

# Retningslinjer



## **Retningslinjer 02/2021 vedrørende digitale stemmestyrede assistenter**

**Version 2.0**

**Vedtaget den 7. juli 2021**

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

## Versionsoversigt

Version 2.0	7. juli 2021	Vedtagelse af retningslinjerne efter offentlig høring
Version 1.0	9. marts 2021	Vedtagelse af retningslinjerne til offentlig høring

## RESUMÉ

En digital stemmestyret assistent (i det følgende benævnt "digital assistent") er en tjeneste, der forstår talekommandoer og udfører dem eller interagerer med andre IT-systemer efter behov. Digitale assistenter findes i dag på de fleste smartphones og tablets, traditionelle computere og, i de seneste år, også separate enheder som intelligente højttalere.

Digitale assistenter fungerer som grænseflade mellem brugere og deres databehandlingsenheder og onlinetjenester som for eksempel søgemaskiner og onlinebutikker. Digitale assistenter har som følge af deres rolle adgang til en enorm mængde personoplysninger, herunder alle brugeres kommandoer (f.eks. browserdata og søgehistorik) og svar (f.eks. kalenderaftaler).

Langt de fleste digitale stemmestyrede assistenttjenester er designet af ganske få designere. Digitale assistenter kan dog fungere sammen med applikationer, der er programmeret af tredjeparter (udviklere af applikationer til digitale assistenter) med henblik på at stille mere avancerede kommandoer til rådighed.

En digital assistent kræver en terminalenhed med mikrofoner og højttalere for at fungere korrekt. Enheden lagrer tale og andre data, som de digitale assistenter, der i øjeblikket er på markedet, overfører til fjernservere for digitale assistenter.

Dataansvarlige, der leverer digitale stemmestyrede assistenttjenester, og deres databehandlere skal derfor tage højde for både databeskyttelsesforordningen<sup>1</sup> og e-databeskyttelsesdirektivet<sup>2</sup>.

Disse retningslinjer peger på nogle af de mest relevante udfordringer med hensyn til overholdelse og indeholder anbefalinger til relevante interessenter om håndtering af udfordringerne.

Dataansvarlige, der leverer digitale stemmestyrede assistenttjenester via skærmløse terminalenheder, skal i henhold til databeskyttelsesforordningen informere brugerne ved installation af den digitale assistent eller ved installation eller første brug af en assistent-app. Vi anbefaler derfor, at udbydere/designere og udviklere af digitale assistenter udvikler stemmestyrede grænseflader med henblik på at give den obligatoriske information.

I øjeblikket kræver alle digitale assistenter, at mindst én bruger tilmelder sig tjenesten. Som følge af forpligtelsen til databeskyttelse gennem design og databeskyttelse gennem standardindstillinger bør udbydere/designere og udviklere af digitale assistenter overveje, om det er nødvendigt at have en registreret bruger for hver af funktionaliteterne.

Den brugerkonto, der anvendes af mange designere af digitale assistenter, samler den digitale stemmestyrede assistenttjeneste med andre tjenester som for eksempel e-mail eller videostreaming. Det er Databeskyttelsesrådets opfattelse, at dataansvarlige bør afholde sig fra sådanne metoder, da de indebærer brug af omfattende og komplekse persondatapolitikker, som ikke ville være i overensstemmelse med databeskyttelsesforordningens gennemsigtighedsprincip.

---

<sup>1</sup> Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (i det følgende benævnt "databeskyttelsesforordningen").

<sup>2</sup> Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation), ændret ved direktiv 2006/24/EF og direktiv 2009/136/EF (i det følgende benævnt "e--databeskyttelsesdirektivet").

Retningslinjerne omhandler fire af de mest almindelige formål med en digital assistents behandling af personoplysninger: udførelse af anmodninger, forbedring af maskinlæringsmodellen for digitale assistenter, biometrisk identifikation og profilering af individuelt tilpasset indhold og markedsføring.

For så vidt som personoplysningerne i en digital assistent behandles med henblik på at udføre brugerens anmodninger, dvs. som strengt nødvendigt for at kunne levere en tjeneste, som brugeren har anmodet om, er dataansvarlige undtaget fra kravet om forudgående samtykke i henhold til artikel 5, stk. 3, i e-databeskyttelsesdirektivet. Omvendt vil et sådant samtykke i henhold til artikel 5, stk. 3, i e-databeskyttelsesdirektivet være nødvendigt med henblik på at lagre eller opnå adgang til oplysninger til andre formål end at udføre brugernes anmodning.

Nogle digitale assistenttjenester opbevarer personoplysninger, indtil brugerne stiller krav om, at de slettes. Dette er ikke i overensstemmelse med princippet om opbevaringsbegrænsning. Digitale assistenter bør ikke opbevare personoplysninger længere end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles.

Hvis en dataansvarlig bliver bekendt med (f.eks. som følge af kvalitetskontrolprocesser), at der utilsigtet er blevet indsamlet personoplysninger, bør den pågældende kontrollere, at der er et gyldigt retsgrundlag for de enkelte formål med behandlingen af disse oplysninger. Er dette ikke tilfældet, bør de utilsigtet indsamlede personoplysninger slettes.

Digitale assistenter kan behandle flere registreredes personoplysninger. Udbydere/designere af digitale assistenter bør derfor implementere adgangskontrolmekanismer for at sikre personoplysningers fortrolighed, integritet og tilgængelighed. Nogle traditionelle adgangskontrolmekanismer, f.eks. adgangskoder, er imidlertid ikke egnede i forbindelse med digitale assistenter, da de ville skulle siges højt. Retningslinjerne indeholder nogle betragtninger om dette, herunder et særligt afsnit om behandling af særlige kategorier af personoplysninger til biometrisk identifikation.

Udbydere/designere af digitale assistenter bør tage i betragtning, at der i forbindelse med optagelsen af en brugers tale kan blive optaget andre personers tale eller personoplysninger, såsom baggrundsstøj, som ikke er nødvendige for tjenesten. Designere af digitale assistenter bør derfor overveje så vidt muligt at anvende teknologier, der filtrerer unødvendige personoplysninger fra og sikrer, at kun brugerens tale optages.

Ved vurderingen af behovet for en konsekvensanalyse vedrørende databeskyttelse finder Databeskyttelsesrådet det meget sandsynligt, at digitale assistenttjenester falder ind under de kategorier og betingelser, der kræver en konsekvensanalyse vedrørende databeskyttelse.

Dataansvarlige, der leverer digitale assistenttjenester, bør sikre, at brugerne kan udøve deres rettigheder som registrerede ved hjælp af let forståelige talekommandoer. Udbydere/designere af digitale assistenter og udviklere af assistent-apps bør ved processens afslutning informere brugerne om, at der er taget højde for deres rettigheder, enten i form af tale eller ved at sende en skriftlig meddelelse til brugerens mobiltelefon, konto eller ethvert andet middel, som brugeren har valgt.

## Indholdsfortegnelse

<b>RESUMÉ</b> .....	3
<b>1 GENERELT</b> .....	7
<b>2 DEN TEKNISKE BAGGRUND</b> .....	8
2.1 Digitale stemmestyrede assistenters grundlæggende karakteristika .....	8
2.2 Aktører i økosystemet for digitale assistenter .....	9
2.3 Trinvis beskrivelse .....	10
2.4 Aktiveringskommandoer .....	11
2.5 Taleuddrag ("snippets") og maskinlæring .....	11
<b>3 DATABESKYTTELSESELEMENTER</b> .....	12
3.1 Retlig ramme .....	12
3.2 Identifikation af databehandling og interesser.....	14
3.2.1 Behandling af personoplysninger .....	14
3.2.2 Dataansvarliges og databehandlers behandling .....	16
3.3 Gennemsigtighed .....	18
3.4 Formålsbegrænsning og retsgrundlag.....	22
3.4.1 Udføre brugernes anmodninger.....	23
3.4.2 Forbedring af den digitale assistent ved at træne ML-systemerne og foretage manuel kontrol af tale og transskriptioner .....	24
3.4.3 Brugeridentifikation (ved hjælp af taledata).....	25
3.4.4 Brugerprofilering med henblik på individuelt tilpasset indhold eller markedsføring... ..	25
3.5 Behandling af personoplysninger om børn .....	27
3.6 Opbevaring af data .....	27
3.7 Sikkerhed .....	29
3.8 Behandling af særlige kategorier af oplysninger.....	32
3.8.1 Generelle betragtninger ved behandling af særlige kategorier af data.....	32
3.8.2 Generelle betragtninger ved behandling af biometriske data .....	32
3.9 Dataminimering.....	34
3.10 Ansvarlighed .....	35
3.11 Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger.....	35
<b>4 Mekanismer til udøvelse af registreredes rettigheder</b> .....	36
4.1 Ret til indsigt.....	36
4.2 Ret til berigtigelse.....	37
4.3 Ret til sletning.....	38
4.4 Ret til dataportabilitet.....	39

5	Bilag: Automatisk talegenkendelse, talesyntese og behandling af naturligt sprog .....	40
5.1	Automatisk talegenkendelse (ASR) .....	40
5.2	Behandling af naturligt sprog (NLP) .....	41
5.3	Talesyntese .....	41

## Det Europæiske Databeskyttelsesråd har —

under henvisning til artikel 70, stk. 1, litra j) og litra e), i Europa-Parlamentets og Rådets forordning 2016/679/EU af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (i det følgende benævnt "databeskyttelsesforordningen"),

under henvisning til EØS-aftalen, særlig bilag XI og protokol 37 til EØS-aftalen, som ændret ved Det Blandede EØS-Udvalgs afgørelse nr. 154/2018 af 6. juli 2018<sup>3</sup>,

under henvisning til artikel 12 og artikel 22 i forretningsordenen —

### VEDTAGET FØLGENDE RETNINGSLINJER:

## 1 GENERELT

1. De seneste teknologiske fremskridt har i høj grad øget digitale stemmestyrede assistenters pålidelighed og popularitet. Digitale assistenter er blandt andet blevet integreret i smartphones, tilkoblede køretøjer, intelligente højttalere og smart-tv'er. Denne integration har givet digitale assistenter adgang til oplysninger af intim karakter, som, hvis de ikke håndteres korrekt, kan skade privatpersoners ret til databeskyttelse og privatlivets fred. Digitale assistenter og de enheder, der integrerer disse, er derfor blevet undersøgt af en række datatilsynsmyndigheder.
2. Der er flere fordele ved at gøre brug af stemmestyret interaktion, f.eks. interaktion af naturlig karakter, der ikke kræver specifik læring af brugerne, hurtig udførelse af kommandoer samt et større aktionsfelt, hvilket igen kan betyde hurtigere adgang til information. Brug af stemmestyret giver dog også problemer med hensyn til at tolke meddelelsen korrekt som følge af eksempelvis lydsignalets forskellighed i forskellige højttalere, akustik, sprogets tvetydighed osv.
3. I praksis er den primære begrundelse for at anskaffe sig en digital assistent stadig, at opgaver smidiggøres og forenkles. Det gælder for eksempel i forbindelse med at foretage og besvare et opkald og at sætte en timer, navnlig når brugeren ikke har hænderne fri. Stemmestyret er den vigtigste anvendelse, der er udtænkt af designere af digitale assistenter. Ved at forenkle udførelsen af opgaver (tænde lyset, regulere varmen, køre rullegardinerne ned osv.) og centralisere opgaverne i ét værktøj, der nemt kan aktiveres online, passer digitale assistenter godt ind i diskursen som et værktøj, der faciliterer udførelsen af opgaver i hjemmet. Stemmestyret kan foruden til privat brug og brug i hjemmet være interessant i faglige miljøer, hvor det er vanskeligt at håndtere computerværktøjer og anvende skriftlige kommandoer (f.eks. inden for industriproduktion).
4. Teoretisk set kan dem, der har størst nytte af stemmestyret, være personer med funktionsnedsættelser eller plejekrævende personer, som kan have vanskeligt ved at anvende traditionelle grænseflader. Digitale assistenter kan gøre adgangen til information og

---

<sup>3</sup> Henvisninger til "medlemsstater" i dette dokument skal forstås som henvisninger til "EØS-medlemsstater".

computerressourcer nemmere og dermed fremme inklusiv logik, da brugen af tale gør det muligt at overvinde de vanskeligheder, visse brugergrupper har med skriftsproget.

