobitných kategórií.

Pluralita dotknutých osôb

37. Pri použití VVA sa osobné údaje spracúvajú od prvej interakcie s VVA. Pri niektorých dotknutých osobách pôjde o nákup VVA a/alebo konfiguráciu používateľského konta (t. j. registrovaní používatelia). Pri iných dotknutých osobách pôjde o prvý prípad, keď vedome komunikujú s VVA inej dotknutej osoby, ktorá si kúpila a/alebo konfigurovala VVA (t. j. neregistrovaní používatelia). Okrem týchto dvoch kategórií dotknutých osôb existuje tretia kategória: náhodní používatelia, ktorí bez ohľadu na to, či sú registrovaní alebo nie, nevedome VVA o niečo požiadali (napr. vyslovili správny aktivačný výraz bez toho, aby vedeli, že VVA je aktívny, alebo povedali iné slová, ktoré VVA omylom označil ako aktivačný výraz).
38. Pojem pluralita dotknutých osôb sa vzťahuje aj na viacerých používateľov jedného VVA (napr. zariadenie zdieľané medzi registrovanými a neregistrovanými používateľmi, medzi kolegami, v rodine, v škole) a rôzne druhy používateľov podľa ich situácie (napr. dospelá osoba, dieťa, staršia osoba alebo osoba so zdravotným postihnutím). Hoci VVA môže ponúknuť jednoduchšiu interakciu s digitálnym nástrojom a mnohé výhody pre niektoré kategórie dotknutých osôb, je dôležité zohľadniť osobitosti každej kategórie dotknutých osôb a okolnosti, za ktorých sa VVA používa.

Pluralita spracúvania údajov

39. Technológie používané na poskytovanie VVA majú vplyv aj na množstvo spracúvaných údajov a druhy spracúvania. Čím častejšie VVA poskytuje služby alebo funkcie a je prepojený s inými zariadeniami alebo službami, ktoré spravujú iné strany, tým sa zvyšuje množstvo spracúvaných osobných údajov a mení sa účel spracúvania. Výsledkom je pluralita spracúvania vykonávaného automatizovanými prostriedkami, ako je opísané v oddiele 2. Okrem automatizovaných prostriedkov môže niektoré prípady zahŕňať aj spracúvanie človekom. Napríklad v prípade, keď používaná technológia zahŕňa ľudský zásah, ako je preskúmanie prepisu hlasov do textovej podoby alebo poskytovanie anotácií k osobným údajom, ktoré možno použiť na zavádzanie nových modelov do technológie strojového učenia. Platí to aj v prípade, keď ľudia analyzujú osobné údaje (napr. metaúdaje) s cieľom zlepšiť službu, ktorú poskytuje VVA.

¹⁷ V článku 9 ods. 1 všeobecného nariadenia o ochrane údajov sa osobitné kategórie osobných údajov vymedzujú ako „osobné údaje, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, a spracúvanie genetických údajov, biometrických údajov na individuálnu identifikáciu fyzickej osoby, údajov týkajúcich sa zdravia alebo údajov týkajúcich sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby“.

3.2.2 Spracúvanie prevádzkovateľmi a sprostredkovateľmi

40. Dotknuté osoby by mali byť schopné pochopiť a identifikovať príslušné úlohy a mali by byť schopné kontaktovať jednotlivé zainteresované strany alebo konať spolu s nimi, ako sa to vyžaduje podľa všeobecného nariadenia o ochrane údajov. Rozdelenie úloh by nemalo byť na úkor dotknutých osôb, hoci scenáre môžu byť zložité alebo sa môžu vyvíjať. Pri posudzovaní ich úloh sa zainteresované strany odkazujú na usmernenia EDPB 7/2020 k pojmom prevádzkovateľ a sprostredkovateľ podľa všeobecného nariadenia o ochrane údajov.¹⁸
41. Ako sa uvádza v odseku 15, hlavné zainteresované strany môžu plniť úlohu poskytovateľa alebo tvorca, navrhovateľa aplikácie, integrátora, vlastníka alebo kombináciu týchto úloh. V závislosti od úloh v rámci obchodného vzťahu zainteresovaných strán, v závislosti od požiadavky používateľa, od osobných údajov, od spracovateľských činností a ich účelov, prichádzajú do úvahy rôzne scenáre. Zainteresované strany by mali prijať jednoznačné rozhodnutie a informovať dotknuté osoby o podmienkach, za ktorých každá z nich bude konať a plniť príslušné úlohy prevádzkovateľov, spoločných prevádzkovateľov alebo sprostredkovateľov, ako sa stanovuje vo všeobecnom nariadení o ochrane údajov.¹⁹ Každá z nich môže prevziať jednu alebo viacero úloh, keďže môžu byť samostatným prevádzkovateľom, spoločným prevádzkovateľom alebo sprostredkovateľom pri jednom spracúvaní údajov, zatiaľ čo plnia inú úlohu pri inom spracúvaní údajov.
42. Zo všeobecnejšieho pohľadu môže tvorca konať ako prevádzkovateľ pri určovaní účelov a prostriedkov spracúvania, ale môže zasiahnuť ako sprostredkovateľ pri spracúvaní osobných údajov v mene iných strán, ako je napríklad vývojár aplikácií. Používateľ VVA by preto podliehal viacerým prevádzkovateľom: vývojárovi aplikácie a tvorcovi. Okrem toho je možné, že tvorca, integrátor a vývojár sú zoskupení v jednom subjekte, ktorý koná ako samostatný prevádzkovateľ. V každom prípade sa príslušné úlohy musia vymedzovať na základe individuálnej analýzy.

Príklad 1:

Tvorca VVA spracúva údaje používateľov na mnohé účely vrátane zlepšovania schopnosti VVA porozumieť hlasu a presne reagovať na požiadavky. Hoci tento účel môže viesť k spracúvaniu údajov vyplývajúcich z používania aplikácií poskytovaných tretími stranami, existuje len jeden prevádzkovateľ: tvorca VVA, v mene ktorého a na ktorého účely sa vykonáva spracúvanie.

Príklad 2:

Banka ponúka svojim zákazníkom aplikáciu na správu ich účtov, na ktorú sa možno priamo obracať prostredníctvom VVA.

Do spracúvania osobných údajov sú zapojené dva subjekty: tvorca VVA a vývojár aplikácie banky.

V tomto scenári je banka prevádzkovateľom na poskytovanie služby, pretože určuje účely a základné prostriedky [essential means] spracúvania súvisiaceho s aplikáciou, ktorá

¹⁸ Usmernenia EDPB 07/2020 k pojmom prevádzkovateľ a sprostredkovateľ podľa všeobecného nariadenia o ochrane údajov, V2.0, prijaté 7. júla 2021 (ďalej len „usmernenia 7/2020“).

¹⁹ Všeobecné nariadenie o ochrane údajov, články 12 až 14, článok 26.

umožňuje interakciu s asistentom. Banka ponúka vlastne špecializovanú aplikáciu, ktorá jej používateľovi, zákazníkovi banky, umožňuje spravovať svoje účty na diaľku. Okrem toho rozhoduje o prostriedkoch spracúvania výberom vhodného sprostredkovateľa, ktorým je tvorca VVA, ktorého odborné znalosti môžu zohrávať dôležitú úlohu pri určovaní týchto prostriedkov (napríklad môže prevádzkovať vývojovú platformu, ktorá umožňuje začlenenie aplikácií tretích strán do VVA, a preto stanovuje rámec a podmienky, ktoré musia vývojári aplikácií dodržiavať).

43. Z hľadiska dotknutej osoby je treba poznamenať, že tie isté osobné údaje môže spracúvať viacero zainteresovaných strán, aj keď dotknutá osoba v skutočnosti neočakáva, že do spracovateľského reťazca budú zapojené iné strany ako poskytovateľ VVA. Ak teda dotknutá osoba koná spolu s poskytovateľom VVA v súvislosti so svojimi osobnými údajmi (napr. uplatňovanie práv dotknutej osoby), neznamená to automaticky, že sa toto konanie bude vzťahovať aj na tie isté osobné údaje, ktoré spracúva iná zainteresovaná strana. Ak sú tieto zainteresované strany nezávislými prevádzkovateľmi, je dôležité, aby sa dotknutým osobám poskytlo jasné oznámenie, v ktorom budú vysvetlené rôzne fázy a účastníci spracúvania. Okrem toho by sa v prípadoch existencie spoločných prevádzkovateľov malo objasniť, či je každý prevádzkovateľ schopný dodržiavať všetky práva dotknutej osoby alebo ktorý prevádzkovateľ zodpovedá za ktoré právo.²⁰

Príklad 3:

V tomto scenári chce tvorca VVA použiť údaje, ktoré boli získané a spracúvané na účely služby poskytovanej bankou, aby zlepšil jej systém rozpoznávania hlasu. Tvorca VVA, ktorý spracúva údaje na vlastné účely, bude mať pri tomto konkrétnom spracúvaní postavenie prevádzkovateľa.

44. Keďže do reťazca spracúvania môže byť zapojených mnoho zainteresovaných strán a prípadne mnohí zamestnanci, môže dochádzať k rizikovým situáciám, ak nie sú zavedené primerané opatrenia a záruky. Zodpovednosť za ne nesú prevádzkovatelia, a preto by sa mali zamerať na ochranu osobných údajov, najmä výberom vhodných obchodných partnerov a sprostredkovateľov, uplatňovaním zásad špecificky navrhutej a štandardnej ochrany údajov²¹, zavedením primeraných bezpečnostných a iných nástrojov všeobecného nariadenia o ochrane údajov, ako sú audity a právne dohody (napr. článok 26 v prípade spoločných prevádzkovateľov alebo článok 28 všeobecného nariadenia o ochrane údajov v prípade sprostredkovateľov).
45. Ekosystém VVA je zložitý, keďže si v jeho rámci potenciálne mnohí účastníci môžu vymieňať a spracúvať osobné údaje ako prevádzkovatelia alebo sprostredkovatelia. Je nanajvýš dôležité objasniť úlohu každého účastníka v súvislosti s každým spracúvaním a dodržiavať zásadu minimalizácie údajov aj v súvislosti s výmenou údajov.
46. Okrem toho by prevádzkovatelia mali byť obozretní, pokiaľ ide o prenosy osobných údajov, a mali by zaručovať požadovanú úroveň ochrany v celom spracovateľskom reťazci, najmä ak využívajú služby nachádzajúce sa mimo EHP.

3.3 Transparentnosť

²⁰ Usmernenia 7/2020, ods. 165.

²¹ Pozri usmernenia EDPB 4/2019 týkajúce sa článku 25 Špecificky navrhnutá a štandardná ochrana údajov, verzia 2.0, prijaté 20. októbra 2020.

