

# Pokyny



## **Pokyny 02/2021 k virtuálním hlasovým asistentům**

**verze 2.0**

**Přijato dne 7. července 2021**

## Historie verzí

verze 2.0	7. července 2021	Přijetí pokynů po veřejné konzultaci
verze 1.0	9. března 2021	Přijetí pokynů k veřejné konzultaci

## SHRNUTÍ

Virtuální hlasový asistent (dále jen „VHA“) je služba, která rozumí hlasovým příkazům a provádí je nebo v případě potřeby zprostředkovává komunikaci s dalšími informačními systémy. VHA jsou v současné době k dispozici na většině chytrých telefonů a tabletů, tradičních počítačů a v posledních letech dokonce i na samostatných zařízeních, jako jsou chytré reproduktory.

VHA fungují jako rozhraní mezi uživateli a jejich výpočetními zařízeními a on-line službami, jako jsou vyhledávače nebo internetové obchody. Vzhledem ke své úloze mají VHA přístup k obrovskému množství osobních údajů včetně všech příkazů uživatelů (např. historie prohlížení internetu nebo historie vyhledávání) a odpovědí (např. plánované schůzky).

Drtivou většinu služeb VHA navrhlo několik málo návrhářů VHA. VHA však mohou spolupracovat i s aplikacemi naprogramovanými třetími stranami (vývojáři aplikací VHA), aby umožňovaly používání sofistikovanějších příkazů.

Aby mohl fungovat, VHA potřebuje koncové zařízení vybavené mikrofonem a reproduktorem. Zařízení ukládá hlasové a další údaje, které současní VHA přenášejí na vzdálené servery.

Správci údajů poskytující služby VHA a jejich zpracovatelé proto musí vzít v úvahu jak obecné nařízení o ochraně údajů (GDPR)<sup>1</sup>, tak i směrnici o soukromí a elektronických komunikacích<sup>2</sup>.

Tyto pokyny identifikují některé z nejzásadnějších problémů s dodržováním předpisů a poskytují příslušným zúčastněným stranám doporučení, jak je řešit.

Správci údajů poskytující služby VHA prostřednictvím koncových zařízení bez obrazovky musí i nadále uživatele informovat podle GDPR při nastavování VHA, při instalaci nebo při prvním použití aplikace VHA. V důsledku toho doporučujeme poskytovatelům, návrhářům a vývojářům VHA vyvinout hlasová rozhraní tak, aby usnadňovala podání povinných informací.

V současné době všechny VHA vyžadují, aby se do služby zaregistroval alespoň jeden uživatel. V návaznosti na povinnost standardní a záměrné ochrany osobních údajů by poskytovatelé, návrháři a vývojáři VHA měli zvážit nutnost mít registrovaného uživatele pro každou z funkcí VHA.

Uživatelský účet používaný mnoha návrháři VHA spojuje službu VHA s dalšími službami, jako je e-mail nebo streamování videa. Evropský sbor pro ochranu osobních údajů se domnívá, že správci údajů by se měli zdržet těchto postupů, protože zahrnují používání zdoluhavých a složitých zásad ochrany osobních údajů, které by nebyly v souladu se zásadou transparentnosti GDPR.

Tyto pokyny se zabývají čtyřmi z nejběžnějších účelů, pro které VHA zpracovávají osobní údaje: prováděním požadavků, zlepšováním modelu strojového učení VHA, biometrickou identifikací a profilováním pro personalizovaný obsah nebo reklamu.

Pokud jsou údaje VHA zpracovávány za účelem vyřízení požadavků uživatele, tj. v míře nezbytně nutné pro poskytování služby požadované uživatelem, jsou správci údajů osvobozeni od požadavku

---

<sup>1</sup> Nařízení Evropského parlamentu a Rady 2016/679/EU ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „GDPR“).

<sup>2</sup> Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích), ve znění směrnice 2006/24/ES a směrnice 2009/136/ES (dále jen „směrnice o soukromí a elektronických komunikacích“).

předchozího souhlasu podle čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích. Naopak tento souhlas, jak vyžaduje čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích, by byl nezbytný pro ukládání informací nebo získání přístupu k nim za jakýmkoli jiným účelem, než je vyřízení žádosti uživatelů.

Některé služby VHA uchovávají osobní údaje, dokud jejich uživatelé nepožádají o jejich odstranění. To není v souladu se zásadou omezení uložení údajů. Služby VHA by neměly uchovávat údaje déle, než je nutné pro účely, pro které jsou osobní údaje zpracovávány.

Pokud se správce údajů dozví (například kvůli procesům kontroly kvality) o náhodném shromáždění osobních údajů, měl by ověřit, zda pro každý účel zpracování těchto údajů existuje platný právní základ. V opačném případě by měly být omylem shromážděné údaje odstraněny.

VHA mohou zpracovávat údaje více subjektů údajů. Poskytovatelé a návrháři VHA by proto měli zavést mechanismy řízení přístupu, aby byla zajištěna důvěrnost, integrita a dostupnost osobních údajů. Některé tradiční mechanismy řízení přístupu, jako jsou hesla, však nejsou v kontextu VHA vhodné, protože by musely být vyslovovány nahlas. Pokyny v tomto ohledu nabízí určité úvahy, také v části zaměřené na zpracování zvláštních kategorií osobních údajů pro biometrickou identifikaci.

Poskytovatelé a návrháři VHA by měli vzít v úvahu, že při zaznamenávání hlasu uživatele může záznam obsahovat hlas nebo údaje jiných osob, například hluk na pozadí, který není pro službu nezbytný. Kdykoli je to možné, návrháři VHA by proto měli zvážit technologie, které filtrují nepotřebné údaje a zajišťují, aby byl zaznamenán pouze hlas uživatele.

Při hodnocení potřeby posouzení vlivu na ochranu osobních údajů Evropský sbor pro ochranu osobních údajů považuje za velmi pravděpodobné, že služby VHA spadají do kategorií a podmínek označených jako vyžadující posouzení vlivu na ochranu osobních údajů.

Správci údajů poskytující služby VHA by měli zajistit, aby uživatelé mohli uplatnit svá práva subjektu údajů pomocí snadno použitelných hlasových příkazů. Poskytovatelé a návrháři VHA a vývojáři aplikací by měli na konci procesu informovat uživatele, že jejich práva byla řádně zohledněna, a to hlasem nebo poskytnutím písemného oznámení na mobilní telefon, účet uživatele nebo jakýmkoli jiným způsobem, který si uživatel zvolí.

## Obsah

<b>SHRNUTÍ</b> .....	3
<b>1 OBECNÉ INFORMACE</b> .....	7
<b>2 TECHNOLOGICKÉ POZADÍ</b> .....	8
2.1 Základní charakteristika virtuálních hlasových asistentů .....	8
2.2 Aktéři v ekosystému VHA .....	9
2.3 Podrobný popis .....	9
2.4 Aktivační výrazy .....	10
2.5 Hlasové úryvky a strojové učení.....	11
<b>3 PRVKY OCHRANY OSOBNÍCH ÚDAJŮ</b> .....	11
3.1 Právní rámec.....	11
3.2 Identifikace zpracování údajů a zúčastněné strany.....	14
3.2.1 Zpracovávání osobních údajů .....	14
3.2.2 Zpracování správci a zpracovateli údajů.....	15
3.3 Transparentnost .....	17
3.4 Omezení účelu a právní základ.....	21
3.4.1 Provádění požadavků uživatele .....	21
3.4.2 Vylepšování VHA trénováním systému strojového učení a manuální kontrolou hlasu a přepisů .....	23
3.4.3 Identifikace uživatele (použitím hlasových údajů) .....	23
3.4.4 Profilování uživatelů pro personalizovaný obsah nebo reklamu .....	24
3.5 Zpracování osobních údajů dětí .....	25
3.6 Uchování údajů.....	25
3.7 Bezpečnost .....	28
3.8 Zpracování zvláštních kategorií osobních údajů.....	30
3.8.1 Obecné úvahy ohledně zpracování zvláštních kategorií osobních údajů.....	30
3.8.2 Konkrétní úvahy ohledně zpracování biometrických údajů .....	30
3.9 Minimalizace údajů .....	32
3.10 Odpovědnost .....	32
3.11 Záměrná a standardní ochrana osobních údajů.....	33
<b>4 Mechanismy výkonu práv subjektu údajů</b> .....	33
4.1 Právo na přístup .....	34
4.2 Právo na opravu .....	35
4.3 Právo na výmaz.....	35
4.4 Právo na přenositelnost údajů .....	36

5	Příloha: Automatické rozpoznávání řeči, syntéza řeči a zpracování přirozeného jazyka.....	38
5.1	Automatické rozpoznávání řeči.....	38
5.2	Zpracování přirozeného jazyka.....	38
5.3	Syntéza řeči .....	39

## Evropský sbor pro ochranu osobních údajů

s ohledem na čl. 70 odst. 1 písm. e) a j) nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „GDPR“),

s ohledem na Dohodu o EHP, a zejména přílohu XI a protokol 37 uvedené dohody ve znění rozhodnutí Smíšeného výboru EHP č. 154/2018 ze dne 6. července 2018<sup>3</sup>,

s ohledem na články 12 a 22 svého jednacího řádu,

### PŘIJAL TYTO POKYNY

## 1 OBECNÉ INFORMACE

1. Nedávné technologické pokroky výrazně zvýšily přesnost a popularitu virtuálních hlasových asistentů (dále jen „VHA“). Služby VHA byly mimo jiné integrovány do chytrých telefonů, propojených vozidel, chytrých reproduktorů a chytrých televizorů. Tato integrace poskytla službám VHA přístup k informacím intimního charakteru, které by mohly, pokud nejsou řádně ošetřeny, poškodit práva jednotlivců na ochranu osobních údajů a soukromí. VHA a zařízení, která je využívají, jsou proto pod drobnohledem různých úřadů pro ochranu osobních údajů.
2. Používání interakcí založených na řeči má několik výhod, například: přirozenost interakce, která od uživatelů nevyžaduje, aby se něco učili, rychlost provedení příkazu a rozšíření pole činnosti, které může umožnit rychlejší přístup k informacím. Spoléhání se na řeč však také přináší potíže se správnou interpretací zprávy: variabilita zvukového signálu mezi různými mluvčími, akustické prostředí, nejednoznačnost jazyka atd.
3. V praxi zůstává plynulost nebo zjednodušení úkolů primární motivací pro používání VHA. To může například zahrnovat uskutečnění či přijetí hovoru, nastavení časovače atd., zejména pokud uživatelé nemají volné ruce. Automatizace domácnosti je jedním z hlavních polí působnosti, pro které návrháři VHA vytvořili. Tím, že navrhují zjednodušit provádění úkolů (rozsvícení světla, nastavení topení, spuštění žaluzií atd.) a centralizovat je jediným nástrojem, který lze snadno aktivovat na dálku, lze je brát jako domácí usnadňující prostředek. Kromě osobního nebo domácího použití mohou být hlasové příkazy zajímavé v profesionálním prostředí, kde je obtížné zvládat počítačové nástroje a používat psané příkazy (např. výrobní činnosti).
4. Teoreticky by mezi uživatele, kterým hlasové rozhraní přinese nejvíce výhod, mohli patřit lidé se zdravotním postižením nebo závislí na péči druhých, protože pro ně je používání tradičních rozhraní problematické. Virtuální hlasová asistence může zajistit snadnější přístup k informacím a počítačovým zdrojům a tím podpořit začlenění těchto uživatelů, neboť používání hlasu umožňuje určitým typům uživatelů překonat potíže spojené s psaným slovem.
5. Zdraví je nakonec také oblastí, kde existuje mnoho případů využití pro konverzační prostředky, ať už hlasové, nebo ne. Například během pandemie Covid-19 byly využívány různé „callboty“

---

<sup>3</sup> Pokud se v tomto dokumentu hovoří o „členských státech“, rozumějí se tím „členské státy EHP“.

(automatické nástroje na odpovídání po telefonu), aby poskytovaly předběžnou diagnostiku volajícím uživatelům. Předpokládá se, že v dlouhodobém horizontu by celý proces péče o pacienta mohl být spojen s interakcemi mezi člověkem a asistentem: nejen v zájmu kvality života a prevence, ale také léčby a podpory.

6. V současné době existují více než 3 miliardy chytrých telefonů a všechny mají integrované VHA, přičemž většina z nich je ve výchozím nastavení zapnutá. Některé z nejrozšířenějších operačních systémů v osobních počítačích a laptotech v sobě také zahrnují VHA. Nedávný vzestup chytrých reproduktorů (v roce 2019 se jich prodalo 147 milionů<sup>4</sup>) přináší VHA do milionů domácností a kanceláří. Současné návrhy VHA však ve výchozím nastavení nenabízejí mechanismy autentizace ani ovládání přístupu.
7. Tento dokument se snaží poskytnout vodítko k uplatňování GDPR v kontextu VHA.

## 2 TECHNOLOGICKÉ POZADÍ

### 2.1 Základní charakteristika virtuálních hlasových asistentů

8. VHA lze definovat jako softwarovou aplikaci, která umožňuje mluvený dialog s uživatelem v přirozeném jazyce.
9. Přirozený jazyk má sémantiku specifickou pro lidskou řeč. V závislosti na vlastnostech jazyka a rozmanitosti slovní zásoby lze stejný pokyn formulovat několika způsoby, zatímco některé příkazy se mohou zdát podobné, ale týkat se odlišných věcí. K vyřešení takových nejasností se pak často využívají inferenční mechanismy, například v závislosti na tom, co bylo řečeno dříve, na době, kdy byl pokyn dán, na místě, zájmech osoby atd.
10. VHA lze rozdělit na moduly, které umožňují provádět různé úkoly: zaznamenání a restituce zvuku, automatický přepis řeči (převod řeči na text), automatické zpracování jazyka, strategie dialogu, přístup k ontologiím (soubory údajů a strukturované koncepty související s danou doménou) a externím zdrojům znalostí, generování jazyka, syntéza hlasu (převod textu na řeč) atd. Asistent by konkrétně měl umožnit interakci za účelem provádění akcí (např. „zapnout rádio“, „zhasnout světla“) nebo přístupu ke znalostem (např. „jaké bude zítra počasí?“, „jede vlak v 7:43 ráno?“). VHA tedy hraje roli prostředníka a organizátora, který má usnadňovat plnění úkolů uživatele.
11. V praxi není VHA chytrým reproduktorem, ale chytrý reproduktor může být vybaven hlasovým asistentem. Tyto dvě věci se často zaměňují, nicméně chytrý reproduktor je pouze fyzickou manifestací VHA. VHA může být součástí chytrého telefonu, chytrého reproduktoru, propojených hodinek, vozidla, domácího spotřebiče atd.
12. Organizace základního zpracování údajů může zahrnovat více vzorců toku informací. Lze izolovat tři hlavní entity:

**Fyzické zařízení:** hardwarový prvek, ve kterém je asistent zabudován (chytrý telefon, reproduktor, chytrá televize atd.) a který obsahuje mikrofony, reproduktory a síťové a má výpočetní schopnosti (více či méně rozvinuté v závislosti na konkrétním případě).

---

<sup>4</sup> Viz například tisková zpráva ze dne 1. srpna 2019 od hamburského úřadu pro ochranu údajů a informací: <https://datenschutz-hamburg.de/pressemitteilungen/2019/08/2019-08-01-google-assistant>



**Softwarový program:** část, jež striktně řečeno umožňuje interakci mezi člověkem a strojem a která zahrnuje moduly pro automatické rozpoznávání řeči, zpracování přirozeného jazyka, dialog a syntézu řeči. Tyto moduly mohou fungovat přímo uvnitř fyzického zařízení, ale v mnoha případech probíhají vzdáleně.