5. Endelig er sundhed også et område, hvor der er mange muligheder for brug af samtalerobotter, hvad enten de er stemmestyrede eller ej. Under covid-19-pandemien blev der eksempelvis anvendt forskellige samtalerobotter til at foretage en indledende diagnose af borgere, der henvendte sig. På langt sigt forventer nogle, at interaktion mellem mennesker og digitale assistenter kan få betydning for hele patientbehandlingsprocessen, ikke kun med henblik på trivsel og forebyggelse, men også i forbindelse med behandling og støtte.
6. Der findes i øjeblikket mere end 3 milliarder smartphones, og de har allesammen integrerede digitale assistenter, hvoraf de fleste er aktiveret som standard. Nogle af de mest udbredte operativsystemer i personlige og bærbare computere integrerer også digitale assistenter. Den seneste stigning i antallet af intelligente højttalere (der blev solgt 147 millioner i 2019<sup>4</sup>) bringer digitale assistenter ind i millioner af hjem og kontorer. De nuværende digitale assistenters design giver dog ikke mulighed for automatisk autentifikations- eller adgangskontrolmekanismer.
7. Dette dokument har til formål at udstikke retningslinjer for anvendelse af databeskyttelsesforordningen i forbindelse med digitale assistenter.

## 2 DEN TEKNISKE BAGGRUND

### 2.1 Digitale stemmestyrede assistenters grundlæggende karakteristika

8. En digital stemmestyret assistent er en softwareapplikation, der giver mulighed for mundtlig dialog med en bruger i naturligt sprog.
9. Naturligt sprog har en semantik, der er specifik for menneskers sprog. Afhængigt af sprogets karakteristika og ordforrådets diversitet kan den samme instruks formuleres på forskellige måder, mens nogle kommandoer kan forekomme ens, men vedrøre to forskellige objekter. Der anvendes derfor ofte inferensmekanismer til at løse disse tvetydigheder, for eksempel afhængigt af, hvad der tidligere er blevet sagt; tidspunktet for, hvornår instruksen blev givet; stedet; personens interesser osv.
10. En digital assistent kan opdeles i moduler, der gør det muligt at udføre forskellige opgaver: lydoptagelse og -gengivelse, automatisk taletransskription (tale til tekst), automatisk sprogbehandling, dialogstrategier, adgang til ontologier (datasæt og strukturerede koncepter vedrørende et givet område) og eksterne videnskilder, sproggenerering, talesyntese (tekst til tale) osv. Konkret bør den digitale assistent give mulighed for interaktion med henblik på at udføre handlinger (f.eks. "tænd radioen", "sluk lyset") eller få adgang til viden (f.eks. "hvordan bliver vejret i morgen?", "kører toget kl. 7:43?"). Den spiller dermed rollen som mellemmand og orkestrator, som skal sikre, at brugerens opgaver udføres.
11. I praksis er en digital assistent ikke en intelligent højttaler, men en intelligent højttaler kan udstyres med en assistent. De to forveksles ofte, men sidstnævnte er kun en materiel inkarnation af førstnævnte. En digital assistent kan installeres i en smartphone, en intelligent højttaler, et tilkøbt ur, et køretøj, et husholdningsapparat osv.

---

<sup>4</sup> Jf. for eksempel en pressemeddelelse af 1. august 2019 fra Hamborgs datatilsynsmyndighed: <https://datenschutz-hamburg.de/pressemitteilungen/2019/08/2019-08-01-google-assistant>



12. Organiseringen af den underliggende databehandling kan omfatte en lang række mønstre af informationsstrømme. Tre hoveddele kan isoleres:

**Den fysiske del:** Hardwareelementet, som den digitale assistent er bygget ind i (smartphone, højttaler, smart-tv osv.), og som indeholder mikrofoner, højttalere samt netværks- og databehandlingskapacitet (mere eller mindre udviklet ud fra omstændighederne).

**Software delen:** Den del, der ret beset implementerer interaktionen mellem menneske og maskine, og som integrerer modulerne for automatisk talegenkendelse, behandling af naturligt sprog, dialog og talesyntese. Betjeningen kan ske direkte i det fysiske udstyr, men finder ofte sted online.

**Ressourcerne:** Eksterne data som indholdsdata-baser, ontologier og forretningsapplikationer, der leverer viden (f.eks. "hvad er klokken på USA's vestkyst" eller "læs mine e-mails") eller gør det muligt at udføre den ønskede handling på en konkret måde (f.eks. "øg temperaturen med 1,5 °C").

13. Digitale assistenter gør det muligt at installere tredjepartskomponenter eller apps, der udvider assistenternes kernefunktioner. Komponenterne i de enkelte digitale assistenter kaldes noget forskelligt, men de indebærer alle udveksling af brugernes personoplysninger mellem designeren af den digitale assistent og udvikleren af appen.
14. Selv om de fleste digitale assistenter ikke deler taleuddrag ("snippets") med appudviklerne, behandler disse aktører stadig personoplysninger. Desuden modtager appudvikleren, afhængigt af arten af den leverede funktionalitet, intentioner og informationsvariabler (slots), som kan omfatte følsomme oplysninger som for eksempel helbredsoplysninger.

## 2.2 Aktører i økosystemet for digitale assistenter

15. En digital assistent kan involvere et stort antal aktører og mellemlid igennem gennemførelseskæden. I praksis kan der fastslås op til fem forskellige aktører. Afhængigt af forretningsmodeller og teknologiske valg kan nogle aktører dog have forskellige kombinationer af roller, f.eks. designer og integrator eller designer og applikationsudvikler:
  - a. **Udbyder (eller designer) af den digitale assistent:** Ansvarlig for udviklingen af den digitale assistent, designer og fastlægger dens muligheder og standardfunktioner: aktiveringsmetoder, valg af arkitektur, dataadgang, håndtering af dataposter, hardware-specifikationer osv.
  - b. **Udvikler af applikation til digital assistent:** Ligesom for mobilapplikationer udvikler udvikleren applikationer, der udvider den digitale assistents standardfunktioner. Det kan kun ske ved at tage højde for de udviklingsmæssige begrænsninger fra designerens side.
  - c. **Integrator:** Producent af tilkoblede objekter, der ønsker at udstyre disse med en digital assistent. Integratoren bør tage højde for de krav, designeren har fastsat.
  - d. **Ejer:** Ansvarlig for de fysiske områder, hvor mennesker befinder sig (overnatningssteder, faglige miljøer, udlejningsbiler osv.). Ejeren ønsker at stille en digital assistent til rådighed for sin målgruppe (eventuelt med specifikke applikationer).

- e. **Bruger:** Slutleddet i værdikæden for digitale assistenter. Brugeren kan anvende den digitale assistent i forskellige enheder (højtaler, tv, smartphone, ur osv.), afhængigt af hvordan og hvor assistenten er blevet installeret.

### 2.3 Trinvis beskrivelse

16. For at en digital assistent kan udføre en handling eller få adgang til oplysninger, skal der udføres en række opgaver:
  - 1) Den digitale assistent, installeret i en enhed (smartphone, højtaler, køretøj), er på standby. Det betyder helt nøjagtigt, at den hele tiden lytter. Men så længe der ikke er registreret en specifik aktiveringskommando, transmitteres der ingen lyd fra den enhed, der modtager stemmeinputtet, og den eneste proces, der finder sted, er registrering af aktiveringskommandoen. Der er en buffer på et par sekunder til dette formål (læs nærmere i næste afsnit).
  - 2) Brugeren siger aktiveringskommandoen, hvorefter den digitale assistent lokalt sammenligner lyden med aktiveringskommandoen. Hvis de matcher hinanden, åbner den digitale assistent en lyttekanal, hvorefter lydindholdet straks transmitteres.
  - 3) Hvis kommandoen udføres online, vil der i mange tilfælde blive foretaget endnu en kontrol af udtalen af nøgleord på serversiden for at begrænse uønsket aktivering.
  - 4) Brugeren fremsætter sin anmodning, som straks sendes til udbyderen af den digitale assistent. Stemmeinputtet transskriberes derefter automatisk (tale til tekst).
  - 5) Kommandoen tolkes ved hjælp af teknologi til behandling af naturligt sprog (NLP). Meddelelsens intentioner trækkes ud, og informationsvariabler (slots) identificeres. Derefter anvendes dialogstyring til at angive det interaktionsscenario, der skal implementeres hos brugeren ved at stille relevante svarmuligheder til rådighed.
  - 6) Hvis kommandoen omfatter en funktionalitet fra en tredjepartsapp (færdighed, handling, genvej osv.), sender udbyderen af den digitale assistent meddelelsens intentioner og informationsvariabler (slots) til appudvikleren.
  - 7) Et svar tilpasset brugerens anmodning identificeres — svaret "Jeg kan ikke svare på dit spørgsmål" er et tilpasset svar, hvis den digitale assistent ikke er i stand til at tolke anmodningen korrekt. Om nødvendigt anvendes der onlineresourcer: offentligt tilgængelige vidensdatabaser (onlineencyklopædier osv.) eller via autentifikation (bankkonto, musikapplikation, kundekonto til onlinekøb osv.), og informationsvariablerne (slots) udfyldes med den erhvervede viden.
  - 8) Der udarbejdes en svarsætning, og/eller der identificeres en handling (sænkning af persienner, øgning af temperatur, afspilning af et stykke musik, besvarelse af et spørgsmål osv.). Sætningen sammenfattes (tekst til tale), og/eller den handling, der skal udføres, sendes til den pågældende enhed.
  - 9) Den digitale assistent vender tilbage til standby.