47. Keďže VVA spracúvajú osobné údaje (napr. hlas používateľov, miesto alebo obsah komunikácie), musia spĺňať požiadavky na transparentnosť stanovené vo všeobecnom nariadení o ochrane údajov, ako sa uvádza v článku 5 ods. 1 písm. a), ako aj v článku 12 a článku 13 (vysvetlené v odôvodnení 58). Prevádzkovatelia sú povinní informovať používateľov o spracúvaní ich osobných údajov v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme.
48. Neposkytnutie potrebných informácií je porušením povinností, ktoré môže ovplyvniť legitímnosť spracúvania údajov. Dodržiavanie požiadavky transparentnosti je nevyhnutné, pretože pri spracúvaní údajov slúži ako kontrolný mechanizmus a umožňuje používateľom uplatňovať svoje práva. Riadnym informovaním používateľov o tom, ako sa používajú ich osobné údaje, sa prevádzkovateľom sťažuje možnosť zneužívania VVA na účely, ktoré presahujú očakávania používateľov. Zámerom patentovaných technológií je napríklad z hlasu používateľa odvodiť zdravotný stav a emocionálne rozpoloženie a zodpovedajúcim spôsobom prispôbiť poskytované služby.
49. Dodržiavanie požiadaviek na transparentnosť môže byť obzvlášť náročné pre poskytovateľa služieb VVA alebo akýkoľvek iný subjekt, ktorý koná ako prevádzkovateľ. Vzhľadom na osobitnú povahu VVA čelia prevádzkovatelia viacerým prekážkam pri dodržiavaní požiadaviek na transparentnosť podľa všeobecného nariadenia o ochrane údajov:
-)] **Viacerí používateľa:** prevádzkovatelia by mali informovať všetkých používateľov (registrovaných, neregistrovaných a náhodných používateľov), nielen používateľov, ktorí nastavujú VVA.
 -)] **Zložitosť ekosystému:** ako je vysvetlené v časti o technologických informáciách, totožnosť a úlohy osôb, ktoré spracúvajú osobné údaje pri používaní VVA, nie sú používateľom vôbec zrejme.
 -)] **Osobitosti hlasového rozhrania:** digitálne systémy zatiaľ nie sú vhodné na interakcie len na základe hlasu, čo vyplýva aj z takmer systematického používania sprievodnej obrazovky. Avšak prispôbiť sa hlasovému rozhraniu a dokázať prostredníctvom tohto prostriedku jasne a správne informovať používateľa je nevyhnutné.
50. VVA možno považovať za konečný automat, ktorý pri bežnom fungovaní prechádza cez množinu stavov. Môžu lokálne počúvať na účely detekcie aktivačných výrazov alebo komunikovať so vzdialeným serverom pri riešení príkazu, ale môžu predpokladať mnohé ďalšie stavy v závislosti od kontextu (napr. ak sa v pozadí vyskytuje šum z prostredia) alebo v závislosti od používateľa, ktorý s nimi hovorí (napr. môžu hovoriť s identifikovaným alebo neznámym používateľom). Tieto situácie, sa žiaľ, odohrávajú v značnej asymetrii informácií, pokiaľ ide o používateľa, ktorý si je sotva vedomý toho, či zariadenie počúva, a ešte menej stavu, v akom sa nachádza.
51. Dôrazne sa odporúča, aby tvorcovia a vývojári VVA prijali primerané opatrenia na riešenie týchto asymetrií, aby sa tak fungovanie VVA stalo interaktívnejším. Používatelia by mali byť informovaní o stave, v akom sa zariadenie práve nachádza. Toto zlepšenie transparentnosti možno dosiahnuť tak, že dialóg medzi človekom a strojom sa stane interaktívnejším (napr. zariadenie môže nejakým spôsobom potvrdiť príjem hlasového príkazu), alebo sa stav zariadenia bude prezentovať pomocou osobitných signálov. V tejto súvislosti je možné preskúmať mnoho možností, ktoré siahajú od používania konkrétnych hlasových potvrdení a viditeľných ikon či svetiel až po používanie obrázkov na zariadení.

52. Tieto otázky sú obzvlášť dôležité vzhľadom na pluralitu používateľov a prítomnosť zraniteľných kategórií osôb, ako sú deti, starší ľudia alebo používatelia s audiovizuálnym zdravotným postihnutím.
53. Z uvedeného vyplývajú dve dôležité otázky: aký je najvhodnejší spôsob informovania používateľov a kedy je vhodné ich informovať? Tieto otázky by sa mali ďalej preskúmať v dvoch rôznych situáciách v závislosti od toho, či VVA má len jedného používateľa (napríklad osobný smartfón) alebo potenciálne viacerých používateľov (napr. inteligentné domáce zariadenie). Pri používaní technológie VVA by mohlo dôjsť aj k zmiešaniu týchto dvoch základných scenárov, napr. keď používateľ má osobný smartfón a pripojí ho k vozidlu. VVA v smartfóne, o ktorom možno odôvodnene predpokladať, že ho bude používať len tento používateľ, sa tým „rozšíri“ na ostatné osoby v aute.
54. V súčasnosti sú všetky VVA pripojené k používateľskému kontu a/alebo sú zriadené prostredníctvom aplikácie, ktorá si konto vyžaduje. Mala by sa riešiť otázka, ako by prevádzkovatelia mohli informovať týchto používateľov o politike ochrany osobných údajov pri nastavovaní VVA, a síce tak, ako sa uvádza v usmerneniach pracovnej skupiny zriadenej podľa článku 29 o transparentnosti. Pred stiahnutím by aplikácie mali sprístupniť potrebné informácie v internetovom obchode.²² Týmto spôsobom sa informácie poskytnú čo najskôr a zároveň najneskôr v čase získania osobných údajov. Niektorí poskytovatelia VVA zahŕňajú aplikácie tretích strán do štandardného nastavenia VVA, aby sa tieto aplikácie mohli používať prostredníctvom osobitných aktivačných výrazov. VVA, ktoré používajú túto stratégiu zahrnutia aplikácií tretej strany, by mali zabezpečiť, aby používatelia dostávali potrebné informácie aj o spracúvaní treťou stranou.
55. Mnohí tvorcovia VVA však požadujú používateľské kontá, ktoré spájajú službu VVA s viacerými ďalšími službami, ako sú e-mail, streamovanie videí alebo nákupy. V dôsledku rozhodnutia tvorca VVA o prepojení konta s mnohými rôznymi službami sa vyžadujú veľmi dlhé a zložité politiky ochrany osobných údajov. Dĺžka a zložitost' takýchto politik ochrany osobných údajov vo veľkej miere bráni dodržiavaniu zásady transparentnosti.

Príklad 4:

Tvorca VVA vyžaduje, aby používatelia VVA mali na prístup k službe VVA zriadené konto. Toto používateľské konto nie je špecifické pre službu VVA a môže sa používať aj pri iných službách, ktoré ponúka tvorca VVA, ako sú e-mail, cloudové úložiská a sociálne médiá. Na vytvorenie konta musia používatelia prečítať a akceptovať dlhú 30-stranovú politiku ochrany osobných údajov. Táto politika zahŕňa informácie o spracúvaní osobných údajov všetkými službami, ktoré by mohli byť spojené s kontom.

Informácie, ktoré v tomto prípade poskytol tvorca VVA, sa nepovažujú za stručné a ich zložitost' znižuje požadovanú úroveň transparentnosti. Tvorca VVA by preto nedodržel požiadavky na transparentnosť stanovené v článkoch 12 a 13 všeobecného nariadenia o ochrane údajov.

56. Hoci najbežnejším spôsobom poskytovania potrebných informácií je písomná forma, vo všeobecnom nariadení o ochrane údajov sa umožňujú aj „iné prostriedky“. V odôvodnení 58 sa výslovne uvádza, že informácie sa môžu poskytovať v elektronickej podobe, napr.

²² Usmernenia k transparentnosti podľa nariadenia 2016/679, WP260 rev. 01, schválené EDPB (ďalej len „usmernenia pracovnej skupiny zriadenej podľa článku 29 WP260“), ods. 11.

prostredníctvom webového sídla. Okrem toho by sa pri výbere vhodnej metódy informovania dotknutých osôb mali zohľadniť osobitné okolnosti, ako napríklad spôsob komunikácie medzi prevádzkovateľom a dotknutou osobou.²³ Alternatívou pri zariadeniach bez obrazovky môže byť poskytnutie ľahko zrozumiteľného odkazu, či už priamo alebo prostredníctvom e-mailu. Už existujúce riešenia by mohli pri informovaní poslúžiť ako príklad, napr. postupy telefonických centier, ktoré volajúceho informujú, že telefonický hovor sa zaznamenáva a odkazujú ho na svoju politiku ochrany osobných údajov. Obmedzenia VVA pri zariadeniach bez obrazovky nezbavujú prevádzkovateľa povinnosti poskytovať potrebné informácie podľa všeobecného nariadenia o ochrane údajov pri nastavovaní VVA alebo inštalácii alebo používaní aplikácie VVA. Tvorcovia a vývojári VVA by mali vyvinúť hlasové rozhrania na uľahčenie poskytovania povinných informácií.

57. VVA by mohli byť veľmi zaujímavé pre používateľov so zrakovým postihnutím, keďže poskytujú alternatívnu možnosť interakcie so službami IT, ktoré sa tradične opierajú o vizuálne informácie. Podľa článku 12 ods. 1 všeobecného nariadenia o ochrane údajov je poskytnutie potrebných informácií ústne možné výlučne na žiadosť dotknutej osoby, nie je to však štandardným spôsobom. Obmedzenia VVA pri zariadeniach bez obrazovky by si však vyžadovali možnosť automatického ústneho poskytovania informácií, ktorá by sa mohla rozšíriť o možnosť ich písomného poskytovania. Pri používaní zvuku na informovanie dotknutých osôb by prevádzkovatelia mali potrebné informácie poskytovať stručne a zrozumiteľne. Okrem toho by dotknuté osoby mali mať možnosť vypočuť si informácie znovu.²⁴
58. Prijatie primeraných opatrení na dodržiavanie požiadaviek na transparentnosť podľa všeobecného nariadenia o ochrane údajov je zložitejšie, ak existuje viac používateľov VVA, ktorí sú iní ako vlastník zariadenia. Tvorcovia VVA musia zvážiť, ako riadne informovať neregistrovaných a náhodných používateľov o spracúvaní ich osobných údajov. Ak je súhlas právnym základom pre spracúvanie údajov používateľov, používatelia musia byť riadne informovaní, aby súhlas platil²⁵.
59. Zabezpečenie súladu so všeobecným nariadením o ochrane údajov si vyžaduje, aby prevádzkovatelia našli spôsob, ako informovať nielen registrovaných používateľov, ale aj neregistrovaných používateľov a náhodných používateľov VVA. Títo používatelia by mali byť informovaní čo najskôr a **najneskôr v čase** spracúvania. Táto podmienka by mohla byť v praxi obzvlášť ťažko splniteľná.
60. Určité osobitosti podnikového prostredia by takisto nemali byť na úkor dotknutých osôb. Keďže mnohé zainteresované strany sú globálne spoločnosti alebo sú dobre známe svojou konkrétnou podnikateľskou činnosťou (napr. telekomunikácie, elektronický obchod, informačné technológie, webové činnosti), spôsob, akým poskytujú službu VVA by mal byť jasný. Primerané informácie by mali dotknutým osobám umožniť pochopiť, či ich používanie VVA bude spojené s inými spracovateľskými činnosťami, ktoré spravuje poskytovateľ služieb VVA (napr. telekomunikácie, elektronický obchod, informačné technológie alebo webové činnosti), oddelene od samotného používania VVA.

Príklad 5:

²³ Usmernenia pracovnej skupiny zriadenej podľa článku 29, WP260, bod 19.

²⁴ Usmernenia pracovnej skupiny zriadenej podľa článku 29, WP260, bod 21.

²⁵ Všeobecné nariadenie o ochrane údajov, článok 4 ods. 11.

Aby mohol používateľ svojho asistenta použiť, tvorca VVA, ktorý poskytuje aj platformu sociálnych médií a vyhľadávač, požaduje, aby používateľ prepojiť svoje konto s asistentom. Prepojením svojho konta s používaním VVA, môže tvorca vylepšovať profil svojich používateľov prostredníctvom využitia asistenta, aplikácií (alebo zručností), ktoré sú nainštalované, realizovaných objednávok atď. Interakcie s asistentom sú novým zdrojom informácií súvisiacich s používateľom. Tvorca VVA by mal používateľom poskytnúť jasné informácie o tom, ako budú ich údaje spracúvané v prípade každej služby, ako aj kontrolu, ktorá používateľovi umožní vybrať si, či sa údaje použijú alebo nepoužijú pri profilovaní.

Odporúčania

61. Keď sú používatelia informovaní o spracúvaní osobných údajov prostredníctvom VVA na základe politiky ochrany osobných údajov, ktoré sa vzťahujú na používateľské konto a konto je prepojené s inými nezávislými službami (napr. e-mailom alebo online nákupmi), EDPB odporúča, aby sa v rámci politiky ochrany osobných údajov jasne vymedzila časť týkajúca sa spracúvania osobných údajov prostredníctvom VVA.
62. Informácie poskytnuté používateľovi by mali zodpovedať presnému zhromažďovaniu a spracúvaniu, ktoré sa vykonáva. Hoci niektoré metaúdaje sú obsiahnuté v hlasovej vzorke (napr. úroveň stresu hovoriacej osoby), nie je automaticky jasné, či sa takáto analýza vykonáva. Je veľmi dôležité, aby prevádzkovatelia boli transparentní, pokiaľ ide o konkrétne aspekty nespracovaných údajov [raw data], ktoré spracúvajú.
63. Okrem toho by malo byť vždy zrejmé, v akom stave sa VVA nachádza. Používatelia by mali vždy byť schopní určiť, či VVA práve počúva v rámci uzavretého okruhu, a najmä či vysiela informácie do systému na pozadí. Tieto informácie by mali byť prístupné aj osobám so zdravotným postihnutím, ako je napríklad farbosleposť (daltonizmus), hluchota (anakúzia). Osobitná pozornosť by sa mala venovať skutočnosti, že VVA umožňujú spôsob používania, pri ktorom nie je potrebný očný kontakt. Preto by všetka spätná väzba pre používateľov vrátane zmien stavu mala byť dostupná minimálne vo vizuálnej a akustickej forme.
64. Osobitná pozornosť by sa mala venovať prípadom, ak zariadenia umožňujú pridať funkciu tretej strany („aplikácie“ pre VVA). Zatiaľ čo niektoré všeobecné informácie môžu byť poskytnuté používateľovi, keď takúto funkciu pridáva (vzhľadom na to, že je to voľba používateľa), pri bežnom používaní zariadenia môžu byť hranice medzi rôznymi zúčastnenými prevádzkovateľmi oveľa menej jasné, t. j. používateľ nemusí byť dostatočne informovaný o tom, ako a kto jeho údaje spracúva (a do akej miery) pri konkrétnej otázke.
65. Všetky informácie o spracúvaní na základe údajov získaných a odvodených zo spracúvania zaznamenaného hlasu by mali byť dostupné aj používateľom podľa článku 12 všeobecného nariadenia o ochrane údajov.
66. Prevádzkovatelia VVA by mali transparentne informovať o tom, aký druh informácií môže VVA získavať o svojom okolí, napríklad, okrem iného, o iných osobách v miestnosti, hudbe v pozadí, akékoľvek spracúvanie hlasu na zdravotné alebo iné marketingové účely, o spoločenských zvieratách atď.