**Zdroje:** externí data, jako jsou databáze obsahu, ontologie nebo obchodní aplikace, které poskytují znalosti (např. „kolik je hodin na západním pobřeží USA“, „přečíst mé e-mail“) nebo umožňují provedení požadované akce konkrétním způsobem (např. „zvýšit teplotu o 1,5°C“).

13. VHA umožňují instalaci součástí nebo aplikací třetích stran, které rozšiřují jejich základní funkce. Každý VHA nazývá tyto součásti jinak, ale všechny zahrnují výměnu osobních údajů uživatelů mezi návrhářem VVA a vývojářem aplikace.
14. Ačkoli většina VHA nesdílí s vývojáři aplikací hlasový záznam uživatele, tito aktéři přesto zpracovávají osobní údaje. V závislosti na povaze poskytované funkce má navíc vývojář aplikace přístup k údajům, které mohou obsahovat citlivé informace, jako jsou údaje o zdravotním stavu.

## 2.2 Aktéři v ekosystému VHA

15. VHA může v rámci celého procesu provádění funkcí zahrnovat velký počet aktérů a zprostředkovatelů. V praxi lze identifikovat až pět různých aktérů. V závislosti na obchodních modelech a technologických volbách však někteří aktéři mohou zaujmout kombinace více rolí, například návrhář a integrátor nebo návrhář a vývojář aplikací:
  - a. **Poskytovatel (nebo návrhář) VHA:** zodpovědný za vývoj VHA, navrhuje a definuje jeho možnosti a výchozí funkce: způsoby aktivace, výběr architektury, přístup k údajům, správu záznamů, specifikaci hardwaru atd.
  - b. **Vývojář aplikací VHA:** pokud jde o mobilní aplikace, vytváří aplikace rozšiřující výchozí funkce VHA. Přitom musí respektovat vývojářská omezení nastavená návrhářem.
  - c. **Integrátor:** výrobce propojených objektů, který je chce vybavit VHA. Tyto objekty by měly respektovat požadavky definované návrhářem.
  - d. **Majitel:** zodpovědný za fyzické prostory, které jsou otevřené lidem (ubytovací zařízení, profesionální prostředí, pronájem vozidel atd.), kde si majitel přeje zákazníkům poskytovat VHA (případně spolu se specializovanými aplikacemi).
  - e. **Uživatel:** konečný článek v řetězci VHA, který službu může používat na různých zařízeních (reproduktor, televizor, chytrý telefon, hodinky atd.) v závislosti na tom, jak a kde byl VHA instalován a nastaven.

## 2.3 Podrobný popis

16. Aby VHA mohl provést akci nebo vyhledat informace, proběhne řada kroků:
  - 1) VHA nainstalovaný v zařízení (chytrý telefon, reproduktor, vozidlo) je v pohotovostním režimu. Přesněji řečeno, neustále poslouchá. Dokud však není detekován konkrétní aktivační výraz, zařízení přijímající hlas žádný zvuk dál neodesílá a neprovádí žádnou jinou operaci než detekci aktivačního výrazu. K tomuto účelu se používá vyrovnávací paměť na několik sekund (další podrobnosti viz následující část).

- 2) Uživatel vysloví aktivační výraz a VHA lokálně porovná zachycený zvuk s nastaveným aktivačním výrazem. Pokud se shodují, VHA otevře poslechový kanál a zvukové údaje se okamžitě odešlou.
- 3) V mnoha případech, pokud se příkazy zpracovávají vzdáleně, proběhne na straně serveru druhá kontrola výslovnosti klíčového slova, aby se omezily nechtěné aktivity.
- 4) Uživatel vysloví svůj požadavek, který se průběžně odesílá poskytovateli VHA. Sekvence mluveného projevu je poté automaticky přepsána (převod řeči na text).
- 5) Příkaz je interpretován pomocí technologií zpracování přirozeného jazyka. Z příkazu se extrahují příslušné záměry a identifikují se informační proměnné (tzv. sloty). Poté se použije správce dialogů k určení scénáře interakce, který se má s uživatelem provést poskytnutím příslušného režimu odezvy.
- 6) Pokud příkaz zahrnuje funkce poskytované aplikací třetí strany (dovednosti, akce, zástupce atd.), poskytovatel VVA odešle záměry a informační proměnné (sloty) vývojáři aplikace.
- 7) Je určena odpověď přizpůsobená požadavku uživatele – aspoň v ideálním případě, přičemž odpověď „nemám odpověď na vaši otázku“ je přizpůsobenou odpovědí v případě, že VHA nebyl schopen správně interpretovat požadavek. V případě potřeby se používají vzdálené zdroje: veřejně přístupné znalostní databáze (on-line encyklopedie atd.) nebo autentizace (bankovní účet, hudební aplikace, zákaznický účet pro on-line nákup atd.) a informační proměnné (sloty) se zaplní vyhledanými znalostmi.
- 8) Vytvoří se věta pro odpověď nebo se identifikuje akce (spuštění žaluzií, zvýšení teploty, přehrání skladby, zodpovězení otázky atd.). Věta je syntetizována (převod textu na řeč) nebo je akce, která má být provedena, odeslána do příslušného zařízení.
- 9) VHA se vrátí do pohotovostního režimu.

Upozorňujeme, že zatímco v současné době je většina zpracování souvisejícího s hlasem prováděna na vzdálených serverech, někteří poskytovatelé VHA vyvíjejí systémy, které by mohly část tohoto zpracování provádět lokálně<sup>5</sup>.

## 2.4 Aktivační výrazy

17. Před použitím musí být VHA aktivován. Aktivace znamená, že se asistent přepne do aktivního režimu poslechu, aby mohl od svého uživatele přijímat příkazy a pokyny. I když této aktivace lze někdy dosáhnout i fyzickou akcí (např. stisknutím tlačítka, dotykem na chytrém reproduktoru atd.), téměř všichni VHA na trhu jsou založeni na detekci aktivačního výrazu nebo slova, které jej přepne do aktivního režimu poslechu (také známého jako klíčové slovo, probouzeční slovo nebo slovo pro probuzení).
18. Asistent přitom spoléhá na použití mikrofonu a jednoduchých výpočetních schopností, aby zjistil, zda bylo aktivační slovo vysloveno. Tato analýza, která probíhá nepřetržitě od okamžiku zapnutí VHA, se provádí výhradně lokálně. Teprve po rozpoznání aktivačního slova se hlasový

---

<sup>5</sup> To se uvádí například zde: <https://www.amazon.science/blog/alexa-new-speech-recognition-abilities-showcased-at-interspeech>

záznam zpracuje pro interpretaci a provedení příkazu, což v mnoha případech znamená jejich odeslání na vzdálené servery přes internet. Detekce aktivačního slova je založena na technikách strojového učení. Hlavní výzvou při používání těchto metod je, že detekce má pravděpodobnostní charakter. Systém tedy pro každé vyslovené slovo nebo výraz spočítá skóre spolehlivosti, zda bylo aktivační slovo skutečně vysloveno. Pokud je toto skóre vyšší než předem definovaná prahová hodnota, zachycený zvuk se považuje za aktivační slovo. Takový systém proto není prostý chyb: v některých případech nemusí být aktivace detekována, i když bylo aktivační slovo vysloveno (falešné odmítnutí), zatímco v jiných případech může být aktivace spuštěna, i když uživatel aktivační slovo nevyslovil (falešné přijetí).

19. V praxi by měl být mezi těmito dvěma typy chyb nalezen přijatelný kompromis pro definování prahové hodnoty. Protože však důsledkem falešné detekce aktivačního slova může být zasílání zvukových záznamů, pravděpodobně dojde k neočekávaným a nechtěným přenosům údajů. Poskytovatelé VHA uplatňující vzdálené zpracování záznamu velmi často používají pro tuto detekci dvoustupňový mechanismus: první ověření proběhne lokálně na úrovni zařízení a druhé proběhne na vzdálených serverech, kde poté probíhá další zpracování údajů. V tomto případě vývojáři obvykle nastaví relativně nízkou prahovou hodnotu, aby zlepšili uživatelské prostředí a zajistili, že když uživatel aktivační slovo vysloví, bude téměř vždy rozpoznáno – i když to znamená „nadměrné detekování“ – a poté se provede druhé ověření detekce na straně serveru, které je restriktivnější.

## 2.5 Hlasové úryvky a strojové učení

20. VHA spoléhají na metody strojového učení k provádění široké škály úkolů (detekce aktivačních slov, automatické rozpoznávání řeči, zpracování přirozeného jazyka, syntéza řeči atd.), a proto vyžadují shromažďování, výběr, označování atd. velkých souborů údajů.
21. Nadměrné nebo nedostatečné zastoupení určitých statistických charakteristik může ovlivnit vývoj úkolů založených na strojovém učení a následně se může odrazit ve výpočtech, a tedy i ve způsobu fungování úkolů. Stejně jako množství údajů hraje důležitou roli v přesnosti procesu učení rovněž kvalita údajů.
22. Aby zvýšili kvalitu VHA a zlepšili používané metody strojového učení, mohou návrháři VHA chtít mít přístup k údajům souvisejícím s používáním zařízení v reálných podmínkách – tj. k hlasovým úryvkům – aby je využili v práci na vylepšení systému.
23. Ať už jde o posouzení učební databáze, nebo o opravu chyb vzniklých při nasazení algoritmu, učení a trénování systémů umělé inteligence nutně vyžaduje zásah člověka. Tato část práce, známá jako digitální práce, vyvolává otázky jak o pracovních podmínkách, tak o bezpečnosti. V této souvislosti sdělovací prostředky rovněž informovaly o přenosech údajů mezi návrháři VHA a subdodavateli údajně bez nezbytných záruk ochrany soukromí.

## 3 PRVKY OCHRANY OSOBNÍCH ÚDAJŮ

### 3.1 Právní rámec

24. Příslušným právním rámcem EU pro VHA je v první řadě GDPR, protože zpracování osobních údajů patří k základní funkci VHA. Kromě GDPR stanoví směrnice o soukromí a elektronických

komunikací<sup>6</sup> specifický standard pro všechny aktéry, kteří si přejí ukládat informace nebo přistupovat k informacím uloženým v koncovém zařízení uživatele v EHP.

25. V souladu s definicí „*koncového zařízení*“<sup>7</sup> jsou příklady koncových zařízení chytré telefony, chytré televize a podobná zařízení internetu věcí. I když jsou služby VHA samy o sobě softwarovými službami, vždy fungují prostřednictvím fyzického zařízení, jako je chytrý reproduktor nebo chytrá televize. **VHA využívají k přístupu k těmto fyzickým zařízením, která tvoří „koncové zařízení“ ve smyslu směrnice o soukromí a elektronických komunikacích, sítě elektronických komunikací. Ustanovení čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích se proto použije vždy, když VHA ukládá informace nebo přistupuje k informacím ve fyzickém zařízení, v němž je nainstalován**<sup>8</sup>.
26. Jakékoli operace zpracování osobních údajů následující po výše uvedených operacích zpracování, včetně zpracování osobních údajů získaných přístupem k informacím v koncovém zařízení, musí mít také právní základ podle článku 6 GDPR, aby byly zákonné<sup>9</sup>.
27. Vzhledem k tomu, že správce údajů při žádosti o souhlas s ukládáním informací nebo získáním přístupu k nim podle čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích bude muset subjekt údajů informovat o všech účelech zpracování (myšleno „následné zpracování“) – včetně jakéhokoli zpracování následujícího po výše uvedených operacích – souhlas podle článku 6 GDPR bude obecně nejvhodnějším právním základem pro pokrytí následného zpracování osobních údajů. Souhlas tedy bude pravděpodobně představovat právní základ jak pro ukládání informací a získání přístupu k již uloženým informacím, tak pro zpracování osobních údajů po výše uvedených operacích zpracování. Při posuzování souladu s článkem 6 GDPR je třeba vzít v úvahu, že zpracování jako celek zahrnuje specifické činnosti, pro které se zákonodárce EU snažil poskytnout dodatečnou ochranu<sup>10</sup>. Kromě toho musí správci při stanovování příslušného právního základu zohlednit dopad na práva subjektů údajů, aby byla dodržena zásada korektnosti<sup>11</sup>. Podstatné je, že se správci nemohou spoléhat na článek 6 GDPR, aby snížili dodatečnou ochranu poskytovanou čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích.

---

<sup>6</sup> Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích), ve znění směrnice 2006/24/ES a směrnice 2009/136/ES (dále jen „směrnice o soukromí a elektronických komunikacích“).

<sup>7</sup> Článek 1 směrnice Komise 2008/63/ES ze dne 20. června 2008 o hospodářské soutěži na trhu s telekomunikačními koncovými zařízeními definuje *koncové zařízení* jako a) „zařízení přímo nebo nepřímo připojené k rozhraní veřejné telekomunikační sítě, které může vysílat, zpracovávat nebo přijímat informace; připojení přímé či nepřímé může být provedeno kabelově, za použití optického paprsku nebo elektromagnetických vln; připojení je nepřímé, jestliže je mezi rozhraní sítě a koncové zařízení připojeno další zařízení; b) družicové pozemské stanice“;

<sup>8</sup> Podobnou úvahu týkající se propojených vozidel naleznete v pokynech Evropského sboru pro ochranu osobních údajů 1/2020, odstavec 12 (dále jen „pokyny EDPB 1/2020“). Viz také Evropský sbor pro ochranu osobních údajů, stanovisko 5/2019 ke vzájemnému působení mezi směrnicí o soukromí a elektronických komunikacích a obecným nařízením o ochraně osobních údajů (GDPR), zejména pokud jde o příslušnost, úkoly a pravomoci úřadů pro ochranu údajů.

<sup>9</sup> Tamtéž, bod 41.

<sup>10</sup> Stanovisko 5/2019, odstavec 41.

<sup>11</sup> Evropský sbor pro ochranu osobních údajů, pokyny 2/2019 o zpracování osobních údajů podle čl. 6 odst. 1 písm. b) GDPR v souvislosti s poskytováním on-line služeb subjektům údajů, verze 2.0, 8. října 2019, odstavec 1.

28. Jak je ukázáno v oddíle 2.3 (kroky 2 a 3), v současné době vyžadují VHA přístup k hlasovým údajům uloženým v zařízení VHA<sup>12</sup>. Proto se použije čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích. Použitelnost čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích znamená, že ukládání informací a přístup k informacím již uloženým ve VHA vyžaduje zpravidla předchozí souhlas<sup>13</sup> koncového uživatele, ale umožňuje dvě výjimky: zaprvé, provádění nebo usnadňování přenosu komunikace přes síť elektronických komunikací, nebo zadruhé, je-li to nezbytně nutné k poskytnutí služby informační společnosti výslovně požadované uživatelem.
29. Druhá výjimka („je-li to nezbytně nutné k poskytnutí služby informační společnosti výslovně požadované uživatelem“) by poskytovateli služeb VHA umožnila zpracovávat údaje uživatelů k provádění požadavků uživatelů (viz odst. 72 v oddíle 3.4.1) bez souhlasu předpokládaného v čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích. Naopak takový **souhlas, jak vyžaduje čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích, by byl nezbytný pro** ukládání informací nebo získávání přístupu k nim za **jakýmkoli jiným účelem, než je vyřízení žádosti uživatelů** (např. k profilování uživatelů). Správci údajů by museli přiřadit souhlas konkrétním uživatelům. V důsledku toho by měli správci údajů zpracovávat pouze údaje neregistrovaných uživatelů, aby mohli vykonávat jejich požadavky.
30. VHA mohou omylem zachytit hlasy jednotlivců, kteří neměli v úmyslu službu VHA využít. Zaprvé, do určité míry a v závislosti na VHA, lze změnit aktivační výraz. Jedinci, kteří si této změny nejsou vědomi, mohou omylem použít nově nastavený aktivační výraz. Zadruhé, VHA může detekovat aktivační výraz omylem nebo v důsledku chyby. Je vysoce nepravděpodobné, že by v případě náhodné aktivace byla použita některá z výjimek předpokládaných v čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích. Kromě toho musí být souhlas definovaný v GDPR „jednoznačným projevem vůle subjektu údajů“. Je tedy vysoce nepravděpodobné, že by náhodná aktivace mohla být interpretována jako platný souhlas. Pokud se správci údajů dozvědí (např. prostřednictvím automatizovaného nebo osobního přezkoumání), že služba VHA zpracovala osobní údaje omylem, měli by ověřit, zda pro každý účel zpracování těchto údajů existuje platný právní základ. V opačném případě by měly být omylem shromážděné údaje odstraněny.
31. Kromě toho je třeba poznamenat, že osobní údaje zpracovávané VHA mohou být velmi citlivé povahy. VHA může zpracovávat osobní údaje jak po stránce obsahu (význam mluveného slova), tak v podobně metainformací (pohlaví nebo věk mluvčího apod.). Evropský sbor pro ochranu osobních údajů připomíná, že hlasové údaje jsou ve své podstatě biometrickými osobními údaji<sup>14</sup>. V důsledku toho, pokud jsou tyto údaje zpracovávány za účelem jednoznačné identifikace fyzické osoby nebo jsou ze své podstaty nebo jinak určeny jako osobní údaje zvláštní kategorie, musí mít jejich zpracování platný právní základ v článku 6 a musí být doprovázeno výjimkou z článku 9 GDPR (viz oddíl 3.7 níže).