Bemærk, at selv om hovedparten af al stemmestyret aktivitet i øjeblikket foregår på fjernservere, arbejder nogle udbydere af digitale assistenter på at udvikle systemer, der kan udføre en del af denne aktivitet lokalt.<sup>5</sup>

## 2.4 Aktiveringskommandoer

17. En digital assistent kan kun anvendes, hvis den er "aktiv". Assistenten skifter således til en aktiv lyttetilstand for at kunne modtage instrukser og kommandoer fra brugeren. Selvom aktivering i nogle tilfælde også kan finde sted ved en fysisk handling (f.eks. tryk på en knap, tryk på en intelligent højttaler), er næsten alle digitale assistenter på markedet baseret på, at assistenten skal registrere en aktiveringskommando eller et aktiveringsord (kaldes også "hot word") for at skifte til aktiv lyttetilstand.
18. Assistenten kræver brug af mikrofon samt en vis mindre beregningsmæssig kapacitet for at registrere, om nøgleordet er blevet sagt. Denne analyse, som finder sted kontinuerligt, fra det øjeblik assistenten er tændt, udføres udelukkende lokalt. Først når nøgleordet er blevet genkendt, behandles lydoptagelserne med henblik på tolkning og udførelse af kommandoen, hvilket i mange tilfælde betyder, at de sendes til fjernservere via internettet. Registrering af nøgleord er baseret på maskinlæringsteknikker. Den største udfordring ved at anvende sådanne metoder er, at registreringen er baseret på sandsynlighed. For hvert ord eller kommando, der siges, afgiver systemet således en tillidsscore, ud fra om nøgleordet reelt er blevet sagt. Hvis scoren viser sig at være højere end en forudfastsat tærskelværdi, anses dette for at være tilfældet. Et sådant system er derfor ikke uden fejl: I nogle tilfælde registreres aktivering ikke, selv om nøgleordet er blevet sagt (falsk afvisning), og i andre tilfælde registreres der aktivering, selv om brugeren ikke har sagt nøgleordet (falsk accept).
19. I praksis bør der findes et acceptabelt kompromis mellem disse to typer fejl for at definere tærskelværdien. Men da forkert registrering af nøgleordet kan have til følge, at der sendes lydoptagelser, vil der sandsynligvis ske uventede og uønskede overførsler af data. Meget ofte anvender assistentudbydere, der foretager behandling online, en totrinsmekanisme til denne registrering: Et første trin, der er indbygget lokalt på enhedsniveau, og et andet trin, der udføres på fjernservere, hvor den næste databehandling finder sted. I dette tilfælde fastsætter udviklere normalt en relativt lav tærskelværdi med henblik på at forbedre brugeroplevelsen og sikre, at nøgleordet, når det siges af brugeren, næsten altid bliver genkendt — også selv om det betyder "overregistrering" — ligesom de implementerer endnu et registreringstrin på serversiden, som er mere restriktivt.

## 2.5 Taleuddrag ("snippets") og maskinlæring

20. Digitale assistenter udfører på grundlag af maskinlæringsmetoder en lang række opgaver (registrering af nøgleord, automatisk talegenkendelse, behandling af naturligt sprog, talesyntese osv.), hvilket gør det nødvendigt at indsamle, udvælge, mærke osv. store datasæt.
21. Over- eller underrepræsentationen af bestemte statistiske karakteristika kan påvirke udviklingen af maskinlæringsbaserede opgaver og efterfølgende afspejle disse i beregningerne og dermed i funktionsmåden. Det betyder, at ikke bare dataenes kvantitet, men også deres kvalitet spiller en væsentlig rolle for læringsprocessens smidighed og pålidelighed.

---

<sup>5</sup> Dette omtales for eksempel her: <https://www.amazon.science/blog/alexas-new-speech-recognition-abilities-showcased-at-interspeech>

22. For at øge kvaliteten af den digitale assistent og forbedre de anvendte maskinlæringsmetoder kan designere af digitale assistenter ønske at få adgang til data vedrørende brug af enheden under virkelige forhold — dvs. taleuddrag ("snippets") — med henblik på at forbedre brugen.
23. Hvad enten det drejer sig om at kvalificere læringsdatabasen eller rette fejl, der opstår under brug af algoritmen, kræver læring og træning af systemer baseret på kunstig intelligens nødvendigvis menneskers medvirken. Denne del af arbejdet, der kaldes digital arbejdskraft, rejser spørgsmål om både arbejdsvilkår og sikkerhed. I den forbindelse har nyhedsmedier også rapporteret om tilfælde, hvor data er blevet overført mellem designere af digitale assistenter og underleverandører angiveligt uden de nødvendige garantier for beskyttelse af personoplysninger.

### 3 DATABESKYTTELSESELEMENTER

#### 3.1 Retlig ramme

24. Den relevante EU-lovramme for digitale assistenter er først og fremmest databeskyttelsesforordningen, idet behandling af personoplysninger udgør en central funktion i en digital assistent. Foruden databeskyttelsesforordningen fastsætter e-databeskyttelsesdirektivet<sup>6</sup> en konkret standard for alle aktører, der ønsker at lagre eller opnå adgang til oplysninger, der er lagret i en abonnents eller brugers terminaludstyr i EØS.
25. Smartphones, smart-tv og lignende IoT-enheder er eksempler på terminaludstyr i overensstemmelse med definitionen på "*terminaludstyr*"<sup>7</sup>. Selv om digitale assistenter i sig selv er softwaretjenester, fungerer de altid ved hjælp af en fysisk enhed som for eksempel en intelligent højttaler eller et smart-tv. **Digitale assistenter anvender elektroniske kommunikationsnet til at få adgang til disse fysiske enheder, der udgør "terminaludstyr" i e-databeskyttelsesdirektivets forstand. Derfor finder bestemmelserne i artikel 5, stk. 3, i e-databeskyttelsesdirektivet anvendelse, når digitale assistenter lagrer eller opnår adgang til oplysninger i den fysiske enhed, de er forbundet med.**<sup>8</sup>
26. Enhver behandling af personoplysninger i forbindelse med ovennævnte behandlingsaktiviteter, herunder behandling af personoplysninger, der er indhentet ved at

---

<sup>6</sup> Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation), ændret ved direktiv 2006/24/EF og direktiv 2009/136/EF (i det følgende benævnt "e-databeskyttelsesdirektiv").

<sup>7</sup> I artikel 1 i Kommissionens direktiv 2008/63/EF af 20. juni 2008 om konkurrence på markederne for teleterminaludstyr defineres "*terminaludstyr*" som a) "*alt udstyr, der direkte eller indirekte er tilsluttet et offentligt telekommunikationsnets grænseflade med henblik på at transmittere, behandle eller modtage informationer; i begge tilfælde, ved såvel direkte som indirekte tilslutning, kan denne etableres gennem ledning, lysleder eller elektromagnetisk; tilslutningen er indirekte, hvis der er indskudt et apparat mellem terminaludstyr og det offentlige grænsefladenet; b) satellitjordstationsudstyr*".

<sup>8</sup> Jf. Databeskyttelsesrådets retningslinjer 1/2020, punkt 12, vedrørende en lignende begrundelse for så vidt angår forbundne køretøjer (i det følgende benævnt "Databeskyttelsesrådets retningslinjer 1/2020"). Jf. også Databeskyttelsesrådets udtalelse 5/2019 om samspillet mellem e-databeskyttelsesdirektivet og databeskyttelsesforordningen, navnlig med hensyn til datatilsynsmyndighedernes kompetence, opgaver og beføjelser.

tilgå oplysninger i terminaludstyr, skal også have et retsgrundlag i henhold til artikel 6 i databeskyttelsesforordningen for at være lovlig.<sup>9</sup>

27. Eftersom den dataansvarlige, når denne søger at indhente samtykke til at lagre eller opnå adgang til oplysninger i henhold til artikel 5, stk. 3, i e-databeskyttelsesdirektivet, skal informere den registrerede om alle formålene med behandlingen (dvs. den "efterfølgende behandling") — herunder enhver behandling i forbindelse med ovennævnte aktiviteter — vil samtykke i henhold til databeskyttelsesforordningens artikel 6 generelt være det mest relevante retsgrundlag til at dække den efterfølgende behandling af personoplysningerne. Samtykke vil derfor sandsynligvis udgøre retsgrundlaget for både opbevaring og adgang til oplysninger, der allerede opbevares, og behandlingen af personoplysninger i forbindelse med ovennævnte behandlingsaktiviteter. Ved vurderingen af, hvorvidt artikel 6 i databeskyttelsesforordningen overholdes, bør der tages højde for, at behandlingen som helhed omfatter specifikke aktiviteter, som EU-lovgiveren har ønsket at beskytte yderligere.<sup>10</sup> Dataansvarlige skal desuden tage højde for indvirkningen på de registreredes rettigheder, når de fastlægger det relevante retsgrundlag, med henblik på at overholde princippet om rimelighed.<sup>11</sup> Bundlinjen er, at dataansvarlige ikke kan påberåbe sig databeskyttelsesforordningens artikel 6 for at mindske den yderligere beskyttelse, der er fastsat i artikel 5, stk. 3, i e-databeskyttelsesdirektivet.
28. Som vist i afsnit 2.3 (trin 2 og 3) kræver de digitale assistenter, der i øjeblikket er på markedet, adgang til de taledata, der opbevares af assistentenheden.<sup>12</sup> Derfor finder artikel 5, stk. 3, i e-databeskyttelsesdirektivet anvendelse. Anvendelsen af artikel 5, stk. 3, i e-databeskyttelsesdirektivet betyder, at lagring af oplysninger samt adgang til oplysninger, der allerede er lagret i en digital assistent, som hovedregel kræver slutbrugerens forudgående samtykke<sup>13</sup>, men tillader dog to undtagelser: for det første udførelse eller facilitering af overførsel af en meddelelse via et elektronisk kommunikationsnet, og for det andet i det omfang, det er strengt nødvendigt for at levere en informations-samfundstjeneste, som abonnenten eller brugeren udtrykkeligt har anmodet om.
29. Den anden undtagelse ("strengt nødvendigt for at levere en informations-samfundstjeneste, som abonnenten eller brugeren udtrykkeligt har anmodet om") vil gøre det muligt for en udbyder af digitale assistenttjenester at behandle brugernes data med henblik på at udføre brugernes anmodninger (jf. punkt 72 i afsnit 3.4.1) uden det samtykke, der er omhandlet i artikel 5, stk. 3, i e-databeskyttelsesdirektivet. Omvendt vil et sådant **samtykke i henhold til artikel 5, stk. 3, i e-databeskyttelsesdirektivet være nødvendigt** for at lagre eller opnå adgang til oplysninger til **andre formål end at efterkomme brugernes anmodning** (f.eks. brugerprofilering). Dataansvarlige ville skulle henføre samtykke til bestemte brugere. Dataansvarlige bør derfor kun behandle ikke-registrerede brugeres oplysninger med henblik på at efterkomme deres anmodninger.

---

<sup>9</sup> Ibid., punkt 41.

<sup>10</sup> Udtalelse 5/2019, punkt 41.

<sup>11</sup> Databeskyttelsesrådets retningslinjer 2/2019 for behandling af personoplysninger i henhold til artikel 6, stk. 1, litra b), i databeskyttelsesforordningen i forbindelse med levering af onlinetjenester til registrerede, version 2.0, 8. oktober 2019, punkt 1.

<sup>12</sup> Det er muligt, at fremtidige assistentenheder vil anvende edge computing-paradigmet og være i stand til i nogen grad at levere tjenesten lokalt. I så fald vil det være nødvendigt at revurdere anvendelsen af e-databeskyttelsesdirektivet.

<sup>13</sup> Jf. også Databeskyttelsesrådets retningslinjer 1/2020, punkt 14.