3.4 Obmedzenie účelu a právny základ

67. Spracúvanie hlasových požiadaviek zo strany VVA má zrejmý účel, ktorým je plnenie danej požiadavky. Často však existujú ďalšie účely, ktoré nie sú také zrejmé, ako napríklad zlepšenie schopnosti VVA porozumieť prirodzenému jazyku prostredníctvom tréningu modelu VVA

technikami strojového učenia. K najbežnejším účelom spracúvania osobných údajov zo strany VVA patria:

- J plnenie požiadaviek používateľov
- J zlepšovanie VVA prostredníctvom tréovania modelu strojového učenia a kontroly ľuďmi a označovania hlasových prepisov
- J identifikácia používateľa (pomocou hlasových údajov)
- J profilovanie používateľov na účely personalizácie obsahu alebo reklamy

68. Vzhľadom na svoju úlohu sprostredkovateľov [intermediaries] a na spôsob, akým boli navrhnuté, VVA spracúvajú širokú škálu osobných a iných ako osobných údajov. Umožňuje to spracúvanie osobných údajov na mnohé účely, ktoré idú nad rámec odpovedania na požiadavky používateľov a ktoré by mohli byť úplne nepovšimnuté. Analýzou údajov získaných prostredníctvom VVA je možné zistiť alebo odvodiť záujmy používateľov, ich časový rozvrh, jazdné trasy alebo zvyky. To by mohlo umožniť spracúvanie osobných údajov na nepredvídané účely (napr. analýza sentimentu alebo posúdenie zdravotného stavu²⁶), čo by výrazne presahovalo primerané očakávania používateľov.
69. Prevádzkovatelia by mali jasne špecifikovať svoj účel (účely) vo vzťahu ku kontextu, v ktorom sa VVA používa, aby ho dotknuté osoby jasne pochopili (napr. uvádzanie účelov v kategóriách). V súlade s článkom 5 ods. 1 všeobecného nariadenia o ochrane údajov by údaje mali byť získavané na konkrétne stanovené, výslovne uvedené a legitímne účely a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmito účelmi.

3.4.1 Plnenie požiadaviek používateľov

70. VVA sa v prvom rade používajú na vydávanie hlasových príkazov, ktoré musí vykonať VVA alebo súvisiaca aplikácia alebo služba (napr. služba streamovania hudby, služba mapovania alebo elektronický zámok). Spracúvať by sa preto mohli hlas používateľa a potenciálne ďalšie údaje (napr. poloha používateľa, keď žiada o vyhľadanie trasy do určitej destinácie).

Príklad 6:

Cestujúci v inteligentnom vozidle, ktoré je vybavené VVA požiada o trasu k najbližšej čerpacej stanici. VVA spracúva hlas používateľa, aby pochopil príkaz a zistil polohu vozidla s cieľom nájsť trasu a zaslať ju inteligentnému zariadeniu, ktorý ho zobrazí na obrazovke vozidla.

71. Pokiaľ spracúvanie hlasových príkazov zahŕňa uchovávanie informácií uložených v koncových zariadeniach koncového používateľa alebo prístup k nim, musí sa dodržať článok 5 ods. 3 smernice o súkromí a elektronických komunikáciách. Hoci článok 5 ods. 3 obsahuje všeobecnú zásadu, že takéto uchovávanie alebo prístup si vyžaduje predchádzajúci súhlas koncového používateľa, stanovuje sa v ňom aj výnimka z požiadavky súhlasu, ak je to „nevyhnutne potrebné k tomu, aby mohol poskytovateľ služby informačnej spoločnosti poskytovať služby, o ktorú účastník alebo užívateľ výslovne požiadal“. Pokiaľ sa hlasové údaje spracúvajú na účely plnenia požiadaviek používateľa, sú oslobodené od požiadavky predchádzajúceho súhlasu.

²⁶ Eoghan Furey, Juanita Blue, „Alexa, Emotion, Privacy and GDPR“, dokument z konferencie, Human Computer Interaction Conference, júl [2018].

72. Ako už bolo uvedené, všetky spracovateľské operácie osobných údajov po ich uchovaní alebo prístupe k nim v koncovom zariadení koncových používateľov musia mať právny základ podľa článku 6 všeobecného nariadenia o ochrane údajov, aby boli zákonné.
73. V rámci VVA sa vykonávajú dve po sebe nasledujúce spracovateľské operácie. Ako už bolo uvedené, prvá si vyžaduje prístup k VVA (a preto musia byť splnené podmienky uvedené v článku 5 ods. 3 smernice o súde a elektronických komunikáciách). Okrem podmienok v článku 5 ods. 3 smernice o súde a elektronických komunikáciách si druhý krok vyžaduje aj právny základ podľa článku 6 všeobecného nariadenia o ochrane údajov.
74. Ak sa jednotlivец rozhodne použiť VVA, vo všeobecnosti to znamená, že tento používateľ si musí najprv zaregistrovať konto, aby mohol aktivovať VVA. Inými slovami, táto situácia sa týka zmluvného vzťahu²⁷ medzi registrovaným používateľom a prevádzkovateľom VVA. Vzhľadom na jej podstatu a základný cieľ je hlavným účelom tejto zmluvy použitie VVA na vybavenie požiadavky používateľa.
75. Akékoľvek spracúvanie osobných údajov, ktoré je potrebné na plnenie požiadaviek používateľa, sa preto môže opierať o právny základ plnenia zmluvy.²⁸ Takéto spracúvanie zahŕňa najmä zaznamenanie hlasovej požiadavky používateľa, jej prepis do textovej formy, jej interpretáciu, informácie vymieňané so zdrojmi informácií na prípravu odpovede a potom prepis na konečnú hlasovú odpoveď, ktorou sa ukončuje žiadosť používateľa.
76. Plnenie zmluvy môže byť právnym základom pre spracúvanie osobných údajov pomocou strojového učenia, ak je to potrebné na poskytovanie služby. Spracúvanie osobných údajov pomocou strojového učenia na iné účely, ktoré nie sú potrebné, ako napríklad zlepšenie služieb, by sa nemalo opierať o tento právny základ.
77. V neposlednom rade by sa nemali zamieňať právne základy plnenia zmluvy a súhlasu podľa všeobecného nariadenia o ochrane údajov. Súhlas poskytnutý na uzavretie zmluvy, t. j. súhlas so zmluvou, je súčasťou platnosti tejto zmluvy a neodkazuje na špecifický význam súhlasu podľa všeobecného nariadenia o ochrane údajov²⁹.
78. Ak sa pri použití VVA nevyžaduje predchádzajúca konfigurácia používateľského konta pre VVA, súhlas by mohol byť možným právnym základom.

3.4.2 Zlepšovanie VVA tréningom systémov strojového učenia a manuálnou kontrolou hlasu a prepisov

79. Ľudská reč má obrovské množstvo prízvukov a variácií. Zatiaľ čo všetky VVA sú funkčné hneď po vybalení, ich výkonnosť sa môže zlepšiť tým, že sa prispôbia špecifickým vlastnostiam reči používateľov. Ako sa uvádza v oddiele 2.6, tento proces nastavovania sa opiera o metódy strojového učenia a pozostáva z dvoch procesov: dopĺňanie nových údajov získaných od používateľov do tréningového súboru údajov VVA a kontrola údajov ľuďmi, ktoré boli spracúvané pri plnení časti požiadavky.

²⁷ Za predpokladu, že „zmluva je platná podľa platného vnútroštátneho zmluvného práva“, výňatok z usmernení 2/2019 o spracúvaní osobných údajov podľa článku 6 ods. 1 písm. b) všeobecného nariadenia o ochrane údajov v súvislosti s poskytovaním on-line služieb dotknutým osobám (ďalej len „usmernenia 2/2019“), bod 26.

²⁸ V súlade s usmerneniami 2/2019, v ktorých sa navyše uvádza, že stanovisko 6/2014 je naďalej relevantné pre článok 6 ods. 1 písm. b) a GDPR (pozri najmä strany 11, 16, 17, 18 a 55 tohto stanoviska 6/2014).

²⁹ Pozri usmernenia 2/2019, body 18, 19, 20, 21 a 27.

Príklad 7:

Používateľ VVA musí trikrát zopakovať rovnaký hlasový príkaz, pretože VVA mu nerozumie. Tieto tri hlasové príkazy a ich súvisiace prepisy sa postúpia ľudským kontrolórom, aby preskúmali a opravili prepisy. Hlasové príkazy a skontrolované prepisy sa pridávajú do tréningového súboru údajov VVA s cieľom zlepšiť jeho výkonnosť.

80. Spracovateľské činnosti opísané v príklade by sa nemali považovať za (striktne) „*nevyhnutné na plnenie zmluvy*“ v zmysle článku 6 ods. 1 písm. b) všeobecného nariadenia o ochrane údajov, a preto si vyžadujú iný právny základ z článku 6 všeobecného nariadenia o ochrane údajov. Hlavným dôvodom je, že VVA sú funkčne už po ich vybalení a už môžu fungovať ako (striktne) nevyhnutné na plnenie zmluvy. EDPB sa nedomnieva, že by článok 6 ods. 1 písm. b) vo všeobecnosti bol vhodným zákonným základom pre spracúvanie na účely vylepšenia služby alebo rozvoja nových funkcií v rámci existujúcej služby. Vo väčšine prípadov používateľ uzavrie zmluvu s cieľom využiť existujúcu službu. Zatiaľ čo možnosť vylepšenia a úprav služby sa môže bežne zahrnúť do zmluvných podmienok, takéto spracúvanie zvyčajne nemožno považovať za objektívne nevyhnutné na plnenie zmluvy s používateľom.

3.4.3 Identifikácia používateľa³⁰ (pomocou hlasových údajov)

81. Používanie hlasových údajov na identifikáciu používateľa znamená spracúvanie biometrických údajov, ako sa vymedzuje v článku 4 ods. 14 všeobecného nariadenia o ochrane údajov. Prevádzkovateľ bude preto musieť okrem určenia právneho základu podľa článku 6 všeobecného nariadenia o ochrane údajov identifikovať aj výnimku podľa článku 9 všeobecného nariadenia o ochrane údajov.³¹
82. Z výnimiek uvedených v článku 9 všeobecného nariadenia o ochrane údajov sa na tento konkrétny účel uplatňuje len výslovný súhlas dotknutých osôb.
83. Keďže si však tento účel vyžaduje uplatňovanie osobitného právneho režimu podľa článku 9 všeobecného nariadenia o ochrane údajov, ďalšie podrobnosti sú uvedené v oddiele 3.8, ktorý sa týka spracúvania osobitných kategórií údajov.

3.4.4 Profilovanie používateľov na účely personalizácie obsahu alebo reklamy

84. Ako už bolo uvedené, VVA majú prístup k obsahu všetkých hlasových príkazov, aj keď sa tieto týkajú služieb poskytovaných tretími stranami. Tento prístup môže umožniť tvorcom VVA vytvoriť veľmi presné používateľské profily, ktoré sa môžu použiť na poskytovanie personalizovaných služieb alebo reklám.

³⁰ Z technického hľadiska sa pojem identifikácia musí odlišovať od overovania [verification] (autentifikácia). Identifikácia je vyhľadávanie a porovnávanie jedného údaju s viacerými údajmi (1: N) a v zásade si vyžaduje databázu, v ktorej sú uvedené viaceré osoby. Na rozdiel od toho je spracúvanie na účely overenia porovnaním jedna k jednej (1:1) a používa sa na overenie a potvrdenie biometrickým porovnaním, či je jednotlivец tou istou osobou ako tá, od ktorej biometrické údaje pochádzajú. Podľa informácií EDPB sa VVA na trhu spoliehajú výlučne na používanie technológií na identifikáciu hovoriaceho.