---

<sup>12</sup> Je možné, že budoucí zařízení VHA přijmou paradigma edge computing a budou schopna poskytovat některé služby lokálně. V takovém případě bude nutné znovu posoudit použitelnost směrnice o soukromí a elektronických komunikacích.

<sup>13</sup> Viz také pokyny EDPB 1/2020, odstavec 14.

<sup>14</sup> Ustanovení čl. 4 odst. 14 GDPR definuje biometrické údaje jako „osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje“.

## 3.2 Identifikace zpracování údajů a zúčastněné strany

32. Vzhledem k mnoha možnostem asistence, které může VHA nabízet v tolika různých prostředích každodenního života subjektu údajů<sup>15</sup>, stojí za zmínku, že zpracování osobních údajů by mělo být pečlivě zváženo, což může být rovněž ovlivněno různými zúčastněnými stranami.

### 3.2.1 Zpracovávání osobních údajů

33. Z hlediska ochrany osobních údajů lze pozorovat několik konstant bez ohledu na typ VHA (tj. typ zařízení, funkce, služby nebo jejich kombinace), který může subjekt údajů používat. Tyto konstanty se týkají plurality dotčených osobních údajů, subjektů údajů a zpracování údajů.

#### **Pluralita typů osobních údajů**

34. Definice osobních údajů podle čl. 4 odst. 1 GDPR zahrnuje širokou škálu různých údajů a vztahuje se v technologicky neutrálním kontextu na jakékoli informace, které se týkají „identifikované nebo identifikovatelné fyzické osoby“<sup>16</sup>. Jakákoli interakce subjektu údajů s VHA může spadat do oblasti působnosti této definice. Jakmile k interakci dojde, může být během provozu VHA zpracováváno různorodé množství osobních údajů, jak je popsáno v oddíle 2.4.
35. Od počátečního požadavku po příslušnou odpověď, akci nebo pozdější akci (např. nastavení týdenního upozornění) proto první zadání osobních údajů vytváří i následné osobní údaje. To zahrnuje primární údaje (např. údaje o účtu, hlasové záznamy, historie žádostí), pozorované údaje (např. údaje zařízení, která se týkají subjektu údajů, protokoly aktivit, on-line aktivity), jakož i odvozené nebo domyslitelné údaje (např. profilování uživatelů). VHA používají řeč ke zprostředkování mezi uživateli a všemi připojenými službami (např. vyhledávačem, on-line obchodem nebo službou streamování hudby), ale na rozdíl od jiných zprostředkovatelů mohou mít VHA plný přístup k obsahu požadavků a následně poskytovat návrháři VHA širokou škálu osobních údajů v závislosti na účelech zpracování.
36. Pluralita osobních údajů zpracovávaných při používání VHA také odkazuje na pluralitu kategorií osobních údajů, kterým by měla být věnována pozornost (viz oddíl 3.7 níže). Evropský sbor pro ochranu osobních údajů připomíná, že při zpracování zvláštních kategorií údajů<sup>17</sup> článek 9 GDPR vyžaduje, aby správce identifikoval platnou výjimku ze zákazu zpracování podle čl. 9 odst. 1 a platný právní základ podle čl. 6 odst. 1 vhodným způsobem podle čl. 9 odst. 2. Výslovný souhlas může být jednou z vhodných výjimek, pokud je souhlas právním základem, na který se vztahuje čl. 6 odst. 1. Článek 9 rovněž uvádí (podrobně), že členské státy mohou zavést další podmínky zpracování biometrických nebo jiných zvláštních kategorií údajů.

---

<sup>15</sup> Například: doma, ve vozidle, na ulici, v práci nebo v jakémkoli jiném soukromém, veřejném nebo pracovním prostoru nebo v kombinaci těchto prostorů.

<sup>16</sup> Ustanovení čl. 4 odst. 1 GDPR také stanoví, že „identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, údaje o poloze, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby“.

<sup>17</sup> Ustanovení čl. 9 odst. 1 GDPR při definici zvláštních kategorií osobních údajů uvádí, že se „zakazuje zpracování osobních údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby“.

### **Pluralita subjektů údajů**

37. Při používání VHA jsou osobní údaje zpracovávány ihned od první interakce s VHA. U některých subjektů údajů se to týká nákupu VHA a/nebo konfigurace uživatelského účtu (tj. registrování uživatelé). U dalších subjektů údajů se jedná o první vědomou interakci s VHA jiného subjektu údajů, který tohoto VHA koupil a/nebo nakonfiguroval (tj. neregistrování uživatelé). Kromě těchto dvou kategorií subjektů údajů existuje ještě třetí: náhodní uživatelé, kteří, ať už jsou registrovaní, či nikoli, nevědomky vznášejí požadavky na VHA (např. vyslovením správného aktivačního výrazu, aniž by věděli, že tímto VHA aktivují, nebo vyslovením jiných slov, která VHA omylem vyhodnotí jako aktivační výraz).
38. Termín pluralita subjektů údajů také označuje více uživatelů jednoho VHA (např. zařízení sdílené mezi registrovanými a neregistrovanými uživateli, mezi kolegy, v rodině, ve škole) a různé typy uživatelů na základě jejich stavu (např. dospělý, dítě, starší nebo zdravotně postižená osoba). Zatímco VHA může nabídnout snazší interakci s digitálním nástrojem a mnoho výhod pro některé kategorie subjektů údajů, je důležité vzít v úvahu specifika každé kategorie subjektů údajů a kontext používání VHA.

### **Pluralita zpracování údajů**

39. Technologie používané k poskytování služeb VHA mají také dopad na množství zpracovávaných údajů a druhy zpracování. Čím více služeb nebo funkcí VHA poskytuje a je připojen k jiným zařízením nebo službám spravovaným třetími stranami, tím více se zvyšuje množství zpracovávaných osobních údajů a zpracování pro jiné účely. To má za následek pluralitu zpracování prováděných automatizovanými prostředky, jak je popsáno v oddílu 2. Kromě automatizovaných prostředků mohou některé případy zahrnovat i zpracování člověkem. To je například případ, kdy zavedená technologie zahrnuje lidský zásah, jako je kontrola přepisu hlasu do textu nebo poskytování anotací k osobním údajům, které lze použít k vložení nových modelů do technologie strojového učení. Jde i o případ, kdy lidé analyzují osobní údaje (např. metadata) za účelem zlepšení služby poskytované VHA.

#### **3.2.2 Zpracování správci a zpracovateli údajů**

40. Subjekty údajů by měly být schopny porozumět a identifikovat příslušné role a měly by být schopny kontaktovat nebo jednat s každou zúčastněnou stranou podle požadavků GDPR. Rozdělení rolí by nemělo být na úkor subjektů údajů, přestože scénáře mohou být komplikované nebo se vyvíjet. Pro posouzení jednotlivých rolí se zúčastněným stranám doporučuje nahlédnout do pokynů EDPB 7/2020, pokud jde o pojmy „správce“ a „zpracovatel“ používané v GDPR<sup>18</sup>.
41. Jak je uvedeno v odstavci 15, hlavní zúčastněné strany lze podle role rozdělit na poskytovatele či návrháře, vývojáře aplikace, integrátora, majitele nebo jejich kombinace. Jsou možné různé scénáře v závislosti na tom, kdo co dělá v obchodním vztahu zúčastněných stran, podle požadavku uživatele, osobních údajů, činnosti zpracování údajů a podle jejich účelů. Zúčastněné strany by měly jasně informovat subjekty údajů o podmínkách, za kterých bude každý z nich jednat a pak dodržovat z toho vyplývající role správců, společných správců nebo zpracovatelů, jak stanoví GDPR<sup>19</sup>. Každý z nich může zaujmout jednu roli nebo několik rolí,

---

<sup>18</sup> Pokyny Evropského sboru pro ochranu osobních údajů 07/2020 ohledně pojmů správce a zpracovatel v GDPR, V2.0, přijaté dne 7. července 2021 (dále jen „pokyny 7/2020“).

<sup>19</sup> Články 12 až 14, článek 26 GDPR.

protože může být jediným správcem údajů, společným správcem nebo zpracovatelem pro jedno zpracování údajů zatímco pro jiné zpracování údajů vykonává jinou roli.

42. Z obecného hlediska může návrhář působit jako správce údajů při určování účelů a prostředků zpracování, ale může zasahovat jako zpracovatel údajů při zpracování osobních údajů jménem jiných stran, například vývojáře aplikací. Uživatel VHA by pak podléhal několika správcům údajů: vývojáři aplikací a návrháři. Je také možné, že návrhář, integrátor a vývojář jsou seskupeni do jediného subjektu, který funguje jako jediný správce údajů. V každém případě musí být příslušná kvalifikace stanovena na základě analýzy případ od případu.

Příklad č. 1:

Návrhář VHA zpracovává uživatelské údaje pro mnoho účelů, včetně zlepšování schopností VHA porozumět hlasu a přesněji reagovat na požadavky. Přestože tento účel může vést ke zpracování údajů vyplývajících z používání aplikací poskytovaných třetími stranami, existuje pouze jeden správce údajů: návrhář VHA, jehož jménem a pro jehož účely je zpracování prováděno.

Příklad č. 2:

Banka nabízí svým zákazníkům aplikaci, kterou lze přímo ovládat prostřednictvím VHA za účelem správy účtů.

Na zpracování osobních údajů se podílejí dva aktéři: návrhář VHA a vývojář bankovní aplikace.

V uvedeném scénáři je banka správcem údajů pro poskytování služby, protože určuje účely a základní způsoby zpracování související s aplikací umožňující interakci s asistentem. Banka nabízí specializovanou aplikaci, která umožňuje uživateli, zákazníkovi banky, vzdáleně spravovat své účty. Kromě toho rozhoduje o způsobech zpracování výběrem vhodného zpracovatele, jímž je návrhář VHA a může hrát důležitou roli poskytnutím svých odborných znalostí při určování způsobů zpracování (například může provozovat vývojovou platformu, která umožňuje zapojení aplikací třetích stran do VHA, a proto stanoví rámec a podmínky, které musí vývojáři aplikací respektovat).

43. Z hlediska subjektu údajů je třeba poznamenat, že několik zúčastněných stran může zpracovávat stejné osobní údaje, i když subjekt údajů ve skutečnosti neočekává, že by do zpracovatelského řetězce byly zapojeny jiné strany než poskytovatel VHA. Pokud tedy subjekt údajů jedná s poskytovatelem VHA ve vztahu k jeho osobním údajům (např. výkon práv subjektu údajů), neznamená to automaticky, že se tato akce bude vztahovat na stejné osobní údaje, které zpracovává jiný zúčastněný subjekt. Jsou-li tyto zúčastněné strany nezávislými správci, je důležité, aby subjektům údajů bylo zasláno jasné informační sdělení s vysvětlením různých fází a aktérů zpracování. Kromě toho by v případech společného správce mělo být objasněno, zda je každý správce způsobilý k dodržování všech práv subjektu údajů nebo který správce je způsobilý pro které právo<sup>20</sup>.

<sup>20</sup> Pokyny 7/2020, odst. 165.



#### Příklad 3:

V tomto scénáři si návrhář VHA přeje použít údaje shromážděné a zpracované pro službu poskytovanou bankou ke zlepšení svého systému rozpoznávání hlasu. Návrhář VHA, který zpracovává údaje pro své vlastní účely, pak bude mít status správce pro toto konkrétní zpracování.

44. Vzhledem k tomu, že do zpracovatelského řetězce může být zapojeno mnoho zúčastněných stran a mnoho pracovníků, mohou nastat rizikové situace, pokud nejsou zavedena vhodná opatření a záruky. Správci za osobní údaje zodpovídají, a proto by se měli zaměřit na jejich ochranu, zejména výběrem vhodných obchodních partnerů a zpracovatelů údajů, uplatňováním zásad záměrné a standardní ochrany osobních údajů<sup>21</sup>, zaváděním odpovídajícího zabezpečení a dalších nástrojů GDPR, jako jsou audity a právní dohody (např. článek 26 pro společné správce nebo článek 28 pro zpracovatele).
45. Ekosystém VHA je komplexní systém, v němž může mnoho aktérů potenciálně sdílet a zpracovávat osobní údaje jako správci nebo zpracovatelé údajů. Je nanejvýš důležité vyjasnit úlohu každého aktéra v souvislosti s každým zpracováním a dodržovat zásadu minimalizace údajů také ve vztahu k výměně údajů.
46. Kromě toho by správci měli být ostražití při předávání osobních údajů a zaručovat požadovanou úroveň ochrany v celém zpracovatelském řetězci, zejména pokud využívají služby umístěné mimo EHP.

### 3.3 Transparentnost

47. Jelikož VHA zpracovávají osobní údaje (např. hlas uživatele, místo pobytu uživatele nebo obsah sdělení), musí splňovat požadavky GDPR na transparentnost podle čl. 5 odst. 1 písm. a), jakož i článku 12 a článku 13 (objasněných 58. bodem odůvodnění). Správci údajů jsou povinni informovat uživatele o zpracování jejich osobních údajů stručnou, transparentní a srozumitelnou formou a snadno přístupným způsobem.
48. Neposkytnutí nezbytných informací je porušením povinností, což může ovlivnit legitimitu zpracování údajů. Splnění požadavku transparentnosti je nezbytné, protože slouží jako kontrolní mechanismus zpracování údajů a umožňuje uživatelům uplatňovat jejich práva. Řádné informování uživatelů o tom, jak jsou jejich osobní údaje používány, ztěžuje správcům údajů zneužívání VHA k účelům, které jsou výrazně mimo očekávání uživatelů. Patentované technologie mají například za cíl odvodit zdravotní stav a emoční stavy z hlasu uživatele a podle toho přizpůsobit poskytované služby.
49. Dodržování požadavků na transparentnost může být obzvláště obtížné pro poskytovatele služeb VHA nebo jakýkoli jiný subjekt jednající jako správce údajů. Vzhledem ke specifické povaze VHA se správci údajů potýkají s několika překážkami, které jim brání v plnění požadavků GDPR na transparentnost:
  - ) **Více uživatelů:** Správci údajů by měli informovat všechny uživatele (registrované, neregistrované a náhodné uživatele), nejen uživatele, který VHA nainstaloval.