30. Digitale assistenter kan utilsigtet komme til at optage lyd fra personer, der ikke har til hensigt at anvende en digital assistenttjeneste. For det første kan aktiveringskommandoen i et vist omfang ændres afhængigt af den pågældende digitale assistent. Personer, der ikke er opmærksomme på denne ændring, kan utilsigtet komme til at bruge den nye aktiveringskommando. For det andet kan den digitale assistent registrere aktiveringskommandoen ved en fejl. Det er højst usandsynligt, at en af undtagelserne i artikel 5, stk. 3, i e-databeskyttelsesdirektivet finder anvendelse i tilfælde af utilsigtet aktivering. Desuden skal samtykke som defineret i databeskyttelsesforordningen være en "*utvetydig viljestilkendegivelse fra den registrerede*". Det er derfor højst usandsynligt, at et tilfælde af utilsigtet aktivering kan tolkes som et gyldigt samtykke. Hvis en dataansvarlig bliver bekendt med (for eksempel som følge af automatisk eller menneskelig kontrol), at den digitale assistenttjeneste utilsigtet har behandlet personoplysninger, bør den pågældende kontrollere, at der er et gyldigt retsgrundlag for de enkelte formål med behandlingen af disse oplysninger. Er dette ikke tilfældet, bør de utilsigtet indsamlede personoplysninger slettes.
31. Det skal desuden bemærkes, at de personoplysninger, som den digitale assistent behandler, kan have en meget følsom karakter. Assistenten kan indeholde oplysninger, der udgør personoplysninger i kraft af både indhold (betydningen af den talte tekst) og metainformation (den talendes køn, alder osv.). Databeskyttelsesrådet minder om, at taledata i sagens natur er biometriske personoplysninger.<sup>14</sup> Det betyder, at når sådanne oplysninger behandles med det formål at identificere en fysisk person entydigt, eller når de i sagens natur er eller anses for at være personoplysninger i en særlig kategori, skal behandlingen have et gyldigt retsgrundlag i henhold til artikel 6 og være ledsaget af en undtagelse fra artikel 9 i databeskyttelsesforordningen (jf. afsnit 3.7 nedenfor).

## 3.2 Identifikation af databehandling og interessenter

32. I betragtning af de mange muligheder for bistand, en digital assistent kan yde i mange forskellige situationer af en registrerets dagligdag,<sup>15</sup> er det vigtigt at bemærke, at behandlingen af personoplysninger, der også kan influeres af forskellige interessenter, skal foregå omhyggeligt.

### 3.2.1 Behandling af personoplysninger

33. Ud fra et databeskyttelsesmæssigt perspektiv er der en række konstanter, uanset typen af digital assistent (dvs. enhedstype, funktionaliteter, tjenester eller en kombination heraf), der kan anvendes af en registreret. Disse konstanter vedrører mangfoldigheden af personoplysninger, registrerede og databehandling.

#### **Mangfoldighed af personoplysningstyper**

34. Definitionen på personoplysninger i artikel 4, stk. 1, i databeskyttelsesforordningen omfatter en lang række forskellige oplysninger og finder anvendelse i en teknologineutral sammenhæng

---

<sup>14</sup> Artikel 4, stk. 14, i databeskyttelsesforordningen definerer biometriske data som "personoplysninger, der som følge af specifik teknisk behandling vedrørende en fysisk persons fysiske, fysiologiske eller adfærdsmæssige karakteristika muliggør eller bekræfter en entydig identifikation af vedkommende, såsom ansigtsbillede eller fingeraftryksoplysninger".

<sup>15</sup> For eksempel: i hjemmet, i et køretøj, på gaden, på arbejdspladsen eller i enhver anden privat, offentlig eller arbejdsrelateret sammenhæng eller en kombination af sammenhænge.

på alle oplysninger, der vedrører "*en identificeret eller identificerbar fysisk person*".<sup>16</sup> Enhver interaktion mellem en registreret og en digital assistent kan høre under denne definition. Når interaktionen finder sted, kan forskellige former for personoplysninger blive behandlet igennem hele brugen af den digitale assistent som beskrevet i afsnit 2.4.

35. Fra den oprindelige forespørgsel til det/den tilknyttede svar, tiltag eller opfølgning (f.eks. oprettelse af en ugentlig alarm) vil det første input af personoplysninger derfor generere efterfølgende personoplysninger. Det omfatter primære data (f.eks. kontodata, taleoptagelser, anmodningshistorik), observerede data (f.eks. enhedsdata, der vedrører en registreret, aktivitetslogfiler, onlineaktiviteter) samt afledte data (f.eks. brugerprofilering). Digitale assistenter bruger tale til at skabe forbindelse mellem brugere og alle de tilkoblede tjenester (f.eks. en søgemaskine, en onlinebutik eller en musikstreamingtjeneste), men i modsætning til andre mellemlid kan assistenten have fuld adgang til anmodningens indhold og dermed give assistentens designer en lang række personoplysninger afhængigt af formålet med behandlingen.
36. Mangfoldigheden af personoplysninger, der behandles ved anvendelse af en digital assistent, henviser også til en mangfoldighed af kategorier af personoplysninger, som man bør være særligt opmærksom på (jf. afsnit 3.7 nedenfor). Databeskyttelsesrådet minder om, at når der behandles særlige kategorier af oplysninger<sup>17</sup>, skal den dataansvarlige i henhold til databeskyttelsesforordningens artikel 9 fastslå en gyldig fravigelse fra forbuddet mod behandling i artikel 9, stk. 1, og et gyldigt retsgrundlag i henhold til artikel 6, stk. 1, under anvendelse af en relevant metode som identificeret i artikel 9, stk. 2. Udtrykkeligt samtykke kan være en af de relevante fravigelser, hvis samtykket er det retsgrundlag, der henvises til i artikel 6, stk. 1. I artikel 9 anføres det også (detaljeret), at medlemsstaterne kan indføre yderligere betingelser for behandling af biometriske oplysninger eller andre særlige kategorier af oplysninger.

### ***Mangfoldighed af registrerede***

37. Ved anvendelse af en digital assistent behandles personoplysninger fra den første interaktion med assistenten. For nogle registrerede forstås der ved dette købet af en digital assistent og/eller konfigurationen af en brugerkonto (dvs. registrerede brugere). For andre registrerede forstås der ved dette den første gang, de bevidst interagerer med en digital assistent tilhørende en anden registreret, som har købt og/eller konfigureret denne assistent (dvs. ikke-registrerede brugere). Foruden disse to kategorier af registrerede er der en tredje: Utilsigtede brugere, som, uanset om de er registreret eller ej, uden at vide det fremsætter anmodninger til den digitale assistent (for eksempel ved at sige den korrekte aktiveringskommando uden at vide, at assistenten er aktiv, eller sige andre ord, som assistenten fejlagtigt identificerer som aktiveringskommando).

---

<sup>16</sup> Artikel 4, stk. 1, i databeskyttelsesforordningen fastsætter også, at der ved en "*identificerbar fysisk person forstås en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, en onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet*".

<sup>17</sup> Artikel 9, stk. 1, i databeskyttelsesforordningen definerer særlige kategorier af personoplysninger som "*personoplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering*".

38. Ved "mangfoldighed af registrerede" forstås der desuden flere brugere af én digital assistent (f.eks. en enhed, der deles mellem registrerede og ikke-registrerede brugere, mellem kolleger, i en familie, i skolen) og forskellige typer brugere baseret på deres forhold (f.eks. en voksen, et barn, en ældre eller en person med funktionsnedsættelse). Selv om en digital assistent kan tilbyde nemmere interaktion med et digitalt værktøj og mange fordele for visse kategorier af registrerede, er det vigtigt at tage højde for de særlige forhold, der gør sig gældende for de enkelte kategorier af registrerede, og konteksten for anvendelsen af den digitale assistent.

### **Mangfoldighed af databehandlingsaktiviteter**

39. De teknologier, der anvendes til at udvikle en digital assistent, har også indvirkning på mængden af de behandlede data og typen af behandling. Jo mere en digital assistent leverer tjenester eller funktioner og er forbundet med andre enheder eller tjenester, der håndteres af andre parter, desto mere øges mængden af personoplysninger, der behandles og genbruges. Det medfører en mangfoldighed af behandlingsaktiviteter, der udføres automatisk som beskrevet i afsnit 2. Ud over automatisk databehandling kan der for visse behandlingsaktiviteters vedkommende være tale om menneskelig behandling. Det er for eksempel tilfældet, når den implementerede teknologi indebærer menneskers medvirken såsom kontrol af transskription af tale til tekst eller udarbejdelse af kommentarer til personoplysninger, der kan bruges til at indsætte nye modeller i en maskinlæringsteknologi. Dette er også tilfældet, når mennesker analyserer personoplysninger (f.eks. metadata) med henblik på at forbedre den tjeneste, der leveres af en digital assistent.

#### 3.2.2 Dataansvarliges og databehandleres behandling

40. Registrerede bør være i stand til at forstå og identificere de pågældende roller og bør kunne kontakte og agere med de enkelte interessenter i henhold til databeskyttelsesforordningen. Rolledelingen bør ikke være til ulempe for de registrerede, omend scenarier kan være komplicerede eller under udvikling. For at vurdere deres roller henvises interessenter til Databeskyttelsesrådets retningslinjer 7/2020 om begreberne dataansvarlig og databehandler i databeskyttelsesforordningen.<sup>18</sup>
41. Som nævnt i punkt 15 kan de vigtigste interessenter identificeres i rollerne udbyder eller designer, applikationsudvikler, integrator, ejer eller en kombination af disse. Der er mulighed for forskellige scenarier, alt efter hvem der gør hvad i interessenternes forretningsforhold, efter anmodning fra brugeren, personoplysningerne, databehandlingsaktiviteterne og disses formål. De bør tydeligt fastlægge og informere de registrerede om de betingelser, under hvilke de hver især skal handle og overholde de deraf følgende roller for dataansvarlige, fælles dataansvarlige eller databehandlere som fastsat i databeskyttelsesforordningen.<sup>19</sup> De kan hver især påtage sig én eller flere roller, da de kan være en unik dataansvarlig, en fælles dataansvarlig eller en databehandler i forbindelse med én databehandlingsaktivitet, samtidig med at de udfører en anden rolle i forbindelse med en anden databehandlingsaktivitet.
42. I et overordnet perspektiv kan designeren fungere som dataansvarlig ved fastlæggelsen af behandlingsformålene og -metoderne, men kan involveres som databehandler i forbindelse med behandling af personoplysninger på vegne af andre parter, f.eks. en applikationsudvikler. Brugeren af den digitale assistent ville derfor være underlagt flere dataansvarlige:

---

<sup>18</sup> EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR, V2.0, vedtaget den 7. juli 2021 (herefter benævnt "Retningslinjer 7/2020").

<sup>19</sup> Databeskyttelsesforordningen, artikel 12-14, 26.



applikationsudvikleren og designeren. En mulighed er også, at designeren, integratoren og udvikleren samles i ét organ, der fungerer som unik dataansvarlig. Under alle omstændigheder skal de gældende kvalifikationer fastlægges på grundlag af en individuel analyse.

Eksempel 1:

Designeren af den digitale assistent behandler brugerdata til mange formål, herunder forbedring af assistentens taleforståelsesfærdigheder og pålidelig udførelse af anmodninger. Af den grund, og selv om dette formål kan betyde, at der foretages behandling af oplysninger, der stammer fra tredjeparters brug af applikationer, er der kun én dataansvarlig: designeren af den digitale assistent, på hvis vegne og til hvis formål behandlingen udføres.

Eksempel 2:

En bank tilbyder sine kunder en applikation, der kan rettes direkte anmodninger til via den digitale assistent med henblik på at administrere deres konti.

