Riktlinjer 02/2021 för användning av virtuella röstassistenter

Version 2.0

Antagna den 7 juli 2021

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Versionshistorik

Version 2.0	7 juli 2021	Antagande av riktlinjerna efter offentligt samråd
Version 1.0	9 mars 2021	Antagande av riktlinjerna inför offentligt samråd

SAMMANFATTNING

En virtuell röstassistent (VVA, Virtual Voice Assistant) är en tjänst som förstår röstkommandon och utför dem eller vid behov förmedlar kontakt med andra it-system. Virtuella röstassistenter finns i dag i de flesta smarttelefoner, pekdatorer och vanliga datorer. På senare år ingår de även i många fristående enheter, såsom smarta högtalare.

De fungerar som gränssnitt mellan användarna och deras datorenheter och onlinetjänster såsom sökmotorer eller nätbutiker. Deras syfte gör att de virtuella röstassistenterna får tillgång till mängder av personuppgifter, däribland användarkommandon (t.ex. webb- eller sökhistorik) och svar (t.ex. inplanerade besök i kalendern).

Det stora flertalet virtuella röstassistenttjänster har utformats av ett fåtal konstruktörer. Virtuella röstassistenter kan dock samarbeta med applikationer som programmerats av tredje part (virtuella röstassistenters applikationsutvecklare) för att möjliggöra mer sofistikerade kommandon.

För att fungera behöver en virtuell röstassistent en terminalenhet som utrustats med mikrofoner och högtalare. Enheten lagrar röstdata och annan data som de virtuella röstassistenterna överför till fjärrservrar för virtuella röstassistenter.

Personuppgiftsansvariga som levererar virtuella röstassistenttjänster och deras personuppgiftsbiträden måste därför både beakta den allmänna dataskyddsförordningen[1] och direktivet om integritet och elektronisk kommunikation[2].

I dessa riktlinjer identifieras vissa av de mest relevanta problemen med efterlevnaden och rekommendationer ges till relevanta intressenter om hur de kan få bukt med dessa problem.

Personuppgiftsansvariga som tillhandahåller virtuella röstassistenttjänster genom skärmlösa terminalenheter måste enligt den allmänna dataskyddsförordningen ändå informera användarna när de inrättar den virtuella röstassistenten eller för första gången installerar eller använder en applikation till en virtuell röstassistent. Vi rekommenderar därför leverantörer/konstruktörer och utvecklare av virtuella röstassistenter att ta fram röstbaserade gränssnitt för att underlätta tillhandahållandet av den obligatoriska informationen.

För närvarande kräver alla virtuella röstassistenter att minst en användare registrerar sig för tjänsten. I enlighet med skyldigheten att ha ett inbyggt dataskydd och dataskydd som standard bör leverantörer/konstruktörer och utvecklare av virtuella röstassistenter överväga om det är nödvändigt att ha en registrerad användare för varje funktion.

I den typ av användarkonto som många av konstruktörerna av virtuella röstassistenter använder kombineras den virtuella röstassistenttjänsten med andra tjänster, såsom e-post eller direktuppspelad video. Europeiska dataskyddsstyrelsen anser att personuppgiftsansvariga bör undvika sådana metoder eftersom de medför långa och komplicerade integritetspolicyer som innebär att öppenhetsprincipen i den allmänna dataskyddsförordningen inte kan uppfyllas.

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (nedan kallat *den allmänna dataskyddsförordningen*).

[2] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) ändrat genom direktiv 2006/24/EG och direktiv 2009/136/EG (nedan kallat *direktivet om integritet och elektronisk kommunikation*).

I riktlinjerna beaktas fyra av de vanligaste ändamålen för vilka virtuella röstassistenter behandlar personuppgifter, nämligen utförande av begäranden, förbättring av den virtuella röstassistentens maskininlärningsmodell, biometrisk identifiering och profilering för individualiserat innehåll eller annonser.

I den mån de virtuella röstassistentuppgifterna behandlas för att utföra användarens begäran, dvs. begränsas till vad som är absolut nödvändigt för att leverera den tjänst som användaren begärt, undantas personuppgiftsansvariga från kravet på föregående samtycke enligt artikel 5.3 i direktivet om integritet och elektronisk kommunikation. Omvänt skulle ett sådant samtycke som krävs enligt artikel 5.3 i direktivet om integritet och elektronisk kommunikation behövas för att lagra eller tillgå information för alla andra ändamål än utförandet av användarens begäran.

Vissa virtuella röstassistenttjänster lagrar personuppgifterna tills användaren begär att de ska raderas. Detta överensstämmer inte med principen om lagringsbegränsning. Virtuella röstassistenter ska inte lagra data längre än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas.

Om en personuppgiftsansvarig får kännedom (t.ex. genom kvalitetsgranskning) om en oavsiktlig insamling av personuppgifter ska denne kontrollera att det finns en giltig rättslig grund för varje ändamål med behandlingen av dessa uppgifter. I annat fall ska de oavsiktligt insamlade uppgifterna raderas.

Virtuella röstassistenter får behandla data från flera registrerade. Leverantörer/konstruktörer av virtuella röstassistenter ska därför införa mekanismer för åtkomstkontroll för att säkerställa personuppgifternas konfidentialitet, integritet och tillgänglighet. Vissa traditionella mekanismer för åtkomstkontroll, såsom lösenord, är dock inte lämpliga för virtuella röstassistenter eftersom det skulle krävas att de anges muntligt. Riktlinjerna ger viss information om detta, till exempel ett avsnitt som särskilt avser behandlingen av särskilda kategorier av uppgifter för biometrisk identifiering.

När den virtuella röstassistentens leverantörer/konstruktörer samlar in användarens röst ska de tänka på att inspelningarna kan innehålla andra personers röster eller data, såsom bakgrundsljud som inte behövs för tjänsten. När så är möjligt ska konstruktörer av virtuella röstassistenter därför söka införa tekniker som filtrerar bort onödiga uppgifter och säkerställer att bara användarens röst spelas in.

Under sin utvärdering av behovet av konsekvensbedömningar avseende dataskydd fann Europeiska dataskyddsstyrelsen det mycket troligt att virtuella röstassistenttjänster omfattas av de kategorier och villkor som innebär att konsekvensbedömningar avseende dataskydd kommer att krävas för dessa tjänster.

Personuppgiftsansvariga som levererar virtuella röstassistenttjänster ska säkerställa att användarna kan utöva sina rättigheter som registrerade med hjälp av lättförståeliga röstkommandon. Både leverantörer/konstruktörer av virtuella röstassistenter och applikationsutvecklare ska vid förfarandets slut informera användarna om att deras rättigheter vederbörligen beaktats, genom ett röstmeddelande eller skriftligt meddelande till användarens mobiltelefon, konto eller via någon annan kommunikationskanal som användaren valt.

Innehållsförteckning

Europeiska dataskyddsstyrelsen har

med beaktande av artikel 70.1 j och 70.1 e i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (nedan kallad *den allmänna dataskyddsförordningen*),

med beaktande av EES-avtalet, särskilt bilaga XI och protokoll 37, ändrat genom gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018[3],

med beaktande av artikel 12 och artikel 22 i arbetsordningen,

ANTAGIT FÖLJANDE RIKTLINJER

1 ALLMÄNT

1. Den senaste tidens tekniska utveckling har medfört att virtuella röstassistenter nu fungerar med mycket större precisionen, vilket i sin tur gjort att de börjat användas i mycket större utsträckning. Virtuella röstassistenter har liksom andra enheter integrerats i smarttelefoner, uppkopplade fordon, smarta högtalare och smarta tv-apparater. Denna integration har gjort att virtuella röstassistenter fått tillgång till privat information som vid fel hantering kan åsidosätta enskilda personers rätt till data- och integritetsskydd. Virtuella röstassistenter och de enheter i vilka de ingår har därför varit föremål för olika dataskyddsmyndigheters granskning.
2. Användning av röstbaserad automatiserad interaktion har flera fördelar, såsom att interaktionen sker naturligt och inte kräver någon specifik inlärning av användarna, att kommandot utförs snabbt och att åtgärdsområdet är stort, vilket kan göra påskynda tillgången till information. Att använda röstkommunikation kan dock göra det svårt att tolka meddelanden rätt, till exempel på grund av variationer i ljudsignalen mellan olika högtalare, den akustiska miljön, det muntliga språkets mångtydighet, osv.
3. I praktiken är smidigheten eller förenklingen av arbetsuppgifterna fortfarande de främsta skälen till att virtuella röstassistenter används. Detta kan innefatta att ringa upp/svara på ett samtal, ställa in en timer, osv., och är särskilt praktiskt när användarna har händerna upptagna med annat. Smarta hus är det användningsområde som främst föreslås av konstruktörerna av virtuella röstassistenter. De förenklar utförandet av olika uppgifter (såsom att tända lampor, justera värmen, dra igen jalusier och fönsterluckor, osv.). De här uppgifterna centraliseras i ett enda verktyg som enkelt kan fjärraktiveras, vilket gör att de här assistenterna kommit att definieras som underlättande teknik för hemmet. Förutom för eget bruk eller bruk i hemmet kan röstkommandon också vara av intresse i yrkesmiljöer där dataverktyg och skriftliga kommandon är svåra att använda (t.ex. arbete i tillverkningsindustrin).

[3] Hänvisningar till ”medlemsstater” som görs i hela detta dokument ska förstås som hänvisningar till ”EES-medlemsstater”.

4. I teorin kan personer med funktionsnedsättningar eller beroendeproblem dra störst fördel av röstgränssnittet, eftersom användning av traditionella gränssnitt ofta är problematisk för dessa personer. Virtuell röstassistans kan förenkla tillgången till information och datorresurser och därigenom understödja inkludering, eftersom röstanvändning gör det möjligt att komma förbi svårigheter i samband med skriftspråk som vissa grupper av användare kan ha.

5. Hälsovård är slutligen också ett område där konversationsagenter kan användas på många olika sätt, oavsett om de är röstbaserade eller inte. Under covid-19-pandemin sattes t.ex. många olika samtalsrobotar (eller ”callbots”) in för att erbjuda förhandsdiagnos till användare som ringde särskilda vårdinformationsnummer. På längre sikt kan hela patientvårdsförfarandet komma att ändras av interaktionen människa/röstassistent, inte bara i fråga om välbefinnande och förebyggande vård, utan också för behandling och stöd.

6. Det finns för tillfället över tre miljarder smarttelefoner och samtliga har integrerade virtuella röstassistenter, de flesta påslagna som standard. Också i en del av de vanligaste operativsystemen i persondatorer och bärbara datorer finns det virtuella röstassistenter. Ökningen av smarta högtalare (147 miljoner såldes under 2019[4]) gör att virtuella röstassistenter nu även förs in i miljontals hem och kontor på det sättet. Dagens virtuella röstassistenter är dock inte konstruerade för att som standard erbjuda mekanismer för autentisering eller åtkomstkontroll.

7. Detta dokument ger vägledning om tillämpningen av den allmänna dataskyddsförordningen inom ramen för virtuella röstassistenter.

2 TEKNISK BAKGRUND

2.1 Grundläggande kännetecken för virtuella röstassistenter

8. En virtuell röstassistent kan definieras som en programvaruapplikation som kan hålla en muntlig dialog med en användare på ett naturligt språk.

9. Ett naturligt språk har en semantik som är specifik för människans språk. Beroende på språkets kännetecken och ordrikedom kan samma instruktion formuleras på olika sätt, medan vissa kommandon kan likna varandra trots att de syftar på två olika objekt. Slutledningsmekanismer används sedan ofta för att lösa denna typ av tvetydigheter. Exempelvis kan det som sagts tidigare beaktas, den tid då instruktionen gavs, platsen, användarens intressen osv.

10. En virtuell röstassistent kan delas in i moduler som möjliggör utförandet av olika arbetsuppgifter: uppfångande och återgivning av ljud, automatisk taltranskription (tal till text), automatisk språkbearbetning, dialogstrategier, tillgång till ontologi (dataset och strukturerade begrepp som är relaterade till ett visst område) samt externa kunskapskällor, språkgenerering, röstsyntes (text till tal), osv. Konkret innebär detta att assistenten möjliggör interaktion för att olika åtgärder ska kunna utföras (t.ex. ”sätt på radion”, ”släck lampan”) eller erhålla kunskap (t.ex. ”hur blir vädret i morgon?”, ”går tåget klockan 7:43?”). Den fungerar därför som intermediär och samordnare för att möjliggöra utförandet av de uppgifter som användaren efterfrågar.

[4] Se till exempel ett pressmeddelande från den 1 augusti 2019 från Hamburgs myndighet för dataskydd och informationsfrihet: https://datenschutz-hamburg.de/pressemitteilungen/2019/08/2019-08-01-google-assistant

11. I praktiken är en virtuell röstassistent inte en smart högtalare, men en smart högtalare kan vara utrustad med en virtuell röstassistent. Det är vanligt att dessa två förväxlas, då den ena är något av en fysisk gestaltning av den andra. En virtuell röstassistent kan installeras i en smartmobil, en smart högtalare, ett uppkopplat armbandsur, ett fordon, en hushållsapparat, osv.

12. Beroende på hur den bakomliggande databehandlingen går till kan detta ge upphov till ett flertal informationsflöden. Tre huvudsakliga delar kan identifieras:

    Hårdvaran: det hårdvaruelement som assistenten är inbyggd i (smartmobil, smarta högtalare, smart-tv, osv.) och som är försedd med mikrofoner, högtalare, nätverksuppkoppling och beräkningskapacitet (mer eller mindre utvecklad allt efter fallet).

    Programvaran: den del som i strikt mening genomför interaktionen mellan människa och maskin och som integrerar modulerna för automatisk taligenkänning, bearbetning av naturligt språk, dialog och röstsyntes. Denna kan användas direkt via den fysiska utrustningen eller som i många fall, via fjärrstyrning.

    Resurserna: externa data såsom innehållsdatabaser, ontologier eller företagsapplikationer som tillhandahåller information eller kunskap (t.ex. ”vad är klockan på USA:s västkust”, ”läs upp mina e-postmeddelanden”) eller som gör det möjligt att konkret utföra den begärda åtgärden (t.ex. ”höj temperaturen med 1,5 °C”).

13. Med virtuella röstassistenter kan tredjepartskomponenter eller tredjepartsappar installeras för att utöka assistentens funktioner. I varje virtuell röstassistent namnges komponenterna på ett eget sätt, men i samtliga sker ett utbyte av användarnas personuppgifter mellan den virtuella röstassistentens konstruktör och applikationsutvecklaren.

14. Även om de flesta virtuella röstassistenter inte delar med sig av röstfragmentet till applikationsutvecklarna behandlar dessa aktörer ändå personuppgifter. Allt efter vilken typ av funktion som tillhandahålls får applikationsutvecklaren tillgång till avsikter och informationsvariabler som kan innehålla känsliga uppgifter, exempelvis hälsoinformation.