<sup>21</sup> Viz pokyny Evropského sboru pro ochranu osobních údajů 4/2019 k článku 25: Záměrná a standardní ochrana osobních údajů, verze 2.0, přijatá dne 20. října 2020.

- J) **Složitost ekosystému:** jak je vysvětleno v oddíle o technologickém pozadí, identity a role stran zpracovávajících osobní údaje během používání VHA nejsou pro uživatele zdaleka zřejmé.
- J) **Specifika hlasového rozhraní:** digitální systémy zatím nejsou vhodné pro interakce založené výhradně na hlase, jak dokazuje téměř systémové používání doprovodné obrazovky. Přizpůsobit se hlasovému rozhraní a umět tímto způsobem jasně a správně informovat uživatele je však nutností.
50. VHA lze považovat za tzv. konečné automaty, které během svého běžného fungování procházejí řadou různých stavů. Mohou poslouchat lokálně za účelem detekce aktivačních výrazů nebo komunikovat se vzdáleným serverem za účelem vyřešení příkazu, ale mohou zaujmout mnoho dalších stavů v závislosti na kontextu (např. pokud je slyšet okolní zvuk prostředí) nebo podle uživatele, kteří s nimi hovoří (např. mohou hovořit s identifikovaným nebo neznámým uživatelem). Tyto situace se bohužel odehrávají ve značné asymetrii informací vzhledem k uživateli, který si je stěžejně vědom, zda zařízení právě poslouchá, a ještě méně si je vědom stavu, v němž se zařízení právě nachází.
51. Důrazně doporučujeme, aby návrháři a vývojáři VHA podnikli odpovídající kroky k vyrovnaní těchto asymetrií, čímž bude fungování VHA interaktivnější. Uživatelé by měli být informováni o stavu, ve kterém se zařízení aktuálně nachází. Tohoto vylepšení transparentnosti lze dosáhnout jednak tím, že bude dialog mezi člověkem a strojem interaktivnější (např. zařízení může nějakým způsobem potvrdit příjem hlasového příkazu), a jednak signalizováním stavu zařízení pomocí konkrétních signálů. V tomto ohledu lze prozkoumat mnoho možností, od použití konkrétních hlasových potvrzení a viditelných ikon nebo kontrol nebo používání displejů na zařízení.
52. Tyto problémy jsou obzvláště důležité s ohledem na pluralitu uživatelů a přítomnost zranitelných kategorií jednotlivců, jako jsou děti, starší lidé nebo uživatelé se zrakovým postižením.
53. Z výše uvedených problémů vyplývají dvě důležité otázky: jaký je nejschůdnější způsob, jak informovat uživatele a kdy je vhodné je informovat? Tyto problémy by měly být dále zkoumány ve dvou různých situacích v závislosti na tom, zda má VHA pouze jednoho uživatele (například osobní chytrý telefon) nebo potenciálně více uživatelů (např. chytré domácí zařízení). Při použití technologie VHA se tato dvě základní nastavení mohou snadno křížit, např. když má uživatel osobní chytrý telefon a připojí jej k automobilu. VHA chytrého telefonu, u kterého lze rozumně očekávat, že jej bude používat pouze tento uživatel, je nyní „rozšířen“ i na ostatní v autě.
54. V současné době jsou všichni VHA připojeni k uživatelskému účtu a/nebo jsou nastaveni aplikací, která to vyžaduje. Otázka, jak by správci údajů mohli zvážit informování těchto uživatelů o zásadách ochrany osobních údajů při nastavování VHA, by měla být řešena tak, jak je popsáno v pokynech pracovní skupiny zřízené podle článku 29 k transparentnosti. Před stažením by aplikace měly zpřístupnit potřebné informace v internetovém obchodě<sup>22</sup>. Tímto způsobem jsou informace poskytnuty co nejdříve a nejpozději v okamžiku získání osobních údajů. Někteří poskytovatelé VHA zahrnují aplikace třetích stran ve výchozím nastavení VHA, takže VHA může tyto aplikace spouštět pomocí konkrétních aktivačních výrazů. VHA využívající

<sup>22</sup> Pokyny k transparentnosti podle nařízení (EU) 2016/679, WP260 rev. 01, potvrzené Evropským sborem pro ochranu osobních údajů (dále jen „pokyny pracovní skupiny zřízené podle článku 29, WP260“), odstavec 11.

tuto strategii instalace aplikací třetích stran by měli zajistit, aby uživatelé též získali potřebné informace o zpracování třetími stranami.

55. Mnoho návrhářů VHA však vyžaduje uživatelské účty k VHA, které spojují službu VHA s několika dalšími službami, jako je e-mail, streamování videa nebo nákupy. V důsledku rozhodnutí návrháře VHA o propojení účtu s mnoha různými službami jsou vyžadovány velmi zdlouhavé a složité zásady ochrany osobních údajů. Délka a složitost těchto zásad ochrany osobních údajů výrazně brání naplnění zásady transparentnosti.

Příklad č. 4:

Návrhář VHA vyžaduje, aby jeho uživatelé měli účet pro přístup ke službě VHA. Tento uživatelský účet není specifický pro službu VHA a lze jej použít i pro další služby nabízené návrhářem VHA, jako je e-mail, cloudové úložiště a sociální média. K vytvoření účtu si uživatelé musí přečíst a přijmout zásady ochrany osobních údajů o délce 30 stran. Zásady obsahují informace o zpracování osobních údajů všemi službami, které by mohly být s účtem propojeny.

Informace poskytnuté návrhářem VHA v tomto případě nelze považovat za stručné a jejich složitost snižuje požadovanou transparentnost. Návrhář VHA by proto nesplňoval požadavky na transparentnost stanovené v článcích 12 a 13 GDPR.

56. Ačkoli nejběžnějším způsobem, jak poskytnout potřebné informace, je písemná forma, GDPR umožňuje i „jiné způsoby“. 58. bod odůvodnění výslovně uvádí, že informace mohou být poskytnuty v elektronické podobě, např. prostřednictvím webové stránky. Kromě toho by se při výběru vhodné metody informování subjektů údajů měly brát v úvahu konkrétní okolnosti, například způsob, jakým správce a subjekt údajů jinak vzájemně komunikují<sup>23</sup>. Alternativou pro zařízení bez obrazovky může být poskytnutí snadno srozumitelného odkazu, a to buď přímo nebo v e-mailu. Již existující řešení by mohla sloužit jako příklad pro informace, např. postupy telefonických středisek při upozorňování volajícího na zaznamenávaný telefonní hovor a jeho nasměrování na zásady ochrany osobních údajů. Omezení VHA bez obrazovky nezbavuje správce údajů povinnosti poskytovat potřebné informace podle GDPR při nastavování VHA nebo instalaci či používání aplikace VHA. Poskytovatelé a vývojáři VHA by měli vyvinout hlasová rozhraní pro usnadnění povinných informací.
57. Velký zájem o VHA by mohli mít uživatelé s poruchami zraku, protože poskytují alternativní způsoby interakce se službami IT, které se tradičně spoléhají na vizuální informace. Podle čl. 12 odst. 1 GDPR je poskytnutí nezbytných informací ústně možné výlučně na žádost subjektu údajů, nikoli však jako základní metoda. Omezení VHA bez obrazovky by však vyžadovala automatizované ústní prostředky podání informací, které by bylo možné rozšířit o písemným prostředky. Při použití zvuku k informování subjektů údajů by měli správci údajů poskytnout potřebné informace stručným a jasným způsobem. Subjekty údajů by navíc měly mít možnost poslechnout si informace znovu<sup>24</sup>.
58. Přijetí příslušných opatření ke splnění požadavků GDPR na transparentnost je složitější, pokud existuje více uživatelů VHA než jen vlastník zařízení. Návrháři VHA musí zvážit, jak správně informovat neregistrované a náhodné uživatele při zpracování jejich osobních údajů. Pokud je

<sup>23</sup> Pokyny pracovní skupiny zřízené podle článku 29, WP260, odst. 19.

<sup>24</sup> Pokyny pracovní skupiny zřízené podle článku 29, WP260, odst. 21.

právním základem pro zpracování údajů uživatelů souhlas, musí být uživatelé řádně informováni, aby byl souhlas platný<sup>25</sup>.

59. Aby byli v souladu s GDPR, měli by správci údajů najít způsob, jak informovat nejen registrované uživatele, ale i neregistrované uživatele a náhodné uživatele VHA. Tito uživatelé by měli být informováni co nejdříve, a to **nejpozději v okamžiku** zpracování. Tato podmínka by mohla být v praxi obzvláště obtížně splnitelná.
60. Některá specifika korporátních společností by rovněž neměla být na úkor subjektů údajů. Protože mnoho zúčastněných stran jsou globální společnosti nebo jsou dobře známé pro konkrétní obchodní činnost (např. telekomunikace, elektronický obchod, informační technologie, webové aktivity), způsob poskytování služby VHA by měl být jasný. Odpovídající informace by měly subjektům údajů umožnit pochopit, zda jejich používání VHA bude či nebude spojeno s dalšími zpracovatelskými aktivitami řízenými poskytovatelem služeb VHA (např. telekomunikace, elektronický obchod, informační technologie nebo webové aktivity) vedle samotného používání VHA.

**Příklad č. 5:**

Návrhář VHA, který také poskytuje platformu sociálních médií a vyhledávač, vyžaduje, aby uživatel propojil svůj účet se svým asistentem, aby asistenta mohl použít. Propojením svého účtu s používáním VHA tak může návrhář zlepšit profil svých uživatelů pomocí asistenta, aplikací (nebo dovedností), které jsou nainstalovány, provedených objednávek atd. Interakce s asistentem jsou tedy novým zdrojem informací souvisejících s uživatelem. Návrhář VHA by měl uživatelům poskytnout jasné informace o tom, jak budou jejich údaje zpracovány pro každou službu, a současně jim poskytnout ovládací prvky, které uživateli umožní vybrat si, zda budou údaje použity k profilování.

## Doporučení

61. Když jsou uživatelé informováni o zpracování osobních údajů VHA pomocí zásad ochrany osobních údajů uživatelského účtu a účet je propojen s jinými nezávislými službami (např. e-mailem nebo on-line nákupy), Evropský sbor pro ochranu osobních údajů doporučuje, aby zásady ochrany osobních údajů měly jasně oddělenou část týkající se zpracování osobních údajů VHA.
62. Informace poskytnuté uživateli by měly odpovídat přesně tomu shromažďování a zpracování údajů, které se provádí. I když jsou v hlasovém vzorku obsaženy určité metainformace (např. úroveň stresu mluvčího), není automaticky jasné, zda se taková analýza provádí. Je klíčové, aby správci byli transparentní v tom, jaké konkrétní aspekty surových dat zpracovávají.
63. Kromě toho by mělo být vždy zřejmé, ve kterém stavu se VHA nachází. Uživatelé by měli být schopni určit, zda VHA aktuálně lokálně naslouchá a zejména zda souběžně odesílá informace do vzdáleného serveru. Tyto informace by měly být dostupné také pro osoby se zdravotním postižením, jako je barvoslepost (daltonismus) nebo hluchota. Zvláštní pozornost by měla být věnována skutečnosti, že VHA umožňují používání způsobem, u něhož není nutný oční kontakt se zařízením. Veškerá zpětná vazba pro uživatele, včetně změn stavu, by tedy měla být k dispozici alespoň ve vizuální i akustické podobě.

<sup>25</sup> Ustanovení čl. 4 odst. 11 GDPR.

64. Zvláštní pozornost je třeba věnovat situaci, kdy zařízení umožňují přidávat funkce třetích stran (aplikace pro VHA). Zatímco některé obecné informace mohou být poskytnuty uživatelům, pokud právě oni přidávají tuto funkci (vzhledem k tomu, že se jedná o volbu uživatele), při běžném používání zařízení mohou být hranice mezi různými zúčastněnými správci údajů mnohem méně jasné, tj. uživatel nemusí být dostatečně informován o tom, jak a kým jsou jeho údaje zpracovávány (a v jakém rozsahu) při konkrétním dotazu.
65. Všechny informace o zpracování na základě údajů shromážděných a odvozených ze zpracování zaznamenaného hlasu by měly být k dispozici i uživatelům podle článku 12 GDPR.
66. Správci údajů VHA by měly transparentně sdělit, jaké informace může VHA o svém okolí získávat, například pokud jde o ostatní lidi v místnosti, hudbu hrající v pozadí, jakékoli zpracování hlasu z lékařských, marketingových či jiných důvodů, domácí zvířata atd.

### 3.4 Omezení účelu a právní základ

67. Zpracování hlasových požadavků VHA má zřejmý účel: provedení požadavku. Často však existují další účely, které nejsou tak zjevné, jako je zlepšení schopností VHA porozumět přirozenému jazyku trénováním modelu VHA pomocí technik strojového učení. Mezi nejběžnější účely zpracování osobních údajů u VHA patří:
  - ) provádění požadavků uživatele
  - ) zlepšení VHA prostřednictvím strojového učení a kontrolou a označováním přepisů hlasu člověkem
  - ) identifikace uživatele (použitím hlasových údajů)
  - ) profilování uživatelů pro personalizovaný obsah nebo reklamu
68. Vzhledem ke své roli zprostředkovatele a způsobu, jakým jsou navrženi, zpracovávají VHA širokou škálu osobních i neosobních údajů. To umožňuje zpracování osobních údajů pro mnoho účelů, které přesahují rámec reakce na požadavky uživatelů a které mohou zůstat zcela bez povšimnutí. Analýzou údajů shromážděných prostřednictvím VHA je možné zjistit nebo odvodit zájmy uživatelů, jejich časový rozvrh, jízdní trasy nebo návyky. To by mohlo umožnit zpracování osobních údajů pro nepředvídané účely (např. analýza sentimentu nebo hodnocení zdravotního stavu<sup>26</sup>), což by bylo výrazně nad rámec rozumných očekávání uživatelů.
69. Správci údajů by měli jasně specifikovat svůj účel (účely) v souvislosti s kontextem, ve kterém se VHA používá, aby jim subjekty údajů jasně rozuměly (např. uvedením účelů v kategoriích). V souladu s čl. 5 odst. 1 GDPR by osobní údaje měly být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a neměly by být dále zpracovávány způsobem, který je s těmito účely neslučitelný.

#### 3.4.1 Provádění požadavků uživatele

70. Hlavní použití VHA je udělování hlasových příkazů, které má následně provést VHA nebo přidružená aplikace či služba (např. služba streamování hudby, mapovací služba nebo elektronický zámek). Hlas uživatele a případně další údaje (např. poloha uživatele při žádosti o vyhledání trasy na určité cílové místo) proto mohou být zpracovány.

---

<sup>26</sup> Eoghan Furey, Juanita Blue, „Alexa, Emotion, Privacy and GDPR“, konferenční příspěvek, konference Interakce člověka s počítačem, červenec [2018].

Příklad č. 6:

Cestující v chytrém autě vybaveném VHA si vyžádá trasu k nejbližší čerpací stanici. VHA zpracuje hlas uživatele, aby porozuměl příkazu, a polohu vozu, aby našel trasu, a odešle ji do chytrého zařízení, aby se trasa ukázala na obrazovce v autě.