To aktører er involveret i behandlingen af personoplysninger: designeren af den digitale assistent og udvikleren af bankapplikationen.

I det beskrevne scenarie er banken den dataansvarlige med hensyn til levering af tjenesten, da den fastlægger formålene med behandlingen og de vigtigste behandlingsmetoder i forbindelse med applikationen, der muliggør interaktion med assistenten. Den tilbyder nemlig en særskilt applikation, der gør det muligt for brugeren, dvs. bankens kunde, at administrere sine konti online. Desuden fastlægger den metoderne til behandling ved at vælge en relevant databehandler, som er designeren af den digitale assistent og kan spille en vigtig rolle med hensyn til at bistå med sin ekspertise med henblik på at fastlægge disse metoder (for eksempel kan databehandleren drive den udviklingsplatform, der gør det muligt at integrere tredjepartsapplikationer i den digitale assistent, og som derfor fastsætter de rammer og betingelser, applikationsudviklerne skal overholde).

43. På den registreredes side er det vigtigt at bemærke, at flere interessenter kan behandle de samme personoplysninger, selv om den registrerede reelt ikke forventer, at andre parter end udbyderen af den digitale assistent er involveret i behandlingskæden. Når en registreret derfor agerer med udbyderen af den digitale assistent i forbindelse med sine personoplysninger (f.eks. udøvelse af den registreredes rettigheder), betyder dette ikke automatisk, at denne handling vil finde anvendelse på de samme personoplysninger, som behandles af en anden interessent. Når disse interessenter er uafhængige dataansvarlige, er det vigtigt, at der gives klar besked til de registrerede med en redegørelse for behandlingens forskellige trin og aktører. I tilfælde af fælles dataansvar bør det desuden præciseres, om de enkelte dataansvarlige har kompetence til at tage højde for alle registreredes rettigheder, eller hvilken dataansvarlig der har kompetence med hensyn til hvilken rettighed.<sup>20</sup>

---

<sup>20</sup> Retningslinjer 7/2020, punkt 165.

### Eksempel 3:

I dette scenarie ønsker designeren af den digitale assistent at anvende de indsamlede og behandlede oplysninger til den tjeneste, der leveres af banken, til at forbedre sit talegenkendelsessystem. Designeren af den digitale assistent, som behandler oplysningerne til egne formål, får her status som dataansvarlig for denne specifikke behandlingsaktivitet.

44. Da mange interessenter henholdsvis medarbejdere kan være involveret i behandlingskæden, kan der opstå risikobetonede situationer, hvis der ikke er etableret passende foranstaltninger og garantier. Dataansvarlige er ansvarlige over for disse og bør derfor have fokus på at beskytte personoplysninger, navnlig ved at vælge egnede forretningspartnere og databehandlere, anvende principperne om databeskyttelse gennem standardindstillinger og design,<sup>21</sup> implementere relevante sikkerhedsværktøjer og andre databeskyttelsesrelevante værktøjer som for eksempel revisioner og retlige aftaler (f.eks. artikel 26 i databeskyttelsesforordningen for fælles dataansvarlige og artikel 28 i databeskyttelsesforordningen for databehandlere).
45. Økosystemet for digitale assistenter er komplekst, og potentielt kan mange aktører udveksle og behandle personoplysninger som dataansvarlige eller databehandlere. Det er yderst vigtigt at præcisere den enkelte aktørs rolle i forbindelse med de enkelte behandlingsaktiviteter og at følge princippet om dataminimering også i forbindelse med udveksling af oplysninger.
46. Desuden bør dataansvarlige være opmærksomme på overførsel af personoplysninger og sikre det nødvendige beskyttelsesniveau i hele behandlingskæden, navnlig når de benytter tjenester uden for EØS.

### 3.3 Gennemsigtighed

47. Eftersom digitale assistenter behandler personoplysninger (f.eks. brugernes tale og placering samt kommunikationsindholdet), skal de overholde gennemsigtighedskravene i artikel 5, stk. 1, litra a), artikel 12 og artikel 13 i databeskyttelsesforordningen (uddybes i betragtning 58). Dataansvarlige er forpligtet til at informere brugerne om behandlingen af deres personoplysninger i en kortfattet, gennemsigtig, letforståelig og lettilgængelig form.
48. Manglende fremlæggelse af den nødvendige information er et brud på forpligtelserne, der kan påvirke databehandlingens lovlighed. Det er ubetinget nødvendigt at overholde gennemsigtighedskravet, da det fungerer som kontrolmekanisme for databehandlingen og giver brugerne mulighed for at udøve deres rettigheder. Korrekt information af brugerne om, hvordan deres personoplysninger anvendes, gør det vanskeligere for dataansvarlige at misbruge den digitale assistent til formål, der rækker langt ud over brugernes forventninger. For eksempel har patenterede teknologier til formål at udlede en brugers helbredstilstand og følelsesmæssige tilstand af den pågældendes tale og tilpasse de leverede tjenester hertil.
49. Navnlig for udbyderen af digitale assistenttjenester eller enhver anden enhed, der fungerer som dataansvarlig, kan det være vanskeligt at overholde gennemsigtighedskravene. På grund af digitale assistenters særlige karakter møder dataansvarlige en række hindringer for at overholde databeskyttelsesforordningens gennemsigtighedskrav:
  - )] **Flere brugere:** Dataansvarlige bør informere alle brugere (registrerede, ikke-registrerede og utilsigtede brugere), ikke kun den bruger, der installerer den digitale assistent.

<sup>21</sup> Jf. Databeskyttelsesrådets retningslinjer 4/2019 vedrørende artikel 25 — Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, version 2.0, vedtaget den 20. oktober 2020.

- J) **Økosystemers kompleksitet:** Som der blev redegjort for i afsnittet om teknologisk baggrund, er identiteten på og rollerne for dem, der behandler personoplysninger i forbindelse med en digital assistent, langt fra indlysende for brugerne.
- J) **Særlige forhold for talegrænseflader:** Digitale systemer er endnu ikke egnede til kun tale-interaktion, hvilket den næsten systemiske brug af ledsagende skærme viser. Det er imidlertid nødvendigt at tilpasse sig talegrænsefladen og være i stand til at informere brugeren klart og korrekt på denne måde.
50. Digitale assistenter kan ses som maskiner med et endeligt antal tilstande, der gennemgår en række tilstande i deres normale funktion. De kan lytte lokalt med henblik på at registrere aktiveringskommandoer eller interagere med en fjernserver for at udføre en kommando, men de kan antage mange andre tilstande afhængigt af konteksten (for eksempel hvis der er baggrundsstøj fra omgivelserne), eller brugeren taler til dem (for eksempel kan det være, at de taler til en identificeret eller ukendt bruger). Desværre sker dette på en baggrund af betydelig informationsasymmetri i forhold til brugeren, som næppe er vidende om, hvorvidt enheden lytter, og endnu mindre om den tilstand, enheden befinder sig i.
51. Det anbefales stærkt, at designere og udviklere af digitale assistenter tager relevante skridt til at fjerne disse asymmetrier for på den måde at gøre digitale assistenters funktion mere interaktiv. Brugere bør oplyses om enhedens aktuelle tilstand. En sådan forbedring af gennemsigtigheden kan opnås både ved at gøre dialogen mellem menneske og maskine mere interaktiv (for eksempel kan enheden måske på en eller anden måde anerkende modtagelsen af en talekommando) og oplyse om maskinens tilstand ved hjælp af specifikke signaler. Hvad det angår, er der mange muligheder, der kan undersøges, lige fra brug af specifikke stemmebekræftelser og synlige ikoner eller lys eller brug af skærme på enheden.
52. Disse spørgsmål er særligt relevante i betragtning af de mange forskellige typer brugere, heriblandt sårbare mennesker som børn, ældre eller brugere med audiovisuelle funktionsnedsættelser.
53. Ovenstående problemer giver anledning til to væsentlige spørgsmål: Hvad er den bedst tænkelige måde at informere brugerne på, og hvad er det rette tidspunkt at informere dem? Disse spørgsmål bør undersøges nærmere i to forskellige situationer, afhængigt af om den digitale assistent kun har én bruger (f.eks. en privat smartphone) eller potentielt flere brugere (f.eks. intelligente enheder i hjemmet). Teknologien bag digitale assistenter kan også bruges til at kombinere disse to grundlæggende rammer, for eksempel når en bruger har en privat smartphone og kobler denne til en bil. Den digitale assistent i smartphonen, som med rimelighed kan forventes kun at blive anvendt af den pågældende bruger, "udvides" nu til bilens passagerer.
54. På nuværende tidspunkt er alle digitale assistenter koblet til en brugerkonto og/eller er installeret ved hjælp af en applikation, der kræver en sådan. Spørgsmålet om, hvordan dataansvarlige kan informere disse brugere om persondatapolitikken i forbindelse med installationen af den digitale assistent, bør behandles som beskrevet i Artikel 29-Gruppens retningslinjer vedrørende gennemsigtighed. Apps bør stille den nødvendige information til rådighed i en onlinebutik inden download.<sup>22</sup> På den måde gives informationen så tidligt som muligt og senest på det tidspunkt, hvor personoplysningerne indhentes. Nogle udbydere af digitale assistenter medtager tredjepartsapps i den digitale assistents standardopsætning, så

---

<sup>22</sup> Retningslinjer vedrørende gennemsigtighed i henhold til forordning 2016/679, WP260 rev. 01, godkendt af Databeskyttelsesrådet (i det følgende benævnt "WP29-retningslinjerne WP260"), punkt 11.

disse apps kan aktivere de pågældende apps ved hjælp af specifikke aktiveringskommandoer. Digitale assistenter, der anvender denne strategi for anvendelse af tredjepartsapplikationer, bør sikre, at brugerne også får den nødvendige information om tredjepartsbehandlingen.

55. Mange designere af digitale assistenter kræver imidlertid brugerkonti til assistenterne, der knytter den digitale assistenttjeneste sammen med en række andre tjenester som for eksempel e-mail, videostreaming eller onlinekøb for at nævne et par stykker. Designernes beslutning om at knytte kontoen til mange forskellige tjenester betyder, at det er nødvendigt med meget omfattende og komplekse persondatapolitikker. At sådanne persondatapolitikker er omfattende og komplekse, er i høj grad en hindring for overholdelse af gennemsigtighedsprincippet.

Eksempel 4:

En designer af en digital assistent kræver, at brugerne har en konto for at få adgang til assistenttjenesten. Denne brugerkonto er ikke specifik for assistenttjenesten og kan anvendes til andre tjenester udbudt af designeren, f.eks. e-mail, cloudlagring og sociale medier. For at oprette kontoen skal brugerne læse og acceptere en databeskyttelsespolitik på 30 sider. Politikken omfatter information om behandling af personoplysninger i alle de tjenester, der kan kobles til kontoen.

Den information, som designeren af assistenten har fremlagt i dette tilfælde, bør ikke betragtes som kortfattet, og dens kompleksitet betyder, at der ikke er den påkrævede gennemsigtighed. Designeren overholder dermed ikke gennemsigtighedskravene i henhold til databeskyttelsesforordningens artikel 12 og 13.