2.2 Aktörer i den virtuella röstassistentens ekosystem

15. I utförandekedjan till en virtuell röstassistent kan det finnas ett flertal aktörer och intermediärer. I praktiken kan upp till fem olika aktörer identifieras. Beroende på affärsmodell och tekniska val kan vissa aktörer dock anta olika kombinationer av roller, såsom konstruktör och integrator eller konstruktör och applikationsutvecklare:

    a. **Den virtuella röstassistentens leverantör (eller konstruktör):** ansvarar för den virtuella röstassistentens utveckling, konstruerar och definierar dess möjligheter och standardfunktioner: aktiveringslägen, arkitekturval, tillgång till data, registerhantering, hårdvaruspecifikationer, osv.

    b. **Den virtuella röstassistentens applikationsutvecklare:** skapar, liksom för mobilapplikationer, applikationer som utökar den virtuella röstassistentens standardfunktioner. När detta görs måste de utvecklingsbegränsningar som konstruktören infört respekteras.

    c. **Integratorn:** tillverkare av anslutna produkter som vill utrusta dem med en virtuell röstassistent. Integratorn måste respektera de villkor som konstruktören fastställt.

d. **Ägaren:** bestämmer över fysiska utrymmen där människor vistas (inkvarteringsplatser, yrkesmiljöer, hyrbilar, osv.) och där han eller hon vill förse sina kunder med en virtuell röstassistent (eventuellt med särskilda applikationer).

e. **Användaren:** den sista länken i den virtuella röstassistentens värdekedja, som kan använda den virtuella röstassistenten i olika enheter (högtalare, tv, smartmobil, armbandsur, osv.) beroende på hur och var den har installerats och konfigurerats.

2.3 Beskrivning steg för steg

16. För att en virtuell röstassistent ska utföra en åtgärd eller tillgå information måste en rad uppgifter utföras:

1) Den virtuella röstassistenten befinner sig i viloläge när den är installerad i en utrustningsdel (smartmobil, högtalare, fordon). Den ”lyssnar” dock ständigt. Men det är först när ett specifikt ”väckningsuttryck” upptäcks som ljud överförs från enheten som mottar rösten, och ingen annan funktion än lyssning efter väckningsuttryck utförs i detta läge. För detta används en buffert på några sekunder (se nästa avsnitt för en närmare beskrivning).

2) Användaren uttalar väckningsuttrycket och den virtuella röstassistenten jämför ljudet lokalt med det programmerade väckningsuttrycket. Om de matchar öppnar den virtuella röstassistenten en lyssningskanal och överför omedelbart ljudinnehållet.

3) I många fall, om behandlingen av kommandot görs på distans, utförs en andra kontroll av det uttalade nyckelordet på serverhåll för att begränsa oönskade aktiveringar.

4) Användaren uttrycker sin begäran, som överförs direkt till den virtuella röstassistentens leverantör. Den intalade ljudföljden transkriberas sedan automatiskt (tal till text).

5) Kommandot tolkas med en teknik för bearbetning av naturligt språk. Meddelandets avsikter utvinns och informationsvariabler identifieras. Sedan används en dialoghanterare för att ange det interaktionsscenario som ska genomföras med användaren genom att tillhandahålla det lämpliga svarsschemat.

6) Om kommandot innehåller en funktion som tillhandahålls av en tredjepartsapp (färdighet, åtgärd, genväg, osv.), skickar den virtuella röstassistentens leverantör meddelandets avsikter och informationsvariabler till applikationsutvecklaren.

7) Ett svar som anpassats efter användarens begäran identifieras – åtminstone i teorin, då svaret ”jag har inget svar på din fråga” är ett anpassat svar när den virtuella röstassistenten inte förmår tolka begäran. Vid behov används distansresurser: offentligt tillgängliga kunskapsdatabaser (encyklopedier på nätet, osv.) eller resurser som kräver autentisering (bankkonton, musikapplikationer, kundkonton för inköp på nätet, osv.) och informationsvariablerna fylls i med den inhämtade informationen.

8) En svarsfras skapas och/eller en åtgärd identifieras (dra ner rullgardiner, höja temperaturen, spela musik, svara på en fråga, osv.). Meningen syntetiseras (text till tal) och/eller åtgärden som ska utföras skickas till utrustningen som ska utföra den.

9) Den virtuella röstassistenten återgår därefter till viloläge.

Lägg märke till att de flesta röstbearbetningar utförs i fjärrservrar men att vissa leverantörer av virtuella röstassistenter utvecklar system som kan utföra en del av denna bearbetning lokalt[5].

2.4 Väckningsuttryck

17. För att kunna användas måste den virtuella röstassistenten först ”väckas”. Detta innebär att assistenten växlar till ett aktivt lyssningsläge för att ta emot order och kommandon från användaren. Denna väckning kan ibland också utföras fysiskt (t.ex. genom att trycka på en knapp, trycka på smarthögtalaren, osv.), och nästan alla virtuella röstassistenter på marknaden bygger på upptäckten av ett väckningsuttryck eller -ord för att växla till aktivt lyssningsläge (kallas även aktiveringsord eller väckningsord/”hot word”).

18. För att göra detta använder assistenten mikrofonen och en mindre beräkningskapacitet för att upptäcka om detta nyckelord har uttalats. Denna analys, som sker kontinuerligt från den stund den virtuella röstassistenten är på, utförs enbart lokalt. Först när nyckelordet har känts igen kommer ljudinspelningarna att bearbetas för att tolka och utföra kommandot, vilket i många fall innebär att de skickas till fjärrservrar via internet. För att enheten ska identifiera nyckelordet används maskininlärningstekniker. Det största problemet med dessa metoder är att upptäckten är sannolikhetsbaserad. För varje ord eller uttryck som uttalas tillhandahåller systemet en trovärdighetspoäng för huruvida nyckelordet har uttalats. Om denna poäng är högre än ett fördefinierat tröskelvärde anses det att nyckelordet angetts. Ett sådant system är med andra ord inte felfritt: i vissa fall upptäcks kanske ingen aktivering trots att nyckelordet har sagts (felaktigt avvisande) och i andra fall upptäcks kanske aktivering trots att användaren inte har angett nyckelordet (felaktig acceptans).

19. I praktiken ska det fastställas en godtagbar kompromiss mellan dessa två typer av fel för att definiera ett passande tröskelvärde. Men eftersom en felaktig upptäckt av nyckelordet skulle kunna medföra att ljudinspelningar skickas, är det troligt att oväntade och oönskade dataöverföringar sker. Leverantörer av virtuella röstassistenter som genomför fjärrbehandling använder mycket ofta en tvåstegsmekanism för denna detektering: ett första steg som är lokalt inbyggt på utrustningsnivå och ett andra steg som utförs av fjärrservrar där nästa databehandling utförs. I detta fall tenderar utvecklarna att fastställa ett relativt lågt tröskelvärde för att förbättra användarupplevelsen och säkerställa att nyckelordet nästan alltid känns igen när användaren säger det, även om det innebär att det ”överdetekteras”. Därefter genomförs ett andra detekteringssteg på serverhåll, som är mer restriktivt.

2.5 Röstfragment och maskininlärning

20. Virtuella röstassistenter använder maskininlärningsmetoder för att utföra en lång rad arbetsuppgifter (upptäckt av nyckelord, automatisk taligenkänning, bearbetning av naturligt språk, talsyntes, osv.), vilket gör att stora dataset behöver samlas in, väljas, klassificeras, osv.

21. För många eller för få statistiska variabler av en viss typ kan påverka utvecklingen av maskininlärningsbaserade uppgifter så att de återges i dess beräkningar på ett senare stadium och därmed påverkar hur de utförs. På samma sätt som kvantiteten är viktig spelar även uppgifternas kvalitet en stor roll när det gäller inlärningsprocessens korrekthet och precision.

[5] Detta har t.ex. rapporterats här: https://www.amazon.science/blog/alexas-new-speech-recognition-abilities-showcased-at-interspeech

22. För att öka den virtuella röstassistentens kvalitet och förbättra de använda maskininlärningsmetoderna kan den virtuella röstassistentens konstruktörer vilja få tillgång till data över enhetens användning under verkliga förhållanden – dvs. röstfragment – för att förbättra den.

23. Oavsett om avsikten är att godkänna inlärningsdatabasen eller att rätta fel som uppstod när algoritmen lades in behövs det människor för att lära och träna upp de artificiella intelligenssystemen. Denna del av arbetet, ett s.k. digitalt arbete (”digital labor”), väcker frågor om såväl arbetsvillkor som säkerhet. I detta sammanhang har nyhetsmedier också rapporterat om överföring av data mellan konstruktörer och underleverantörer av virtuella röstassistenter, där de nödvändiga garantierna för integritetsskydd ska ha saknats.

3 DATASKYDDSASPEKTER

3.1 Rättslig ram

24. EU:s relevanta rättsliga ram för virtuella röstassistenter är i första hand den allmänna dataskyddsförordningen, eftersom behandling av personuppgifter är en central funktion hos virtuella röstassistenter. Utöver den allmänna dataskyddsförordningen fastställs det i direktivet om integritet och elektronisk kommunikation[6] en specifik standard för alla aktörer som önskar lagra eller få tillgång till information som lagras i den terminalutrustning som tillhör en abonnent eller användare i EES.

25. Exempel på ”*terminalutrustning*”[7] är enligt dess definition smartmobiler, smart-tv-apparater och liknande enheter med teknik för sakernas internet. Virtuella röstassistenter är programvarutjänster, men de drivs alltid av en fysisk enhet, t.ex. en smart högtalare eller smart-tv. **Virtuella röstassistenter använder elektroniska kommunikationsnät för att få tillgång till dessa fysiska enheter, vilka betecknas som ”terminalutrustning” enligt direktivet om integritet och elektronisk kommunikation. Följaktligen är alltid bestämmelserna i artikel 5.3 i direktivet om integritet och elektronisk kommunikation tillämpliga när en virtuell röstassistent lagrar eller får tillgång till information i den fysiska enhet som är kopplad till den**.[8]

26. All behandling av personuppgifter i enlighet med de tidigare nämnda behandlingsprocesserna, inräknat behandling av personuppgifter som erhållits genom att tillgå information från

[6] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktivet om integritet och elektronisk kommunikation) ändrat genom direktiv 2006/24/EG och direktiv 2009/136/EG (nedan kallat *direktivet om integritet och elektronisk kommunikation*).

[7] I artikel 1 i kommissionens direktiv 2008/63/EG av den 20 juni 2008 om konkurrens på marknaderna för teleterminalutrustning, definieras ”*terminalutrustning*” som a) en ”*utrustning direkt eller indirekt ansluten till en nätanslutningspunkt i ett allmänt tillgängligt telenät för att sända, bearbeta eller ta emot information; i ettdera fallet (direkt eller indirekt) kan anslutningen göras med tråd, optisk fiber eller elektromagnetiskt; en anslutning är indirekt om utrustningen är placerad mellan terminalutrustningen och nätanslutningspunkten; b) jordstationsutrustning*”.

[8] Se punkt 12 i EDPB:s riktlinjer 1/2020 för ett liknande resonemang kring uppkopplade fordon (nedan kallade *EDPB:s riktlinjer 1/2020*). Se även EDPB:s yttrande 5/2019 om samspelet mellan direktivet om integritet och elektronisk kommunikation och den allmänna dataskyddsförordningen, särskilt när det gäller dataskyddsmyndigheternas behörighet, uppgifter och befogenheter.

terminalutrustningen, måste för att vara laglig ha en rättslig grund enligt artikel 6 i den allmänna dataskyddsförordningen.[9]

27. När den personuppgiftsansvarige söker samtycke till att lagra eller få tillgång till information enligt artikel 5.3 i direktivet om integritet och elektronisk kommunikation måste denne informera den registrerade om alla ändamål med behandlingen (dvs. ”efterföljande behandling”), inräknat all behandling i enlighet med de tidigare nämnda processerna. Därför är samtycke enligt artikel 6 i den allmänna dataskyddsförordningen oftast den lämpligaste rättsliga grunden för att täcka den efterföljande behandlingen av personuppgifter. Samtycke kommer därför troligen att utgöra den rättsliga grunden för att både lagra och få tillgång till information som redan finns lagrad och för att behandla personuppgifter i enlighet med de tidigare nämnda behandlingsåtgärderna. Vid bedömningen av efterlevnad av artikel 6 i den allmänna dataskyddsförordningen ska hänsyn tas till att behandlingen som helhet inbegriper specifika åtgärder för vilka EU:s lagstiftning har eftersträvat att tillhandahålla ytterligare skydd.[10] Personuppgiftsansvariga måste vidare beakta inverkan på de registrerades rättigheter när de fastställer den lämpliga rättsliga grunden för att respektera rättviseprincipen.[11] Grundbudskapet är att personuppgiftsansvariga inte får dra nytta av artikel 6 i den allmänna dataskyddsförordningen för att minska det ytterligare skydd som artikel 5.3 i direktivet om integritet och elektronisk kommunikation föreskriver.

28. Såsom visas i avsnitt 2.3 (steg 2 och 3) kräver dagens virtuella röstassistenter tillgång till de röstdata som lagras i den virtuella röstassistentenheten.[12] Därför gäller artikel 5.3 i direktivet om integritet och elektronisk kommunikation. Tillämpligheten av artikel 5.3 i direktivet om integritet och elektronisk kommunikation innebär att både lagringen av information och tillgången till information som redan finns lagrad i en virtuell röstassistent i regel kräver slutanvändarens samtycke[13] i förväg, dock med två undantag: 1) behandling för att utföra eller underlätta överföringen av en kommunikation via ett elektroniskt kommunikationsnät , eller 2) sådan behandling som är absolut nödvändig för att leverera en av informationssamhällets tjänster som användaren eller abonnenten uttryckligen har begärt.

29. Det andra undantaget (”behandling som är absolut nödvändig för att leverera en av informationssamhällets tjänster som användaren eller abonnenten uttryckligen har begärt”) skulle göra det möjligt för en leverantör av virtuella röstassistenter att behandla användaruppgifter för att utföra användarens begäran (se punkt 72 i avsnitt 3.4.1) utan det samtycke som avses i artikel 5.3 i direktivet om integritet och elektronisk kommunikation. Omvänt skulle ett sådant **samtycke som krävs enligt artikel 5.3 i direktivet om integritet och elektronisk kommunikation behövas** för att lagra eller tillgå information för **alla andra ändamål än utförandet av användarens begäran** (t.ex. profilering av användare). Personuppgiftsansvariga skulle behöva tillskriva samtycke till specifika användare. Personuppgiftsansvariga ska således bara behandla icke registrerade användares uppgifter för att utföra deras begäranden.

[9] Ibidem, punkt 41.

[10] Yttrande 5/2019, punkt 41.

[11] EDPB:s riktlinjer 2/2019 om behandling av personuppgifter enligt artikel 6.1 b i dataskyddsförordningen i samband med tillhandahållandet av onlinetjänster till registrerade, Version 2.0, 8 oktober 2019, punkt 1.

[12] Det är möjligt att framtida virtuella röstassistentenheter anpassas till edge computing-paradigmet och förmår tillhandahålla vissa tjänster lokalt. Om så sker måste en ny bedömning genomföras av tillämpligheten av direktivet om integritet och elektronisk kommunikation.

[13] Se även EDPB:s riktlinjer 1/2020, punkt 14.

30. Virtuella röstassistenter kan råka fånga upp ljud från enskilda personer som inte är användare av en virtuell röstassistenttjänst. För det första kan väckningsuttrycket ändras i viss mån, beroende på vilken virtuell röstassistent som används. Enskilda personer som inte är medvetna om denna ändring kan av en olyckshändelse använda det uppdaterade väckningsuttrycket. För det andra kan virtuella röstassistenter uppfatta väckningsuttrycket av misstag eller till följd av ett fel. Det är högst osannolikt att något av undantagen i artikel 5.3 i direktivet om integritet och elektronisk kommunikation gäller vid oavsiktlig aktivering. Vidare måste samtycke enligt definitionen i den allmänna dataskyddsförordningen vara en ”*otvetydig viljeyttring*”. Det är därför högst osannolikt att en oavsiktlig aktivering kan tolkas som ett giltigt samtycke. Om personuppgiftsansvariga får kännedom (t.ex. genom automatiserad eller mänsklig granskning) om den virtuella röstassistenttjänstens oavsiktliga insamling av personuppgifter ska de kontrollera att det finns en giltig rättslig grund för varje ändamål med behandlingen av sådana uppgifter. I annat fall ska de oavsiktligt insamlade uppgifterna raderas.