³¹ Podľa všeobecného nariadenia o ochrane údajov samotná povaha údajov nie je vždy dostatočná na určenie toho, či sa majú považovať za osobitné kategórie údajov, keďže „*na spracúvanie fotografií sa [...] vymedzenie pojmu biometrické údaje bude vzťahovať len v prípadoch, keď sa spracúvajú osobitnými technickými prostriedkami, ktoré umožňujú alebo potvrdzujú jedinečnú identifikáciu fyzickej osoby*“ (odôvodnenie 51). To isté odôvodnenie platí aj v prípade hlasu.

Príklad 8:

Zakaždým, keď používateľ VVA vyhľadáva na internete, VVA pridáva do profilu používateľa označenia tém, ktoré sú predmetom jeho záujmu. Výsledky každého nového vyhľadávania sa používateľovi zobrazujú v poradí, ktoré tieto označenia zohľadňuje.

Príklad 9:

Zakaždým, keď používateľ VVA uskutoční nákup prostredníctvom služby elektronického obchodu, VVA uloží záznam o objednávke. Poskytovateľ VVA umožňuje tretím stranám smerovať na používateľa VVA cieleňú reklamu na základe doterajších nákupov.

85. Personalizácia obsahu môže (ale nemusí) predstavovať prirodzený a očakávaný prvok VVA. To, či takéto spracúvanie možno považovať za prirodzený aspekt služby VVA, bude závisieť od presnej povahy poskytovanej služby, očakávaní priemernej dotknutej osoby nielen vzhľadom na podmienky poskytovania služby, ale aj spôsob, akým sa služba propaguje používateľom, a od toho, či sa služba môže poskytovať bez personalizácie.³²
86. Ak sa personalizácia uskutočňuje v kontexte zmluvného vzťahu a ako súčasť služby, ktorú výslovne požaduje koncový používateľ (a spracúvanie sa obmedzuje na to, čo je nevyhnutne potrebné na poskytovanie tejto služby), takéto spracúvanie môže byť založené na článku 6 ods. 1 písm. b) všeobecného nariadenia o ochrane údajov.
87. Ak spracúvanie nie je striktne „*nevyhnutné na plnenie zmluvy*“ v zmysle článku 6 ods. 1 písm. b) všeobecného nariadenia o ochrane údajov, poskytovateľ VVA musí v zásade požiadať o súhlas dotknutú osobu. Keďže sa na uchovávanie alebo získanie prístupu k informáciám bude vyžadovať súhlas podľa článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách (pozri body 28 – 29 vyššie), súhlas podľa článku 6 ods. 1 písm. a) všeobecného nariadenia o ochrane údajov bude v zásade tiež vhodným právnym základom pre spracúvanie osobných údajov po týchto operáciách, keďže spoliehanie sa na oprávnený záujem v konkrétnych prípadoch môže ohroziť dodatočnú úroveň ochrany stanovenú v článku 5 ods. 3 smernice o súkromí a elektronických komunikáciách.
88. Pokiaľ ide o profilovanie používateľov na účely reklamy, treba poznamenať, že tento účel sa nikdy nepovažuje za službu, ktorú koncový používateľ výslovne požaduje. V prípade spracúvania na tento účel by sa preto mal systematicky získavať súhlas používateľov.

Odporúčania

89. Používatelia by mali byť informovaní o účele spracúvania osobných údajov a tento účel by mal byť v súlade s ich očakávaniami týkajúcimi sa zariadenia, ktoré si kupujú. V prípade VVA je z pohľadu používateľa týmto účelom jednoznačne spracúvanie jeho hlasu výlučne na účely interpretácie jeho požiadavky a poskytnutia zmysluplných odpovedí (či už ide o odpovede na otázky alebo iné reakcie, ako je diaľkové ovládanie vypínača osvetlenia).
90. Ak sa spracúvanie osobných údajov zakladá na súhlase, takýto súhlas „*musí byť poskytnutý na jeden alebo viaceré konkrétne účely a že dotknutá osoba má možnosť voľby vo vzťahu ku každému z nich*“. Okrem toho, „*prevádzkovateľ, ktorý žiada o súhlas na viaceré rôzne účely, by mal zabezpečiť samostatnú možnosť voľby [opt-in] pre každý účel, aby používateľom umožnil*

³² Pozri aj Usmernenia 2/2019, bod 57.

poskytnúť konkrétny súhlas na konkrétne účely.”³³ Používatelia by napríklad mali mať možnosť samostatne súhlasiť alebo nesúhlasiť s manuálnou kontrolou a označovaním hlasových prepisov alebo s použitím ich hlasových údajov na identifikáciu/autentifikáciu používateľa (pozri oddiel 3.7).

3.5 Spracúvanie osobných údajov detí

91. A v prípade detí môže dochádzať k interakcii s VVA alebo si deti môžu vytvoriť vlastné profily pripojené k profilom dospelých. Niektoré VVA sú zabudované v zariadeniach, ktoré sú osobitne zamerané na deti.
92. Ak je právnym základom spracúvania plnenie zmluvy, podmienky spracúvania údajov detí budú závisieť od vnútroštátnych právnych predpisov v oblasti zmluvného práva.
93. Ak je právnym základom spracúvania súhlas a podľa článku 8 ods. 1 všeobecného nariadenia o ochrane údajov, spracúvanie osobných údajov o deťoch je zákonné len vtedy, „ak má dieťa aspoň 16 rokov. Ak má dieťa menej než 16 rokov, takéto spracúvanie je zákonné iba za podmienky a v rozsahu, v akom takýto súhlas vyjadril alebo schválil nositeľ rodičovských práv a povinností“. V záujme súladu so všeobecným nariadením o ochrane údajov by sa preto v prípade, že je právnym základom súhlas, malo od rodičov alebo opatrovníkov vyžiadať výslovné povolenie získavať, spracúvať a uchovávať osobné údaje detí (hlas, prepisy atď.).
94. Rodičovské kontroly sú do určitej miery dostupné, ale vo svojej súčasnej podobe nie sú používateľsky najpriateľnejšie (napr. je potrebné prihlásiť sa do novej služby) alebo majú obmedzené možnosti. Prevádzkovatelia by mali investovať do vývoja prostriedkov pre rodičov alebo opatrovníkov, pomocou ktorých by mohli kontrolovať, ako deti používajú VVA.

3.6 Uchovávanie údajov

95. VVA spracúva a vytvára širokú škálu osobných údajov, ako sú hlas, prepisy hlasu, metaúdaje alebo systémové logy. Tieto druhy údajov by sa mohli spracúvať na rôznorodé účely, ako sú poskytovanie služby, zlepšenie spracovania prirodzeného jazyka, personalizácia alebo vedecký výskum. V súlade so zásadou minimalizácie uchovávanie by VVA mali údaje uchovávať len dovtedy, kým je to potrebné na účely, na ktoré sa osobné údaje spracúvajú. Lehoty uchovávanie údajov by preto mali závisieť od rôznych účelov spracúvania. Poskytovatelia služieb VVA alebo tretie strany poskytujúce služby prostredníctvom VVA by mali posúdiť maximálne obdobie uchovávanie pre každý súbor údajov a každý účel.
96. Zásada minimalizácie údajov úzko súvisí so zásadou minimalizácie uchovávanie údajov. Prevádzkovatelia musia obmedziť nielen obdobie uchovávanie údajov, ale aj druh a množstvo údajov.
97. Prevádzkovatelia by sa okrem iného mali zaoberať týmito otázkami: Je na dosiahnutie účelu X potrebné uložiť všetky hlasové záznamy alebo všetky prepisy hlasu? Ak sa uchováva prepis hlasu, je potrebné uchovávať aj hlasové údaje? Ak áno, tak na aký účel? Ako dlho je potrebné na každý účel ukladať hlasové údaje alebo údaje o prepise hlasu? Na základe odpovedí na tieto a iné podobné otázky sa určia obdobia uchovávanie, ktoré by mali byť súčasťou informácií, ktoré majú k dispozícii dotknuté osoby.
98. Niektoré VVA štandardne uchováujú osobné údaje, ako sú hlasové úryvky alebo prepisy na neurčité obdobie, pričom používateľom poskytujú prostriedky na vymazanie takýchto údajov.

³³ Pozri Usmernenia EDPB 5/2020 k súhlasu podľa nariadenia 2016/679, prijaté 4. mája 2020, oddiel 3.2.

Uchovávanie osobných údajov na dobu neurčitú je v rozpore so zásadou minimalizácie uchovávaní. Poskytnutie prostriedkov dotknutým osobám, aby si vymazali svoje osobné údaje, ešte nezabavuje prevádzkovateľov zodpovednosti za vymedzenie a presadzovanie politiky uchovávaní údajov.

99. Do návrhu VVA je potrebné zahrnúť ovládacie prvky pre používateľov, ktoré im umožňujú vymazať ich osobné údaje zo svojich zariadení a zo všetkých vzdialených systémov uchovávaní údajov. Tieto ovládacie prvky sa môžu vyžadovať na vyriešenie rôznych požiadaviek používateľov, napríklad žiadosti o vymazanie alebo odvolanie predtým udeleného súhlasu. V návrhu niektorých VVA sa táto požiadavka nezohľadnila.³⁴
100. Rovnako ako v iných kontextoch môže byť potrebné, aby prevádzkovatelia uchovávali osobné údaje ako dôkaz o službe poskytovanej používateľovi na účely splnenia zákonnej povinnosti. Prevádzkovateľ môže na tomto základe uchovávať osobné údaje. Uchovávané údaje by však mali mať minimálny rozsah potrebný na splnenie takejto zákonnej povinnosti a mali by sa uchovávať počas minimálneho obdobia. Údaje uchovávané na účely splnenia zákonnej povinnosti by sa samozrejme nemali používať na žiadne iné účely bez právneho základu podľa článku 6 všeobecného nariadenia o ochrane údajov.

Príklad 10:

Používateľ nakupuje televízny prijímač prostredníctvom služby elektronického obchodu tak, že dá VVA hlasový príkaz. Aj keď používateľ následne požiada o vymazanie svojich údajov, poskytovateľ VVA alebo vývojár by stále mohli uchovať niektoré údaje na základe ich zákonnej povinnosti stanovenej daňovými právnymi predpismi, podľa ktorých majú uchovávať dôkazy o nákupe. Údaje uchovávané na tento účel by však nemali presiahnuť minimum potrebné na splnenie zákonnej povinnosti a nemôžu sa spracúvať na žiadne iné účely bez právneho základu podľa článku 6 všeobecného nariadenia o ochrane údajov.

101. Ako sa uvádza v oddiele 2, schopnosť rozpoznávania hlasu VVA sa zlepšuje tréningom systémov strojového učenia pomocou údajov používateľov. Ak používatelia neudelia súhlas alebo odvolajú svoj súhlas s použitím svojich údajov na tento účel, ich údaje nemôžu byť zákonne použité na tréningovanie žiadneho ďalšieho modelu a prevádzkovateľ by ich mal vymazať za predpokladu, že neexistuje žiadny iný účel, ktorý by odôvodňoval pokračovanie ich uchovávaní. Existujú však dôkazy, že pri niektorých modeloch strojového učenia môže existovať riziko opätovnej identifikácie.³⁵
102. Prevádzkovatelia a sprostredkovatelia by mali používať modely, ktoré neobmedzujú ich schopnosť zastaviť spracúvanie, ak fyzická osoba svoj súhlas odvolá, ani by nemali používať modely, ktoré obmedzujú ich schopnosť uľahčiť výkon práv dotknutej osoby. Prevádzkovatelia a sprostredkovatelia by mali uplatňovať zmierňujúce opatrenia na zníženie rizika opätovnej identifikácie na prijateľnú úroveň.
103. V prípade, že používateľ odvolá svoj súhlas, údaje získané od tohto používateľa sa už nemôžu používať na ďalšie tréningovanie modelu. Model, ktorý bol predtým tréningovaný za pomoci týchto

³⁴ Pozri list od spoločnosti Amazon z 28. júna 2019 v odpovedi americkému senátorovi Christopherovi Coonsovi: [https://www.coons.senate.gov/imo/media/doc/Amazon%20Senator%20Coons Response%20Letter 6.28.19 \[3\].pdf](https://www.coons.senate.gov/imo/media/doc/Amazon%20Senator%20Coons%20Response%20Letter%206.28.19%20[3].pdf).