56. Selv om det er mest almindeligt at give den nødvendige information skriftligt, giver databeskyttelsesforordningen også mulighed for "andre metoder". Det fremgår udtrykkeligt af betragtning 58, at information kan gives i elektronisk form, for eksempel via et websted. Ved valg af en passende metode til information af de registrerede bør der desuden tages højde for de særlige omstændigheder, for eksempel den måde, hvorpå den dataansvarlige og den registrerede på anden måde interagerer med hinanden.<sup>23</sup> En mulighed for enheder uden skærm kan være at indsætte et link, der er letforståeligt, enten direkte eller i en e-mail. Allerede eksisterende løsninger kan tjene som eksempel på information, for eksempel callcentres praksis med at oplyse den, der foretager opkaldet, om, at telefonsamtalen optages, samt om deres persondatapolitik. Begrænsningerne ved skærmløse digitale assistenter fritager ikke den dataansvarlige for at give den nødvendige information i henhold til databeskyttelsesforordningen i forbindelse med installation af assistenten eller installation og brug af en assistent-app. Udbydere og udviklere af digitale assistenter bør udvikle stemmestyrede grænseflader for at give mulighed for at give den obligatoriske information.
57. Digitale assistenter kan være af stor interesse for brugere med nedsat syn, da de udgør et alternativt middel til interaktion med de IT-tjenester, der traditionelt er baseret på visuel information. I henhold til artikel 12, stk. 1, i databeskyttelsesforordningen må de nødvendige oplysninger kun gives mundtligt, hvis den registrerede anmoder herom, dvs. ikke som standard. Begrænsningerne ved skærmløse digitale assistenter ville dog kræve automatisk mundtlig information, som kan suppleres med skriftlige metoder. Dataansvarlige bør, når de

<sup>23</sup> WP29-retningslinjerne WP260, punkt 19.

anvender lyd til at informere registrerede, give den nødvendige information på en kortfattet og tydelig måde. Registrerede bør desuden kunne aflytte meddelelsen igen.<sup>24</sup>

58. Det er mere komplekst at træffe passende foranstaltninger til at overholde databeskyttelsesforordningens gennemsigtighedskrav, når der er flere brugere af den digitale assistent end enhedens ejer. Designere af digitale assistenter skal tage i betragtning, hvordan de kan informere ikke-registrerede og utilsigtede brugere korrekt, når disses personoplysninger behandles. Når samtykke er retsgrundlaget for behandling af brugeres data, skal brugerne informeres korrekt, for at samtykket er gyldigt <sup>25</sup>.
59. Med henblik på overholdelse af databeskyttelsesforordningen bør dataansvarlige finde en måde at informere ikke blot registrerede brugere, men også ikke-registrerede brugere og utilsigtede brugere af digitale assistenter på. Disse brugere bør informeres så hurtigt som muligt **og senest på behandlingstidspunktet**. Denne betingelse kan være særligt vanskelig at opfylde i praksis.
60. Bestemte virksomhedsspecifikke forhold bør heller ikke være til ulempe for de registrerede. Da mange interessenter er globale virksomheder eller er kendt for en specifik forretningsaktivitet (f.eks. telekommunikation, e-handel, informationsteknologi, webaktiviteter), bør måden, de leverer en digital assistenttjeneste på, være tydelig. Relevant information bør gøre det muligt for de registrerede at forstå, om deres anvendelse af assistenten vil blive knyttet til andre behandlingsaktiviteter, der administreres af udbyderen af assistenttjenesten (f.eks. telekommunikation, e-handel, informationsteknologi eller webaktiviteter), bortset fra den udtrykkelige brug af assistenten.

#### Eksempel 5:

En designer af en digital assistent, der også udbyder et socialt medie og en søgemaskine, kræver, at en bruger for at kunne bruge assistenten forbinder sin konto med assistenten. Ved at forbinde sin konto til brugen af assistenten kan designeren således ved hjælp af assistenten forbedre brugernes profil, de applikationer (eller færdigheder), der er installeret, de afgivne ordrer osv. Derfor er assistentinteraktioner en ny kilde til information knyttet til en bruger. Designeren bør for hver enkelt tjeneste give brugerne klar information om, hvordan deres data vil blive behandlet i de enkelte tjenester, og bør stille en funktion til rådighed, der giver brugerne mulighed for at vælge, om dataene må anvendes til profilering.

## Anbefalinger

61. Når brugere informeres om, at den digitale assistent behandler personoplysninger på grundlag af en brugerkontos persondatapolitik, og kontoen er knyttet til andre selvstændige tjenester (f.eks. e-mail eller onlinekøb), anbefaler Databeskyttelsesrådet, at persondatapolitikken har et tydeligt adskilt afsnit om assistentens behandling af personoplysninger.
62. Indholdet af den information, der gives til brugeren, bør præcist matche den udførte indsamling og behandling. Selv om nogle metaoplysninger er indeholdt i en taleprøve (f.eks. den talendes stressniveau), står det ikke automatisk klart, om der udføres en sådan analyse.

<sup>24</sup> WP29-retningslinjerne WP260, punkt 21.

<sup>25</sup> Artikel 4, stk. 11, i databeskyttelsesforordningen.

Det er afgørende, at dataansvarlige udviser gennemsigtighed med hensyn til de konkrete aspekter af de rådata, de behandler.

63. Det bør til enhver tid være klart, hvilken tilstand den digitale assistent befinder sig i. Brugere bør kunne afgøre, om en assistent aktuelt lytter til dens lukkede kredsløb, og navnlig om den streamer information til sin back-end. Denne information bør også være tilgængelig for personer med funktionsnedsættelse som for eksempel farveblindhed (daltonisme), døvhed (anacusia). Man bør særligt bemærke, at den digitale assistent foreslår et brugsscenario, hvor det ikke er nødvendigt at have øjenkontakt med enheden. Derfor bør al brugerfeedback, herunder tilstandsændringer, som minimum være tilgængelig i visuel og lydlig form.
64. Der bør tages særligt højde for, om enheder gør det muligt at tilføje tredjepartsfunktionalitet ("apps" til digitale assistenter). Selv om der kan gives bestemt generel information til brugeren, når det er denne, der tilføjer en sådan funktionalitet (eftersom det er brugerens valg), under normal brug af enheden, kan grænserne mellem de forskellige involverede dataansvarlige være langt mindre tydelige, dvs. at brugeren måske ikke er tilstrækkeligt informeret om, hvordan og af hvem den pågældendes data behandles (og i hvilket omfang) i en bestemt søgning.
65. Alle oplysninger om behandling baseret på data, der er indsamlet i forbindelse med og udledt af behandlingen af optaget tale, bør også være tilgængelige for brugerne i henhold til artikel 12 i databeskyttelsesforordningen.
66. Dataansvarlige for digitale assistenter bør gøre det klart, hvilke typer oplysninger en assistent kan udlede af sine omgivelser, for eksempel, men ikke begrænset til, andre personer i lokalet; musik, der kører i baggrunden; eventuel behandling af talen af sundhedsfaglige eller markedsføringsmæssige grunde; kæledyr osv.

### 3.4 Formålsbegrænsning og retsgrundlag

67. En digital assistents behandling af taleanmodninger har et klart formål, nemlig udførelse af anmodningen. Der er dog ofte også andre formål, som ikke er så tydelige, som for eksempel forbedring af assistentens evne til at forstå naturligt sprog ved at træne assistentmodellen ved hjælp af maskinindlæringsteknikker. Blandt de mest almindelige formål med assistentens behandling af personoplysninger er følgende:
  - ) Udføre brugernes anmodninger
  - ) Forbedring af assistenten gennem træning af maskinlæringsmodellen, menneskelig kontrol samt mærkning af taletransskription
  - ) Brugeridentifikation (ved hjælp af taledata)
  - ) Brugerprofilering med henblik på individuelt tilpasset indhold eller markedsføring
68. Digitale assistenters rolle som mellemlid samt måden, de er designet på, betyder, at de behandler en lang række forskellige personoplysninger og ikke-personoplysninger. Det gør det muligt at behandle personoplysninger til mange formål, der rækker ud over at udføre brugernes anmodninger, og som kan foregå helt ubemærket. Ved at analysere data, der er indsamlet via digitale assistenter, er det muligt at få kendskab til eller udlede brugernes interesser, tidsplaner, køreruter og vaner. Det kan gøre det muligt at behandle

personoplysninger til ikke-tilsigtede formål (f.eks. følelsesanalyse og vurdering af helbredstilstand<sup>26</sup>), hvilket ville række langt ud over brugernes rimelige forventninger.

69. Dataansvarlige bør klart angive deres formål i relation til den sammenhæng, assistenten anvendes i, så de registrerede har en klar forståelse af dette/disse (f.eks. angivelse af formål i kategorier). I henhold til artikel 5, stk. 1, i databeskyttelsesforordningen bør personoplysningerne indsamles til specifikke, eksplicite og legitime formål og ikke behandles yderligere på en måde, der er uforenelig med disse formål.

### 3.4.1 Udføre brugernes anmodninger

70. Digitale assistenter anvendes primært til at afgive talekommandoer, der skal udføres af assistenten eller en tilhørende app eller tjeneste (f.eks. en musikstreamingtjeneste, en korttjeneste eller en elektronisk lås). Brugerens stemme og potentielt andre data (f.eks. brugerens position ved anmodning om en rute til et bestemt bestemmelsessted) kan derfor blive behandlet.

#### Eksempel 6:

Passageren i en intelligent bil, der har en digital assistent, anmoder om en rute til den nærmeste tankstation. Assistenten behandler brugerens tale for at forstå kommandoen samt bilens position for at finde frem til ruten og sender den til den intelligente komponent, hvorefter ruten vises på bilens skærm.

71. I det omfang behandling af talekommandoer indebærer lagring af eller adgang til oplysninger, der lagres på slutbrugerens terminaludstyr, gælder artikel 5, stk. 3, i e-databeskyttelsesdirektivet. Selv om artikel 5, stk. 3, indeholder et generelt princip om, at sådan lagring og adgang kræver slutbrugerens forudgående samtykke, indeholder den også en undtagelse fra kravet om samtykke, hvis det "er absolut påkrævet for at levere en informationssamfundstjeneste, abonnenten eller brugeren udtrykkelig ønsker". For så vidt som taledataene behandles med henblik på at udføre en brugers anmodninger, er de undtaget fra kravet om forudgående samtykke.
72. Som tidligere nævnt skal enhver behandlingsaktivitet vedrørende personoplysninger efter opbevaring af eller adgang til oplysninger i slutbrugerens terminaludstyr have et retsgrundlag i henhold til artikel 6 i databeskyttelsesforordningen for at være lovlig.
73. I en digital assistent finder der to på hinanden følgende behandlinger sted. Som nævnt ovenfor kræver den første adgang til assistenten (og betingelserne i artikel 5, stk. 3, i e-databeskyttelsesdirektivet skal derfor være opfyldt). Ud over betingelserne i artikel 5, stk. 3, i e-databeskyttelsesdirektivet kræver dette andet trin også et retsgrundlag i henhold til artikel 6 i databeskyttelsesforordningen.
74. Når en person beslutter at anvende en digital assistent, indebærer denne handling generelt, at den oprindelige bruger først skal oprette en konto for at aktivere assistenten. Denne situation vedrører med andre ord et aftaleforhold<sup>27</sup> mellem den registrerede bruger og den

<sup>26</sup> Eoghan Furey, Juanita Blue, "Alexa, Emotion, Privacy and GDPR", Conference paper, Human Computer Interaction Conference, juli [2018].