31. Vidare bör det noteras att de personuppgifter som behandlas av virtuella röstassistenter kan vara mycket känsliga. De kan ha personuppgifter både i sitt innehåll (den akustiskt återgivna textens innebörd) och i sin metainformation (talarens kön eller ålder, osv.). Europeiska dataskyddsstyrelsen vill påpeka att röstdata är biometriska personuppgifter.[14] När sådana data behandlas i syfte att entydigt identifiera en fysisk person eller i sig själva är eller bestäms vara en särskild kategori av personuppgifter, måste behandlingen ha en giltig rättslig grund i artikel 6 och åtföljas av ett undantag från artikel 9 i den allmänna dataskyddsförordningen (se avsnitt 3.7 nedan).

3.2 Identifiering av behandling av uppgifter och intressenter

32. Med tanke på de många möjligheter till assistans som en virtuell röstassistent kan erbjuda och de många olika sammanhang de kan användas inom i den registrerades dagliga liv[15], är det viktigt att särskilt beakta behandlingen av personuppgifter, som också kan påverkas av olika intressenter.

3.2.1 Behandling av personuppgifter

33. Sett ur ett personuppgiftsskyddsperspektiv finns det flera konstanter som inte beror på typen av virtuell röstassistent (dvs. typ av enhet, funktioner, aktuella tjänster eller kombinationer av dessa) som kan användas av den registrerade. Dessa konstanter avser den mångfald av personuppgifter, registrerade och behandlingar av uppgifter som berörs.

Mångfald av personuppgiftstyper

34. Definitionen av personuppgifter enligt artikel 4.1 i den allmänna dataskyddsförordningen omfattar många olika uppgifter och tillämpas teknologineutralt på all information som avser *”en identifierad eller identifierbar fysisk person*”.[16] Alla interaktioner mellan den registrerade

[14] I artikel 4.14 i den allmänna dataskyddsförordningen definieras biometriska uppgifter som ”personuppgifter som erhållits genom en särskild teknisk behandling som rör en fysisk persons fysiska, fysiologiska eller beteendemässiga kännetecken och som möjliggör eller bekräftar identifieringen av denna fysiska person, såsom ansiktsbilder eller fingeravtrycksuppgifter”.

[15] Assistenten kan till exempel användas i hemmet, i fordon, på gatan, på arbetsplatsen eller på andra privata, offentliga eller yrkesmässiga platser eller en kombination av dessa.

[16] I artikel 4.1 i den allmänna dataskyddsförordningen anges även att *”en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras, särskilt med hänvisning till en identifierare som ett namn, ett*

och en virtuell röstassistent kan omfattas av denna definition. Under interaktionen kan många olika typer av personuppgifter behandlas av den virtuella röstassistenten, såsom beskrivs avsnitt 2.4.

35. Från den ursprungliga begäran till svaret, åtgärden eller uppföljningen (t.ex. upprättande av veckovisa varningar) kommer därför den först inlagda personuppgiften att generera efterföljande personuppgifter. Dessa omfattar primära data (t.ex. kontouppgifter, röstinspelningar, historik över begäranden), observerade data (t.ex. enhetens data avseende den registrerade, verksamhetsloggar, internetaktivitet), samt utvunna data (t.ex. profilering av användare). Virtuella röstassistenter använder tal för att förmedla kontakt mellan användare och de uppkopplade tjänsterna (t.ex. en sökmotor, nätbutik eller musikströmningstjänst), men till skillnad från andra intermediärer kan virtuella röstassistenter ha fullständig tillgång till innehållet i begäran, och förser därför den virtuella röstassistentens konstruktör med många olika personuppgifter beroende på behandlingens ändamål.

36. Mångfalden av personuppgifter som behandlas vid användningen av en virtuell röstassistent avser även mångfalden av personuppgiftskategorier som bör beaktas (se avsnitt 3.7 nedan). Europeiska dataskyddsstyrelsen påminner om att när särskilda kategorier av uppgifter[17] behandlas, fastställs det i artikel 9 i den allmänna dataskyddsförordningen att den personuppgiftsansvarige måste identifiera ett giltigt undantag från behandlingsförbudet i artikel 9.1 och en giltig rättslig grund enligt artikel 6.1, med hjälp av en lämplig metod i enlighet med artikel 9.2. Uttryckligt samtycke kan vara ett av de lämpliga undantagen i de fall där samtycke är den rättsliga grunden i enlighet med artikel 6.1. I artikel 9 anges det även (utförligt) att medlemsstaterna får införa ytterligare villkor för behandling av biometriska eller andra särskilda kategorier av uppgifter.

Mångfald av registrerade

37. När en virtuell röstassistent används behandlas personuppgifter från den första interaktionen med den virtuella röstassistenten. För vissa registrerade sker denna första interaktion i samband med inköpet av den virtuella röstassistenten och/eller när ett användarkonto (dvs. En registrerad användare) skapas. För andra registrerade sker den första medvetna interaktionen med en virtuell röstassistent när de interagerar med en sådan assistent som tillhör en annan registrerad som köpt och/eller konfigurerat den virtuella röstassistenten (dvs. i egenskap av icke-registrerad användare). Utöver dessa två kategorier av registrerade finns det också en tredje typ: oavsiktliga användare som, oavsett om de är registrerade eller inte, ovetande utfärdar begäranden till den virtuella röstassistenten (exempelvis kanske de anger rätt väckningsuttryck utan att veta att den virtuella röstassistenten aktiveras, eller uttalar andra ord som den virtuella röstassistenten misstolkar som väckningsuttrycket).

38. Med begreppet ”mångfald av registrerade” avses även många olika användare av en en och samma virtuella röstassistent (t.ex. en enhet som delas mellan registrerade och icke

identifikationsnummer, en lokaliseringsuppgift eller en onlineidentifikator eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet”.

[17] I artikel 9 i den allmänna dataskyddsförordningen definieras särskilda kategorier av personuppgifter: *”personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning ska vara förbjuden”*.

registrerade användare, mellan kollegor, i en familj, på en skola) och olika typer av användare som klassificeras utifrån deras omständigheter (t.ex. en vuxen, ett barn, en äldre person eller en person med funktionsnedsättning). Samtidigt som en virtuell röstassistent kan underlätta interaktionen med ett digitalt verktyg och betyda mycket för vissa kategorier av registrerade, är det viktigt att beakta specificiteten hos varje kategori av registrerade och det sammanhang i vilket den virtuella röstassistenten används.

Uppgiftsbehandlingens mångfaldiga karaktär

39. De tekniker som används för att tillhandahålla en virtuell röstassistent påverkar också mängden behandlade uppgifter och typerna av behandling. Ju mer en virtuell röstassistent tillhandahåller tjänster eller funktioner och kopplas upp till andra enheter eller tjänster som sköts av andra parter, desto större är mängden behandlade personuppgifter, samtidigt som användningen för nya ändamål ökar. Detta skapar en mångfald av utförda behandlingar med automatiserade metoder, såsom beskrivs i avsnitt 2. Förutom automatiserade metoder kan det i vissa behandlingar också ingå metoder som hanteras av människor. Detta kan till exempel vara när den utförda tekniken innefattar mänskliga ingripanden, såsom granskning av transkriptionen av röst till text, eller tillhandahållande av anteckningar om personuppgifter som kan användas för att lägga in nya modeller i en teknik för maskininlärning. Detta är också fallet när människor analyserar personuppgifter (t.ex. metadata) för att förbättra den tjänst som en virtuell röstassistent tillhandahåller.

3.2.2 Personuppgiftsansvarigas och personuppgiftsbiträdens behandling

40. Registrerade ska kunna förstå och identifiera de berörda rollerna och ska kunna kontakta eller agera tillsammans med varje intressent i enlighet med den allmänna dataskyddsförordningen. Fördelningen av roller ska inte vara till de registrerades nackdel, även om scenarierna kan vara komplicerade eller föränderliga. För att bedöma rollerna hänvisas intressenter till EDPB:s riktlinjer 07/2020 om begreppen personuppgiftsansvarig och personuppgiftsbiträde i den allmänna dataskyddsförordningen.[18]

41. Såsom framgår i punkt 15 kan de främsta intressenterna identifieras som leverantörer eller konstruktörer, applikationsutvecklare, integratorer, ägare eller en kombination av dessa. Olika scenarier är möjliga beroende på vem som gör vad i intressentens affärsrelation, på användarens begäran, personuppgifter, behandling av personuppgifter och deras ändamål. De ska tydligt besluta och informera de registrerade om de villkor som gäller för var och en av dem och uppfylla de resulterande rollerna som personuppgiftsansvariga, gemensamt personuppgiftsansvariga eller personuppgiftsbiträden vilka föreskrivs i den allmänna dataskyddsförordningen.[19] Var och en kan ha en eller flera roller, då de kan vara enda personuppgiftsansvariga, gemensamt personuppgiftsansvariga eller personuppgiftsbiträde för en personuppgiftsbehandling medan de har en annan roll för en annan personuppgiftsbehandling.

42. Ur ett övergripande perspektiv kan konstruktören fungera som personuppgiftsansvarig vid bestämningen av en behandlings ändamål och metoder, men kan också träda in som personuppgiftsbiträde vid behandlingen av personuppgifter för andra parters räkning, såsom

[18] EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR (EDPB:s riktlinjer 07/2020 om begreppen personuppgiftsansvarig och personuppgiftsbiträde i den allmänna dataskyddsförordningen), V2.0, antagna den 7 juli 2021 (nedan kallade *riktlinjerna 7/2020*).

[19] Den allmänna dataskyddsförordningen, artiklarna 12–14, artikel 26.

en applikationsutvecklare. Användaren av en virtuell röstassistent skulle därför ha för flera personuppgiftsansvariga, närmare bestämt applikationsutvecklaren och konstruktören. Det är också möjligt att konstruktören, integratorn och utvecklaren samlas i en enda grupp där de fungerar som en gemensam personuppgiftsansvarig. Hur som helst måste de tillämpliga kvalifikationerna fastställas vid en analys från fall till fall.

Exempel 1:

Den virtuella röstassistentens konstruktör behandlar användardata för många olika ändamål, såsom att förbättra den virtuella röstassistentens talförståelse och förmåga att korrekt svarar på en begäran. Trots att detta kan leda till behandling av personuppgifter som härrör från användningen av applikationer som tillhandahålls av tredje parter, finns det därför bara en enda personuppgiftsansvarig: den virtuella röstassistentens konstruktör, på vars vägnar behandlingen utförs.

Exempel 2:

En bank erbjuder sina kunder en applikation som de kan använda direkt via den virtuella röstassistenten för att sköta sina konton.

Två aktörer deltar i behandlingen av personuppgifter: den virtuella röstassistentens konstruktör och bankapplikationens utvecklare.

I det presenterade scenariot är banken personuppgiftsansvarig för tillhandahållandet av tjänsten, eftersom den bestämmer behandlingens ändamål och centrala metoder till applikationen som gör det möjligt att interagera med assistenten. Den erbjuder en särskild applikation som gör att användaren, en bankkund, kan sköta sina konton på distans. Dessutom beslutar den om behandlingsmetoden genom att välja ett lämpligt personuppgiftsbiträde, som är den virtuella röstassistentens konstruktör och kan spela en viktig roll genom att assistera med sin sakkunskap när denna metod bestäms (den kan till exempel sköta den utvecklingsplattform som gör att tredjepartsapplikationer kan integreras i den virtuella röstassistenten, och fastställer därför de ramar och villkor som applikationsutvecklarna ska respektera).

43. Vad gäller den registrerade är det viktigt att notera att flera intressenter kan behandla samma personuppgifter, också om den registrerade inte verkligen förväntar sig att andra parter än leverantören av den virtuella röstassistenten deltar i behandlingskedjan. När en registrerad agerar tillsammans med leverantören av den virtuella röstassistenten i förhållande till sina personuppgifter (t.ex. för att utöva den registrerades rättigheter), innebär därför inte detta automatiskt att denna åtgärd kommer att gälla för samma personuppgifter som en annan intressent behandlar. När dessa intressenter är oberoende personuppgiftsansvariga är det viktigt att skicka ett tydligt informationsmeddelande till de registrerade, som förklarar de olika stegen och aktörerna i behandlingen. Vid gemensam personuppgiftsansvarighet bör det även klargöras huruvida alla personuppgiftsansvariga är behöriga att uppfylla alla registrerades rättigheter eller vilken personuppgiftsansvarig som är behörig för vilken rättighet.[20]

[20] Riktlinjer 7/2020, punkt 165.

Exempel 3:

I detta scenario vill den virtuella röstassistentens konstruktör använda de uppgifter som samlats in och behandlats för den tjänst som banken tillhandahållit för att förbättra sitt röstigenkänningssystem. Den virtuella röstassistentens konstruktör, som behandlar uppgifterna för dess egna ändamål, kommer sedan att vara personuppgiftsansvarig för denna specifika behandling.

44. Eftersom många intressenter kan ingå i behandlingskedjan, och därför också många anställda, kan riskabla situationer uppstå om lämpliga mekanismer och skyddsåtgärder saknas. Personuppgiftsansvariga är ansvarsskyldiga för dessa och ska därför inrikta sig på att skydda personuppgifter, särskilt genom att välja lämpliga affärspartner och personuppgiftsbiträden, tillämpa principerna för inbyggt dataskydd och dataskydd som standard[21], införa lämpliga säkerhetsverktyg och andra verktyg enligt den allmänna dataskyddsförordningen, såsom granskningar och rättsliga avtal (t.ex. artikel 26 för gemensamt personuppgiftsansvariga eller artikel 28 i den allmänna dataskyddsförordningen för personuppgiftsbiträden).

45. Den virtuella röstassistentens ekosystem är komplicerat, med många aktörer som potentiellt kan utbyta och behandla personuppgifter i egenskap av personuppgiftsansvariga eller personuppgiftsbiträden. Det är av yttersta vikt att förtydliga varje aktörs roll inom varje behandling och att följa principen om uppgiftsminimering också vad gäller datautbyte.

46. Personuppgiftsansvariga bör även vara vaksamma på överföringar av personuppgifter och garantera den efterfrågade skyddsnivån inom hela behandlingskedjan, särskilt när de använder tjänster utanför ESS.

3.3 Öppenhet

47. Virtuella röstassistenter behandlar personuppgifter (t.ex. användarens röst, position eller kommunikationens innehåll) vilket gör att de måste uppfylla öppenhetskraven i den allmänna dataskyddsförordningen i enlighet med artikel 5.1 a) samt artiklarna 12 och 13 (förtydligade i skäl 58). De personuppgiftsansvariga måste informera användarna om behandlingen av deras personuppgifter i en koncis, klar, tydlig och begriplig form och på ett lättillgängligt sätt.

48. Att inte tillhandahålla nödvändig information innebär ett åsidosättande av skyldigheter som kan påverka databehandlingens legitimitet. Öppenhetskravet måste uppfyllas eftersom det utgör en kontrollmekanism över databehandlingen och gör att användare kan utöva sina rättigheter. När användarna får korrekt information om hur deras personuppgifter används blir det svårare för personuppgiftsansvariga att missbruka den virtuella röstassistenten för ändamål som går bortom vad användarna förväntar sig. Till exempel finns det patenterade tekniker för att utläsa hälsotillstånd och känslomässiga tillstånd från en användares röst och anpassa de tjänster som tillhandahålls därefter.