71. Pokud zpracování hlasových příkazů zahrnuje ukládání nebo přístup k informacím uloženým v koncových zařízeních koncového uživatele, musí být dodržen čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích. Přestože čl. 5 odst. 3 obsahuje obecnou zásadu, že takové ukládání nebo přístup vyžaduje předchozí souhlas koncového uživatele, stanoví rovněž výjimku z požadavku na souhlas tam, kde je „to nezbytně nutné k tomu, aby mohl poskytovatel služeb informační společnosti poskytovat služby, které si účastník nebo uživatel výslovně vyžádal“. Pokud jsou hlasové údaje zpracovány za účelem vyřízení požadavků uživatele, jsou vyňaty z požadavku předchozího souhlasu.
72. Jak již bylo uvedeno výše, jakékoli operace zpracování osobních údajů po uložení informací nebo přístupu k nim v koncovém zařízení koncových uživatelů musí mít právní základ podle článku 6 GDPR, aby byly zákonné.
73. U VHA probíhají dvě po sobě jdoucí operace zpracování. Jak je uvedeno výše, první vyžaduje přístup k VHA (a proto musí být splněny podmínky čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích). Kromě podmínek čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích vyžaduje tento druhý krok také právní základ podle článku 6 GDPR.
74. Když se jednotlivec rozhodne použít VHA, obecně to znamená, že počáteční uživatel nejprve potřebuje zaregistrovat účet, aby VHA aktivoval. Jinými slovy, tato situace se týká smluvního vztahu<sup>27</sup> mezi registrovaným uživatelem a správcem údajů VHA. S ohledem na její podstatu a základní cíl je hlavním účelem této smlouvy použití VHA k vyřízení žádosti uživatele o asistenci.
75. Jakékoli zpracování osobních údajů, které je nezbytné k vyřízení žádosti uživatele, se proto může opírat o právní základ plnění smlouvy<sup>28</sup>. Takové zpracování zejména zahrnuje zaznamenání hlasové žádosti uživatele, její přepis do textu, její interpretaci, informace získané ze zdroje znalostí k přípravě odpovědi a poté přepis konečné odpovědi do hlasové podoby, čímž je žádost uživatele ukončena.
76. Plnění smlouvy může být právním základem pro zpracování osobních údajů pomocí strojového učení, pokud je to pro poskytování služby nutné. Zpracování osobních údajů pomocí strojového učení pro jiné účely, které nejsou nutné, jako je zlepšení služeb, by se nemělo o tento právní základ opírat.
77. V neposlední řadě by nemělo dojít k zaměnění právních základů plnění smlouvy a souhlasu podle GDPR. Souhlas poskytnutý pro uzavření smlouvy, tj. souhlas se smlouvou, je součástí platnosti této smlouvy a neodkazuje na konkrétní význam souhlasu podle GDPR<sup>29</sup>.

<sup>27</sup> Za předpokladu, že „smlouva je platná podle příslušných vnitrostátních právních předpisů závazkového práva“, výňatek z pokynů 2/2019 o zpracování osobních údajů podle čl. 6 odst. 1 písm. b) GDPR v souvislosti s poskytováním on-line služeb subjektům údajů („pokyny 2/2019“), odst. 26.

<sup>28</sup> V souladu s pokyny 2/2019, které navíc stanoví, že stanovisko 06/2014 zůstává relevantní pro čl. 6 odst. 1 písm. b) GDPR (viz zejména strany 11, 16, 17, 18 a 55 stanoviska 06/2014).

<sup>29</sup> Viz pokyny 2/2019, a to odstavce 18, 19, 20, 21 a 27.

78. Pokud použití VHA nevyžaduje předchozí konfiguraci uživatelského účtu pro VHA, souhlas by mohl být možným právním základem.

### 3.4.2 Vylepšování VHA trénováním systému strojového učení a manuální kontrolou hlasu a přepisů

79. Nářečí lidské řeči jsou nesčetná a jejich různorodost nesmírná. I když jsou všichni VHA funkční ihned po nainstalování, jejich výkon se může zlepšit jejich přizpůsobením konkrétním charakteristikám řeči uživatelů. Jak je uvedeno v oddíle 2.6, tento proces přizpůsobení se opírá o metody strojového učení a skládá se ze dvou procesů: přidání nových údajů shromážděných od jeho uživatelů do tréninkového souboru údajů VHA a lidská kontrola údajů zpracovaných za účelem provedení zlomku požadavků.

#### Příklad č. 7:

Uživatel VHA musí vyslovit třikrát stejný hlasový příkaz, protože mu VHA nerozumí. Tyto tři hlasové příkazy a jejich přepisy jsou předány lidským ověřovatelům, aby přepisy zkontrolovali a opravili. Hlasové příkazy a zkontrolované přepisy jsou přidány do tréninkového souboru údajů VHA, aby se jeho fungování zlepšilo.

80. Činnosti zpracování popsané v tomto příkladu by neměly být považovány za (striktně) „*nezbytné pro splnění smlouvy*“ ve smyslu čl. 6 odst. 1 písm. b) GDPR, a vyžadují proto jiný právní základ z článku 6 GDPR. Hlavním důvodem je, že VHA jsou již funkční ihned po nainstalování, a mohou tedy fungovat, jak je (striktně) nezbytné pro splnění smlouvy. Evropský sbor pro ochranu osobních údajů se nedomnívá, že by právní základ podle čl. 6 odst. 1 písm. b) byl obecně vhodný pro zpracování za účelem vylepšování služeb nebo rozvíjení nových funkcí v rámci stávajících služeb. Ve většině případů uzavírá uživatel smlouvu o poskytnutí stávající služby. I když možnost zlepšování a upravování služeb může být běžně zahrnuta do smluvních podmínek, takové zpracování obvykle nelze považovat za objektivně nezbytné pro plnění smlouvy s uživatelem.

### 3.4.3 Identifikace uživatele<sup>30</sup> (použitím hlasových údajů)

81. Použití hlasových údajů k identifikaci uživatele předpokládá zpracování biometrických údajů, jak je definováno v článku 4.14 GDPR. V důsledku toho bude muset správce údajů kromě identifikace právního základu podle článku 6 GDPR určit výjimku podle článku 9 GDPR<sup>31</sup>.
82. Z výjimek uvedených v článku 9 GDPR se zdá, že pro tento konkrétní účel platí pouze výslovný souhlas subjektů údajů.

<sup>30</sup> Technicky vzato je třeba pojem identifikace odlišit od ověření (autentizace). Identifikace je vyhledáváním a porovnáváním mnoha uživatelů (1: N) a v zásadě vyžaduje databázi, ve které je uvedeno více jednotlivců. Naopak zpracování pro účely ověření je srovnáváním jedna k jedné (1:1) a slouží k ověření a potvrzení biometrickým porovnáním, zda je jednotlivec tatáž osoba jako osoba, od které biometrické údaje pocházejí. Podle informací Evropského sboru pro ochranu osobních údajů spoléhají VHA na trhu na výhradní použití technologií identifikace mluvčích.

<sup>31</sup> GDPR míní, že pouhá povaha údajů není vždy dostačující k určení, zda se považuje za zvláštní kategorii údajů, protože „*na fotografie se definice biometrických údajů vztahuje pouze v případech, kdy jsou zpracovávány zvláštními technickými prostředky umožňujícími jedinečnou identifikaci nebo autentizaci fyzické osoby*“ (51. bod odůvodnění). Stejně odůvodnění platí i pro hlas.

83. Jelikož však tento účel vyžaduje použití zvláštního právního režimu podle čl. 9 GDPR, následují další podrobnosti v oddíle 3.8, týkající se zpracování zvláštních kategorií údajů.

#### 3.4.4 Profilování uživatelů pro personalizovaný obsah nebo reklamu

84. Jak bylo uvedeno výše, VHA mají přístup k obsahu všech hlasových příkazů, i když jsou zaměřeny na služby poskytované třetími stranami. Tento přístup by umožnil návrháři VHA sestavovat velmi přesné uživatelské profily, které by bylo možné použít k nabídce personalizovaných služeb nebo reklam.

Příklad č. 8:

Pokaždé, když uživatel VHA provede vyhledávání na internetu, přidá VHA do uživatelského profilu štítky označující témata, která uživatele zajímají. Výsledky pro každé nové vyhledávání se zobrazí uživateli v pořadí zohledňujícím tyto štítky.

Příklad č. 9:

Pokaždé, když uživatel VHA provede nákup prostřednictvím služby elektronického obchodování, uloží VHA záznam o objednávce. Poskytovatel VHA umožní třetím stranám směřovat na uživatele VHA cílenou reklamou na základě minulých nákupů.

85. Personalizace obsahu může (ale nemusí) představovat podstatný, očekávaný prvek VHA. Zda bude takové zpracování považováno za podstatný aspekt služby VHA, bude záviset na povaze poskytované služby, očekávání běžného subjektu údajů s ohledem nejen na podmínky služby, ale také na způsob, jakým je služba propagována uživatelům, a na tom, zda lze službu poskytovat bez personalizace<sup>32</sup>.
86. Pokud k personalizaci dochází v rámci smluvního vztahu a jako součást služby výslovně vyžadované koncovým uživatelem (a zpracování je omezeno na to, co je nezbytně nutné k poskytování této služby), může být takové zpracování založeno na článku 6 odst. 1 písm. b) GDPR.
87. Pokud zpracování není striktně „*nezbytné pro splnění smlouvy*“ ve smyslu čl. 6 odst. 1 písm. b) GDPR, musí poskytovatel VHA v zásadě požádat o souhlas subjektu údajů. Protože souhlas podle čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích bude vyžadován pro ukládání informací nebo získávání přístupu k nim (viz odstavce 28–29 výše), souhlas podle čl. 6 odst. 1 písm. a) GDPR bude rovněž v zásadě vhodným právním základem pro zpracování osobních údajů po těchto operacích, protože spoléhání se na oprávněný zájem by v určitých případech mohlo narušit další úroveň ochrany stanovenou v čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích.
88. Pokud jde o profilování uživatelů pro reklamu, je třeba poznamenat, že tento účel není nikdy považován za službu výslovně požadovanou koncovým uživatelem. V případě zpracování pro tento účel by tedy měl být systematicky získáván souhlas uživatelů.

<sup>32</sup> Viz také pokyny 2/2019, odstavec 57.



## Doporučení

89. Uživatelé by měli být informováni o účelu zpracování osobních údajů a tento účel by měl odpovídat jejich očekáváním od zařízení, které si koupí. V případě VHA je tímto účelem – z pohledu uživatele – jednoznačně zpracování hlasu za jediným účelem interpretace jejich dotazu a poskytnutí smysluplných odpovědí (ať už jde o odpovědi na dotaz, nebo jiné reakce, jako je dálkové ovládání osvětlení).
90. Pokud je zpracování osobních údajů založeno na souhlasu, takový souhlas „by měl být udělen pro jeden či více konkrétních účelů“ a „subjekt údajů má možnost volby ve vztahu ke každému z nich“. Navíc „správce, který žádá o souhlas pro různé účely, by měl poskytnout samostatnou volbu pro každý účel, aby uživatelům umožnil udělit konkrétní souhlas pro konkrétní účely“<sup>33</sup>. Uživatelé by například měli mít možnost samostatně souhlasit nebo nesouhlasit s ručním prohlížením a označováním hlasových záznamů nebo s používáním jejich hlasových údajů pro identifikaci/autentizaci uživatele (viz oddíl 3.7).

### 3.5 Zpracování osobních údajů dětí

91. Děti mohou také komunikovat s VHA nebo si mohou vytvořit vlastní profily připojené k profilům dospělých. Někdy jsou VHA zabudovány do zařízení, která jsou specificky zaměřena na děti.
92. Pokud je právním základem zpracování plnění smlouvy, podmínky zpracování údajů o dětech budou záviset na vnitrostátních právních předpisech smluvního práva.
93. Pokud je právním základem zpracování souhlasje podle čl. 8 odst. 1 GDPR zpracování údajů dětí zákonné pouze tehdy, „*je-li dítě ve věku nejméně 16 let. Je-li dítě mladší 16 let, je takové zpracování zákonné pouze tehdy a do té míry, pokud byl tento souhlas vyjádřen nebo schválen osobou, která vykonává rodičovskou zodpovědnost k dítěti*“. V důsledku toho by pro dosažení souladu s GDPR, pokud je právním základem souhlas, mělo být získáno výslovné povolení od rodičů nebo opatrovníků ke shromažďování, zpracování a ukládání údajů dětí (hlas, přepisy atd.).
94. Rodičovská kontrola je do určité míry k dispozici, ale ve své současné podobě není uživatelsky přívětivá (např. je nutné se přihlásit k nové službě) nebo má omezené schopnosti. Správci údajů by měli investovat do vývoje prostředků pro rodiče nebo opatrovníky, které by měly kontrolu nad používáním VHA dětmi.

### 3.6 Uchování údajů

95. VHA zpracovávají a vytvářejí širokou škálu osobních údajů, jako je hlas, přepisy hlasu, metadata nebo systémové protokoly. Tyto typy údajů lze zpracovávat pro celou řadu účelů, jako je poskytování služby, zlepšování zpracování přirozeného jazyka, personalizace obsahu nebo vědecký výzkum. Podle zásady omezení uložení údajů uvedeného v GDPR by služby VHA neměly uchovávat údaje déle, než je nutné pro účely, pro které jsou osobní údaje zpracovávány. Proto by doby uchování údajů měly být vázány na jednotlivé účely zpracování. Poskytovatelé služeb VHA nebo třetí strany poskytující služby prostřednictvím VHA by měli posoudit maximální dobu uchování pro každý soubor údajů a pro každý účel.
96. Zásada minimalizace údajů úzce souvisí se zásadou omezení uložení údajů. Správci údajů musí omezit nejen dobu uchování údajů, ale také jejich typ a množství.

---

<sup>33</sup> Viz [pokyny EDPB k souhlasu podle nařízení 2016/679](#), přijaté dne 4. května 2020, oddíl 3.2.

97. Správci údajů by si měli položit mimo jiné následující otázky: Je nutné k dosažení účelu X uložit všechny hlasové záznamy nebo všechny přepisy hlasu? Je nutné mít nadále uložené hlasové údaje, jakmile byl uložen přepis hlasu? V takovém případě, za jakým účelem? Na jak dlouho je pro každý účel hlasové nebo přepisové údaje nutné ukládat? Odpověď na tyto a další podobné otázky určí doby uchování, které by měly být součástí informací dostupných subjektům údajů.
98. Některé VHA ukládají ve výchozím nastavení osobní údaje, jako jsou hlasové úryvky nebo přepisy, po dobu blíže neurčenou, přičemž uživatelům poskytují možnost takové údaje odstranit. Uchovávání osobních údajů na neurčitou dobu je v rozporu se zásadou omezení uložení. Pokud správci údajů poskytnou subjektům údajů prostředky na odstranění osobních údajů, nezbavuje je to odpovědnosti za stanovení a vymáhání zásad uchovávání údajů.
99. Návrh VHA musí brát v úvahu ovládací prvky uživatelů k odstranění jejich osobních údajů z jejich zařízení a ze všech systémů vzdáleného úložiště. Tyto ovládací prvky mohou být vyžadovány k vyřešení různých požadavků uživatelů, například žádosti o vymazání nebo odvolání dříve uděleného souhlasu. Návrh některých VHA tento požadavek nebral v úvahu<sup>34</sup>.
100. Stejně jako v jiných souvislostech mohou správci údajů uchovávat osobní údaje jako důkaz služby poskytované uživateli za účelem splnění zákonné povinnosti. Správce může na základě toho uchovávat osobní údaje. Pro splnění této zákonné povinnosti by však uchovávaných údajů mělo zůstat jen nezbytné minimum a jen po minimální dobu. Údaje uchovávané za účelem splnění zákonné povinnosti by samozřejmě neměly být použity pro jiné účely bez právního základu podle článku 6 GDPR.

Příklad č. 10:

Uživatel si koupí televizi ve službě elektronického obchodování pomocí hlasového příkazu přes VHA. I když uživatel poté požádá o vymazání svých údajů, poskytovatel nebo vývojář VHA by mohl stále uchovávat některé údaje na základě své zákonné povinnosti stanovené daňovými předpisy uchovávat doklady o nákupu. Údaje uložené za tímto účelem by však neměly překročit minimum nezbytné pro splnění zákonné povinnosti a nemohou být zpracovány pro jiné účely bez právního základu podle článku 6 GDPR.