³⁵ Veale Michael, Binns Reuben a 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

údajov, sa však nemusí vymazať. EDPB však zdôrazňuje, že existujú dôkazy o tom, že v niektorých modeloch strojového učenia môže existovať riziko úniku osobných údajov. Z početných štúdií vyplynulo najmä, že je možné vykonať rekonštrukciu, ako aj útoky zamerané na zistenie, či jednotlivec bol súčasťou tréningových údajov, čo útočníkom umožňuje získavať informácie o jednotlivcoch.³⁶ Prevádzkovatelia a sprostredkovatelia by preto mali uplatňovať zmierňujúce opatrenia na zníženie rizika opätovnej identifikácie na prijateľnú úroveň, aby zabezpečili, že používajú modely, ktoré neobsahujú osobné údaje.

104. Dotknuté osoby by nemali byť povzbudzované, aby svoje údaje uchovávali počas neurčeného obdobia. Hoci vymazanie uložených hlasových údajov alebo prepisov môže mať vplyv na výkonnosť služby, takýto vplyv by sa mal používateľom vysvetliť jasným a primeraným spôsobom. Poskytovatelia služieb VVA by sa mali vyhnúť všeobecným vyhláseniam o zhoršení poskytovanej služby po vymazaní osobných údajov.
105. Anonymizácia hlasových záznamov je obzvlášť náročná, pretože používateľov je možné identifikovať na základe obsahu samotnej správy a vlastností samotného hlasu. Napriek tomu sa uskutočňuje určitý výskum³⁷ technik, ktoré by mohli umožniť odstránenie situačných informácií, ako sú šum pozadia a anonymizácia hlasu.

Odporúčania

106. Z pohľadu používateľa je hlavným účelom spracúvania jeho údajov vyhľadávanie a získavanie odpovedí a/alebo spúšťanie činností, ako je hranie hudby alebo zapínanie alebo vypínanie svetiel. Po zodpovedaní otázky alebo vykonaní príkazu by sa osobné údaje mali vymazať, pokiaľ tvorca alebo vývojár VVA nemá platný právny základ na ich uchovanie na konkrétny účel.
107. Pred zvážením anonymizácie ako prostriedku na splnenie zásady minimalizácie uchovávaní údajov, by poskytovatelia a vývojári VVA mali skontrolovať, či proces anonymizácie vedie k tomu, že hlas nie je možné identifikovať.
108. Štandardné konfigurácie by mali tieto požiadavky zohľadňovať tým, že sú štandardne nastavené na absolútne minimum ukladania informácií o používateľovi. Ak sú tieto možnosti prezentované ako súčasť sprievodcu nastavením [setup wizard], štandardné nastavenie by to malo odrážať a všetky možnosti by mali byť zobrazené ako rovnocenné bez vizuálnej diskriminácie.
109. Keď počas procesu kontroly poskytovateľ alebo vývojár VVA nájde záznam vytvorený na základe chybných aktivácií, tento záznam a všetky súvisiace údaje by sa mali okamžite vymazať a nemali by sa použiť na žiadny účel.

3.7 Bezpečnosť

110. Bezpečné spracúvanie osobných údajov si vyžaduje, aby VVA chránili ich dôvernosť, integritu a dostupnosť. Okrem rizík vyplývajúcich z prvkov ekosystému VVA sa používaním hlasu ako komunikačného prostriedku vytvára nový súbor bezpečnostných rizík.

³⁶ N. Carlini et al, „[Extracting Training Data from Large Language Models](#)“ december 2020.

³⁷ Pozri napríklad VoicePrivacy (<https://www.voiceprivacychallenge.org>), iniciatíva na vývoj riešení na ochranu súkromia pre rečové technológie.

Pozri tiež nástroje na anonymizáciu hlasu s otvoreným zdrojovým kódom, vyvinuté v rámci výskumného a inovačného projektu Horizont 2020 COMPRISE: https://gitlab.inria.fr/comprise/voice_transformation.

111. VVA využívajú viacerí používatelia. Do úvahy pri nich prichádza viac ako jeden registrovaný používateľ a ktokoľvek v ich okolí môže dávať príkazy a využívať ich služby. Každá služba VVA vyžadujúca dôvernosť bude zahŕňať určitý mechanizmus kontroly prístupu a autentifikáciu používateľa. Bez kontroly prístupu by ktokoľvek, kto môže vydať hlasové príkazy VVA, mohol mať prístup k akýmkoľvek osobným údajom používateľov, meniť ich alebo vymazať (napr. vyžiadať si prijaté správy, adresu používateľa alebo podujatia v kalendári). Vydávanie hlasových príkazov VVA si nevyžaduje fyzickú blízkosť k zariadeniu, pretože sa ich dá ovládať, napríklad, prostredníctvom vysielania signálu³⁸ (napr. rozhlas alebo televízia). Niektoré zo známych metód vydávania príkazov VVA na diaľku, ako sú laserové³⁹ alebo ultrazvukové (nepočuteľné) vlny⁴⁰, nie sú ani zistiteľné ľudskými zmyslami.
112. Autentifikácia používateľa môže vychádzať z jedného alebo viacerých týchto faktorov: informácia, ktorú poznáte (napr. heslo), predmet, ktorý máte (napr. inteligentná karta) alebo vaša charakteristika (ako napríklad hlasový odtlačok). Z bližšieho pohľadu na tieto faktory autentifikácie v kontexte VVA vyplýva, že:
-)] Autentifikácia pomocou informácie, ktorú používateľ pozná, je problematická. Tajný kľúč, ktorý by umožnil používateľom preukázať svoju totožnosť, by sa mal vysloviť nahlas, čím by sa odhalil každému, kto sa nachádza v okolí. Komunikačným kanálom pre VVA je okolitý vzduch, čo je typ kanála, ktorý nemožno zabezpečiť spôsobom, akým sa zabezpečujú tradičné kanály (napr. obmedzením prístupu alebo zašifrovaním jeho obsahu).
 -)] Autentifikácia pomocou predmetu, ktorý používateľ má, by si od poskytovateľov služieb VVA vyžadovala, aby vytvorili, distribuovali a spravovali „tokeny“, ktoré by sa mohli používať na preukázanie totožnosti.
 -)] Autentifikácia pomocou charakteristiky používateľa znamená použitie biometrických údajov na účely individuálnej identifikácie fyzickej osoby (pozri oddiel 3.7 ďalej).
113. Používateľské kontá VVA sú prepojené so zariadeniami, v ktorých sa služba poskytuje. Konto, ktoré sa používa na správu VVA, sa často používa na správu iných služieb. Napríklad majitelia mobilného telefónu Android a reproduktora Google Home môžu, a s najväčšou pravdepodobnosťou prepájajú svoje konto Google s oboma zariadeniami. Väčšina VVA nevyžaduje ani neponúka mechanizmus identifikácie alebo autentifikácie, ak zariadenie poskytujúce službu VVA má len jedno používateľské konto.
114. Ak je k zariadeniu pripojené viac ako jedno používateľské konto, niektoré VVA ponúkajú možnosť základnej kontroly prístupu vo forme PIN čísla bez skutočnej autentifikácie používateľa. Niektoré ďalšie VVA majú možnosť používať ako mechanizmus identifikácie rozpoznávanie hlasových odtlačkov.
115. Hoci identifikácia alebo autentifikácia používateľa nemusí byť potrebná na prístup ku všetkým službám VVA, pri niektorých bude určite potrebná. Bez mechanizmu identifikácie alebo autentifikácie by ktokoľvek mohol mať prístup k údajom iných používateľov a zmeniť alebo vymazať ich podľa ľubovôle. Napríklad ktokoľvek v blízkosti inteligentného reproduktora by

³⁸ X. Yuan et al., „All Your Alexa Are Belong to Us: A Remote Voice Control Attack against Echo“ 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 2018, s. 1-6, doi: 10.1109/GLOCOM.2018.8647762.

³⁹ Pozri napríklad <https://lightcommands.com>.

⁴⁰ Pozri napríklad <https://surfingattack.github.io>.

mohol vymazať zoznamy skladieb iných používateľov zo služby streamovania hudby, príkazy z histórie alebo kontakty zo zoznamu kontaktov.

116. Väčšina VVA bezvýhradne dôveruje svojim miestnym sieťam. Akékoľvek napadnuté zariadenie v tej istej sieti by mohlo zmeniť nastavenia inteligentného reproduktora alebo umožniť inštaláciu škodlivého softvéru [malware] alebo pripojiť falošné aplikácie/zručnosti bez vedomia alebo súhlasu používateľa.⁴¹
117. VVA, tak ako akýkoľvek iný softvér, majú zraniteľné miesta. Avšak, vzhľadom na koncentráciu trhu s VVA,⁴² každá zraniteľnosť môže ovplyvniť milióny používateľov VVA. Pokiaľ fungujú tak, ako sú aktuálne navrhnuté, VVA neposielajú žiadne informácie do cloudovej služby rozpoznávania reči, kým nedôjde k detekcii aktivačného výrazu. Zraniteľné miesta softvéru by však mohli útočníkovi umožniť obísť nastavenie VVA a bezpečnostné opatrenia. Potom by napríklad mohlo byť možné získať kópiu všetkých údajov zaslaných do cloudu VVA a zaslať ich na server ovládaný útočníkom.
118. Údaje, ktoré VVA zákonne spracúvajú alebo odvodzujú, umožňujú vytvoriť pomerne presný profil ich používateľov, keďže VVA pozná alebo dokáže odvodiť polohu, vzťahy a záujmy svojich používateľov. VVA sú v čoraz väčšej miere prítomné v domácnostiach a smartfónoch používateľov. Zvyšuje sa tým riziko hromadného sledovania a hromadného profilovania. Bezpečnostné opatrenia na ochranu údajov pri prenose aj pri používaní, v zariadeniach aj v cloude, by preto mali zodpovedať týmto rizikám.
119. Nárast využívania VVA v spojení s nedostatočne vyváženými prístupovými právami zo strany orgánov presadzovania práva by mohol mať odradzujúci účinok, ktorý by ohrozoval základné práva ako je sloboda slova.
120. Orgány presadzovania práva v EÚ⁴³ aj mimo nej⁴⁴ už vyjadrili záujem o prístup k hlasovým úryvkom, ktoré VVA zaznamenáva. Prístup k údajom, ktoré spracúvajú alebo odvodzujú VVA v EÚ, by mal byť v súlade s existujúcim rámcom EÚ v oblasti ochrany osobných údajov a súkromia. V prípade, že niektoré členské štáty uvažujú o vydaní osobitných právnych predpisov obmedzujúcich základné práva na súkromie a ochranu osobných údajov, takéto obmedzenia by mali byť vždy v súlade s požiadavkou stanovenou v článku 23 všeobecného nariadenia o ochrane údajov.⁴⁵
121. Kontrola hlasových záznamov a súvisiacich údajov vykonávaná ľuďmi na zlepšenie kvality služieb VVA je bežnou praxou poskytovateľov VVA. Vzhľadom na citlivú povahu údajov, ktoré spracúvajú títo ľudskí kontrolóri, a na skutočnosť, že tento proces je často zadávaný subdodávateľsky sprostredkovateľom, je mimoriadne dôležité, aby sa zaviedli primerané bezpečnostné opatrenia.

⁴¹ Pozri napríklad Deepak Kumar et al., *Skill Squatting Attacks on Amazon Alexa*, USENIX Security Symposium, august 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 Trh s VVA si v súčasnosti delí menej než tucet poskytovateľov služieb.

⁴³ Pozri napríklad <https://www.ft.com/content/ad765972-87a2-11e9-a028-86cea8523dc2>.

⁴⁴ Pozri napríklad <https://cdt.org/insights/alexa-is-law-enforcement-listening>.

⁴⁵ Pozri aj usmernenia EDPB 10/2020 k obmedzeniam podľa článku 23 všeobecného nariadenia o ochrane údajov.

Odporúčania

122. Tvorcovia VVA a vývojári aplikácií by používateľom mali poskytovať zabezpečené najmodernejšie [state-of-the-art] postupy autentifikácie.
123. Ľudskí kontrolóri by mali vždy dostávať nevyhnutne potrebné pseudonymizované údaje. Právne dohody upravujúce kontrolu by mali výslovne zakázať akékoľvek spracúvanie, ktoré by mohlo viesť k identifikácii dotknutej osoby.
124. Ak sa tiesňové volanie poskytuje ako služba prostredníctvom VVA, mala by sa zaručiť stabilná prevádzkyschopnosť [stable uptime]⁴⁶.