49. Uppfyllande av öppenhetskravet kan vara särskilt svårt för den virtuella röstassistentens tjänsteleverantör eller någon annan enhet som fungerar som personuppgiftsansvarig. De virtuella röstassistenternas särskilda egenskaper gör att de personuppgiftsansvariga ställs inför flera hinder när de ska uppfylla den allmänna dataskyddsförordningens öppenhetskrav:

[21] Se EDPB:s riktlinjer 4/2019 om inbyggt dataskydd enligt artikel 25 och dataskydd som standard, version 2.0, antagna den 20 oktober 2020.

- **Många olika användare**: personuppgiftsansvariga ska informera alla användare (registrerade, icke registrerade och oavsiktliga användare), och inte bara den användare som installerar den virtuella röstassistenten.
- **Ekosystemets komplexitet**: såsom förklaras i avsnittet om teknisk bakgrund är det långt ifrån tydligt för användarna vilka identiteter och roller de som behandlar personuppgifter har när de använder en virtuell röstassistent.
- **Röstgränssnittets specificitet**: digitala system är ännu inte utformade för interaktioner med enbart röst, vilket bevisas av det näst intill systematiska bruket av en tillhörande skärm. Anpassning till röstgränssnittet och att kunna informera användaren tydligt och korrekt genom detta medel är dock en nödvändighet.

50. Virtuella röstassistenter kan betraktas som ändliga tillståndsautomater som genomgår ett antal tillstånd under sin normala drift. De kan lyssna lokalt efter väckningsuttryck eller interagera med en fjärrserver för att förstå ett kommando, men de kan också aktivera andra lägen beroende på sammanhanget (t.ex. vid bakgrundsljud) eller om användaren talar till assistenten (det kan t.ex. gälla processer för att fastställa om den som talar är en identifierad eller okänd användare). Dessvärre råder det inom ramen för dessa situationer en betydande asymmetri i fråga om information till användaren, som ofta inte vet om enheten lyssnar eller vilken status den har vid ett givet tillfälle.

51. Det förordas starkt att de virtuella röstassistenternas konstruktörer och utvecklare vidtar lämpliga åtgärder för att åtgärda dessa asymmetrier, så att de virtuella röstassistenterna blir mer interaktiva. Användarna bör informeras om enhetens aktuella status. Denna ökade öppenhet kan uppnås både genom att göra dialogen mellan människa och maskin mer interaktiv (t.ex. skulle enheten på något sätt kunna bekräfta att den har mottagit ett röstkommando), eller genom att sända apparatens status genom särskilda signaler. Det finns många olika möjligheter som kan utforskas här: allt från användning av specifika röstbaserade bekräftelser och synliga ikoner eller ljussignaler, till användning av bildskärmar på enheten.

52. Dessa problem är särskilt relevanta med tanke på hur olika användarna är och att de innefattar känsliga kategorier av personer, t.ex. barn, äldre personer eller användare med nedsatt hörsel eller syn.

53. Två viktiga frågor framträder tydligt av de problem som presenteras ovan: vilket är det lättaste sättet att informera användarna och vilken är den lämpligaste tidpunkten för att informera dem? Dessa frågor bör granskas närmare i två olika situationer, beroende på huruvida den virtuella röstassistenten bara har en enda användare (t.ex. en smartmobil) eller potentiellt många användare (t.ex. en smart husenhet). Vid användning av virtuell röstassistentteknik kan dessa två grundinställningar också undermineras, t.ex. när en användare har en personlig smartmobil och ansluter den till sin bil. Den virtuella röstassistenten i smartmobilen, som rimligen bara denna användare använder, ”utökas” nu till de andra i bilen.

54. Alla virtuella röstassistenter är i dag uppkopplade till ett användarkonto och/eller är installerade av en applikation som kräver ett sådant. När den virtuella röstassistenten inrättas bör personuppgiftsansvariga informera dessa användare om integritetspolicyn på det sätt som beskrivs i artikel 29-gruppens riktlinjer om öppenhet. Vad gäller appar bör den nödvändiga informationen tillgängliggöras i en nätbutik före nedladdning[22]. Därigenom tillhandahålls

[22] Guidelines on transparency under Regulation 2016/679 (riktlinjer om öppenhet enligt förordning 2016/679), WP260 rev. 01, godkänd av EDPB (nedan kallade *WP29-gruppens riktlinjer WP260*), punkt 11.

informationen så tidigt som möjligt och senast när personuppgifterna erhålls. Vissa leverantörer av virtuella röstassistenter låter tredjepartsappar ingå i standardinstallationen av den virtuella röstassistenten så att dessa applikationer kan starta apparna genom särskilda väckningsuttryck. Virtuella röstassistenter som har denna driftsättningsstrategi med användning av tredjepartsappar bör säkerställa att användarna får den nödvändiga informationen också om tredjepartsbehandlingen.

55. Många konstruktörer av virtuella röstassistenter behöver dock användarkonton för virtuella röstassistenter som kombinerar den virtuella röstassistenttjänsten med andra tjänster, såsom e-post, direktuppspelad video eller tjänster för inköp. När den virtuella röstassistentens konstruktör beslutar att koppla kontot till många olika tjänster krävs det mycket långa och komplicerade integritetspolicyer. Längden och komplexiteten hos sådana integritetspolicyer sätter stora hinder i vägen för uppfyllandet av öppenhetsprincipen.

> Exempel 4:
>
> En konstruktör av en virtuell röstassistent kräver att användarna har ett konto för att kunna använda den virtuella röstassistenttjänsten. Detta användarkonto är inte specifikt för den virtuella röstassistenttjänsten och kan användas för andra tjänster som konstruktören av den virtuella röstassistenten erbjuder, såsom e-post, lagring i molnet och sociala medier. För att skapa kontot måste användare läsa och godkänna en 30 sidor lång integritetspolicy. I policyn ingår information om behandling av personuppgifter som utförts av alla tjänster som kan kopplas till kontot.
>
> Den information som i detta fall tillhandahålls av den virtuella röstassistentens konstruktör kan inte betraktas som kortfattad och dess komplexitet minskar den öppenhet som krävs. Därför skulle inte konstruktören av den virtuella röstassistenten uppfylla de öppenhetskrav som fastställs i artiklarna 12 och 13 i den allmänna dataskyddsförordningen.

56. Även om skrift är det vanligaste sättet att lämna nödvändig information medger den allmänna dataskyddsförordningen också andra metoder för detta. I skäl 58 anges det uttryckligen att informationen kan tillhandahållas elektroniskt, exempelvis på en webbplats. Vid valet av lämplig metod för att informera de registrerade ska hänsyn dessutom tas till de specifika förhållandena, såsom det sätt på vilket den personuppgiftsansvarige och den registrerade i övrigt samverkar med varandra.[23] Ett alternativ till skärmlösa enheter kan vara att tillhandahålla en länk som är lätt att förstå, antingen direkt eller i ett e-postmeddelande. Redan befintliga lösningar kan tjäna som exempel för informationen, t.ex. teletjänstcentralers praxis att meddela den som ringer om att ett telefonsamtal spelas in och att hänvisa dem till sina integritetspolicyer. Begränsningarna hos skärmlösa virtuella röstassistenter gör inte att den personuppgiftsansvarige undantas från kravet att lämna nödvändig information i enlighet med den allmänna dataskyddsförordningen vid inrättandet av virtuella röstassistenter eller installation eller användning av en virtuell röstassistentapp. Leverantörer och utvecklare av virtuella röstassistenter ska ta fram röstbaserade gränssnitt för att göra det lättare att tillhandahålla den obligatoriska informationen.

57. Virtuella röstassistenter kan vara av stort intresse för användare med nedsatt syn eftersom de ger ett annat sätt att interagera än de it-tjänster som traditionellt sett använder visuell information. I enlighet med artikel 12.1 i den allmänna dataskyddsförordningen kan den

[23] WP29-gruppens riktlinjer WP260, punkt 19.

nödvändiga informationen bara lämnas muntligen om så begärs av den registrerade, men inte som standardmetod. Begränsningarna hos skärmlösa virtuella röstassistenter skulle dock göra det nödvändigt att införa automatiserade metoder för muntlig information som kan stödjas av skrift. När ljud används för att informera de registrerade bör de personuppgiftsansvariga lämna den nödvändiga informationen på ett klart och tydligt sätt. Vidare bör de registrerade ha möjlighet att lyssna flera gånger på meddelandet[24].

58. Det är svårare att vidta lämpliga åtgärder för att uppfylla den allmänna dataskyddsförordningens öppenhetskrav när den virtuella röstassistenten har flera användare, och inte bara enhetens ägare. Konstruktörer av virtuella röstassistenter måste överväga hur de ska informera icke registrerade och oavsiktliga användare på rätt sätt vid behandlingen av deras personuppgifter. När samtycke är den rättsliga grunden för att behandla användaruppgifter måste användarna informeras om detta för att samtycket ska vara giltigt[25].

59. För att följa den allmänna dataskyddsförordningen bör personuppgiftsansvariga hitta ett sätt att inte bara informera registrerade användare, utan även icke registrerade och oavsiktliga användare av virtuella röstassistenter. Dessa användare ska informeras så snart som möjligt **och <u>senast vid tiden för</u>** behandlingen. Detta villkor kan vara särskilt svårt att uppfylla i praktiken.

60. Affärsmässiga särdrag ska heller inte vara till men för de registrerade. Eftersom många intressenter är globala företag eller är välkända för en viss affärsverksamhet (t.ex. telekommunikation, elektronisk handel, informationsteknik, webbverksamhet), bör det tydligt anges hur de levererar en virtuell röstassistenttjänst. Med hjälp av adekvat information bör de registrerade förstå om deras användning av den virtuella röstassistenten kommer eller inte kommer att kopplas till andra behandlingsaktiviteter som sköts av den virtuella röstassistentens tjänsteleverantör (t.ex. telekommunikation, elektronisk handel, informationsteknik eller webbverksamhet), utöver det som krävs för den specifika användningen av den virtuella röstassistenten.

> Exempel 5:
>
> En konstruktör av en virtuell röstassistent, som också tillhandahåller en plattform för sociala medier och en sökmotor, kräver att användaren kopplar sitt konto till assistenten för att få använda den. Genom att koppla sitt konto till användningen av den virtuella röstassistenten kan konstruktören förstärka sina användares profiler med hjälp av assistenten, de applikationer (eller färdigheter) som installerats, skickade beställningar, osv. Assistentinteraktioner är på så sätt en ny informationskälla som är kopplad till en användare. Konstruktören av en virtuell röstassistent ska förse användarna med tydlig information om hur deras uppgifter kommer att behandlas för varje tjänst och med kontroller med vars hjälp användaren kan välja om uppgifterna ska användas för profilering eller inte.

Rekommendationer

61. När användare informeras om en virtuell röstassistents behandling av personuppgifter genom ett användarkontos integritetspolicy och kontot är kopplat till andra oberoende tjänster (t.ex.

[24] WP29-gruppens riktlinjer WP260, punkt 21.
[25] Artikel 4.11 i den allmänna dataskyddsförordningen.

e-post eller internetköp), rekommenderar EDPB att integritetspolicyn har ett separat avsnitt om den virtuella röstassistentens behandling av personuppgifter.

62. Den information som användaren får ska exakt motsvara den insamling och behandling som utförs. Även om en viss metainformation ingår i ett röstprov (t.ex. talarens stressnivå), är det inte automatiskt tydligt huruvida en sådan analys utförs. Det är av avgörande vikt att de personuppgiftsansvariga öppet anger vilka specifika aspekter av rådatan som de behandlar.

63. Vidare bör det alltid tydligt framgå i vilket tillstånd/läge den virtuella röstassistenten befinner sig. Användarna ska kunna avgöra om en virtuell röstassistent för närvarande lyssnar på sin slutna krets och särskilt om den direktuppspelar information till sin back-end. Denna information ska vara tillgänglig för personer med funktionsnedsättningar såsom färgblindhet (daltonism) och dövhet (anaccousia). Man bör särskilt tänka på att virtuella röstassistenter innebär ett användningsscenario där det inte krävs någon ögonkontakt med enheten. Därför bör all användarfeedback, inklusive ändringar av läge/tillstånd, åtminstone finnas tillgänglig i visuell och akustisk form.

64. Man bör rikta särskild uppmärksamhet på enheter som gör det möjligt att lägga till en tredjepartsfunktion (”appar” för virtuella röstassistenter). Även om en viss allmän information kan ges till användare som lägger till en sådan funktion (om det är användarens val), under enhetens normala användning, kan gränserna mellan de olika ingående personuppgiftsansvariga vara mycket mindre tydliga, dvs. användarna kanske inte informeras i tillräcklig grad om hur och av vem deras uppgifter behandlas (och i vilken utsträckning) vid en viss begäran.

65. All information om behandling som baseras på uppgifter som insamlats och utvunnits ur behandlingen av en inspelad röst ska också vara tillgänglig för användare i enlighet med artikel 12 i den allmänna dataskyddsförordningen.

66. Personuppgiftsansvariga för virtuella röstassistenter ska öppet ange vilken typ av information som en virtuell röstassistent kan utvinna om sin omgivning, inklusive men inte begränsat till andra personer i rummet, bakgrundsmusik, all behandling av rösten av medicinska skäl, marknadsföringsskäl eller andra skäl, sällskapsdjur, osv.

3.4 Ändamålsbegränsning och rättslig grund

67. Virtuella röstassistenters behandling av intalade begäranden har ett tydligt ändamål, dvs. att utföra begäran. Ofta finns det dock också andra ändamål som inte är så uppenbara, t.ex. att förbättra den virtuella röstassistentens förmåga att förstå naturligt språk genom att använda maskininlärningstekniker för att träna den virtuella röstassistentmodellen. Några av de vanligaste ändamålen med virtuella röstassistenters behandling av personuppgifter:

- Att utföra användarnas begäran
- Att förbättra den virtuella röstassistenten genom att träna maskininlärningsmodellen samt mänsklig granskning och att märka rösttranskriptioner
- Användaridentifiering (genom röstdata)
- Användarprofilering för individanpassat innehåll eller annonser

68. Deras roll som intermediärer och deras utformning gör att virtuella röstassistenter behandlar många olika personuppgifter och icke-personuppgifter. Detta medför att de kan behandla personuppgifter för många andra syften än att besvara användarnas begäranden, som kan gå obemärkta förbi. Genom att analysera data som samlats in via virtuella röstassistenter är det

möjligt att ta reda på eller utvinna användarintressen, scheman, körrutter eller vanor. Detta kan möjliggöra behandling av personuppgifter för oförutsedda ändamål (t.ex. känsloanalys eller hälsotillståndsbedömning[26]), som skulle gå långt bortom användarnas rimliga förväntningar.

69. De personuppgiftsansvariga ska tydligt ange sitt eller sina syften i förhållande till det sammanhang som den virtuella röstassistenten används inom, så att de klart förstås av de registrerade (t.ex. genom att indela syftena i kategorier). I enlighet med artikel 5.1 i den allmänna dataskyddsförordningen ska personuppgifter samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte genomgå ytterligare behandling på ett sätt som är oförenligt med dessa ändamål.

3.4.1 Utförande av användarnas begäranden

70. Virtuella röstassistenter, eller de appar eller tjänster som de samarbetar med, utför olika åtgärder som de instrueras om genom röstkommandon (t.ex. en musikströmningstjänst, en karttjänst eller ett elektroniskt lås). Användarens röst och potentiellt andra data (t.ex. användarens position när denne begär att få veta vägen till en viss destination) skulle därför kunna behandlas.