101. Jak je uvedeno v oddíle 2, schopnost rozpoznávání hlasu VHA se zlepšuje trénováním systémů strojového učení pomocí údajů uživatelů. Pokud uživatelé nesouhlasí s použitím svých údajů k takovému účelu nebo svůj souhlas stáhnou, jejich údaje by nemohly být legálně použity k trénování modelu a měly by být vymazány správcem údajů za předpokladu, že neexistuje žádný jiný účel, který by odůvodňoval jejich další uchovávání. Existují však důkazy, že v některých modelech strojového učení může existovat riziko opětovné identifikace.<sup>35</sup>
102. Správci a zpracovatelé údajů by měli používat modely, které neomezují jejich schopnost zastavit zpracovávání, pokud jednotlivci odvolá svůj souhlas, ani by neměli používat modely, které omezují jejich schopnost usnadnit uplatnění práv subjektu údajů. Správci a zpracovatelé údajů by měli používat zmírňující opatření ke snížení rizika opětovné identifikace na přijatelnou prahovou hodnotu.

<sup>34</sup> Viz dopis Amazonu ze dne 28. června 2019 jako odpověď americkému senátoru Christopheru 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)

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

103. V případě, že uživatel odvolá svůj souhlas, údaje shromážděné od uživatele již nemohou být použity pro další trénování modelu. Nicméně, model dříve natrénovaný pomocí těchto údajů odstraněn být nemusí. Evropský sbor pro ochranu osobních údajů však zdůrazňuje, že existují důkazy o tom, že v některých modelech strojového učení může existovat riziko úniku osobních údajů. Mnoho studií zejména ukázalo, že lze provádět rekonstrukce i útoky, které útočníkům umožňují získávat informace o jednotlivcích<sup>36</sup>. Správci a zpracovatelé údajů by proto měli používat zmírňující opatření ke snížení rizika opětovné identifikace na přijatelnou prahovou hodnotu s cílem zajistit, aby používali modely, které neobsahují osobní údaje.
104. Subjekty údajů by neměly být pobízeny k tomu, aby svolily k uchovávání svých údajů po neurčitou dobu. Odstranění uložených hlasových údajů nebo přepisů může mít dopad na výkon služby, ale tento dopad by měl být uživatelům vysvětlen jasným a měřitelným způsobem. Poskytovatelé služeb VHA by se měli vyvarovat obecných prohlášení o zhoršení služby po vymazání osobních údajů.
105. Anonymizace hlasových záznamů je obzvláště náročná, protože uživatele je možné identifikovat podle obsahu samotné zprávy a vlastností samotného hlasu. Nicméně probíhá výzkum<sup>37</sup> technik, které by mohly umožnit odstranění situačních informací, jako jsou zvuky v pozadí, a anonymizovat hlas.

## Doporučení

106. Z pohledu uživatele je hlavním účelem zpracování jeho údajů dotazování a přijímání odpovědí a/nebo spouštění akcí, jako je přehrávání hudby nebo rozsvěcení či zhasínání světel. Po zodpovězení dotazu nebo provedení příkazu by měly být osobní údaje odstraněny, pokud návrhář nebo vývojář VHA nemá platný právní základ k jejich uchovávání pro konkrétní účel.
107. Před zvažováním anonymizace jako prostředku k naplnění zásady omezení uložení údajů by měli poskytovatelé a vývojáři VHA zkontrolovat, že anonymizační proces činí hlas neidentifikovatelným.
108. Výchozí hodnoty konfigurace by měly odrážet tyto požadavky tím, že jsou nastaveny na absolutní minimum uložených informací o uživateli. Pokud jsou tyto možnosti uvedeny jako součást průvodce nastavením, výchozí nastavení by to mělo odrážet a všechny možnosti by měly být prezentovány jako rovnocenné možnosti bez vizuální diskriminace.
109. Pokud během procesu kontroly poskytovatel nebo vývojář VHA detekuje záznam pocházející z chybné aktivace, záznam samotný i všechny související údaje by měly být okamžitě odstraněny a neměly by být použity k žádnému účelu.

---

<sup>36</sup> N. Carlini a kol., „[Extracting Training Data from Large Language Models](#)“, prosinec 2020.

<sup>37</sup> Viz například: VoicePrivacy (<https://www.voiceprivacychallenge.org>), iniciativa k vývoji řešení ochrany soukromí pro technologii řeči.

Viz také nástroje pro hlasovou anonymizaci s otevřeným zdrojovým kódem vyvinuté v rámci výzkumného a inovačního projektu H2020 COMPRISE: [https://gitlab.inria.fr/comprise/voice\\_transformation](https://gitlab.inria.fr/comprise/voice_transformation).

### 3.7 Bezpečnost

110. Za účelem bezpečného zpracování osobních údajů by VHA měly chránit jejich důvěrnost, integritu a dostupnost. Kromě rizik vyplývajících z prvků ekosystému VHA vyvolává používání hlasu jako komunikačního prostředku řadu nových bezpečnostních rizik.
111. Jednoho VHA používá více uživatelů. VHA mohou dovolovat více než jednoho registrovaného uživatele a kdokoli v jejich okolí může vydávat příkazy a používat jejich služby. Jakákoli služba VHA vyžadující důvěrnost bude zahrnovat nějaký mechanismus řízení přístupu a autentizace uživatelů. Bez řízení přístupu by kdokoli, kdo může hlasovému asistentovi udělovat hlasové příkazy, mohl přistupovat k osobním údajům uživatelů, upravovat je nebo je mazat (např. vyžádat si přijaté zprávy, adresu uživatele nebo události v kalendáři). Udělování hlasových příkazů hlasovému asistentovi nevyžaduje fyzickou blízkost, protože je lze ovládat například prostřednictvím vysílání signálu<sup>38</sup> (např. rozhlas nebo televize). Některé ze známých metod vzdáleného vydávání příkazů pro VHA, jako jsou laserové<sup>39</sup> nebo ultrazvukové (neslyšitelné) vlny<sup>40</sup>, ani nejsou lidskými smysly detekovatelné.
112. Autentizace uživatelů může záviset na jednom nebo více z následujících faktorů: něco, co znáte (například heslo), něco, co máte (například čipová karta), nebo něco, čím jste (například hlasový profil). Bližší pohled na tyto faktory autentizace v kontextu VHA ukazuje, že:
  - )] Autentizace pomocí něčeho, co uživatel ví, je problematická. Tajný klíč, který by uživatelům umožnil prokázat svou totožnost, má být vysloven nahlas, a tím odhalen komukoli v okolí. Komunikačním kanálem VHA je okolní vzduch, což je typ kanálu, který nelze střežit způsoby, jakými jsou hlídány tradiční kanály (např. omezením přístupu ke kanálu nebo šifrováním jeho obsahu).
  - )] Autentizace pomocí něčeho, co uživatel má, by vyžadovala, aby poskytovatelé služeb VHA vytvářeli, distribuovali a spravovali „tokeny“, které by se mohly používat jako důkaz totožnosti.
  - )] Autentizace pomocí něčeho, čím uživatelem je, znamená použití biometrických údajů za účelem jednoznačné identifikace fyzické osoby (viz oddíl 3.7 níže).
113. Uživatelské účty VHA jsou přidruženy k zařízením, ve kterých je služba poskytována. Stejný účet používaný ke správě VHA se často používá ke správě dalších služeb. Například majitelé mobilního telefonu Android a reproduktoru Google Home mohou přidružit a s největší pravděpodobností přidruží svůj účet Google k oběma zařízením. Většina zařízení VHA nevyžaduje ani nenabízí mechanismus identifikace ani autentizace, pokud má zařízení poskytující službu VHA pouze jeden uživatelský účet.
114. Pokud je k zařízení přidružen více než jeden uživatelský účet, někteří VHA nabízejí volitelné základní řízení přístupu ve formě čísla PIN bez skutečné autentizace uživatele. Někteří další VHA mají možnost použít jako identifikační mechanismus rozpoznávání hlasového profilu.

---

<sup>38</sup> X. Yuan a kol., „All Your Alexa Are Belong to Us: A Remote Voice Control Attack against Echo“, 2018 IEEE Global Communications Conference (GLOBECOM), Abú Dhabí, Spojené arabské emiráty, 2018, s. 1–6, doi: 10.1109/GLOCOM.2018.8647762.

<sup>39</sup> Viz například: <https://lightcommands.com>

<sup>40</sup> Viz například: <https://surfingattack.github.io>

115. Přestože identifikace nebo autentizace uživatele nemusí být nezbytná pro přístup ke všem službám VHA, pro některé určitě bude. Bez mechanismu identifikace nebo autentizace by mohl kdokoli přistupovat k údajům ostatních uživatelů a libovolně je upravovat nebo mazat. Kdokoli v blízkosti chytrého reproduktoru může například odstranit seznamy skladeb jiných uživatelů ze služby streamování hudby, příkazy z historie příkazů nebo kontakty ze seznamu kontaktů.
116. Většina VHA slepě důvěřuje svým lokálním sítím. Jakékoli napadené zařízení ve stejné síti by mohlo změnit nastavení chytrého reproduktoru nebo umožnit instalaci škodlivého softwaru nebo k němu přidružit falešné aplikace či dovednosti bez vědomí nebo souhlasu uživatele<sup>41</sup>.
117. VHA je, stejně jako jakýkoli jiný software, vystaven riziku softwarové zranitelnosti. Kvůli koncentraci trhu VHA<sup>42</sup> by však jakákoli zranitelnost mohla postihnout miliony uživatelů VHA. Pokud fungují tak, jak jsou aktuálně navrženy, VHA neposílají žádné informace do cloudové služby rozpoznávání řeči, dokud není detekován aktivační výraz. Softwarová zranitelnost však může útočnickovi umožnit obejít nastavení VHA a jeho bezpečnostní opatření. Pak by například bylo možné získat kopii všech údajů odeslaných do cloudu VHA a přeposlat je na server ovládaný útočníkem.
118. Údaje zákonně zpracované nebo odvozené VHA umožňují vybudovat poměrně přesný profil jejich uživatelů, protože VHA zná nebo může odvodit polohu, vztahy a zájmy svých uživatelů. VHA jsou stále častěji přítomni v domácnostech a v chytrých telefonech uživatelů. Tato okolnost zvyšuje riziko hromadného sledování a hromadného profilování. V důsledku toho by bezpečnostní opatření na ochranu údajů během přenosu i v klidu, v zařízeních i v cloudu měla těmto rizikům odpovídat.
119. Rostoucí využívání VHA ve spojení s nedostatečně vyváženými přístupovými právy donucovacích orgánů by mohlo mít odrazující účinek, který by podkopával základní práva, jako je svoboda slova.
120. Donucovací orgány v EU<sup>43</sup> i mimo EU<sup>44</sup> již projevíly zájem o přístup k hlasovým úryvkům zaznamenaným hlasovými asistenty. Přístup k údajům zpracovávaným nebo odvozeným hlasovými asistenty v EU by měl být v souladu se stávajícím rámcem EU pro ochranu údajů a soukromí. V případě, že některé členské státy zvažují vydání konkrétních právních předpisů omezujících základní práva na soukromí a ochranu údajů, měla by taková omezení vždy splňovat požadavek stanovený v článku 23 GDPR<sup>45</sup>.
121. Lidská kontrola hlasových záznamů a souvisejících údajů za účelem zlepšení kvality služeb VHA je mezi poskytovateli VHA běžnou praxí. Vzhledem k citlivé povaze údajů zpracovávaných těmito lidskými kontrolory a skutečnosti, že tento proces je často zadáván subdodavatelským zpracovatelům, je nanejvýš důležité, aby byla zavedena odpovídající bezpečnostní opatření.

---

<sup>41</sup> Viz například: Deepak Kumar a kol., *Skill Squatting Attacks on Amazon Alexa*, USENIX Security Symposium, srpen 2018, <https://www.usenix.org/conference/usenixsecurity18/presentation/kumar>  
Security Research Labs, *Smart Spies: Alexa and Google Home expose users to vishing and eavesdropping*, listopad 2019, <https://srlabs.de/bites/smart-spies>

<sup>42</sup> Trh VHA je v současné době sdílen mezi méně než dvanácti poskytovateli služeb.

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

<sup>44</sup> Viz například: <https://cdt.org/insights/alexa-is-law-enforcement-listening>.

<sup>45</sup> Viz také EDPB, pokyny 10/2020 k omezením podle článku 23 GDPR.

## Doporučení

122. Návrháři VHA a vývojáři aplikací by měli uživatelům poskytovat zabezpečené nejmodernější postupy autentizace.
123. Lidští kontrolóři by měli vždy obdržet jen nezbytně nutné pseudonymizované údaje. Právní dohody upravující kontrolu by měly výslovně zakázat jakékoli zpracování, které by mohlo vést k identifikaci subjektu údajů.
124. Pokud je prostřednictvím služby VHA poskytováno jako služba nouzové volání, měla by být zaručena stabilní doba provozuschopnosti<sup>46</sup>.

### 3.8 Zpracování zvláštních kategorií osobních údajů

125. Jak již bylo zmíněno, VHA mají přístup k důvěrným informacím, které lze chránit podle článku 9 GDPR (viz oddíl 3.7.1), jako jsou biometrické údaje (viz oddíl 3.7.2). Proto musí návrháři a vývojáři VHA pečlivě rozeznat, v jakých případech zpracování zahrnuje zvláštní kategorie údajů.

#### 3.8.1 Obecné úvahy ohledně zpracování zvláštních kategorií osobních údajů

126. VHA mohou zpracovávat zvláštní kategorie údajů za různých okolností:
  - ) Jako součást svých vlastních služeb, například při správě objednáni u lékaře v kalendáři uživatelů.
  - ) Když poskytovatelé VHA zpracovávají obsah příkazů v rámci rozhraní pro služby třetích stran. V závislosti na typu služby požadované uživatelem by poskytovatelé VHA mohli zpracovávat speciální kategorie údajů. Příkladem může být situace, kdy uživatelka zadá hlasovému asistentovi příkazy k použití aplikace třetí strany používané ke sledování její ovulace<sup>47</sup>.
  - ) Když jsou hlasové údaje použity za účelem jednoznačné identifikace uživatele, jak je uvedeno níže.

#### 3.8.2 Konkrétní úvahy ohledně zpracování biometrických údajů

127. Některé VHA mají schopnost jednoznačně identifikovat své uživatele pouze na základě jejich hlasu. Tento proces je známý jako rozpoznávání hlasového vzoru. Během fáze registrace rozpoznávání hlasu VHA zpracuje hlas uživatele a vytvoří hlasový vzor (nebo hlasový profil). Během běžného používání může VHA vypočítat hlasový vzor jakéhokoli uživatele a porovnat jej se zaregistrovanými vzory, aby jednoznačně identifikoval uživatele, který příkaz vyslovil.

##### Příklad č. 11:

Skupina uživatelů nastaví VHA k používání rozpoznávání hlasového vzoru. Poté každý z nich zaregistruje svůj hlasový vzor.

Později jeden z uživatelů požaduje od VHA přístup ke schůzkám ve svém kalendáři. Protože přístup ke kalendáři vyžaduje identifikaci uživatele, VHA extrahuje a vypočítá hlasový vzor

<sup>46</sup> Doba, kdy může být zařízení nebo služba ponechána bez dozoru, aniž by došlo k selhání systému nebo k nutnosti restartovat zařízení či služby pro účely správy nebo údržby.