3.8 Spracúvanie osobitných kategórií údajov

125. Ako už bolo uvedené, VVA majú prístup k informáciám intímnej povahy, ktoré môžu byť chránené podľa článku 9 všeobecného nariadenia o ochrane údajov (pozri oddiel 3.7.1), napríklad biometrické údaje (pozri oddiel 3.7.2). Tvorcovia a vývojári VVA preto musia starostlivo identifikovať, v ktorých prípadoch spracúvanie zahŕňa osobitné kategórie údajov.

3.8.1 Všeobecné otázky pri spracúvaní osobitných kategórií údajov

126. VVA môžu spracúvať osobitné kategórie údajov za rôznych okolností:
 -) Ako súčasť svojich vlastných služieb, napríklad pri správe termínov u lekára v kalendároch používateľov.
 -) Keď poskytovatelia VVA spracúvajú obsah príkazov v rámci rozhrania pre služby tretích strán. V závislosti od druhu služby, ktorú požaduje používateľ, by poskytovatelia VVA mohli spracúvať osobitné kategórie údajov. Príkladom môže byť situácia, keď používateľka vydá príkazy VVA, aby použil aplikáciu tretej strany na sledovanie jej ovulácie.⁴⁷
 -) Ak sa hlasové údaje používajú na účely individuálnej identifikácie používateľa, ako sa uvádza ďalej v texte.

3.8.2 Osobitné otázky pri spracúvaní biometrických údajov

127. Niektoré VVA majú schopnosť individuálne identifikovať svojich používateľov len na základe ich hlasu. Tento proces je známy ako rozpoznávanie hlasového vzoru [voice model recognition]. Počas procesu registrácie rozpoznávania hlasu VVA spracúva hlas používateľa s cieľom vytvoriť hlasový vzor (alebo hlasový odtlačok [voiceprint]). Počas pravidelného používania môže VVA vypočítať hlasový vzor ktoréhokoľvek používateľa a porovnať ho so zaregistrovanými vzormi s cieľom individuálne identifikovať používateľa, ktorý príkaz vyslovil.

Príklad 11:

Skupina používateľov nastaví VVA na používanie rozpoznávania hlasového vzoru. Potom každý z nich zaregistruje svoj hlasový vzor.

⁴⁶ Čas, počas ktorého môže byť zariadenie alebo služba ponechané bez dozoru, bez toho, aby došlo k zlyhaniu alebo by bolo potrebné reštartovanie na účely správy a údržby.

⁴⁷ Pozri napríklad produkt, ktorý je k dispozícii tu: <https://www.amazon.com/Ethan-Fan-Ovulation-Period-Tracker/dp/B07CRLSHKY>.

Používateľ neskôr požiada VVA o prístup k termínom stretnutí vo svojom kalendári. Keďže prístup ku kalendáru si vyžaduje identifikáciu používateľa, VVA extrahuje a vypočíta hlasový vzor z hlasu, ktorým bola požiadavka vyslovená, a skontroluje, či zodpovedá registrovanému používateľovi a či má tento konkrétny používateľ prístup ku kalendáru.

128. Vo vyššie uvedenom príklade, rozpoznávanie hlasu používateľa na základe hlasového vzoru zodpovedá spracúvaniu osobitných kategórií osobných údajov v zmysle článku 9 všeobecného nariadenia o ochrane údajov (spracúvanie biometrických údajov na účely individuálnej identifikácie fyzickej osoby).⁴⁸ Spracúvanie biometrických údajov na účely identifikácie používateľa, ako sa vyžaduje v príklade, si bude vyžadovať výslovný súhlas dotknutej(-ých) osoby(osôb) [článok 9 ods. 2 písm. a) všeobecného nariadenia o ochrane údajov]. Preto pri získavaní súhlasu používateľov musia prevádzkovatelia spĺňať podmienky článku 7 a ako sa vysvetľuje v odôvodnení 32 všeobecného nariadenia o ochrane údajov a mali by ponúkať okrem biometrie alternatívnu metódu identifikácie so zohľadnením slobodnej povahy súhlasu.
129. Pri používaní hlasových údajov na biometrickú identifikáciu alebo autentifikáciu sa od prevádzkovateľov vyžaduje, aby transparentne informovali o tom, kde sa používa biometrická identifikácia a ako sa hlasové odtlačky (biometrické modely) uchovávajú a šíria medzi rôznymi zariadeniami. Na splnenie tejto požiadavky transparentnosti EDPB odporúča poskytnúť odpovede na tieto otázky:
- J Dochádza pri aktivácii identifikácie hlasu na jednom zariadení automaticky k aktivácii tejto funkcie na všetkých ostatných zariadeniach, ktoré používajú rovnaké konto?
 - J Šíri sa aktivácia identifikácie hlasu prostredníctvom infraštruktúry prevádzkovateľa zariadenia s VVA aj do zariadení, ktoré vlastní iní používatelia?
 - J Kde sa vytvárajú, uchovávajú a porovnávajú biometrické vzory?
 - J Sú biometrické vzory prístupné poskytovateľom a vývojárom VVA alebo iným subjektom?
130. Keď registrovaný používateľ nakonfiguruje VVA tak, aby identifikoval hlas jeho používateľov, hlas neregistrovaných a náhodných používateľov sa taktiež spracuje na účely ich individuálnej identifikácie.
131. Detekcia hlasu správneho hovoriaceho v skutočnosti zahŕňa aj porovnanie s hlasom iných ľudí v blízkosti asistenta. Inými slovami, funkcia rozpoznávania hovoriaceho (speaker recognition functionality), ktorú využívajú hlasoví asistenti si môže vyžadovať zaznamenanie hlasovej biometrie ľudí rozprávajúcich v domácnosti, aby bolo možné odlišiť charakteristiky hlasu používateľa od charakteristík osoby, ktorá chce byť rozoznaná. Biometrická identifikácia môže mať preto za následok, že sa spracujú biometrické údaje neinformovaných osôb, a to tak, že sa zaregistruje ich vzor a porovná sa so vzorom používateľa, ktorý chce byť rozpoznaný.
132. Aby sa predišlo takémuto získavaniu biometrických údajov bez vedomia dotknutých osôb a zároveň umožnilo asistentovi rozpoznať používateľa, mali by sa uprednostniť riešenia založené len na údajoch používateľa. Konkrétne to znamená, že biometrické rozpoznávanie sa aktivuje pri každom použití len z iniciatívy používateľa, a nie trvalou analýzou hlasov, ktoré asistent počuje. Prítomným osobám by sa napríklad mohlo poskytnúť osobitné kľúčové slovo alebo by sa mohla položiť otázka na získanie ich súhlasu so spustením biometrického spracúvania.

Používateľ môže napríklad povedať „identifikácia“ alebo sa asistent môže opýtať „chcete byť identifikovaný“ a na základe kladnej odpovede aktivuje biometrické spracúvanie.

Príklad 12:

Ak chce používateľ zaviesť biometrickú autentifikáciu na účely prístupu k určitým chráneným údajom, ako je napríklad jeho bankový účet, hlasový asistent by mohol aktivovať overenie hovoriaceho, iba keď hovoriaci spustí aplikáciu, a týmto spôsobom overiť jeho totožnosť.

Odporúčania

133. Hlasové vzory by sa mali vytvárať, uchovávať a porovnávať výlučne na lokálnom zariadení, nie na vzdialených serveroch.
134. Vzhľadom na citlivosť hlasových odtlačkov by sa mali dôkladne uplatňovať normy ako ISO/IEC 24745 a techniky ochrany biometrických vzorov⁴⁹.
135. Ak VVA používa biometrickú identifikáciu na základe hlasu, poskytovatelia VVA by mali:
 -) Zabezpečiť, aby bola identifikácia dostatočne presná, aby bolo možné spoľahlivo priradiť osobné údaje k správnym dotknutým osobám.
 -) Zabezpečiť, aby presnosť bola podobná pre všetky skupiny používateľov, a to tak, že sa skontroluje, či nedochádza k výraznej zaujatosti [bias] voči rôznym demografickým skupinám.

3.9 Minimalizácia údajov

136. Prevádzkovatelia by mali minimalizovať množstvo údajov, ktoré sa zhromažďujú priamo alebo nepriamo a získavajú spracúvaním a analýzou, napr. by nemali analyzovať hlas používateľa alebo iné zvukové informácie na odvodenie informácií o jeho duševnom stave, novej chorobe alebo okolnostiach jeho života.
137. Vo východiskovom [roll out] nastavení by malo byť získavanie a/alebo spracúvanie údajov obmedzené na minimálny požadovaný objem potrebný na poskytovanie služby.
138. V závislosti od polohy, kontextu použitia a citlivosti mikrofónu by VVA mohol pri získavaní hlasu používateľov zhromažďovať hlasové údaje tretích strán ako súčasť šumu pozadia. Aj keď šum pozadia nezahŕňa hlasové údaje, stále môže zahŕňať situačné údaje, ktoré by sa mohli spracúvať na odvodenie informácií o subjekte (napr. polohe).

Odporúčania

139. Tvorcovia VVA by mali zvážiť použitie technológií, ktoré odstraňujú šum pozadia, aby sa zabránilo zaznamenávaniu a spracúvaniu hlasov v pozadí a situačných informácií.

3.10 Zodpovednosť

⁴⁹ Pozri napríklad:

Jain, Anil & Nandakumar, Karthik & Nagar, Abhishek. (2008). „*Biometric Template Security*“. EURASIP Journal on Advances in Signal Processing. 2008. 10.1155/2008/579416.

S. K. Jami, S. R. Chalamala a A. K. Jindal, „*Biometric Template Protection Through Adversarial Learning*“ 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2019, s. 1– 6, doi: 10.1109/ICCE.2019.8661905.

140. V prípade akéhokoľvek spracúvania založeného na súhlase sú prevádzkovatelia povinní preukázať súhlas dotknutých osôb podľa článku 7 ods. 1 všeobecného nariadenia o ochrane údajov. Hlasové údaje sa môžu použiť na vyvodenie zodpovednosti (napr. na preukázanie súhlasu). Povinnosť uchovávať takéto hlasové údaje by potom vyplývala z požiadaviek na zodpovednosť stanovených v príslušných osobitných právnych predpisoch.
141. Pri hodnotení potreby posúdenia vplyvu na ochranu údajov (DPIA) stanovil EDPB kritériá⁵⁰, ktoré majú orgány pre ochranu osobných údajov používať pri vytváraní zoznamov spracovateľských operácií, ktoré si vyžadujú povinné posúdenie vplyvu na ochranu údajov, a uviedol príklady spracúvania, ktoré si pravdepodobne budú takéto posúdenie vyžadovať. Je veľmi pravdepodobné, že služby VVA patria do kategórií a podmienok, ktoré si vyžadujú posúdenie vplyvu na ochranu údajov. Zahŕňa to zváženie, či zariadenie môže sledovať, monitorovať alebo kontrolovať dotknuté osoby alebo vo veľkom rozsahu systematicky monitorovať podľa článku 35 ods. 3 písm. c), používanie „novej technológie“ alebo spracúvanie citlivých údajov a údajov týkajúcich sa zraniteľných dotknutých osôb.
142. Všetky činnosti získavania a spracúvania údajov sa musia zdokumentovať v súlade s článkom 30 všeobecného nariadenia o ochrane údajov. Zahŕňa to každé spracúvanie obsahujúce hlasové údaje.

Odporúčania

143. Ak sa majú na informovanie používateľov podľa článku 13 používať hlasové správy, prevádzkovatelia by mali takéto správy uverejniť na svojom webovom sídle, aby boli prístupné používateľom a orgánom pre ochranu osobných údajov.

3.11 Špecificky navrhnutá a štandardná ochrana údajov

144. Poskytovatelia a vývojári VVA by mali zvážiť potrebu mať registrovaného používateľa pri každej z ich funkcií. Hoci je jasné, že správa kalendára alebo adresára si vyžaduje registrovaného užívateľa, nie je až tak zrejmé, či uskutočnenie telefonického hovoru alebo internetového vyhľadávania si vyžaduje, aby VVA mal registrovaného používateľa.
145. Služby, ktoré si nevyžadujú identifikovaného používateľa, by v štandardnom nastavení nemali spájať s príkazmi žiadneho z identifikovaných používateľov VVA. Pri štandardnom nastavení VVA, ktoré je prijateľné s ochranou súkromia a osobných údajov, by sa spracúvali len údaje používateľov na účely plnenia požiadaviek používateľov a neuchovávali by sa ani hlasové údaje ani register vykonaných príkazov.
146. Zatiaľ čo niektoré zariadenia môžu prevádzkovať len jednu VVA, iné si môžu vybrať spomedzi rôznych VVA. Poskytovatelia VVA by mali vypracovať odvetvové normy umožňujúce prenosnosť údajov v súlade s článkom 20 všeobecného nariadenia o ochrane údajov.
147. Niektorí poskytovatelia VVA tvrdia, že ich VVA nemôžu vymazať všetky údaje používateľov ani na žiadosť dotknutej osoby. Poskytovatelia VVA by mali zabezpečiť, aby sa všetky údaje používateľov mohli na žiadosť používateľa vymazať v súlade s článkom 17 všeobecného nariadenia o ochrane údajov.