> Exempel 6:
>
> En passagerare i en smartbil som är försedd med en virtuell röstassistent begär att få veta vägen till närmaste bensinstation. Den virtuella röstassistenten behandlar användarens röst för att förstå kommandot och bilens position för att hitta rutten, och skickar den till smartkomponenten för att visa den på bilens skärm.

71. Om behandlingen av röstkommandon involverar lagring eller tillgång till information som lagras i slutanvändarens terminalenheter måste artikel 5.3 i direktivet om integritet och elektronisk kommunikation beaktas. Samtidigt som artikel 5.3 innehåller den allmänna principen att en sådan lagring eller tillgång kräver slutanvändarens föregående samtycke anger den även ett undantag till kravet på samtycke när det är ”absolut nödvändigt för att leverera en av informationssamhällets tjänster som användaren eller abonnenten uttryckligen har begärt”. Om röstdata behandlas för att utföra användarens begäran är de undantagna från kravet på föregående samtycke.

72. Såsom tidigare angetts måste all behandling av personuppgifter som utförs efter lagringen eller åtkomsten av information i slutanvändares terminalenhet ha en rättslig grund enligt artikel 6 i den allmänna dataskyddsförordningen för att vara laglig.

73. Det sker två behandlingsåtgärder efter varandra på den virtuella röstassistenten. Som tidigare nämnts kräver den första åtgärden åtkomst till den virtuella röstassistenten (varför villkoren i artikel 5.3 i direktivet om integritet och elektronisk kommunikation måste uppfyllas). Utöver villkoren i artikel 5.3 i direktivet om integritet och elektronisk kommunikation kräver detta andra steg en rättslig grund enligt artikel 6 i den allmänna dataskyddsförordningen.

74. När en enskild person beslutar att använda en virtuell röstassistent innebär detta vanligtvis att den ursprungliga användaren först måste registrera ett konto för att aktivera den virtuella

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

röstassistenten. Med andra ord innebär denna situation ett avtalsförhållande[27] mellan den registrerade användaren och den virtuella röstassistentens personuppgiftsansvarige. Med tanke på dess ämne och slutgiltiga mål är detta avtals centrala syfte att använda den virtuella röstassistenten för att utföra användarens begäran om assistans.

75. All behandling av personuppgifter som krävs för att utföra användarens begäran kan därför bygga på den rättsliga grunden för fullgörandet av avtalet[28]. En sådan behandling innefattar i synnerhet upptagningen av användarens intalade begäran, dess transkription till text, dess tolkning, den information som utbyts med kunskapskällor för att förbereda svaret samt transkriptionen till ett intalat slutligt svar som avslutar användarens begäran.

76. Fullgörandet av ett avtal kan vara en rättslig grund för behandling av personuppgifter genom maskininlärning när så krävs för tjänstens tillhandahållande. Behandling av personuppgifter genom maskininlärning för andra syften som inte är nödvändiga, såsom förbättringen av en tjänst, bör inte ha denna rättsliga grund.

77. Sist men inte minst ska inte de rättsliga grunderna för att fullgöra avtalet och samtycket i enlighet med den allmänna dataskyddsförordningen förväxlas. Samtycket för ingående, dvs. avtalsöverenskommelsen, är en del av detta avtals giltighet och avser inte samtyckets specifika innebörd enligt den allmänna dataskyddsförordningen[29].

78. När ett användarkonto inte först måste konfigureras till den virtuella röstassistenten för att kunna använda den, kan samtycke vara en möjlig rättslig grund.

3.4.2 Förbättra den virtuella röstassistenten genom att träna maskininlärningssystemen och manuellt granska rösten och transkripten

79. Mänskligt tal har mängder av dialekter och variationer. Även om alla virtuella röstassistenter är fullt fungerande när de installeras kan deras prestanda förbättras genom att justera dem efter särdragen i användarens tal. Såsom nämnts i avsnitt 2.6 utnyttjar denna justeringsåtgärd maskininlärningsmetoder och utgörs av två förfaranden: att till den virtuella röstassistentens utbildningsdataset lägga till nya uppgifter som samlats in från dess användare, samt den mänskliga granskningen av de behandlade uppgifterna för utförandet av en bråkdel av begärandena.

> Exempel 7:
>
> En användare av en virtuell röstassistent är tvungen att utfärda samma röstkommando tre gånger på grund av att den virtuella röstassistenten först inte förstår kommandot. De tre röstkommandona och de relaterade transkriptionerna förs över till mänskliga granskare som granskar och korrigerar transkriptionerna. Röstkommandona och de granskade transkriptionerna förs in i den virtuella röstassistentens utbildningsdataset för att förbättra dess prestanda.

[27] Under förutsättning att ”*avtalet är giltigt i enlighet med tillämpliga nationella avtalslagar*”, utdrag ur riktlinjer 2/2019 om behandling av personuppgifter enligt artikel 6.1 b i dataskyddsförordningen i samband med tillhandahållandet av onlinetjänster till registrerade (nedan kallade *riktlinjer 2/2019*), punkt 26.

[28] I enlighet med riktlinjer 2/2019, som i övrigt anger att yttrande 06/2014 förblir relevant för artikel 6.1 b i dataskyddsförordningen (se särskilt sidorna 11, 16, 17, 18 och 55 i yttrande 06/2014).

[29] Se riktlinjer 2/2019, punkterna 18, 19, 20, 21 och 27.

80. Den behandlingsaktivitet som beskrivs i exemplet bör inte anses vara (absolut) ”*nödvändig för att fullgöra ett avtal*” i den mening som avses i artikel 6.1 b i den allmänna dataskyddsförordningen, och kräver därför en annan rättslig grund än artikel 6 i den allmänna dataskyddsförordningen. Det främsta skälet är att virtuella röstassistenter redan är fullt fungerande när de lämnar kartongen och redan kan prestera såsom är (absolut) nödvändigt för att fullgöra avtalet. Europeiska dataskyddsstyrelsen anser inte att artikel 6.1 b i allmänhet skulle vara en lämplig rättslig grund för behandling i syfte att förbättra en tjänst eller utveckla nya funktioner inom ramen för en befintlig tjänst. I de flesta fall ingår en användare ett avtal för att använda en befintlig tjänst. Även om möjligheten att göra förbättringar och ändringar av en tjänst rutinmässigt kan ingå i avtalsvillkoren kan en sådan behandling vanligen inte anses vara objektivt sett nödvändig för att fullgöra avtalet med användaren.

3.4.3 Användaridentifiering[30] (genom röstdata)

81. Användning av röstdata för användaridentifiering innebär behandling av biometriska uppgifter enligt definitionen i artikel 4.14 i den allmänna dataskyddsförordningen. Följaktligen kommer den personuppgiftsansvarige att behöva identifiera ett undantag enligt artikel 9 i den allmänna dataskyddsförordningen förutom att identifiera en rättslig grund enligt artikel 6 i den allmänna dataskyddsförordningen[31].

82. Av undantagen i artikel 9 i den allmänna dataskyddsförordningen verkar bara de registrerades uttryckliga samtycke vara tillämpbart för just detta ändamål.

83. Men eftersom detta ändamål kräver tillämpning av det specifika rättsliga regelverket i artikel 9 i den allmänna dataskyddsförordningen kommer närmare beskrivning att ges i avsnitt 3.8, gällande behandling av särskilda kategorier av uppgifter.

3.4.4 Användarprofilering för individanpassat innehåll eller annonser

84. Som tidigare nämnts har virtuella röstassistenter tillgång till innehållet i alla röstkommandon, också när de är avsedda för tjänster som levereras av tredje parter. Denna tillgång skulle göra det möjligt för den virtuella röstassistentens konstruktör att konstruera mycket exakta användarprofiler som kan användas för att erbjuda individanpassade tjänster eller annonser.

> Exempel 8:
>
> Varje gång en användare av en virtuell röstassistent söker på internet lägger den virtuella röstassistenten till noteringar som signalerar ämnen av intresse för användarprofilen. Resultaten av varje ny sökning presenteras för användaren med hänsyn tagen till dessa noteringar.
>
> Exempel 9:

[30] I tekniskt hänseende måste begreppet identifiering skiljas från verifiering (autentisering). Identifiering bygger på en ”ett-till-många” (1: N) sökning och jämförelse och kräver i princip en databas i vilken flera enskilda personer finns förtecknade. Behandling i verifieringssyfte bygger däremot på en jämförelse ”ett-mot-ett” (1:1) och används för att verifiera och bekräfta genom biometrisk jämförelse huruvida en enskild person är samma person som den som de biometriska uppgifterna härrör från. Såvitt Europeiska dataskyddsstyrelsen vet använder virtuella röstassistenter på marknaden endast teknik för identifiering av talaren.

[31] I den allmänna dataskyddsförordningen anses uppgifter till sin natur inte alltid vara tillräckliga för att medge bestämning av om de räknas som särskilda kategorier av uppgifter eftersom *”behandling av foton […] endast definieras som biometriska uppgifter när de behandlas med särskild teknik som möjliggör identifiering eller autentisering av en fysisk person*” (skäl 51). Samma resonemang gäller för rösten.

Varje gång en användare av en virtuell röstassistent köper något från en elektronisk handelstjänst sparar den virtuella röstassistenten en registerpost om köpordern. Den virtuella röstassistentens leverantör gör det möjligt för tredje parter att rikta in sig på den virtuella röstassistentens användare med riktad reklam på grundval av tidigare inköp.

85. Individanpassning av innehåll kan (men inte alltid) utgöra en integrerad och förväntad del av en virtuell röstassistent. Huruvida denna behandling kan anses utgöra en integrerad aspekt av den virtuella röstassistenttjänsten beror på den exakta beskaffenheten av den tjänst som tillhandahålls, den genomsnittlige registrerades förväntningar mot bakgrund av inte bara tjänstevillkoren utan också hur tjänsten marknadsförs till användarna, och huruvida tjänsten kan tillhandahållas utan individanpassning.[32]

86. Där individanpassning sker i samband med ett avtalsförhållande och som del av en tjänst som uttryckligen begärts av slutanvändaren (och behandlingen är begränsad till vad som är absolut nödvändigt för att leverera denna tjänst) kan en sådan behandling baseras på artikel 6.1 b i den allmänna dataskyddsförordningen.

87. Om behandlingen inte är absolut *”nödvändig för att fullgöra ett avtal”* i enlighet med artikel 6.1 b i den allmänna dataskyddsförordningen, måste den virtuella röstassistentens leverantör, i princip, söka den registrerades samtycke. Eftersom det i artikel 5.3 i direktivet om integritet och elektronisk kommunikation fastställs att det krävs samtycke för att lagra eller tillgå information (se punkterna 28–29 ovan), kommer samtycke enligt artikel 6.1 a i den allmänna dataskyddsförordningen också i princip vara en lämplig rättslig grund för behandling av personuppgifter efter dessa åtgärder. Att förlita sig på ett berättigat intresse kan nämligen i vissa fall riskera att underminera den ytterligare skyddsnivån enligt artikel 5.3 i direktivet om integritet och elektronisk kommunikation.

88. Vad gäller användarprofilering för annonser bör det noteras att detta ändamål aldrig anses vara en tjänst som uttryckligen begärs av slutanvändaren. Vid behandling för detta ändamål bör därför användarnas samtycke systematiskt samlas in.

Rekommendationer

89. Användare bör informeras om ändamålet med behandlingen av personuppgifter och detta ändamål ska stämma med deras förväntningar på den enhet de köper. Vad gäller en virtuell röstassistent är det tydligt att detta ändamål – ur användarnas synvinkel – är bearbetningen av deras röst för det enda ändamålet att tolka deras begäran och ge användbara svar (om det så gäller svar på en fråga eller åtgärder såsom att fjärrkontrollera en strömbrytare).

90. När behandlingen av personuppgifter baseras på samtycke ska den registrerade ha lämnat ett sådant samtycke*”för ett eller flera specifika ändamål och att han eller hon har en valmöjlighet med avseende på vart och ett av dessa*”. Vidare: ”*en personuppgiftsansvarig som begär samtycke för flera olika ändamål bör ge möjlighet till opt-in för respektive ändamål, så att användarna kan ge särskilt samtycke till specifika ändamål*”[33]. Användare bör t.ex. kunna separat samtycka eller inte samtycka till den manuella granskningen och noteringen av rösttranskriptioner eller användningen av deras röstdata för att identifiera eller autentisera användare (se avsnitt 3.7).

[32] Se även riktlinjer 2/2019, punkt 57.

[33] Se EDPB:s riktlinjer 05/2020 om samtycke enligt förordning 2016/679, antagna den 4 maj 2020, avsnitt 3.2.

3.5 Behandling av barns uppgifter

91. Barn kan också samverka med de virtuella röstassistenterna eller skapa sina egna profiler som kopplas till de vuxnas motsvarigheter. Vissa virtuella röstassistenter är inbyggda i enheter som är särskilt avsedda för barn.

92. Om behandlingens rättsliga grund är att fullgöra ett avtal kommer villkoren för behandlingen av barns uppgifter att vara beroende av nationella avtalslagar.

93. Om behandlingens rättsliga grund är samtycke är behandling av barns uppgifter, enligt artikel 8.1 i den allmänna dataskyddsförordningen, endast tillåten ”*om barnet är minst 16 år. Om barnet är under 16 år ska sådan behandling vara tillåten endast om och i den mån samtycke ges eller godkänns av den person som har föräldraansvar för barnet*”. För att följa den allmänna dataskyddsförordningen, om samtycke är den rättsliga grunden, ska uttrycklig tillåtelse följaktligen sökas från föräldrar eller särskilt förordnade vårdnadshavare för att registrera, behandla och lagra barns uppgifter (röst, transkript, osv.).

94. Föräldrakontroll är till viss grad tillgänglig men i sin nuvarande form är den inte användarvänlig (en ny tjänst måste t.ex. loggas in) eller har begränsad kapacitet. De personuppgiftsansvariga bör investera i att ta fram metoder för att föräldrar eller särskilt förordnade vårdnadshavare ska kunna kontrollera barns användning av virtuella röstassistenter.

3.6 Datalagring

95. Virtuella röstassistenter behandlar och skapar många olika personuppgifter såsom röst, transkriptioner av röst, metadata eller systemloggar. Dessa typer av uppgifter kan behandlas för många olika ändamål, såsom tillhandahållande av en tjänst, förbättring av bearbetningen av naturligt språk, individanpassning eller vetenskaplig forskning. I enlighet med den allmänna dataskyddsförordningens princip om lagringsbegränsning ska virtuella röstassistenter inte lagra data längre än vad som krävs för de syften för vilka personuppgifterna behandlas. Därför bör datalagringsperioderna kopplas till olika syften för behandling. Den virtuella röstassistentens tjänsteleverantörer eller tredje parter som tillhandahåller tjänster genom virtuella röstassistenter bör bedöma den längsta lagringstiden för varje dataset och syfte.

96. Principen om uppgiftsminimering är tätt förknippad med principen om datalagringsbegränsning. De personuppgiftsansvariga behöver inte bara begränsa datalagringsperioden, utan också typen och mängden av uppgifter.

97. De personuppgiftsansvariga bör bland annat fråga sig själva: Måste alla röstinspelningar eller transkriptioner lagras för att uppnå ändamål X? Är det nödvändigt att lagra röstdatan när väl transkriptionen har sparats? Om så är fallet, för vilket ändamål? Hur länge behövs röst- eller transkriptionsdatan för varje ändamål? Svaren på dessa och andra liknande frågor kommer att fastställa de lagringsperioder som bör ingå i den information som de registrerade har tillgång till.