<sup>27</sup> Forudsat at "*aftalen er gyldig i henhold til gældende national aftaleret*", uddrag af retningslinjer 2/2019 om behandling af personoplysninger i henhold til artikel 6, stk. 1, litra b), i databeskyttelsesforordningen i forbindelse med levering af onlinetjenester til registrerede ("*retningslinje 2/2019*"), § 26.

dataansvarlige for assistenten. For så vidt angår aftalens indhold og grundlæggende formål, har aftalen primært til formål at anvende assistenten til at udføre brugerens anmodning om bistand.

75. Enhver behandling af personoplysninger, der er nødvendig for at udføre brugerens anmodning, kan derfor baseres på retsgrundlaget for opfyldelsen af aftalen<sup>28</sup>. En sådan behandling omfatter navnlig registrering af brugerens taleanmodning, transskriptionen af denne til tekst, fortolkningen af denne, de oplysninger, der udveksles med videnskilder med henblik på at udarbejde et svar, og derefter transskription til et stemmestyret endeligt svar, der afslutter brugerens anmodning.
76. Gennemførelse af en aftale kan være et retsgrundlag for behandling af personoplysninger ved hjælp af maskinlæring (ML), når det er nødvendigt for levering af tjenesten. Behandling af personoplysninger ved hjælp af ML til andre formål, som ikke er nødvendige, for eksempel forbedring af tjenesterne, bør ikke være baseret på dette retsgrundlag.
77. Sidst, men ikke mindst bør retsgrundlagene for henholdsvis opfyldelse af aftalen og samtykke i henhold til databeskyttelsesforordningen ikke forveksles. Det samtykke, der er givet for indgåelse, dvs. accept, af aftalen, er en del af aftalens gyldighed og vedrører ikke den specifikke betydning af samtykket i henhold til databeskyttelsesforordningen.<sup>29</sup>
78. Når anvendelsen af en digital assistent ikke kræver, at en brugerkonto forinden konfigureres til assistenten, kan samtykke være et muligt retsgrundlag.

#### 3.4.2 Forbedring af den digitale assistent ved at træne ML-systemerne og foretage manuel kontrol af tale og transskriptioner

79. Udtale m.m. af den menneskelige tale er enormt forskellig. Selv om en digital assistent er umiddelbart funktionsdygtig, er det muligt at forbedre dens effektivitet ved at tilpasse den til de særlige karakteristika ved brugernes tale. Som nævnt i afsnit 2.6 er denne tilpasningsproces baseret på maskinlæringsmetoder og består af to processer: Tilføjelse af nye data indsamlet fra assistentens brugere til dens træningsdatasæt samt den menneskelige kontrol af de data, der behandles med henblik på udførelse af en fraktion af anmodningerne.

##### Eksempel 7:

En bruger af en digital assistent er nødt til at sige den samme talekommando tre gange, fordi assistenten ikke forstår den. De tre talekommandoer og de tilhørende transskriptioner sendes til de menneskelige kontrollører med henblik på kontrol og berigtigelse af transskriptionerne. Talekommandoerne og de kontrollerede transskriptioner føjes til assistentens træningsdatasæt med henblik på at forbedre assistentens effektivitet.

80. De behandlingsaktiviteter, der er beskrevet i eksemplet, bør ikke betragtes som (strengt) "*nødvendige af hensyn til opfyldelse af en kontrakt*" som omhandlet i artikel 6, stk. 1, litra b), i databeskyttelsesforordningen og kræver derfor et andet retsgrundlag end artikel 6 i databeskyttelsesforordningen. Den primære årsag er, at en digital assistent er umiddelbart funktionsdygtig og allerede kan udføre opgaver, der er (strengt) nødvendige af hensyn til

<sup>28</sup> I overensstemmelse med retningslinjer 2/2019, hvori det endvidere anføres, at udtalelse 06/2014 fortsat er relevant for artikel 6, stk. 1, litra b), og databeskyttelsesforordningen (jf. navnlig side 11, 16, 17, 18 og 55 i denne udtalelse 06/2014).

<sup>29</sup> Jf. retningslinjer 2/2019, henholdsvis punkt 18, 19, 20, 21 og 27.



opfyldelse af kontrakten. Databeskyttelsesrådet anser ikke artikel 6, stk. 1, litra b), for generelt at være et relevant retsgrundlag for behandling med henblik på at forbedre en tjeneste eller udvikle nye funktioner i en eksisterende tjeneste. I de fleste tilfælde indgår en bruger en kontrakt for at udnytte en eksisterende tjeneste. Selvom muligheden for forbedringer og ændringer i en tjeneste almindeligvis kan medtages i kontraktvilkår, kan en sådan behandling normalt ikke betragtes som objektivt nødvendig af hensyn til opfyldelse af kontrakten med brugeren.

### 3.4.3 Brugeridentifikation<sup>30</sup> (ved hjælp af taledata)

81. Brugen af taledata til brugeridentifikation indebærer behandling af biometriske data som defineret i artikel 4, stk. 14, i databeskyttelsesforordningen. Den dataansvarlige vil derfor skulle identificere en undtagelse i henhold til artikel 9 i databeskyttelsesforordningen ud over identifikationen af et retsgrundlag i henhold til artikel 6 i databeskyttelsesforordningen<sup>31</sup>.
82. Af de undtagelser, der er anført i artikel 9 i databeskyttelsesforordningen, synes kun registreredes udtrykkelige samtykke at finde anvendelse til dette specifikke formål.
83. Da dette formål imidlertid kræver anvendelse af den specifikke retlige ordning i artikel 9 i databeskyttelsesforordningen, redegøres der nærmere for dette i afsnit 3.8 vedrørende behandling af særlige kategorier af oplysninger.

### 3.4.4 Brugerprofilering med henblik på individuelt tilpasset indhold eller markedsføring

84. Som nævnt ovenfor har den digitale assistent adgang til indholdet af alle talekommandoer, selv når de er rettet mod tjenester, der leveres af tredjeparter. Denne adgang gør det muligt for assistentens designer at konstruere meget præcise brugerprofiler, der kan anvendes til at tilbyde individuelt tilpassede tilbud eller markedsføring.

#### Eksempel 8:

Hver gang en bruger af en digital assistent foretager en internetsøgning, tilføjer assistenten mærkater, der viser emner af interesse for brugerprofilen. Resultaterne for hver ny søgning præsenteres for brugeren i en rækkefølge, der tager højde for disse mærkater.

#### Eksempel 9:

Hver gang en bruger af en digital assistent foretager et køb fra en e-handelstjeneste, lagrer assistenten en registrering af købsordren. Udbyderen af assistenten gør det muligt for

<sup>30</sup> Teknisk set skal der skelnes mellem begreberne identifikation og verifikation (autentifikation). Identifikation er en én til mange- (1:N)-søgning og -sammenligning og kræver i princippet en database, hvor flere personer er opført. Derimod er behandling med henblik på verifikation en én til én- (1:1)-sammenligning og anvendes til at kontrollere og få bekræftet, ved en biometrisk sammenligning, om en person er den samme som den person, de biometriske oplysninger stammer fra. Så vidt det er Databeskyttelsesrådet bekendt, anvender de digitale assistenter, der er på markedet, udelukkende teknologier til identifikation af den talende.

<sup>31</sup> I henhold til databeskyttelsesforordningen er den blotte karakter af oplysninger ikke altid tilstrækkelig til at afgøre, om de kan betragtes som særlige kategorier af oplysninger, eftersom "*behandlingen af fotografier [er] omfattet af definitionen af biometriske data, når de behandles ved en specifik teknisk fremgangsmåde, der muliggør entydig identifikation eller autentifikation af en fysisk person*" (betragtning 51). Det samme ræsonnement gælder for tale.

tredjeparter at målrette markedsføring til brugeren af assistenten på grundlag af tidligere køb.

85. Individuel tilpasning af indhold kan udgøre (men gør det ikke altid) et iboende og forventet element i en digital assistent. Hvorvidt sådan behandling kan betragtes som et underliggende aspekt ved en digital assistenttjeneste, afhænger af den præcise art af den leverede tjeneste, den gennemsnitlige registreredes forventninger i lyset af ikke blot betingelserne for tjenesten, men også måden, tjenesten markedsføres over for brugerne på, og hvorvidt tjenesten kan leveres uden individuel tilpasning.<sup>32</sup>
86. Hvis individuel tilpasning finder sted i forbindelse med et kontraktforhold og som en del af en tjeneste, som slutbrugeren udtrykkeligt har anmodet om (og behandlingen er begrænset til, hvad der er strengt nødvendigt for at levere denne tjeneste), kan sådan behandling baseres på artikel 6, stk. 1, litra b), i databeskyttelsesforordningen.
87. Hvis behandlingen ikke er strengt "*nødvendig for opfyldelsen af en kontrakt*" som omhandlet i artikel 6, stk. 1, litra b), i databeskyttelsesforordningen, skal udbyderen af digitale assistenttjenester i princippet indhente den registreredes samtykke. Eftersom der i henhold til artikel 5, stk. 3, i e-databeskyttelsesdirektivet er krav om samtykke til lagring af oplysninger og adgang til oplysninger (jf. punkt 28-29 ovenfor), er samtykke i henhold til artikel 6, stk. 1, litra a), i databeskyttelsesforordningen i princippet også det relevante retsgrundlag for behandling af personoplysninger i forbindelse med disse handlinger, da der ved påberåbelse af legitim interesse i visse tilfælde kan være en risiko for at underminere det yderligere beskyttelsesniveau, der er fastsat i artikel 5, stk. 3, i e-databeskyttelsesdirektivet.
88. Hvad angår brugerprofilering med henblik på markedsføring, bør det bemærkes, at dette formål aldrig betragtes som en tjeneste, slutbrugeren udtrykkeligt har anmodet om. I tilfælde af behandling til dette formål bør der derfor ske systematisk indsamling af brugernes samtykke.

## Anbefalinger

89. Brugere bør informeres om formålet med behandling af personoplysninger, og dette formål bør være i overensstemmelse med deres forventninger til den enhed, de køber. For digitale assistenters vedkommende er dette formål — set i brugerens perspektiv — tydeligvis at behandle deres tale med det ene formål at tolke deres anmodning og give relevante svar (dvs. svar på en anmodning eller anden respons i form af eksempelvis fjernstyring af en lyskontakt).
90. Når behandlingen af personoplysninger er baseret på samtykke, "*bør samtykket gives i forbindelse med et eller flere specifikke formål, og den registrerede har et valg med hensyn til hvert af dem*". Desuden "*bør en dataansvarlig, der ønsker samtykke til forskellige formål, give mulighed for et særskilt tilvalg i forbindelse med de enkelte formål med henblik på at give brugerne mulighed for at give specifikt samtykke til specifikke formål*"<sup>33</sup>. Brugere bør for eksempel kunne give eller afvise at give særskilt samtykke til manuel kontrol og mærkning af taletransskription eller til brug af deres taledata til brugeridentifikation/autentifikation (jf. afsnit 3.7).

<sup>32</sup> Jf. også retningslinjer 2/2019, punkt 57.

<sup>33</sup> Jf. Databeskyttelsesrådets [retningslinjer 5/2020 vedrørende samtykke i henhold til forordning 2016/679](#), vedtaget den 4. maj 2020, afsnit 3.2.