⁵⁰ Usmernenia pracovnej skupiny zriadenej podľa článku 29 týkajúce sa posúdenia vplyvu na ochranu údajov, wp248rev.01, schválené EDPB.

4 MECHANIZMY NA UPLATŇOVANIE PRÁV DOTKNUTÝCH OSÔB

148. V súlade so všeobecným nariadením o ochrane údajov musia prevádzkovatelia, ktorí poskytujú služby VVA, umožniť všetkým používateľom, ktorí sú alebo nie sú registrovaní, uplatňovať svoje práva dotknutej osoby.
149. Poskytovatelia a vývojári VVA by mali dotknutým osobám uľahčiť kontrolu ich údajov počas celého obdobia spracúvania, najmä uľahčiť ich právo na prístup, opravu, vymazanie, právo na obmedzenie spracúvania a v závislosti od právneho základu spracúvania ich právo na prenosnosť údajov a ich právo namietañ.
150. Prevádzkovateľ by mal poskytnúť informácie o právach dotknutej osoby v čase, keď si dotknuté osoby VVA zapnú a najneskôr v čase spracúvania prvej hlasovej žiadosti používateľa.
151. Vzhľadom na to, že hlavným prostriedkom interakcie pre VVA je hlas, tvorcovia VVA by mali zabezpečiť, aby používatelia, či už registrovaní alebo nie, mohli uplatňovať akékoľvek práva dotknutej osoby pomocou jednoduchých hlasových príkazov. Tvorcovia VVA, ako aj vývojári aplikácií, ak sú súčasťou riešenia, by mali na konci procesu uplatňovania, informovať používateľa, že jeho práva boli riadne zohľadnené, a to v hlasovej forme alebo zaslaním písomného oznámenia na mobilný telefón, konto alebo akýkoľvek iný prostriedok, ktorý si používateľ vybral.
152. Prinajmenšom by tvorcovia VVA a vývojári aplikácií mali zaviesť konkrétne nástroje, ktoré zabezpečia účinný a efektívny spôsob výkonu týchto práv. Mali by preto navrhnúť pre svoje zariadenia spôsob, ako uplatňovať práva dotknutých osôb tým, že poskytnú dotknutej osobe samoobslužné nástroje, ako napríklad systém správy profilu [profile management system].⁵¹ To by mohlo uľahčiť účinné a včasné vykonávanie práv dotknutej osoby a umožniť prevádzkovateľovi zahrnúť mechanizmus identifikácie do samoobslužného nástroja.
153. Pokiaľ ide o výkon práv dotknutých osôb v prípade viacerých používateľov, keď používateľ, ktorý je alebo nie je registrovaný, uplatňuje niektoré zo svojich práv, nemali by byť dotknuté akékoľvek práva iných používateľov. Všetci používatelia, registrovaní aj neregistrovaní, môžu uplatňovať svoje práva, pokiaľ prevádzkovateľ stále spracúva údaje. Prevádzkovateľ by mal zaviesť postup, ktorým sa zabezpečí uplatňovanie práv dotknutej osoby.

4.1 Právo na prístup

154. Podľa článku 12 ods. 1 všeobecného nariadenia o ochrane údajov by sa oznámenia podľa článku 15 mali poskytovať písomne alebo inými prostriedkami, v prípade potreby aj elektronickými prostriedkami. Pokiaľ ide o prístup k osobným údajom, ktoré sa spracúvajú, v článku 15 ods. 3 sa uvádza, že ak dotknutá osoba podá žiadosť elektronickými prostriedkami a pokiaľ dotknutá osoba nepožiadala o iný spôsob, informácie by sa mali poskytovať v bežne používanej elektronickej podobe. To, čo možno považovať za bežne používanú elektronickú formu, by malo vychádzať z primeraných očakávaní dotknutých osôb a nie z toho, aký formát používa prevádzkovateľ pri svojej každodennej prevádzke. Dotknutá osoba by nemala byť povinná kúpiť si konkrétny softvér alebo hardvér na získanie prístupu k informáciám.

⁵¹ Systém správy profilu sa chápe ako miesto v rámci systému VVA, kde používatelia môžu kedykoľvek uložiť svoje preferencie, nastaviť zmeny a ľahko zmeniť nastavenia na ochranu súkromia.

155. Prevádzkovatelia by preto na požiadanie mali zaslať kópiu osobných údajov a najmä zvukových údajov (vrátane hlasových záznamov a prepisov) v bežnom formáte, ktorý si dotknutá osoba vie prečítať.
156. Pri rozhodovaní o druhu formátu, v ktorom by sa informácie podľa článku 15 mali poskytovať, prevádzkovateľ musí mať na pamäti, že formát by mal umožniť prezentáciu informácií spôsobom, ktorý je zrozumiteľný a ľahko dostupný. Prevádzkovatelia by mali tiež prispôbiť informácie konkrétnej situácii dotknutej osoby, ktorá o ne požiadala.

Príklad 13:

Prevádzkovateľ poskytujúci službu VVA dostane od používateľa tak žiadosť o prístup, ako aj žiadosť o prenosnosť údajov. Prevádzkovateľ sa rozhodne poskytnúť informácie podľa článku 15 aj článku 20 vo formáte PDF. V takom prípade by sa nemalo vychádzať z toho, že prevádzkovateľ vyriešil obe žiadosti správnym spôsobom. Súbor vo formáte PDF technicky spĺňa povinnosti prevádzkovateľa podľa článku 15, ale neplní povinnosti prevádzkovateľa podľa článku 20.⁵²

Treba poznamenať, že jednoduché odkázanie používateľov na históriu ich interakcií s hlasovým asistentom podľa všetkého neumožní prevádzkovateľovi splniť všetky povinnosti vyplývajúce z práva na prístup, keďže dostupné údaje vo všeobecnosti predstavujú len časť informácií spracúvaných v rámci poskytovania služby.

157. Právo na prístup by sa nemalo využívať na porušovanie / obchádzanie zásad minimalizácie a uchovávanía údajov, resp. na ich obchádzanie.

4.2 Právo na opravu

158. Aby sa uľahčila oprava údajov, používateľa, či už registrovaní alebo neregistrovaní, by mali mať možnosť kedykoľvek spravovať a aktualizovať svoje údaje hlasovým príkazom priamo pomocou zariadenia VVA, ako už bolo opísané. Okrem toho by sa v rámci zariadenia alebo aplikácie mal zabudovať samoobslužný nástroj, ktorý im umožní ich osobné údaje ľahko opraviť. Používatelia by mali byť informovaní o aktualizácii hlasovou alebo písomnou formou.
159. Všeobecnejšie platí, že právo na opravu sa vzťahuje na všetky názory a závery prevádzkovateľa⁵³ vrátane profilovania a malo by sa zohľadniť, že prevažná väčšina údajov je vysoko subjektívna.⁵⁴

4.3 Právo na výmaz

160. Používatelia, či už registrovaní alebo aj neregistrovaní, by mali mať možnosť kedykoľvek hlasovým príkazom zariadeniu VVA alebo pomocou samoobslužného nástroja zabudovaného do akéhokoľvek zariadenia pripojeného k VVA vymazať údaje, ktoré sa ich týkajú. V tejto

⁵² Usmernenia pracovnej skupiny zriadenej podľa článku 29 k právu na prenosnosť údajov – schválené EDPB, s. 18.

⁵³ Skutočnosť, že názory a závery možno považovať za osobné údaje potvrdil SDEÚ, ktorý uviedol, že výraz „akékoľvek informácie“ v rámci definície pojmu osobných údajov zahŕňa informácie, ktoré sú „tak objektívne, ako aj subjektívne vo forme názoru alebo hodnotení pod podmienkou, že sa „týkajú“ dotknutej osoby“ – vec C-434/16 Peter Nowak/Data Protection Commissioner, ECLI:EU:C:2017:994 [34].

⁵⁴ „Getting Data Subject Rights Right“, podanie predložené EDPB akademickou obcou z oblasti ochrany osobných údajov, november 2019.

súvislosti môže dotknutá osoba vymazať osobné údaje tak ľahko, ako boli odovzdané. Vzhľadom na inherentné ťažkosti spojené s anonymizáciou hlasových údajov a širokú škálu osobných údajov získavaných od dotknutej osoby, pozorovaných a odvodených údajov o dotknutej osobe⁵⁵, by sa v tejto súvislosti mohlo právo na vymazanie len ťažko uplatniť anonymizáciou súborov osobných údajov. Keďže všeobecné nariadenie o ochrane údajov je technologicky neutrálne a technológia sa rýchlo vyvíja, nevylučuje sa, že právo na vymazanie prostredníctvom anonymizácie môže byť v budúcnosti účinné.

161. V niektorých prípadoch je bez obrazovky tretej strany alebo možnosti zobrazovania uložených údajov (napr. mobilná aplikácia alebo tabuľkové zariadenie [tabular device]) ťažké zobraziť zaznamenané údaje, posúdiť relevantnosť návrhov. K hlasovému asistentovi by sa mal dodávať ovládací panel (alebo aplikácia), ktorý by bol používateľom všeobecne prístupný, aby sa uľahčilo jeho používanie a slúžil by na vymazanie histórie žiadostí a prispôbeniu nástroja podľa potrieb používateľa.⁵⁶
162. V prípade akéhokoľvek spracúvania údajov, a najmä v prípade, že registrované dotknuté osoby súhlasia s prepisom hlasových záznamov a ich použitím zo strany poskytovateľa na zlepšenie svojich služieb, by poskytovatelia VVA mali mať na požiadanie používateľa možnosť vymazať pôvodný hlasový záznam, ako aj akýkoľvek súvisiaci prepis osobných údajov.
163. Prevádzkovateľ by mal zabezpečiť, aby po uplatnení práva na vymazanie už nemohlo dôjsť k žiadnemu spracúvaniu. Pokiaľ ide najmä o predchádzajúce opatrenia, právo na vymazanie môže mať určité právne a technické obmedzenia.

Príklad 14:

Ak pred podaním žiadosti o vymazanie používateľ uskutočnil online nákup prostredníctvom svojho VVA, poskytovateľ VVA môže vymazať hlasový záznam súvisiaci s online nákupom a zabezpečiť, aby sa už v budúcnosti nepoužíval. Nákup však zostane platný, ako aj hlasová objednávka alebo písomný prepis, ktorý sa spracúva na webovom sídle elektronického obchodu (v takom prípade je výnimka založená na zákonnej povinnosti webového sídla elektronického obchodu).

Rovnako, ak pred žiadosťou o vymazanie používateľ pridal do svojho zoznamu skladieb prostredníctvom VVA určitú skladbu, poskytovatelia VVA budú môcť vymazať ústnu žiadosť, ale nie minulé dôsledky takejto žiadosti (vymazanie nebude mať vplyv na zoznam skladieb používateľa).

164. Na základe uvedených skutočností by v prípade, že sa tie isté osobné údaje spracúvajú na rôzne účely spracúvania, prevádzkovatelia mali žiadosti o vymazanie interpretovať ako jasný signál na zastavenie spracúvania údajov na všetky účely, na ktoré sa nevzťahuje zákonná výnimka.

V súlade s podmienkami stanovenými v článku 21 ods. 1 všeobecného nariadenia o ochrane údajov by údaje spracúvané na základe oprávnených záujmov poskytovateľov VVA nemali byť výnimkou z práva na vymazanie, najmä preto, že dotknuté osoby odôvodnene neočakávajú ďalšie spracúvanie svojich osobných údajov.

⁵⁵ Pracovná skupina zriadená podľa článku 29, Stanovisko 5/2014 k technikám anonymizácie, prijaté 10. apríla 2014.

⁵⁶ „Assistants vocaux et enceintes connectées, l’impact de la voix sur l’offre et les usages culturels et médias“, francúzska „Conseil Supérieur de l’Audiovisuel“, máj 2019.