98. Vissa virtuella röstassistenter lagrar personuppgifter som standard, såsom röstfragment eller transkriptioner under en odefinierad tid och ger samtidigt användarna sätt att radera dessa data. Att lagra personuppgifter på obestämd tid strider mot principen om lagringsbegränsning. Att förse de registrerade med sätt att radera sina personuppgifter undantar inte de personuppgiftsansvariga från sitt ansvar att definiera och verkställa en datalagringspolicy.

99. När virtuella röstassistenter formges måste hänsyn tas till kontoanvändarnas kontroller för att radera sina personuppgifter i sina enheter och i alla fjärrlagringssystem. Dessa kontroller kan

krävas för att tillmötesgå olika typer av önskemål från användarna, till exempel en önskan att radera eller dra tillbaka ett tidigare avgett samtycke. Formgivningen av vissa virtuella röstassistenter beaktade inte detta krav.[34]

100. Liksom i andra sammanhang kan de personuppgiftsansvariga behöva lagra personuppgifter som bevis på att en tjänst har tillhandahållits till en användare för att uppfylla en rättslig förpliktelse. Den personuppgiftsansvarige kan lagra personuppgifter på denna grund. De lagrade uppgifterna ska dock vara den nödvändiga miniminivån för att uppfylla en sådan rättsliga förpliktelse och under kortast möjliga tid. De uppgifter som lagras för att uppfylla en rättslig förpliktelse ska naturligtvis inte användas för andra syften utan en rättslig grund enligt artikel 6 i den allmänna dataskyddsförordningen.

> Exempel 10:
>
> En användare köper en tv via en elektronisk handelstjänst genom ett röstkommando som utfärdas till en virtuell röstassistent. Också om användaren uttalar begäran efter att ha fått sina uppgifter raderade kan den virtuella röstassistentens leverantör eller utvecklare lagra vissa uppgifter på grundval av sina rättsliga förpliktelser att behålla ett inköpsbevis enligt skatteförordningen. De uppgifter som lagras för detta syfte bör dock inte överstiga den nödvändiga miniminivån för att uppfylla den rättsliga förpliktelsen och kan inte behandlas för andra syften utan rättslig grund enligt artikel 6 i den allmänna dataskyddsförordningen.

101. Såsom nämnts i avsnitt 2 förbättras de virtuella röstassistenternas röstigenkänningskapacitet av att maskininlärningssystemen tränas med användaruppgifter. Om användare inte samtycker eller drar tillbaka sitt samtycke till att deras uppgifter används för ett sådant syfte, kan inte deras uppgifter lagligen användas för att träna någon fler modell utan bör raderas av den personuppgiftsansvarige, förutsatt att det inte finns något annat syfte som motiverar fortsatt lagring. Det finns dock bevis för att vissa maskininlärningsmodeller kan medföra risker för återidentifiering.[35]

102. Personuppgiftsansvariga och personuppgiftsbiträden ska använda modeller som inte begränsar deras förmåga att avbryta behandlingen om en enskild person återkallar sitt samtycke, och de ska se till att inte använda modeller som begränsar deras förmåga att understödja de registrerades rättigheter. Personuppgiftsansvariga och personuppgiftsbiträden ska tillämpa begränsande åtgärder för att minska risken för återidentifiering till ett godtagbart tröskelvärde.

103. Om användaren drar tillbaka sitt samtycke kan inte de uppgifter som insamlats från användaren längre användas för att träna modellen ytterligare. Oavsett detta är det inte nödvändigt att radera den modell som tidigare tränats med hjälp av dessa uppgifter. Europeiska dataskyddsstyrelsen betonar dock att det finns bevis för att vissa maskininlärningsmodeller kan innebära risker för läckage av personuppgifter och att många studier har visat att rekonstruktion liksom angrepp av medlemskapsbedömningar kan ske, med hjälp av vilka angripare kan ta fram information om enskilda personer.[36]

---

[34] Se Amazons svarsskrivelse av den 28 juni 2019 till USA:s senator Christopher Coons: https://www.coons.senate.gov/imo/media/doc/Amazon%20Senator%20Coons__Response%20Letter__6.28.19[3].pdf

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

[36] N. Carlini et al, "Extracting Training Data from Large Language Models" Dec 2020.

Personuppgiftsansvariga och personuppgiftsbiträden ska därför tillämpa begränsande åtgärder för att minska risken för återidentifiering till ett godtagbart tröskelvärde, för att säkerställa att de använder modeller som inte innehåller personuppgifter.

104. Registrerade ska inte övertalas att behålla sina uppgifter på obestämd tid. Samtidigt som raderingen av röstdata eller transkriptioner skulle kunna påverka utförandet av tjänsten ska en sådan påverkan förklaras för användarna på ett tydligt och mätbart sätt. Den virtuella röstassistentens tjänsteleverantörer ska undvika att fälla allmänna omdömen om en försämrad tjänst efter att personuppgifter raderats.

105. Det är särskilt svårt att anonymisera röstinspelningar eftersom det är möjligt att identifiera användare genom innehållet i själva meddelandet och kännetecknen för rösten i sig själv. Trots detta görs det viss forskning[37] om tekniker som kan göra att situationsbetingad information såsom bakgrundsljud kan tas bort och rösten anonymiseras.

Rekommendationer

106. Ur ett användarperspektiv är det främsta syftet med att behandla deras uppgifter att ställa frågor och ta emot svar och/eller sätta igång åtgärder såsom att spela musik eller tända och släcka lampor. Efter att en fråga besvarats eller ett kommando utförts ska personuppgifterna raderas om inte konstruktören eller utvecklaren av den virtuella röstassistenten har en giltig rättslig grund för att lagra dem för ett särskilt ändamål.

107. Innan anonymisering övervägs som ett medel för att uppfylla principen om datalagringsbegränsning ska leverantörerna och utvecklarna av virtuella röstassistenter kontrollera om anonymisering gör att rösten inte kan identifieras.

108. Konfigureringsstandarderna ska återspegla dessa krav som standard genom att välja ett absolut minimum av lagrad användarinformation. Om dessa alternativ läggs fram som en del av en installationsguide ska standardinställningen återspegla detta, och alla alternativ ska läggas fram som likvärdiga utan synlig diskriminering.

109. Om den virtuella röstassistentens leverantör eller utvecklare under granskningen upptäcker en inspelning som härrör från en oavsiktlig aktivering, ska inspelningen och alla kopplade uppgifter genast raderas och inte användas för något ändamål.

3.7 Säkerhet

110. För en säker behandling av personuppgifter ska virtuella röstassistenter skydda sin konfidentialitet, integritet och tillgänglighet. Utöver de risker som härrör från delar av den virtuella röstassistentens ekosystem gör användningen av rösten som kommunikationsmedel att en ny uppsättning säkerhetsrisker uppstår.

111. Virtuella röstassistenter är storskaliga användare. De kan tillåta att fler än en enda registrerad användare eller vem som helst i omgivningen utfärdar kommandon och använder deras tjänster. Alla virtuella röstassistenttjänster som kräver konfidentialitet inbegriper en viss mekanism för åtkomstkontroll och användarautentisering. Utan åtkomstkontroll kan alla som kan utfärda röstkommandon till den virtuella röstassistenttjänsten också tillgå, modifiera eller

[37] Se till exempel VoicePrivacy (https://www.voiceprivacychallenge.org), ett initiativ för utveckling av integritetsbevarande lösningar för talteknologi.
Se även det öppna källkodsverktyget för röstanonymisering som tagits fram av H2020:s forsknings- och innovationsprojekt COMPRISE: https://gitlab.inria.fr/comprise/voice_transformation.

radera en användares personuppgifter (t.ex. efterfråga mottagna meddelanden, användaradresser eller planlagda händelser). Utfärdandet av röstkommandon till virtuella röstassistenttjänster kräver inte att man befinner sig i deras fysiska närhet eftersom de kan manipuleras, till exempel via signalsändning[38] (t.ex. radio eller tv). Vissa av de kända metoderna för att utfärda fjärrkommandon till virtuella röstassistenttjänster såsom laser[39] eller (ohörbara) ultraljudsvågor[40] kan inte ens upptäckas av människans sinnen.

112. Användarautentisering förlitar sig på minst en av följande faktorer: något man vet (t.ex. ett lösenord), något man har (t.ex. ett smartkort) eller något man är (t.ex. ett röstfingeravtryck). Ser man närmare på dessa autentiseringsfaktorer i samband med virtuella röstassistenter framgår följande:

- Autentisering genom något användaren vet skapar problem. Den hemlighet som skulle göra det möjligt för användarna att bevisa sin identitet ska uttalas högt, vilket avslöjar den för alla i omgivningen. Kommunikationskanalen för virtuella röstassistenter är den omgivande luften, som är en typ av kanal som inte kan skyddas som traditionella kanaler (t.ex. genom begränsad åtkomst till kanalen eller kryptering av dess innehåll).
- Autentisering genom något användaren har skulle kräva att de virtuella röstassistenternas tjänsteleverantörer skapar, distribuerar och hanterar ”polletter” som kan användas som identitetsbevis.
- Autentisering genom något användaren är förenklar användningen av biometriska uppgifter i syfte att entydigt identifiera en fysisk person (se avsnitt 3.7 nedan).

113. Den virtuella röstassistentens användarkonton kopplas till de enheter i vilka tjänsten tillhandahålls. Samma konto som används för att hantera den virtuella röstassistenten används ofta för att hantera andra tjänster. Till exempel kan innehavare av en Android-mobil och en Google Home-högtalare koppla sitt Google-konto till båda enheterna, vilket de också troligen gör. De flesta virtuella röstassistenter kräver eller erbjuder ingen identifierings- eller autentiseringsmekanism när en enhet som levererar en virtuell röstassistenttjänst bara har ett enda användarkonto.

114. När mer än ett enda användarkonto är kopplat till enheten erbjuder vissa virtuella röstassistenter en valfri grundläggande åtkomstkontroll i form av ett PIN-nummer utan verklig användarautentisering. Vissa andra virtuella röstassistenter använder alternativet igenkänning av röstfingeravtryck som identifieringsmekanism.

115. Även om användaridentifiering eller -autentisering kanske inte krävs för att tillgå alla virtuella röstassistenttjänster, gäller detta definitivt för vissa. Utan en identifierings- eller autentiseringsmekanism kan vem som helst tillgå alla användaruppgifter och modifiera eller radera dem som de vill. Alla som befinner sig nära intill en smart högtalare kan till exempel radera andra användares spellistor från musikströmningstjänsten, kommandon från kommandohistoriken eller kontakter från kontaktlistan.

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

[39] Se t.ex. https://lightcommands.com

[40] Se t.ex. https://surfingattack.github.io

116. De flesta virtuella röstassistenter litar blint på sina lokala nätverk. En kompromitterad enhet i samma nätverk kan ändra den smarta högtalarens inställningar eller göra att ett sabotageprogram installeras eller att falska appar/färdigheter kopplas till den utan användarens kännedom eller medgivande.[41]

117. Precis som alla andra programvaror har virtuella röstassistenter svagheter i programvaran. De virtuella röstassistenternas stora marknadskoncentration[42] gör dock att en eventuell svaghet påverkar miljontals användare av virtuella röstassistenter. Om de fungerar som de just nu är konstruerade skickar inte de virtuella röstassistenterna någon information till taligenkänningens molntjänst förrän väckningsuttrycket upptäcks. Genom svagheter i programvaran kan dock en angripare komma förbi den virtuella röstassistentens inställnings- och säkerhetsåtgärder. En kopia kan då till exempel erhållas av alla uppgifter som skickats till den virtuella röstassistentens molntjänst, vilken skickas vidare till en server som kontrolleras av angriparen.

118. Uppgifter som lagligen behandlas eller utvinns av virtuella röstassistenter gör att en tämligen exakt profil kan byggas av deras användare eftersom de virtuella röstassistenterna känner till eller kan härleda sina användares position, förhållanden och intressen. Virtuella röstassistenter finns alltmer på plats i användarnas hem och smartmobiler. Detta förhållande ökar risken för massövervakning och massprofilering. Följaktligen ska de säkerhetsåtgärder som skyddar uppgifterna både i transit och i vila, i enheterna och i molnet, motsvara dessa risker.

119. Den ökande användningen av virtuella röstassistenter kopplad till en inte tillräckligt balanserad rätt till tillgång av de brottsbekämpande myndigheterna kan ge en skrämmande effekt som skulle underminera grundläggande rättigheter såsom yttrandefriheten.

120. Brottsbekämpande myndigheter, både inom[43] och utanför[44] EU, har redan uttryckt sitt intresse för att få tillgång till de röstfragment som uppfångas av virtuella röstassistenter. Tillgång till uppgifter som behandlas eller utvinns av virtuella röstassistenter inom EU ska vara förenlig med EU:s befintliga ramverk för dataskydd och förordning om integritet. Ifall vissa medlemsstater överväger att utfärda en särskild lag som begränsar de grundläggande rättigheterna till integritets- och dataskydd, ska sådana begränsningar alltid uppfylla det krav som fastställs i artikel 33 i den allmänna dataskyddsförordningen[45].

121. Bland leverantörer av virtuella röstassistenter är det vanlig praxis med mänsklig granskning av röstinspelningar och kopplade uppgifter för att förbättra den virtuella röstassistenttjänstens kvalitet. På grund av känsligheten hos de uppgifter som dessa mänskliga granskare behandlar och det faktum att detta förfarande ofta läggs ut på underentreprenad till personuppgiftsbiträden, är det ytterst relevant att lämpliga säkerhetsåtgärder vidtas.

---

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

[42] Marknaden för virtuella röstassistenter delas för närvarande av knappt ett dussin tjänsteleverantörer.

[43] Se t.ex. https://www.ft.com/content/ad765972-87a2-11e9-a028-86cea8523dc2.

[44] Se t.ex. https://cdt.org/insights/alexa-is-law-enforcement-listening.

[45] Se även ”EDPB Guidelines 10/2020 on restrictions under Article 23 GDPR” (EDPB:s riktlinjer 10/2020 om begränsningar enligt artikel 23 i den allmänna dataskyddsförordningen).

Rekommendationer

122. Konstruktörerna av virtuella röstassistenter och applikationsutvecklarna bör förse användarna med säkra spetsteknologiska autentiseringsförfaranden.

123. Mänskliga granskare bör alltid få de absolut nödvändiga pseudonymiserade uppgifterna. I de rättsliga avtal som styr granskningen bör all behandling som kan leda till identifiering av den registrerade vara uttryckligen förbjuden.

124. Om nödanrop tillhandahålls som en tjänst via den virtuella röstassistenten bör en stabil upptid[46] garanteras.

3.8 Behandling av särskilda kategorier av uppgifter

125. Som tidigare nämnts har virtuella röstassistenter tillgång till intim information som kan skyddas enligt artikel 9 i den allmänna dataskyddsförordningen (se avsnitt 3.7.1), såsom biometriska uppgifter (se avsnitt 3.7.2). Därför måste konstruktörer och utvecklare av virtuella röstassistenter noga fastställa i vilka fall behandlingen inbegriper särskilda kategorier av uppgifter.