<sup>47</sup> Viz například produkt dostupný zde: <https://www.amazon.com/Ethan-Fan-Ovulation-Period-Tracker/dp/B07CRLSHKY>

z hlasu, jímž byl požadavek vznesen, a zkontroluje, zda odpovídá zaregistrovanému uživateli a zda má tento konkrétní uživatel ke kalendáři přístup.

128. Ve výše uvedeném příkladu je rozpoznání hlasu uživatele na základě hlasového vzoru zpracováním zvláštních kategorií osobních údajů ve smyslu článku 9 GDPR (zpracování biometrických údajů za účelem jednoznačné identifikace fyzické osoby)<sup>48</sup>. Zpracování biometrických údajů za účelem identifikace uživatele, jak je požadováno v příkladu, bude vyžadovat výslovný souhlas dotčeného subjektu údajů (čl. 9 odst. 2 písm. a) GDPR). Proto musí správci údajů při získávání souhlasu uživatelů dodržovat podmínky článku 7, a jak je vysvětleno v 32. bodě odůvodnění GDPR, a měli by vedle biometrie nabídnout alternativní způsob identifikace s ohledem na svobodnou povahu souhlasu.
129. Při používání hlasových údajů pro biometrickou identifikaci nebo autentizaci jsou správci údajů povinni zajistit transparentnost informací o tom, kde se používá biometrická identifikace, a o tom, jak se hlasové profily (biometrické vzory) ukládají a posílají mezi zařízeními. Aby byl splněn tento požadavek transparentnosti, doporučuje Evropský sbor pro ochranu osobních údajů poskytnout odpovědi na následující otázky:
- J Znamená aktivace hlasové identifikace na jednom zařízení automaticky aktivaci této funkce na všech ostatních zařízeních, které používají stejný účet?
  - J Šíří se aktivace hlasové identifikace prostřednictvím infrastruktury správce údajů VHA do zařízení vlastněných jinými uživateli?
  - J Kde jsou generovány, ukládány a porovnávány biometrické vzory?
  - J Jsou biometrické vzory přístupné poskytovatelům VHA, vývojářům nebo dalším stranám?
130. Když registrovaný uživatel nakonfiguruje VHA tak, aby identifikoval hlas uživatelů, bude pro účely jednoznačné identifikace zpracováván i hlas neregistrovaných a náhodných uživatelů.
131. Detekce hlasu správného uživatele totiž zahrnuje také jeho srovnání s hlasem ostatních lidí v blízkosti hlasového asistenta. Jinými slovy, funkce rozpoznávání mluvího zabudovaná do hlasových asistentů může vyžadovat záznam hlasové biometrie lidí, kteří v domácnosti hovoří, aby bylo možné odlišit hlasové charakteristiky uživatele od charakteristik osoby, která si přeje být rozpoznána. Biometrická identifikace proto může mít za následek podrobení neinformovaných osob biometrickému zpracování zaregistrováním jejich hlasového vzoru a jeho porovnáním s hlasovým vzorem uživatele, který si přeje být rozpoznán.
132. Aby se zabránilo takovému shromažďování biometrických údajů bez vědomí subjektů údajů a současně se umožnilo, aby byl uživatel asistentem rozpoznán, měla by být upřednostněna řešení založená pouze na údajích uživatele. Konkrétně to znamená, že biometrické rozpoznávání je aktivováno pouze při každém použití z iniciativy uživatele, a nikoli trvale probíhající analýzou hlasů, které asistent slyší. Například by mohlo být poskytnuto konkrétní klíčové slovo nebo otázka přítomným osobám za účelem získání jejich souhlasu se spuštěním biometrického zpracování. Uživatel může například říci „identifikace“ nebo se asistent může zeptat „chcete být identifikováni“ a čekat na kladnou odpověď, než aktivuje biometrické zpracování.

Příklad č. 12:

Pokud si uživatel přeje nastavit biometrickou autentizaci pro přístup k určitým chráněným údajům, jako je bankovní účet, hlasový asistent by mohl aktivovat ověřování mluvčího pouze tehdy, když spustí příslušnou aplikaci, a poté tímto způsobem ověřit jeho totožnost.

## Doporučení

133. Hlasové vzory by měly být generovány, ukládány a spárovány výhradně na místním zařízení, nikoli na vzdálených serverech.
134. Vzhledem k citlivosti hlasových profilů by měly být důkladně uplatňovány normy jako ISO/IEC 24745 a metody ochrany biometrických vzorů<sup>49</sup>.
135. Pokud VHA používá hlasovou biometrickou identifikaci, poskytovatelé VHA by měli:
  - ) Zajistit, aby byla identifikace dostatečně přesná, aby bylo možné spolehlivě přiřadit osobní údaje správným subjektům údajů.
  - ) Zajistit, aby byla přesnost u všech skupin uživatelů podobná, tím, že budou kontrolovat, zda nedochází k zásadnímu zkreslení vůči různým demografickým skupinám.

### 3.9 Minimalizace údajů

136. Správci údajů by měli minimalizovat množství údajů, které se shromažďují přímo nebo nepřímo a které se získávají zpracováním a analýzou, např. by neměli provádět žádnou analýzu hlasu uživatele ani jiné slyšitelné informace za účelem odvození informací o jejich duševním stavu, možné nemoci nebo okolnostech jejich života.
137. Ve výchozím nastavení by mělo být shromažďování a/nebo zpracování údajů omezené na minimální množství potřebné k poskytování služby.
138. V závislosti na umístění, kontextu použití a citlivosti mikrofону by VHA mohl při shromažďování hlasů uživatelů shromažďovat hlasové údaje třetích stran jako součást hluku na pozadí. I když hluk na pozadí neobsahuje hlasové údaje, může stále obsahovat situační údaje, které by mohly být zpracovány za účelem odvození informací o subjektu (např. o jeho poloze).

## Doporučení

139. Návrháři VHA by měli zvážit technologie odstraňující hluk pozadí, aby se vyhnuli záznamu a zpracování hlasů na pozadí a situačních informací.

### 3.10 Odpovědnost

140. Při jakémkoli zpracování založeném na souhlasu jsou správci údajů povinni prokázat souhlas subjektů údajů podle čl. 7 odst. 1 GDPR. Hlasové údaje lze použít k vymezení odpovědnosti (např. k prokázání souhlasu). Povinnost uchovávat takové hlasové údaje by pak byla dána požadavky na odpovědnost příslušných konkrétních právních předpisů.

---

<sup>49</sup> Viz například:

Jain, Anil a Nandakumar, Karthik a 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.



141. Při vyhodnocování potřeby posouzení vlivu na ochranu osobních údajů stanovil Evropský sbor pro ochranu osobních údajů kritéria<sup>50</sup>, která mají orgány pro ochranu údajů používat při vytváření seznamů operací zpracování, které vyžadují povinné posouzení vlivu na ochranu osobních údajů, a poskytují příklady zpracování, která toto posouzení budou pravděpodobně vyžadovat. Je velmi pravděpodobné, že služby VHA spadají do kategorií a podmínek označených jako vyžadující posouzení vlivu na ochranu osobních údajů. To zahrnuje zvážení toho, zda zařízení může sledovat, monitorovat nebo kontrolovat subjekty údajů nebo systematicky ve velkém měřítku monitorovat podle čl. 35 odst. 3 písm. c), používání „nové technologie“ nebo zpracování citlivých údajů a údajů týkajících se zranitelných subjektů údajů.
142. Veškeré činnosti shromažďování a zpracování údajů musí být dokumentovány v souladu s článkem 30 GDPR. Sem patří veškerá zpracování zahrnující hlasové údaje.

## Doporučení

143. Pokud mají být k informování uživatelů podle článku 13 použity hlasové zprávy, měli by správci údajů tyto zprávy zveřejnit na svých webových stránkách, aby byly přístupné uživatelům a orgánům pro ochranu údajů.

### 3.11 Záměrná a standardní ochrana osobních údajů

144. Poskytovatelé a vývojáři VHA by měli zvážit nutnost mít registrovaného uživatele pro každou ze svých funkcí. I když je zřejmé, že ke správě kalendáře nebo adresáře je nutné mít registrovaného uživatele, není zcela jasné, zda telefonování nebo vyhledávání na internetu vyžaduje, aby VHA měl registrovaného uživatele.
145. Ve výchozím nastavení by služby, které nevyžadují identifikovaného uživatele, neměly k vysloveným příkazům přiřadit žádného z identifikovaných uživatelů VHA. Výchozí nastavení VHA příznivé pro ochranu soukromí a údajů by zpracovávalo údaje uživatelů pouze pro provádění požadavků uživatelů a neukládalo by hlasové údaje ani seznam provedených příkazů.
146. Zatímco některá zařízení mohou provozovat pouze jednoho VHA, u jiných si lze vybrat z různých VHA. Poskytovatelé VHA by měli vyvinout odvětvové standardy umožňující přenositelnost údajů v souladu s článkem 20 GDPR.
147. Někteří poskytovatelé VHA prohlásili, že jejich VHA nemohou vymazat údaje všech uživatelů, i když to subjekt údajů požaduje. Poskytovatelé VHA by měli zajistit, aby údaje všech uživatelů mohly být na žádost uživatele vymazány v souladu s článkem 17 GDPR.

## 4 MECHANISMY VÝKONU PRÁV SUBJEKTU ÚDAJŮ

148. V souladu s GDPR musí správci údajů poskytující služby VHA umožnit všem uživatelům, registrovaným i neregistrovaným, uplatňovat svá práva subjektu údajů.
149. Poskytovatelé a vývojáři VHA by měli usnadňovat subjektům údajů kontrolu nad jejich údaji během celé doby zpracování, zejména usnadnit jejich právo na přístup, opravu a vymazání,

---

<sup>50</sup> Pracovní skupina zřízená podle článku 29, pokyny pro posouzení vlivu na ochranu osobních údajů, wp248, rev.01, schválené Evropským sborem pro ochranu osobních údajů.

právo omezit zpracování a v závislosti na právním základu zpracování též jejich právo na přenositelnost údajů a jejich právo vznést námitku.

150. Správce údajů by měl poskytovat informace o právech subjektu údajů ve chvíli, kdy subjekty údajů VHA zapnou, a nejpozději v okamžiku zpracování hlasového požadavku prvního uživatele.
151. Vzhledem k tomu, že hlavním prostředkem interakce pro VHA je hlas, návrháři VHA by měli zajistit, aby uživatelé, registrovaní i neregistrovaní, mohli uplatňovat veškerá práva subjektu údajů pomocí snadno pochopitelných hlasových příkazů. Návrháři VHA, jakož i vývojáři aplikací v případě, že jsou součástí řešení, by měli na konci procesu informovat uživatele, že jeho práva byla řádně zohledněna, a to hlasem nebo poskytnutím písemného upozornění na mobilní telefon uživatele, na jeho účet nebo jakýmkoli jiným způsobem zvoleným uživatelem.
152. Přínejmenším by návrháři VHA a vývojáři aplikací měli zejména zavádět konkrétní nástroje poskytující účinný a efektivní způsob uplatňování těchto práv. Měli by proto pro svá zařízení navrhnout způsob uplatňování práv subjektů údajů, a to tím, že subjektu údajů poskytnou samoobslužné nástroje jako systém správy profilu<sup>51</sup>. To by mohlo usnadnit efektivní a včasné nakládání s právy subjektu údajů a umožní to správci údajů zahrnout identifikační mechanismus do samoobslužného nástroje.
153. Co se týče výkonu práv subjektů údajů v případě více uživatelů, pokud uživatel, registrovaný, či nikoli, uplatňuje jedno ze svých práv, měl by tak činit, aniž by tím byla dotčena práva ostatních uživatelů. Všichni uživatelé, registrovaní i neregistrovaní, mohou uplatňovat svá práva, pokud správce údajů stále zpracovává jejich údaje. Správce údajů by měl připravit postup zajišťující výkon práv subjektu údajů.

#### 4.1 Právo na přístup

154. Podle čl. 12 odst. 1 GDPR by komunikace podle článku 15 měla být poskytována písemně nebo jinými prostředky, a to případně včetně elektronických prostředků. Pokud jde o přístup ke zpracovávaným osobním údajům, čl. 15 odst. 3 stanoví, že pokud subjekt údajů podá žádost elektronickými prostředky, měly by být informace poskytnuty v běžně používané elektronické formě, pokud subjekt údajů nepožádá o jiný způsob. To, co lze považovat za běžně používanou elektronickou formu, by mělo vycházet z rozumných očekávání subjektů údajů, a nikoli z toho, jaký formát používá ve svém každodenním provozu správce údajů. Subjekt údajů by neměl mít povinnost kupovat konkrétní software nebo hardware, aby získal přístup k informacím.
155. Správci údajů by proto měli na požádání zaslat kopii osobních údajů, a zejména zvukových údajů (včetně hlasových záznamů a přepisů), v běžném formátu, který si může subjekt údajů přečíst.
156. Při rozhodování o typu formátu, v němž mají být poskytnuty informace podle článku 15, musí mít správce údajů na paměti, že by formát měl umožnit prezentaci informací způsobem, který je srozumitelný a snadno dostupný. Správci údajů by rovněž měli přizpůsobit informace konkrétní situaci subjektu údajů, který žádost podal.

---

<sup>51</sup> Systém správy profilu je chápán jako místo v systému VHA, kde mohou uživatelé kdykoli ukládat své preference, nastavovat úpravy a snadno měnit svá nastavení soukromí.

Příklad č. 13:

Správce údajů poskytující službu VHA přijme od uživatele požadavek na přístup a rovněž požadavek ve věci přenositelnosti údajů. Správce údajů se rozhodne poskytnout informace podle článku 15 a článku 20 v souboru PDF. V takovém případě by způsob, jímž správce údajů zpracoval oba požadavky, neměl být považován za správný. Soubor PDF technicky splňuje povinnosti správce údajů podle článku 15, ale nesplňuje povinnosti správce údajů podle článku 20<sup>52</sup>.

Je třeba poznamenat, že pouhé odkázání uživatelů na historii jejich interakcí s hlasovým asistentem podle všeho neumožňuje správci údajů splnit všechny své povinnosti vyplývající z práva na přístup, protože přístupné údaje obecně představují pouze část informací zpracovávaných v kontextu poskytování služby.

157. Právo na přístup by nemělo být používáno k obcházení zásad minimalizace a uchování údajů.

## 4.2 Právo na opravu

158. Aby se usnadnila oprava údajů, uživatelé, registrovaní i neregistrovaní, by měli mít možnost kdykoli spravovat a aktualizovat své údaje hlasem přímo pomocí zařízení VHA, jak je popsáno výše. Kromě toho by mělo zařízení nebo aplikace obsahovat samoobslužný nástroj, který jim pomůže jejich osobní údaje snadno opravit. Uživatelé by měli být na aktualizaci upozorněni hlasem nebo písemně.
159. Obecněji se právo na opravu vztahuje na všechny názory a vyvozené závěry<sup>53</sup> správce údajů, včetně profilování, a mělo by se brát v potaz, že velká většina údajů je vysoce subjektivní<sup>54</sup>.

## 4.3 Právo na výmaz

160. Uživatelé, registrovaní i neregistrovaní, by měli mít možnost kdykoli pomocí zařízení VHA nebo samoobslužného nástroje zabudovaného do jakéhokoli zařízení přidruženého k VHA hlasovým příkazem vymazat údaje, která se jich týkají. V tomto ohledu může subjekt údajů osobní údaje vymazat stejně snadno, jako je zadal. Vzhledem k inherentním potížím s anonymizací hlasových údajů a široké škále shromážděných, pozorovaných a odvozovaných osobních údajů o subjektu údajů<sup>55</sup> by bylo v této souvislosti jen stěží možné uplatnit právo na výmaz anonymizací souborů osobních údajů. Jelikož je GDPR technologicky neutrální a technologie se rychle vyvíjí, nezle nicméně vyloučit, že právo na výmaz anonymizací může být v budoucnu účinné.
161. V některých případech je bez obrazovky třetí strany nebo možnosti zobrazení uložených údajů (např. v mobilní aplikaci nebo tabulkovém zařízení) obtížné mít k dispozici náhled zvukových záznamů a posoudit relevanci návrhů. K hlasovému asistentovi by měl být dodáván řídicí panel

<sup>52</sup> Pokyny pracovní skupiny zřízené podle článku 29 týkající se práva na přenositelnost údajů – schválené Evropským sborem pro ochranu osobních údajů, s. 18.