4.4 Právo na prenosnosť údajov

165. Spracúvanie údajov poskytovateľmi VVA patrí do rozsahu prenosnosti údajov, keďže spracovateľské operácie sú založené najmä na súhlase dotknutej osoby [podľa článku 6 ods. 1 písm. a) alebo článku 9 ods. 2 písm. a), pokiaľ ide o osobitné kategórie osobných údajov], alebo na zmluve, ktorej je dotknutá osoba zmluvnou stranou podľa článku 6 ods. 1 písm. b).
166. V praxi by právo na prenosnosť údajov malo uľahčiť prechod medzi rôznymi poskytovateľmi VVA. Najmä pri VVA, ktoré fungujú v digitálnom prostredí, pričom hlas dotknutej osoby sa zaznamenáva v aplikácii alebo na platforme, by sa právo na prenosnosť údajov malo poskytnúť pre všetky osobné údaje poskytnuté dotknutou osobou. Prevádzkovateľ by okrem toho mal používateľom ponúknuť možnosť priamo získať ich osobné údaje zo svojej používateľskej zóny prostredníctvom samoobslužného nástroja. Používatelia by mali mať možnosť uplatňovať toto právo aj prostredníctvom hlasového príkazu.
167. Poskytovatelia a vývojári VVA by mali dotknutým osobám poskytnúť rozsiahlu kontrolu nad osobnými údajmi, ktoré sa ich týkajú, aby im umožnili prenos osobných údajov od jedného poskytovateľa VVA k druhému. Dotknuté osoby by preto mali dostať svoje osobné údaje, ktoré poskytli prevádzkovateľovi v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte, ako aj z prostriedkov⁵⁷, ktoré prispievajú k plneniu žiadostí o prenosnosť údajov (ako sú nástroje na stiahnutie údajov a aplikačné programovacie rozhrania)⁵⁸. Ako sa uvádza v usmerneniach k právu na prenosnosť údajov, v prípade rozsiahleho alebo komplexného získavania osobných údajov by mal prevádzkovateľ poskytnúť prehľad „*v stručnej, transparentnej, zrozumiteľnej a ľahko dostupnej forme, formulované jasne a jednoducho*“ (pozri článok 12 ods. 1 všeobecného nariadenia o ochrane údajov), a to tak, aby dotknutá osoba mala vždy jasné informácie o tom, ktoré údaje si má stiahnuť alebo preniesť k inému prevádzkovateľovi so zreteľom na daný účel. Dotknuté osoby by mali mať napríklad možnosť používať softvérové aplikácie na ľahkú identifikáciu, rozpoznanie a spracúvanie konkrétnych údajov z týchto aplikácií.
168. Toto právo by používateľovi malo umožniť získať na svoje osobné použitie najmä údaje, ktoré poskytol prostredníctvom svojho hlasu (napr. história hlasových interakcií) a v rámci vytvorenia svojho používateľského konta (napr.: meno a priezvisko).
169. V záujme plného uplatňovania tohto práva dotknutých osôb v kontexte jednotného digitálneho trhu by mali tvorcovia VVA a vývojári aplikácií vyvinúť bežné strojovo čitateľné

⁵⁷ Pozri napríklad odôvodnenie pracovnej skupiny zriadenej podľa článku 29 v usmerneniach k právu na prenosnosť údajov, ktoré schválil EDPB, s. 16:

„Na technickej úrovni by prevádzkovatelia mali preskúmať a posúdiť dva rôzne a navzájom sa dopĺňajúce spôsoby sprístupnenia prenosných údajov dotknutým osobám alebo ďalším prevádzkovateľom:

- priame poskytnutie celkového súboru prenosných údajov (alebo niekoľkých úryvkov častí globálneho súboru údajov),
- automatizovaný nástroj, ktorý umožňuje extrahovanie príslušných údajov.

Druhý spôsob môžu prevádzkovatelia uprednostňovať v prípade komplexných a veľkých súborov údajov, pretože umožňuje výber ktorejkoľvek časti súboru údajov, ktorá je pre dotknutú osobu v kontexte jej žiadosti relevantná, môže pomôcť minimalizovať riziko a prípadne umožňuje použiť mechanizmy synchronizácie údajov (napr. v súvislosti s pravidelnou komunikáciou medzi prevádzkovateľmi). V prípade ‚nového‘ prevádzkovateľa môže ísť o lepší spôsob zabezpečenia súladu a môže to predstavovať osvedčený postup pri znižovaní rizík v oblasti ochrany súkromia na strane pôvodného prevádzkovateľa.“

⁵⁸ V tejto súvislosti: Usmernenia pracovnej skupiny zriadenej podľa článku 29 k právu na prenosnosť údajov – schválené EDPB, s. 1.

formáty, ktoré uľahčia interoperabilitu dátového formátu medzi systémami VVA⁵⁹ vrátane štandardných formátov pre hlasové údaje. Technológie by mali byť štruktúrované tak, aby nový prevádzkovateľ mohol ľahko a v plnom rozsahu opätovne použiť osobné údaje vrátane hlasových údajov.⁶⁰

170. Pokiaľ ide o formát, poskytovatelia VVA by mali poskytovať osobné údaje v bežne používaných otvorených formátoch (napr. mp3, wav, csv, gsm atď.) spolu s vhodnými metaúdajmi používanými na presné opísanie významu vymieňaných informácií.⁶¹

5 PRÍLOHA: AUTOMATICKÉ ROZPOZNÁVANIE REČI, SYNTÉZA REČI A SPRACÚVANIE PRIRODZENÉHO JAZYKA

171. V nadväznosti na teoretické základy spracovania signálov, najmä na teórie informácií a vzorkovania Claudea Shannona sa automatické spracovanie reči stalo základnou súčasťou technických vied. Na križovatke fyziky (akustika, šírenie vln), aplikovanej matematiky (modelovanie, štatistika), počítačovej vedy (algoritmy, techniky učenia) a humanitných vied (vnímanie, odôvodnenie) sa spracovanie reči rýchlo rozdelilo do mnohých predmetov skúmania: identifikácia a overovanie hovoriaceho, automatické rozpoznávanie reči, syntéza hlasu, detekcia emócií atď. Za posledných pätnásť rokov dosiahla táto disciplína ako celok veľmi významný pokrok, pričom k tomu prispeli rôzne faktory: zlepšené metódy, výrazné zvýšenie výpočtovej kapacity a väčšie objemy dostupných údajov.

5.1 Automatické rozpoznávanie reči (ASR)

172. Automatické rozpoznávanie reči (známe aj ako prevod reči na text) zvyklo zahŕňať tri rôzne fázy zamerané na: 1) určenie, ktoré fonémy boli vyslovené na základe akustického modelu; 2) určenie, ktoré slová boli vyslovené na základe fonetického slovníka; 3) prepis sekvencie slov (viet), ktorá bola na základe jazykového modelu s najväčšou pravdepodobnosťou vyslovená. Vďaka pokroku, ktorý umožnilo hĺbkové učenie [deep learning] (technika strojového učenia), mnohé systémy ponúkajú automatické rozpoznávanie reči medzi koncovými bodmi. Predchádza sa tým potrebe komplexného tréningu troch rôznych modelov a zároveň sa ponúka lepšia výkonnosť, pokiaľ ide o výsledky a čas spracovania. Takmer všetci významní aktéri v digitálnej oblasti teraz ponúkajú vlastné verzie automatického rozpoznávania reči, ktoré môžu ľahko využívať systémy API, pričom existujú aj systémy s otvoreným zdrojovým kódom (napríklad DeepSpeech⁶² alebo Kaldi⁶³).

5.2 Spracovanie prirodzeného jazyka

⁵⁹ V tejto súvislosti: odôvodnenie 68 všeobecného nariadenia o ochrane údajov; usmernenia pracovnej skupiny zriadenej podľa článku 29 k právu na prenosnosť údajov – schválené EDPB, s. 17.

⁶⁰ „V tejto súvislosti odôvodnenie 68 nabáda prevádzkovateľov, aby vyvinuli interoperabilné formáty, ktoré umožnia prenosnosť údajov, ale bez toho, aby prevádzkovateľom vznikla povinnosť prijať alebo zachovať systémy spracúvania, ktoré sú technicky kompatibilné. Vo všeobecnom nariadení o ochrane údajov sa však prevádzkovateľom zakazuje vytvárať prekážky pre poskytovanie údajov.“ – Usmernenia pracovnej skupiny zriadenej podľa článku 29 k právu na prenosnosť údajov – schválené EDPB, s. 5.

⁶¹ EDPB dôrazne podporuje spoluprácu medzi zainteresovanými stranami z odvetvia a obchodnými združeniami na účel spolupráce na spoločnom súbore interoperabilných noriem a formátov s cieľom splniť požiadavky na právo na prenosnosť údajov.

⁶² <https://github.com/mozilla/DeepSpeech>

⁶³ <https://github.com/kaldi-asr/kaldi>

173. Spracovanie prirodzeného jazyka je multidisciplinárna oblasť zahŕňajúca lingvistiku, počítačovú vedu a umelú inteligenciu, ktorej cieľom je vytvoriť nástroje na spracovanie prirodzeného jazyka pre rôzne aplikácie. Oblasť výskumu a uplatnenia sú početné: syntaktická analýza, strojový preklad, automatické generovanie a zhrnutie textu, kontrola pravopisu, systémy odpovedí na otázky, hĺbková analýza textu [text mining], rozpoznávanie pomenovaných entít, analýza sentimentu atď. Cieľom spracovania prirodzeného jazyka je poskytnúť počítačom schopnosť čítať a pochopiť ľudské jazyky a odvodzovať z nich význam. Vývoj aplikácií pre spracovanie prirodzeného jazyka je náročný, pretože počítačové nástroje tradične vyžadujú, aby ľudia s nimi komunikovali v programovacom jazyku, ktorý je formálny, t. j. presný, jednoznačný a vysoko štruktúrovaný. Ľudská reč však nie je vždy presná. Často je nejednoznačná a jazyková štruktúra môže závisieť od mnohých zložitých premenných vrátane slangu, regionálnych dialektov a sociálneho kontextu.
174. Pri spracovaní prirodzeného jazyka sú dvoma hlavnými technikami syntaktická a sémantická analýza. Syntax je usporiadanie slov vo vete tak, aby mali gramatický význam. Pri spracovaní prirodzeného jazyka sa používa syntax na posúdenie významu jazyka založeného na gramatických pravidlách. Použité techniky syntaxe zahŕňajú parsovanie (gramatickú analýzu vety), segmentáciu slov (ktorá rozdeľuje dlhší text na krátke úseky), rozdelenie do viet (ktoré v dlhých textoch označuje hranice viet), morfológickú segmentáciu (ktorá rozdeľuje slová do skupín) a stematizácia (pri ktorej sa hľadajú základné tvary ohybných slov). Sémantika zahŕňa používanie a význam slov. Pri spracovaní prirodzeného jazyka sa používajú algoritmy na pochopenie významu a štruktúry viet. Techniky, ktoré sa pri spracovaní prirodzeného jazyka používajú v oblasti sémantiky, zahŕňajú rozpoznávanie významu slova (pri ktorom sa odvodzuje význam slova na základe kontextu), rozpoznávanie pomenovaných entít (pri ktorom sa určujú slová, ktoré možno zaradiť do skupín) a generovanie prirodzeného jazyka (ktoré bude používať databázu na určenie sémantiky jednotlivých slov). Zatiaľ čo predchádzajúce prístupy k spracovaniu prirodzeného jazyka zahŕňali prístupy založené na pravidlách, pri ktorých jednoduché algoritmy strojového učenia obsahovali informáciu o tom, aké slová a frázy by sa mali hľadať v texte, a poskytovali konkrétne odpovede, keď sa tieto frázy objavili, súčasné prístupy k spracovaniu prirodzeného jazyka sú založené na hĺbkovom učení, druhu umelej inteligencie, ktorý skúma a používa vzorce v údajoch na zlepšenie pochopenia programu.

5.3 Syntéza reči

175. Syntéza reči je umelá tvorba ľudskej reči. Syntéza reči sa vykonáva najmä zreťazením hlasových jednotiek, ktoré sú uložené v databáze. Táto technika spočíva vo výbere zvukových prvkov, ktoré zodpovedajú slovám, ktoré má VVA vysloviť, zo všetkých záznamov účastníka, ktoré boli predtým prepísané do foném, slabík a slov, a následne ich spojiť tak, aby tvorili zrozumiteľnú vetu s prirodzenou výslovnosťou. Alternatívne, rečový syntetizátor môže takisto obsahovať model hlasového traktu a iných charakteristík ľudského hlasu, aby dokázal modelovať parametre hlasu, ako je intonácia, rytmus a zafarbenie, pomocou generatívnych štatistických modelov (napr. WaveNet⁶⁴, Tacotron⁶⁵ alebo DeepVoice⁶⁶) a vytvoriť úplne syntetický hlasový výstup.

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

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

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