3.8.1 Allmänna överväganden vid behandling av särskilda kategorier av uppgifter

126. Virtuella röstassistenter kan behandla särskilda kategorier av uppgifter under olika omständigheter:

- Som en del av deras egna tjänster, t.ex. vid hantering av läkarbesök i användarnas dagordning.
- När de tjänar som gränssnitt för tredjepartstjänster behandlas innehållet i kommandona av de virtuella röstassistenternas leverantörer. Beroende på den typ av tjänst som användaren begär kan de virtuella röstassistenternas leverantörer behandla särskilda kategorier av uppgifter. En användare kan t.ex. utfärda kommandon till en virtuell röstassistent om att använda en tredjepartsapp för att hålla koll på hennes ägglossning.[47]
- När röstdata används för att entydigt identifiera användaren, såsom beskrivs nedan.

3.8.2 Särskilda överväganden vid behandling av biometriska uppgifter

127. Vissa virtuella röstassistenter har förmågan att entydigt identifiera sina användare uteslutande baserat på deras röst. Denna process kallas röstmodelligenkänning. I början av röstigenkänningen behandlar den virtuella röstassistenten en användares röst för att skapa en röstmodell (eller ett röstavtryck). Vid normal användning kan den virtuella röstassistenttjänsten beräkna röstmodellen för alla användare och jämföra den med de inregistrerade modellerna för att entydigt identifiera den användare som utfärdade ett kommando.

Exempel 11:

[46] Den tid som en enhet eller en tjänst kan lämnas obevakad utan att den kraschar, eller behöver startas om (”rebooted”) för administrativa ändamål eller underhåll.

[47] Se t.ex. en tillgänglig produkt här: https://www.amazon.com/Ethan-Fan-Ovulation-Period-Tracker/dp/B07CRLSHKY

En grupp användare inrättar en virtuell röstassistent för att använda röstmodelligenkänning. Därefter inregistrerar var och en av dem sin röstmodell.

Senare begär en användare att den virtuella röstassistenten får tillgång till mötena i hans eller hennes dagordning. Eftersom det krävs användaridentifiering för att få tillgång till dagordningen utvinner den virtuella röstassistenten modellen från rösten i begäran, beräknar dess röstmodell och kontrollerar om den motsvarar en inregistrerad användare och om just denna användare har tillgång till dagordningen.

128. I exemplet ovan kommer igenkänning av användarens röst på grundval av en röstmodell att motsvara behandling av särskilda kategorier av personuppgifter i enlighet med artikel 9 i den allmänna dataskyddsförordningen (behandling av biometriska uppgifter för att entydigt identifiera en fysisk person).[48] Behandling av biometriska uppgifter för användaridentifiering som i exemplet kräver att den eller de registrerade lämnar ett uttryckligt samtycke (artikel 9.2 a i den allmänna dataskyddsförordningen). När personuppgiftsansvariga får användarnas samtycke måste de därför uppfylla villkoren i artikel 7 och som förtydligas i skäl 32 i den allmänna dataskyddsförordningen samt erbjuda en alternativ identifieringsmetod till biometri, vad gäller samtyckets frihet.

129. Vid användning av röstdata för biometrisk identifiering eller autentisering måste de personuppgiftsansvariga öppet ange var biometrisk identifiering används och hur röstavtryck (biometriska modeller) lagras och sprids mellan enheter. För att uppfylla detta öppenhetskrav rekommenderar Europeiska dataskyddsstyrelsen att följande frågor besvaras:

- Aktiveringen av röstidentifiering på en enhet: aktiverar denna funktion automatiskt alla andra enheter som körs med samma konto?
- Sprids den aktiverade röstidentifieringen genom infrastrukturen tillhörande den virtuella röstassistentens personuppgiftsansvarige till enheter som tillhör andra användare?
- Var skapas, lagras och matchas biometriska modeller?
- Är biometriska modeller tillgängliga för den virtuella röstassistentens leverantörer, utvecklare eller andra?

130. När den registrerade användaren konfigurerar de virtuella röstassistenterna till att identifiera sina användares röst, kommer också icke registrerade och oavsiktliga användares röster att behandlas i syfte att entydigt identifiera dem.

131. Att upptäcka den rätta talarens röst inbegriper faktiskt också att jämföra den med andra personers röster i assistentens närområde. Med andra ord kan den igenkänningsfunktion för talare som genomförs i röstassistenter också kräva att röstbiometrin för personer som talar i hushållet spelas in, för att särskilja användarens röstkännetecken från dem hos den person som önskar bli igenkänd. Biometrisk identifiering kan därför leda till att oinformerade personer utsätts för biometrisk behandling, genom att deras modell registreras och jämförs med den som tillhör användaren som önskar bli igenkänd.

132. För att undvika en sådan insamling av biometriska uppgifter utan de registrerades vetskap samtidigt som assistenten tillåts att känna igen en användare bör lösningar som endast bygger på användarens uppgifter prioriteras. Konkret innebär detta att biometrisk igenkänning

bara ska aktiveras vid varje användning på användarens initiativ, och inte genom en ständigt pågående analys av de röster som assistenten hör. Ett visst nyckelord eller en viss fråga till de närvarande personerna kan till exempel lämnas för att få deras samtycke till att inleda en biometrisk behandling. Användaren kan till exempel säga ”identifiering” eller assistenten kan fråga ”vill du bli identifierad" och invänta ett jakande svar för att aktivera en biometrisk behandling.

Exempel 12:
Om användaren inrättar biometrisk autentisering för att tillgå vissa skyddade uppgifter såsom sitt bankkonto, kan röstassistenten aktivera talarverifiering när han/hon endast lanserar applikationen, och verifiera sin identitet på så sätt.

Rekommendationer

133. Röstmodeller bör endast skapas, lagras och matchas på den lokala enheten, och inte på fjärrservrar.

134. På grund av röstavtryckens höga känslighet ska standarder såsom ISO/IEC 24745 och tekniker för biometriskt modellskydd[49] genomgående tillämpas.

135. Om en virtuell röstassistent använder röstbaserad biometrisk identifiering ska leverantörer av virtuella röstassistenter göra följande:

    - Säkerställa att identifieringen är tillräckligt exakt för att tillförlitligt koppla personuppgifterna till rätt registrerade.
    - Säkerställa att precisionen är samma för alla användargrupper genom att kontrollera att ingen betydande snedvridning (bias) förekommer mot olika demografiska grupper.

3.9 Uppgiftsminimering

136. Personuppgiftsansvariga ska minimera den mängd uppgifter som samlas in direkt eller indirekt och erhålls genom behandling och analys, t.ex. inte utföra någon analys av användarnas röst eller annan hörbar information för att utvinna information om deras psykiska hälsa, eventuella sjukdomar eller omständigheter i deras liv.

137. Inrätta standardinställningsvärden som begränsar all insamling och/eller behandling av uppgifter till minsta nödvändiga mängd för att tillhandahålla tjänsten.

138. Beroende på position, användningens sammanhang och mikrofonens känslighet kan virtuella röstassistenter samla in tredje parters röstdata som del av bakgrundsljudet vid insamlingen av användarens röst. Även om inte röstdata ingår i bakgrundsljudet kan situationsdata ändå behandlas för att utvinna information om den registrerade (t.ex. position).

Rekommendationer

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

139. Konstruktörer av virtuella röstassistenter bör överväga tekniker som raderar bakgrundsljudet för att undvika att bakgrundsröster och situationsbetingad information spelas in och behandlas.

3.10 Ansvarsskyldighet

140. För all behandling som bygger på samtycke måste de personuppgiftsansvariga bevisa att de registrerade har lämnat sitt samtycke i enlighet med artikel 7.1 i den allmänna dataskyddsförordningen. Röstdata kan användas för ansvarsskyldighet (t.ex. för att bevisa samtycke). Lagringsskyldigheten för sådana röstdata skulle då bestämmas av ansvarighetskraven i den relevanta specifika lagstiftningen.

141. När Europeiska dataskyddsstyrelsen utvärderade behovet av en konsekvensbedömning avseende dataskydd (DPIA) fastställde den kriterier[50] som dataskyddsmyndigheter ska använda när de upprättar förteckningar över behandlingar där konsekvensbedömning avseende dataskydd är obligatoriska, och gav exempel på behandlingar som troligen kräver konsekvensbedömning avseende dataskydd. Det är mycket troligt att virtuella röstassistenttjänster omfattas av de kategorier och villkor som kräver konsekvensbedömning avseende dataskydd. I detta ingår att överväga om enheten kanske genomför övervakning eller kontroll av registrerade eller systematisk och storskalig övervakning enligt artikel 35.3 c, använder ”ny teknik” eller behandlar känsliga uppgifter och uppgifter om sårbara registrerade.

142. Alla insamlingar av uppgifter och behandlingar måste dokumenteras i enlighet med artikel 30 i den allmänna dataskyddsförordningen. Detta innefattar all behandling av röstdata.

Rekommendationer

143. Vid användning av röstmeddelanden för att informera användare i enlighet med artikel 13, ska personuppgiftsansvariga offentliggöra dessa meddelanden på sin webbplats så att användarna och dataskyddsmyndigheterna har tillgång till dem.

3.11 Inbyggt dataskydd och dataskydd som standard

144. Leverantörer och utvecklare av virtuella röstassistenter bör överväga om en registrerad användare behövs för varje funktion. Samtidigt som en registrerad användare tydligtvis behövs för att sköta en dagordning eller en adressbok, är det inte så tydligt att den virtuella röstassistenten kräver en registrerad användare för att ringa ett samtal eller göra en internetsökning.

145. För tjänster som inte kräver en identifierad användare gäller som standard att ingen av de användare som identifierats av den virtuella röstassistenten får kopplas till kommandona. En integritets- och dataskyddsvänlig virtuell röstassistent som standard skulle bara behandla användarnas uppgifter för att utföra användarnas begäran och skulle varken lagra röstdata eller ett register över utförda kommandon.

146. Medan vissa enheter bara kan köra en enda virtuell röstassistent, kan andra välja mellan olika virtuella röstassistenter. Leverantörer av virtuella röstassistenter bör ta fram branschstandarder som möjliggör dataportabilitet i enlighet med artikel 20 i den allmänna dataskyddsförordningen.

[50] Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) wp248, rev.01 (riktlinjer om konsekvensbedömning avseende dataskydd) – godkända av Europeiska dataskyddsstyrelsen

147. Vissa leverantörer av virtuella röstassistenter har intygat att deras virtuella röstassistenter inte ens kan radera alla användaruppgifter när den registrerade så begär. Leverantörer av virtuella röstassistenter ska säkerställa att alla användaruppgifter kan raderas på användarens begäran i enlighet med artikel 17 i den allmänna dataskyddsförordningen.

4 MEKANISMER FÖR ATT UTÖVA REGISTRERADES RÄTTIGHETER

148. I enlighet med den allmänna dataskyddsförordningen måste personuppgiftsansvariga som levererar virtuella röstassistenttjänster medge att alla användare, registrerade och icke registrerade, får utöva sina registrerades rättigheter.

149. Leverantörer och utvecklare av virtuella röstassistenter ska underlätta de registrerades kontroll över sina uppgifter under hela behandlingstiden, särskilt förenkla deras rätt till tillgång, rättelse, radering, deras rätt att begränsa behandlingen och, beroende på den rättsliga grunden för behandlingen, deras rätt till dataportabilitet och rätt att göra invändningar.

150. Den personuppgiftsansvarige ska tillhandahålla information om den registrerades rättigheter när den registrerade sätter igång en virtuell röstassistent och senast när den första användarens intalade begäran behandlas.

151. Eftersom rösten är den huvudsakliga interaktionsvägen för virtuella röstassistenter ska konstruktörer av virtuella röstassistenter tillse att användare, oavsett om de är registrerade eller inte, kan utöva alla registrerades rättigheter, med hjälp av lättförståeliga röstkommandon. Både konstruktörer av virtuella röstassistenter och applikationsutvecklare, om de ingår i lösningen, ska vid förfarandets slut informera användarna om att deras rättigheter har vederbörligen beaktats, genom ett röstmeddelande eller skriftligt meddelande till användarens mobil, konto eller något annat sätt som användaren valt.

152. Konstruktörer av virtuella röstassistenter och applikationsutvecklare ska som minsta åtgärd genomföra särskilda verktyg som ger en ändamålsenlig och effektiv möjlighet att utöva sådana rättigheter. De ska därför föreslå ett sätt som deras enheter kan använda för att utöva registrerades rättigheter, t.ex. genom att förse de registrerade med självbetjäningsverktyg, som ett profilförvaltningssystem[51]. Detta kan göra det lättare att effektivt hantera de registrerades rättigheter i god tid och gör att den personuppgiftsansvarige kan låta identifieringsmekanismen ingå i självbetjäningsverktyget.

153. Vad gäller utövandet av de registrerades rättigheter när det finns många olika användare ska en användare, oavsett om denne är registrerad eller inte, utöva sina rättigheter utan att detta påverkar andra användares rättigheter. Alla användare, registrerade och icke registrerade, kan utöva sina rättigheter så länge som den personuppgiftsansvarige fortfarande behandlar uppgifterna. Den personuppgiftsansvarige ska inrätta ett förfarande som tillser att den registrerades rättigheter utövas.

4.1 Rätten till tillgång

154. I enlighet med artikel 12.1 i den allmänna dataskyddsförordningen ska en kommunikation enligt artikel 15 tillhandahållas i skriftlig, eller någon annan form, inbegripet, när så är lämpligt,

[51] Profilförvaltningssystem förstås som en plats inuti det virtuella röstassistentsystemet, där användare när som helst kan lagra sina preferenser, ställa in modifiering och lätt ändra sina integritetsinställningar

i elektronisk form. Vad gäller tillgång till de personuppgifter som genomgår behandling, anges det i artikel 15.3 att om den registrerade skickar begäran elektroniskt ska informationen tillhandahållas i ett allmänt använt elektroniskt format, om den registrerade inte begär annat. Vad som kan betraktas som ett allmänt använt elektroniskt format ska utgå ifrån de registrerades rimliga förväntningar och inte ifrån vilket format den personuppgiftsansvarige använder i sin dagliga verksamhet. Den registrerade ska inte vara tvungen att köpa en särskild programvara eller maskinvara för att få tillgång till informationen.

155. Därför ska de personuppgiftsansvariga på begäran skicka en kopia av personuppgifterna, och i synnerhet ljuddata (inräknat röstinspelningar och transkriptioner), på ett vanligt format som den registrerade kan läsa.

156. När beslut fattas om den formattyp som ska väljas för tillhandahållandet av informationen enligt artikel 15, måste den personuppgiftsansvarige tänka på att formatet ska göra det möjligt att presentera informationen på ett sätt som är både förståeligt och lättåtkomligt. De personuppgiftsansvariga ska också anpassa informationen efter den specifika situationen för den registrerade som skickar begäran.

> Exempel 13:
>
> En personuppgiftsansvarig som levererar en virtuell röstassistenttjänst får, från en användare, både en begäran om åtkomst och en begäran om dataportabilitet. Den personuppgiftsansvarige beslutar att lämna informationen enligt både artikel 15 och artikel 20 i en pdf-fil. I ett sådant fall ska inte den personuppgiftsansvarige anses hantera de båda begärandena korrekt. Även om en pdf-fil tekniskt sett uppfyller den personuppgiftsansvariges skyldigheter enligt artikel 15, uppfylls inte den personuppgiftsansvariges skyldigheter enligt artikel 20.[52]
>
> Det bör noteras att enbart den omständigheten att användare hänvisas till en historik över deras interaktioner med röstassistenten inte verkar medföra att den personuppgiftsansvarige kan uppfylla alla sina skyldigheter enligt rätten till tillgång, eftersom de tillgängliga uppgifterna oftast bara är en del av den information som behandlas i samband med tillhandahållandet av tjänsten.