<sup>53</sup> Skutečnost, že názory a vyvozené závěry lze považovat za osobní údaje, potvrdil Soudní dvůr Evropské unie, který uvedl, že výraz „veškeré informace“ v definici osobních údajů zahrnuje informace, které jsou „jak objektivní, tak subjektivní ve formě názorů nebo hodnocení pod podmínkou, že jsou ‚o‘ dotčené osobě“ – věc C-434/16 *Peter Nowak proti Data Protection Commissioner* ECLI:EU:C:2017:994 [34].

<sup>54</sup> Getting Data Subject Rights Right (Správné pochopení práv subjektu údajů), příspěvek Evropskému sboru pro ochranu osobních údajů od akademiků ochrany údajů, listopad 2019.

<sup>55</sup> Stanovisko 5/2014 pracovní skupiny zřízené podle článku 29 k technikám anonymizace, přijaté 10. dubna 2014.

(nebo aplikace), který by byl uživatelům široce přístupný s cílem usnadnit jeho používání a jež by sloužil k vymazání historie provedených požadavků a k přizpůsobení nástroje podle potřeb uživatele<sup>56</sup>.

162. Pro jakékoli zpracování údajů, a zejména pokud registrované subjekty údajů souhlasí s tím, aby hlasové záznamy byly přepisovány a používány poskytovatelem pro zlepšení jeho služeb, by poskytovatelé VHA měli být na žádost uživatele schopni vymazat původní hlasový záznam, jakož i jakýkoli související přepis osobních údajů.
163. Správce údajů by měl zajistit, aby po uplatnění práva na výmaz již nemohlo dojít k dalšímu zpracování údajů. Pokud jde o předchozí opatření, právo na výmaz se může zejména týkat některých právních a technických omezení.

Příklad č. 14:

Pokud uživatel před žádostí o vymazání provedl on-line nákup prostřednictvím svého VHA, může poskytovatel VHA vymazat hlasový záznam související s on-line nákupem, a zajistit tak, že již nebude v budoucnu dále používán. Nákup však bude stále platný, stejně jako hlasová objednávka nebo písemný přepis zpracovaný webovou stránkou elektronického obchodu (zde je výjimka založena na zákonné povinnosti webových stránek elektronického obchodu).

Obdobně pokud uživatel před žádostí o vymazání přidal konkrétní skladbu do svého seznamu skladeb prostřednictvím svého VHA, mohou poskytovatelé VHA vymazat ústní žádost, nikoli však důsledky této žádosti (vymazání nebude mít vliv na seznam skladeb uživatele).

164. Na základě výše uvedených skutečností by v případě, že jsou stejné osobní údaje zpracovávány pro různé účely zpracování, měli správci údajů interpretovat žádosti o výmaz jako jasný signál k zastavení zpracování údajů pro všechny účely, které ze zákona nemají výjimku.

V souladu s podmínkami stanovenými v čl. 21 odst. 1 GDPR by údaje zpracovávané na základě oprávněných zájmů poskytovatelů VHA neměly být předmětem výjimky z práva na výmaz, zejména proto, že subjekty údajů nemají důvod očekávat další zpracování svých osobních údajů.

#### 4.4 Právo na přenositelnost údajů

165. Zpracování údajů prováděné poskytovateli VHA spadá do rozsahu přenositelnosti údajů, protože operace zpracování jsou založeny především na souhlasu subjektu údajů (podle čl. 6 odst. 1 písm. a) nebo podle čl. 9 odst. 2 písm. a), pokud jde o zvláštní kategorie osobních údajů) nebo na základě smlouvy, jíž je subjekt údajů smluvní stranou podle čl. 6 odst. 1 písm. b).
166. V praxi by právo na přenositelnost údajů mělo usnadnit přepínání mezi různými poskytovateli VHA. Zejména u VHA fungujících v digitálním prostředí a u zaznamenávání hlasu subjektu údajů v aplikaci nebo na platformě by mělo být poskytnuto právo na přenositelnost údajů pro všechny osobní údaje poskytnuté subjektem údajů. Kromě toho by měl správce údajů uživatelům nabídnout možnost, v podobě samoobslužného nástroje, přímo vyhledávat své osobní údaje ze své uživatelské oblasti. Uživatelé by také měli mít možnost toto právo uplatnit prostřednictvím hlasových příkazů.

<sup>56</sup> „Asistants vocaux et enceintes connectées, l’impact de la voix sur l’offre et les usages culturels et médias“, francouzský orgán „Conseil Supérieur de l’Audiovisuel“, květen 2019.

167. Poskytovatelé a vývojáři VHA by měli dát subjektům údajů rozsáhlou kontrolu nad osobními údaji, které se jich týkají, aby jim umožnili přenos osobních údajů mezi různými poskytovateli VHA. Subjekty údajů by proto měly získat své osobní údaje poskytnuté správci údajů, a to ve strukturovaném, běžně používaném a strojově čitelném formátu, a také způsoby<sup>57</sup>, které přispívají k naplnění požadavků na přenositelnost údajů (jako jsou nástroje pro stahování a rozhraní pro programování aplikací)<sup>58</sup>. Jak je uvedeno v pokynech týkajících se práva na přenositelnost údajů, v případě velkého nebo složitého shromažďování osobních údajů, což by mohl být tento případ, by měl správce údajů poskytnout přehled „*stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků*“ (viz čl. 12 odst. 1 GDPR) takovým způsobem, aby subjekty údajů měly vždy jasné informace o tom, jaké údaje se mají v souvislosti s daným účelem stáhnout nebo odeslat jinému správci údajů. Subjekty údajů by například měly mít možnost používat softwarové aplikace ke snadné identifikaci, rozpoznávání a zpracování příslušných konkrétních údajů.
168. Toto právo by mělo uživateli umožnit získávat pro své osobní použití zejména údaje, které sdělil prostřednictvím svého hlasu (např. historie hlasových interakcí) a v rámci vytvoření svého uživatelského účtu (např. jméno).
169. Aby bylo možné plně uplatňovat právo těchto subjektů údajů v kontextu jednotného digitálního trhu, měli by zejména návrháři VHA a vývojáři aplikací vyvinout společné strojově čitelné formáty, které usnadní interoperabilitu datového formátu mezi systémy VHA<sup>59</sup>, včetně standardních formátů pro hlasové údaje. Technologie by měly být strukturovány tak, aby bylo zajištěno, že zpracované osobní údaje, včetně hlasových, budou snadno a plně znovu použitelné novým správcem<sup>60</sup>.

---

<sup>57</sup> Jako příklad viz odůvodnění pracovní skupiny zřízené podle článku 29 v pokynech týkajících se práva na přenositelnost údajů – schválených Evropským sborem pro ochranu osobních údajů, s. 16:

*„Na technické úrovni by správci údajů měli prozkoumat a posoudit dva odlišné a vzájemně se doplňující způsoby, jak přenositelné údaje zpřístupnit subjektům údajů nebo jiným správcům údajů:*

- *přímé předání celkového souboru přenositelných údajů (nebo několika částí globálního souboru údajů):*
- *automatizovaný nástroj umožňující získávání relevantních údajů.*

*Druhý způsob mohou správci údajů upřednostňovat v případech zahrnujících složité a velké soubory údajů, jelikož umožňuje získání jakékoliv části souboru údajů, která je pro subjekt údajů v souvislosti s jeho žádostí relevantní, může pomoci minimalizovat rizika a případně umožňuje používání mechanismů pro synchronizaci údajů (např. v souvislosti s pravidelnou komunikací mezi správci údajů). Pro „nového“ správce údajů se může jednat o lepší způsob, jak zajistit dodržování souladu, a může to představovat osvědčený postup při snižování rizik v oblasti ochrany soukromí na straně původního správce údajů“.*

<sup>58</sup> V této souvislosti: Pokyny pracovní skupiny zřízené podle článku 29 týkající se práva na přenositelnost údajů – schválené Evropským sborem pro ochranu osobních údajů, s. 1.

<sup>59</sup> V této souvislosti: 68. bod odůvodnění GDPR; pokyny pracovní skupiny zřízené podle článku 29 týkající se práva na přenositelnost údajů – schválené Evropským sborem pro ochranu osobních údajů, s. 17.

<sup>60</sup> „Ustanovení 68. bodu odůvodnění v této souvislosti podporuje správce údajů v rozvíjení interoperabilních formátů umožňujících přenositelnost údajů, aniž by zakládal povinnost správců údajů zavést nebo zachovávat technicky kompatibilní systémy. Obecné nařízení o ochraně osobních údajů však správcům údajů zakazuje vytvářet překážky předávání.“ – Pokyny pracovní skupiny zřízené podle článku 29 týkající se práva na přenositelnost údajů – potvrzené Evropským sborem pro ochranu osobních údajů, s. 5.

170. Pokud jde o formát, poskytovatelé VHA by měli poskytovat osobní údaje v běžně používaných otevřených formátech (např. mp3, wav, csv, gsm atd.) spolu s vhodnými metadaty používanými za účelem přesného popisu významu vyměňovaných informací<sup>61</sup>.

## 5 PŘÍLOHA: AUTOMATICKÉ ROZPOZNÁVÁNÍ ŘEČI, SYNTÉZA ŘEČI A ZPRACOVÁNÍ PŘIROZENÉHO JAZYKA

171. V návaznosti na teoretické základy zpracování signálu, zejména teorie informací a vzorkování Clauda Shannona, se automatické zpracování řeči stalo základní součástí technických věd. Na pomezí fyziky (akustika, šíření vln), aplikované matematiky (modelování, statistika), počítačové vědy (algoritmy, techniky učení) a humanitních věd (vnímání, uvažování) se zpracování řeči rychle rozdělilo do mnoha předmětů studia: identifikace a ověřování mluvčího, automatické rozpoznávání řeči, syntéza hlasu, detekce emocí atd. Za posledních zhruba patnáct let dosáhla disciplína jako celek velmi významného pokroku za přispění různých faktorů: vylepšených metod, výrazného nárůstu výpočetní kapacity a většího objemu dostupných údajů.

### 5.1 Automatické rozpoznávání řeči

172. Automatické rozpoznávání řeči (také známé jako převod řeči na text) dříve zahrnovalo tři různé fáze zaměřené na: 1) určení, které fonémy byly vysloveny, pomocí akustického modelu; 2) určení, která slova byla vyslovena, pomocí fonetického slovníku; 3) přepis posloupnosti slov (vět), která byla nejpravděpodobněji vyslovena, pomocí jazykového modelu. Dnes, s pokrokem umožněným hlubokým učení (technikou strojového učení), mnoho systémů nabízí kompletní automatické rozpoznávání řeči „od začátku až do konce“. Tím se lze vyhnout nutnosti složitě trénovat tři různé modely a zároveň to nabízí lepší výkon, pokud jde o výsledky a dobu zpracování. Téměř všechny hlavní digitální přehrávače nyní nabízejí vlastní implementace automatického rozpoznávání řeči, jež mohou rozhraní pro programování aplikací snadno používat, ale existují i systémy s otevřeným zdrojovým kódem (například DeepSpeech<sup>62</sup> nebo Kaldi<sup>63</sup>).

### 5.2 Zpracování přirozeného jazyka

173. Zpracování přirozeného jazyka je multidisciplinární obor zahrnující lingvistiku, počítačovou vědu a umělou inteligenci, jehož cílem je vytvořit nástroje pro zpracování přirozeného jazyka pro nejrůznější použití. Oblasti výzkumu a použití jsou četné: syntaktická analýza, strojový překlad, automatické generování a sumarizace textu, kontrola pravopisu, systémy pro zodpovídání otázek, dolování z textu, rozpoznávání pojmenovaných entit, analýza sentimentu atd. Konkrétně vzato, cílem zpracování přirozeného jazyka je vybavit počítače schopností číst, chápat a odvozovat význam z lidských jazyků. Vývoj aplikací zpracování přirozeného jazyka je náročný, protože počítačové nástroje tradičně vyžadují, aby s nimi lidé komunikovali v programovacím jazyce, který je formální, což znamená přesný, jednoznačný a vysoce strukturovaný. Lidská řeč však není vždy přesná. Často je nejednoznačná a její jazyková

---

<sup>61</sup> Evropský sbor pro ochranu osobních údajů důrazně vybízí ke spolupráci mezi zúčastněnými stranami z odvětví a obchodními sdruženími, aby spolupracovaly na společném souboru interoperabilních standardů a formátů tak, aby splňovaly požadavky práva na přenositelnost údajů.

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

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

struktura může záviset na mnoha složitých proměnných, včetně slangu, regionálních nářečí a sociálního kontextu.

174. Syntaktická a sémantická analýza jsou dvě hlavní techniky používané v oblasti zpracování přirozeného jazyka. Syntax je uspořádání slov ve větě tak, aby věta dávala gramatický smysl. Zpracování přirozeného jazyka využívá syntax k posouzení významu jazyka založeného na gramatických pravidlech. Mezi používané syntaktické techniky patří syntaktická analýza věty (tzv. parsing), segmentace slov (čímž se delší text rozděluje na jednotky), segmentace textu na věty (která ve větších textech určuje hranice vět), morfologická segmentace (která rozděluje slova do skupin) a stematizace (která rozděluje skloňovaná či časovaná slova na kořenové tvary). Sémantika se týká používání slov a jejich významu. Zpracování přirozeného jazyka používá algoritmy k pochopení významu a struktury vět. Mezi sémantické techniky, které zpracování přirozeného jazyka používá, patří disambiguace významu slova (kterou se odvozuje význam slova na základě kontextu), rozpoznávání pojmenovaných entit (což určuje slova, která lze kategorizovat do skupin) a generování přirozeného jazyka (což určuje význam slov pomocí databáze). Zatímco dřívější přístupy ke zpracování přirozeného jazyka zahrnovaly přístupy založené na pravidlech, kde bylo jednoduchým algoritmům strojového učení sděleno, jaká slova a fráze je třeba v textu hledat, což vedlo ke konkrétním výsledkům, když se tyto fráze v textu objevily, současné přístupy ke zpracování přirozeného jazyka jsou založeny na hlubokém učení, což je typ umělé inteligence, která zkoumá a používá vzorce v datech, a tím zlepšuje porozumění programu.

### 5.3 Syntéza řeči

175. Syntéza řeči je umělé vytváření lidské řeči. Syntéza řeči se provádí především zřetěžením hlasových jednotek, které jsou uloženy v databázi. Tato technika spočívá v tom, že se ze všech hlasových nahrávek aktéra přepsaných do fonémů, slabik a slov, vyberou zvukové jednotky, které dohromady odpovídají slovům, která si VHA přeje vyslovit, a sestaví se jedna po druhé tak, aby vznikla srozumitelná věta s přirozenou dikcí. Alternativně může syntetizátor řeči zahrnovat model hlasového ústrojí a další charakteristiky lidského hlasu za účelem modelování parametrů hlasu, jako je intonace, rytmus a zabarvení, pomocí generativních statistických modelů (například WaveNet<sup>64</sup>, Tacotron<sup>65</sup> nebo DeepVoice<sup>66</sup>) a za účelem vytvoření zcela umělého hlasového výstupu.

---

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

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

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