157. Rätten till tillgång ska inte användas för att motverka/kringgå principerna om minimering och datalagring.

4.2 Rätten till rättelse

158. För att underlätta rättelse av uppgifter ska användare, oavsett om de är registrerade eller inte, när som helst kunna använda rösten för att hantera och uppdatera sina uppgifter direkt till den virtuella röstassistentenheten, såsom beskrivs ovan. Vidare bör självbetjäningsverktyget genomföras inuti enheten eller en applikation för att hjälpa dem att enkelt rätta sina personuppgifter. Användare bör meddelas genom rösten eller skriftligt om uppdateringen.

[52] WP29 Guidelines on the right to data portability – endorsed by the EDPB (WP29-gruppens riktlinjer om dataportabilitet – godkända av EDPB), s. 18.

159. Rätten till rättelse gäller mer allmänt alla åsikter och bedömningar[53] av den personuppgiftsansvarige, däribland profilering, och bör betrakta de allra flesta uppgifter som högst subjektiva.[54]

4.3 Rätt till radering

160. Användare, oavsett om de är registrerade eller inte, ska när som helst kunna använda rösten för att radera uppgifter om sig själva från den virtuella röstassistentenheten, eller från ett självbetjäningsverktyg som integrerats i en enhet som är kopplad till den virtuella röstassistenten. På så sätt kan en registrerad radera personuppgifterna lika lätt som de skickas in. De inneboende svårigheterna i anonymiseringen av röstdata och den stora mångfalden av insamlade, observerade och utvunna personuppgifter från den registrerade[55] gör att rätten till radering här knappast tillgodoses genom anonymisering av personuppgifter. Eftersom den allmänna dataskyddsförordningen är teknikneutral och tekniken utvecklas snabbt är det ändå inte uteslutet att rätten till radering kan ske genom anonymisering.

161. Utan en tredjepartsskärm eller möjlighet att visa de lagrade uppgifterna (t.ex. en mobil applikation eller en tabellarisk enhet), är det i vissa fall svårt att förhandsvisa de inspelade spåren, för att bedöma förslagens relevans. En allmänt tillgänglig instrumentpanel (eller applikation) i syfte att förenkla dess användning för användarna bör levereras med röstassistenten för att radera historiken över inskickade begäranden och anpassa verktyget till användarens behov.[56]

162. För all behandling av uppgifter och särskilt när de registrerade samtycker till att leverantören får transkribera och använda röstinspelningarna för att förbättra sina tjänster ska den virtuella röstassistentens leverantör, på användarens begäran, kunna radera den första röstinspelningen samt alla förknippade transkriptioner av personuppgifterna.

163. Den personuppgiftsansvarige ska säkerställa att ingen mer behandling kan ske efter att rätten till radering har utövats. Vad gäller föregående åtgärder kan rätten till radering i synnerhet stöta på vissa rättsliga och tekniska gränser.

> Exempel 14:
>
> Om en användare använde sin virtuella röstassistent till ett inköp på nätet före begäran om radering, kan den virtuella röstassistentens leverantör radera röstinspelningen av inköpet på nätet och säkerställa att den inte längre används i framtiden. Köpet kommer dock fortfarande att gälla liksom den röstbaserade beställningen eller den skriftliga transkriptionen som behandlas av den elektroniska webbplatsen (här bygger undantaget på den elektroniska webbplatsens rättsliga förpliktelse).

[53] Att åsikter och bedömningar kan godkännas som personuppgifter har bekräftats av Europeiska unionens domstol, som noterade att begreppet ”varje upplysning” i definitionen av personuppgifter innefattar ”såväl objektiva upplysningar som subjektiva upplysningar som lämnas i form av åsikter eller bedömningar, under förutsättning att upplysningarna ”avser” den registrerade Mål C-434/16 *Peter Nowak mot Data Protection Commissioner* ECLI:EU:C:2017:994 [34].

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

[55] Artikel 29-gruppens yttrande 05/2014 om anonymiseringsmetoder, antaget den 10 april 2014.

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

Om användaren på samma sätt använde sin virtuella röstassistent till att lägga till en specifik sång till sin spellista före begäran om radering, kan den virtuella röstassistentens leverantörer radera den muntliga begäran, men inte de tidigare följderna av denna begäran (raderingen kommer inte att påverka användarens spellista).

164. Baserat på ovanstående, om samma personuppgifter behandlas för olika behandlingssyften ska de personuppgiftsansvariga tolka begäran om radering som en tydlig signal att avbryta behandlingen av uppgifter för alla syften som saknar rättsligt undantag.

Enligt villkoren i artikel 21.1 i den allmänna dataskyddsförordningen ska uppgifter som behandlas på grundval av ett berättigat intresse från den virtuella röstassistentens leverantörer inte utgöra ett undantag till rätten till radering, särskilt eftersom de registrerade inte rimligen förväntar sig att deras personuppgifter genomgår ytterligare behandling.

4.4 Rätt till dataportabilitet

165. Behandlingen av uppgifter som utförs av den virtuella röstassistentens leverantörer omfattas av dataportabilitet, eftersom behandlingar främst bygger på den registrerades samtycke (enligt artikel 6.1 a, eller enligt artikel 9.2 a vad gäller särskilda kategorier av personuppgifter), eller på ett avtal i vilket den registrerade är part enligt artikel 6.1 b.

166. I praktiken ska rätten till dataportabilitet underlätta bytet mellan olika leverantörer av virtuella röstassistenter. När virtuella röstassistenter hanteras i en digital miljö och den registrerades röst spelas in en applikation eller på en plattform ska i synnerhet rätten till dataportabilitet beviljas för alla personuppgifter som den registrerade tillhandahåller. Vidare ska den personuppgiftsansvarige göra det möjligt för användarna att direkt hämta sina personuppgifter från sin användararea, som ett självbetjäningsverktyg. Användarna ska också kunna utöva denna rättighet via röstkommando.

167. Leverantörer och utvecklare av virtuella röstassistenter bör ge de registrerade långtgående kontroll över sina personuppgifter så att de kan överföra sina personuppgifter från en leverantör av virtuella röstassistenter till en annan. De registrerade bör därför få sina personuppgifter levererade till den personuppgiftsansvarige, i ett strukturerat, allmänt använt och maskinläsbart format liksom genom metoder[57] som hjälper till att besvara begäran om dataportabilitet (såsom nedladdningsverktyg och applikationsprogrammeringsgränssnitt – ”Application Programming Interfaces”)[58]. Såsom framgår av ”Guidelines on the right to data portability” (riktlinjer om rätten till dataportabilitet) ska den personuppgiftsansvarige vid en

[57] Se som illustration artikel 29-gruppens resonemang i ”Guidelines on the right to data portability – endorsed by the EDPB” (riktlinjer om rätten till dataportabilitet – godkända av EDPB), s. 16:
”*Tekniskt ska de personuppgiftsansvariga utforska och bedöma två olika och kompletterande sätt att tillgängliggöra portabla uppgifter för de registrerade eller för andra personuppgiftsansvariga:*
en direkt överföring av hela datasetet av portabla uppgifter (eller flera utvinningar av delar av hela datasetet);
ett automatiserat verktyg som medger utvinning av relevanta uppgifter.
Det andra sättet kan föredras av personuppgiftsansvariga vid komplicerade och stora dataset, eftersom det medger utvinning av en valfri del av det dataset som är relevant för den registrerade vid dennes begäran, kan hjälpa till att minimera risken, och möjligen göra det möjligt att använda synkronisering av uppgifter (t.ex. i samband med normal kommunikation mellan personuppgiftsansvariga). Det kan vara ett bättre sätt att säkerställa överensstämmelse för den ”nya” personuppgiftsansvarige, och skulle vara god praxis vid minskningen av integritetsrisker för den ursprungliga personuppgiftsansvarige”.

[58] I detta sammanhang gäller följande: Article 29 Working Party Guidelines on the right to data portability – endorsed by the EDPB, s. 1.

stor eller komplicerad insamling av personuppgifter, vilket här kan vara fallet, tillhandahålla en översikt ”*i en koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk*” (se artikel 12.1 i den allmänna dataskyddsförordningen) så att de registrerade alltid innehar tydlig information om vilka uppgifter de ska ladda ned eller överföra till en annan personuppgiftsansvarig för ett visst syfte. Registrerade ska till exempel kunna använda programvaruapplikationer för att lätt identifiera, känna igen och behandla specifika uppgifter från den.

168. Denna rätt skulle särskilt göra att användaren för eget bruk kan hämta de uppgifter som han/hon har förmedlat via rösten (t.ex. historiken över röstinteraktioner) och inom ramarna för upprättandet av sitt användarkonto (t.ex.: förnamn och efternamn).

169. För en fullständig tillämpning av den registrerades rättigheter inom ramen för en digital inre marknad ska konstruktörer av virtuella röstassistenter och applikationsutvecklare särskilt ta fram gemensamma maskinläsbara format som underlättar uppgiftsformatets driftskompatibilitet mellan virtuella röstassistentsystem[59], däribland standardformaten för röstdata. Tekniken ska struktureras för att säkerställa att de behandlade personuppgifterna, inräknat röstdatan, kan enkelt och fullständigt återanvändas av den nya personuppgiftsansvarige[60].

170. Vad gäller formatet ska de virtuella röstassistenternas leverantörer tillhandahålla personuppgifter genom allmänt använda öppna format (t.ex. mp3, wav, csv, gsm, osv.) tillsammans med lämpliga metadata för att exakt beskriva innebörden av den information som utbyts.[61]

5 BILAGA: AUTOMATISK TALIGENKÄNNING, TALSYNTES OCH BEARBETNING AV NATURLIGT SPRÅK

171. I enlighet med signalbehandlingens teoretiska grunder, särskilt Claude Shannons informations- och provtagningsteorier, har automatisk talbehandling blivit en grundkomponent i ingenjörsvetenskapen. I skärningspunkten mellan fysik (akustik, vågfortplantning), tillämpad matematik (modellering, statistik), datavetenskap (algoritmer, inlärningstekniker) och humaniora (perception, resonemang) har talbehandling snabbt delats upp i flera olika studieämnen: identifiering och verifiering av talaren, automatisk taligenkänning, röstsyntes, detektering av känslor, osv. De senaste femton åren på ett ungefär har vetenskapsgrenen som helhet genomgått en betydande utveckling som flera faktorer har bidragit till: förbättrade metoder, en signifikant ökad beräkningskapacitet och större mängder tillgängliga data.

[59] Se i detta hänseende skäl 68 i ”GDPR: WP29 Guidelines on the right to data portability – endorsed by the EDPB”, s. 17.

[60] ”*I detta hänseende förordas det i skäl 68 att de personuppgiftsansvariga tar fram driftskompatibla format som möjliggör dataportabilitet men utan att de personuppgiftsansvariga förpliktas att anta eller upprätthålla behandlingssystem som är tekniskt kompatibla. I den allmänna dataskyddsförordningen förbjuds dock personuppgiftsansvariga att upprätta hinder för överföringen*” – ”WP29 Guidelines on the right to data portability – endorsed by the EDPB”, s. 5.

[61] EDPB förordar på det bestämdaste att industrins intressenter och branschorganisationer samarbetar om en gemensam uppsättning driftskompatibla standarder och format för att uppfylla kraven på rätten till dataportabilitet.

5.1 Automatisk taligenkänning (ASR)

172. I automatisk taligenkänning (även kallat tal till text) brukade tre distinkta stadier ingå, som avser att 1) bestämma de uttalade fonemen med hjälp av en akustisk modell, 2) bestämma de uttalade orden med hjälp av en fonetisk ordbok, 3) transkribera den ordföljd (mening) som troligast uttalades, med hjälp av en språkmodell. Framgångarna till följd av djupinlärning (en maskininlärningsteknik) gör att många system idag erbjuder en ”obruten" automatisk taligenkänning. Detta gör att den komplicerade träningen av tre olika modeller inte behöver genomgås samtidigt som bättre prestanda erbjuds vad gäller resultat och behandlingstid. Nästan all större digitala aktörer erbjuder nu sina egna implementeringar av automatisk taligenkänning som lätt kan användas av API-system, men också öppna källkodssystem är tillgängliga (DeepSpeech[62] eller Kaldi[63] till exempel).

5.2 Bearbetning av naturligt språk (NLP)

173. Bearbetning av naturligt språk är ett tvärvetenskapligt område som täcker lingvistik, datavetenskap och artificiell intelligens och som har som mål att skapa verktyg för bearbetning av naturligt språk för olika applikationer. Områdena för forskning och applikationer är många: syntaxanalys, maskinöversättning, automatisk textgenerering och -sammanfattning, stavningskontroll, frågebesvarande system, textutvinning, igenkänning av namngiven enhet, känsloanalys, osv. Bearbetning av naturligt språk syftar rent konkret till att ge datorer förmåga att läsa, förstå och härleda betydelse ur mänskliga språk. Det är en utmaning att ta fram applikationer för att bearbeta naturligt språk, eftersom dataverktyg brukar behöva människor som interagerar med dem på ett programspråk som är formellt, exakt i sin betydelse, otvetydigt och högt strukturerat. Det mänskliga språket är dock inte alltid exakt. Istället är det ofta mångtydigt, med en språklig struktur som kan vara beroende av många komplicerade variabler, såsom slang, regionala dialekter och sociala sammanhang.

174. Syntax och semantisk analys är två viktiga tekniker vid bearbetning av naturligt språk. Syntax beskriver hur orden ordnas i en mening för att de ska bli grammatiskt begripliga. Bearbetning av naturligt språk använder syntax för att bedöma betydelse från ett språk som bygger på grammatiska regler. Använda syntaxtekniker är till exempel parsning (grammatisk analys av en mening), ordsegmentering (som delar in en lång text i enheter), meningsbrytning (som sätter gränser för meningar i långa texter), morfologisk segmentering (som delar in ord i grupper) och härledning (som delar in ord med inneboende inflektion i rotformer). Semantik inbegriper ordens användning och bakomliggande innebörd. Bearbetning av naturligt språk tillämpar algoritmer för att förstå meningarnas betydelse och struktur. Tekniker som bearbetning av naturligt språk använder med semantik är klargörande av ords betydelse (där ett ords innebörd härleds utifrån sammanhanget), igenkänning av namngiven enhet (där ord bestäms som kan kategoriseras till grupper), och generering av naturligt språk (där en databas används för att bestämma semantiken bakom orden). Medan tidigare strategier för bearbetning av naturligt språk har använt regelbaserade strategier, där enkla maskininlärningsalgoritmer fick söka efter ord och fraser i en text och mottog specifika svar när dessa fraser uppträdde, är de aktuella strategierna för bearbetning av naturligt språk baserade på djupinlärning, en AI-typ som undersöker och använder mönster i data för att förbättra ett programs förståelse.

5.3 Talsyntes

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

175. Talsyntes är den artificiella produktionen av mänskligt tal. Talsyntes har främst genomförts med hjälp av kombinerade röstenheter som lagras i en databas. Denna teknik består i att, från alla inspelningar av en skådespelare som tidigare transkriberats till fonem, stavelser och ord, välja ut de byggstenar av ljud som motsvarar de ord man vill att den virtuella röstassistenten ska uttala, och sätta ihop dem en efter en till en begriplig mening med naturligt uttal. Alternativt kan en talsyntetisator införliva en modell av talorganen och andra mänskliga röstrelaterade kännetecken för att modellera en rösts parametrar såsom intonation, rytm och klangfärg, genom generativa statistiska modeller (t.ex. WaveNet[64], Tacotron[65] eller DeepVoice[66]) och för att skapa ett fullständigt syntetiskt röstresultat.

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

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

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