### 3.5 Behandling af personoplysninger om børn

91. Børn kan også interagere med en digital assistent og oprette egne profiler, der er forbundet med voksnes. Nogle assistenter er indbygget i enheder, der er specifikt rettet mod børn.
92. Når retsgrundlaget for behandling er opfyldelse af en kontrakt, afhænger betingelserne for behandling af personoplysninger om børn af national aftaleret.
93. Når retsgrundlaget for behandlingen er samtykke, og i henhold til artikel 8, stk. 1, i databeskyttelsesforordningen, er behandling af personoplysninger om børn kun lovlig, *"hvis barnet er mindst 16 år. Er barnet under 16 år, er sådan behandling kun lovlig, hvis og i det omfang samtykke gives eller godkendes af indehaveren af forældremyndigheden over barnet"*. Med henblik på efterlevelse af databeskyttelsesforordningen bør der, når retsgrundlaget er samtykke, indhentes udtrykkelig tilladelse fra forældre eller værger til at indsamle, behandle og opbevare børns data (tale, transskriptioner osv.).
94. Der er til en vis grad adgang til forældrekontrol, men den er i sin nuværende form ikke brugervenlig (f.eks. er det nødvendigt at tilmelde sig en ny tjeneste) og har begrænset funktionalitet. Dataansvarlige bør investere i udvikling af metoder, der gør det muligt for forældre og værger at overvåge børns brug af digitale assistenter.

### 3.6 Opbevaring af data

95. Digitale assistenter behandler og genererer en lang række personoplysninger som for eksempel tale, transskription af tale, metadata eller systemlogfiler. Disse typer data kan behandles til mange forskellige formål, f.eks. levering af en tjeneste, forbedring af NLP, individuel tilpasning og forskningsarbejde. I henhold til databeskyttelsesforordningens princip om opbevaringsbegrænsning for data bør digitale assistenter ikke opbevare personoplysninger i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de behandles. Dataopbevaringsperioderne bør derfor være knyttet til forskellige behandlingsformål. Udbydere af digitale assistenttjenester samt tredjeparter, der leverer tjenester via sådanne assistenter, bør fastsætte den maksimale opbevaringsperiode for de enkelte datasæt og formål.
96. Princippet om dataminimering hænger tæt sammen med princippet om opbevaringsbegrænsning for data. Dataansvarlige skal ikke blot begrænse dataopbevaringsperioden, men også typen og mængden af data.
97. Dataansvarlige bør blandt andet stille sig selv følgende spørgsmål: Er det nødvendigt at opbevare alle taleoptagelser eller alle transskriptioner for at opfylde formål X? Er det nødvendigt at opbevare taledataene, når transskriptionen er blevet lagret? I så fald til hvilket formål? Hvor længe er der behov for tale- eller transskriptionsdata til de enkelte formål? Ud fra svaret på disse og andre lignende spørgsmål fastsættes de opbevaringsperioder, der bør indgå i de oplysninger, som de registrerede har adgang til.
98. Nogle digitale assistenter opbevarer som standard personoplysninger i form af taleuddrag ("snippets") eller transskriptioner i et ikke-fastlagt tidsrum, samtidig med at brugerne får mulighed for at slette sådanne oplysninger. Opbevaring af personoplysninger på ubestemt tid er i strid med princippet om opbevaringsbegrænsning. At registrerede får mulighed for at slette deres personoplysninger, fritager ikke den dataansvarlige for at udarbejde og håndhæve en politik for opbevaring af personoplysninger.

99. Ved design af digitale assistenter skal der tages højde for brugerkontrolelementer til brug for brugeres sletning af egne personoplysninger i deres enhed og i alle fjernlagringsystemer. Sådanne kontrolelementer kan være nødvendige for at imødekomme forskellige former for brugeranmodninger, f.eks. en anmodning om sletning eller tilbageskrækning af et tidligere givet samtykke. Nogle digitale assistenters design tager ikke højde for dette krav.<sup>34</sup>
100. Som i andre sammenhænge kan dataansvarlige være nødt til at opbevare personoplysninger som dokumentation for en tjeneste, der er leveret til en bruger, med henblik på at opfylde en retlig forpligtelse. Den dataansvarlige kan opbevare personoplysninger på dette grundlag. For de opbevarede oplysningers vedkommende bør der dog fortsat være tale om det minimum, der er nødvendigt for at opfylde den pågældende retlige forpligtelse, samt det kortest mulige tidsrum. Naturligvis bør de data, der opbevares med henblik på at opfylde en retlig forpligtelse, ikke anvendes til andre formål, uden at der foreligger et retsgrundlag i henhold til artikel 6 i databeskyttelsesforordningen.

Eksempel 10:

En bruger køber et tv gennem en e-handelstjeneste ved hjælp af en talekommando til en digital assistent. Selv om brugeren efterfølgende anmoder om at få slettet sine oplysninger, kan udbyderen eller udvikleren af assistenten fortsat opbevare visse oplysninger af hensyn til sin retlige forpligtelse i henhold til skattelovgivningen til at opbevare købsdokumentation. De oplysninger, der opbevares til dette formål, bør dog ikke række ud over det minimum, der er nødvendigt for at opfylde den retlige forpligtelse, og de kan ikke behandles til andre formål, uden at der foreligger et retsgrundlag i henhold til artikel 6 i databeskyttelsesforordningen.

101. Som nævnt i afsnit 2 forbedres digitale assistenters talegenkendelse ved at træne maskinlæringsystemer ved hjælp af brugeres oplysninger. Hvis brugerne ikke giver deres samtykke til behandling af deres oplysninger til dette formål, eller hvis de trækker samtykket tilbage, kan deres oplysninger ikke lovligt anvendes til at træne en ny model og bør slettes af den dataansvarlige, forudsat at der ikke er noget andet formål, der berettiger til fortsat opbevaring. Der er dog dokumentation for, at der kan være risiko for genkendelse i nogle maskinlæringsmodeller.<sup>35</sup>
102. Dataansvarlige og databehandlere bør ikke anvende modeller, der begrænser deres mulighed for at standse behandlingen, hvis en fysisk person trækker sit samtykke tilbage, og de bør heller ikke anvende modeller, der begrænser deres mulighed for at sikre registreredes rettigheder. Dataansvarlige og databehandlere bør iværksætte risikobegrænsende foranstaltninger for at mindske risikoen for genkendelse til en acceptabel grænseværdi.
103. Hvis brugeren trækker sit samtykke tilbage, kan de oplysninger, der er indsamlet fra den pågældende, ikke længere anvendes til yderligere træning af modellen. Men det er ikke nødvendigt at slette den model, der tidligere er blevet trænet ved hjælp af disse data. Databeskyttelsesrådet pointerer dog, at der er dokumentation for, at der kan være risiko for læk af personoplysninger i visse maskinlæringsmodeller. Navnlig har adskillige undersøgelser

<sup>34</sup> Jf. Amazons brev af 28. juni 2019 som svar til den amerikanske senator Christopher Coons: [https://www.coons.senate.gov/imo/media/doc/Amazon%20Senator%20Coons Response%20Letter 6.28.19 \[3\].pdf](https://www.coons.senate.gov/imo/media/doc/Amazon%20Senator%20Coons%20Response%20Letter%206.28.19%20[3].pdf)

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

vist, at data kan rekonstrueres og henføres til enkeltbrugere, hvilket gør det muligt for angribere at indhente oplysninger om enkeltpersoner.<sup>36</sup> Dataansvarlige og databehandlere bør derfor iværksætte risikobegrænsende foranstaltninger for at mindske risikoen for genkendelse til en acceptabel grænseværdi med henblik på at sikre, at de anvender modeller, der ikke indeholder personoplysninger.

104. Registrerede bør ikke ansøres til at lade deres oplysninger opbevare på ubestemt tid. Sletning af opbevarede taledata og transskriptioner kan have indvirkning på tjenestens effektivitet, men der bør redegøres for indvirkningen over for brugerne på en klar og målbar måde. Udbydere af digitale assistenttjenester bør undgå at fremsætte generelle udtalelser om, at tjenesten forringes, når personoplysningerne er slettet.
105. Det er en særlig udfordring at anonymisere taleoptagelser, da det er muligt at identificere brugere alene via en meddelelses indhold og stemmeegenskaberne. Der forskes dog i et vist omfang<sup>37</sup> i teknikker, der kan gøre det muligt at fjerne situationsspecifikke oplysninger som baggrundsstøj og at anonymisere stemmer.

### Anbefalinger

106. Set i brugerens perspektiv er hovedformålet med at behandle dennes personoplysninger at fremsætte anmodninger og modtage svar og/eller udløse handlinger som for eksempel at afspille musik eller tænde/slukke lys. Når en anmodning er blevet besvaret eller en kommando udført, bør personoplysningerne slettes, medmindre designeren eller udvikleren af den digitale assistent har et gyldigt retsgrundlag til at opbevare dem til et specifikt formål.
107. Inden det overvejes at anonymisere dataene som et middel til at overholde princippet om opbevaringsbegrænsning for dataene, bør udbydere og udviklere af digitale assistenter kontrollere, at anonymiseringsprocessen gør talen uidentificerbar.
108. Konfigureringsstandarder bør afspejle disse krav ved automatisk at indstille assistenten til at opbevare et absolut minimum af brugeroplysninger. Hvis disse muligheder præsenteres som en del af en opsætningsguide, bør standardindstillingen afspejle dette, og alle muligheder bør fremlægges som lige muligheder uden visuel forskelsbehandling.
109. Hvis udbyderen eller udvikleren af assistenten under kontrolprocessen bliver opmærksom på en registrering, der stammer fra en fejlagtig aktivering, bør registreringen og alle de tilknyttede oplysninger straks slettes og ikke anvendes til noget formål.

### 3.7 Sikkerhed

110. For at opretholde sikkerheden i forbindelse med behandling af personoplysninger bør digitale assistenter sikre assistenternes fortrolighed, integritet og tilgængelighed. Ud over risiciene i forbindelse med elementer i økosystemet for digitale assistenter skaber tale som kommunikationsmiddel nye sikkerhedsmæssige risici.
111. Digitale assistenter er multibrugere. De kan have mere end én registreret bruger, og alle i deres omgivelser kan afgive kommandoer og bruge deres tjenester. Enhver digital assistenttjeneste,

---

<sup>36</sup> N. Carlini et al, "[Extracting Training Data from Large Language Models](#)" dec. 2020.

<sup>37</sup> Jf. for eksempel VoicePrivacy (<https://www.voiceprivacychallenge.org>), et initiativ til udvikling af løsninger til beskyttelse af personoplysninger i forbindelse med taleteknologi.

Se også open source-baserede stemmeanonymiseringsværktøjer udviklet i forbindelse med COMPRISE, et projekt under Horisont 2020-programmet: [https://gitlab.inria.fr/comprise/voice\\_transformation](https://gitlab.inria.fr/comprise/voice_transformation).

der kræver fortrolighed, indebærer en vis adgangskontrolmekanisme og brugerautentifikation. Uden adgangskontrol kan enhver, der kan afgive talekommandoer til en digital assistent, få adgang til, ændre eller slette en brugers personoplysninger (f.eks. anmode om modtagne beskeder, brugerens adresse eller kalenderoplysninger). Afgivelse af talekommandoer til en digital assistent kræver ikke, at personen er tæt på assistenten, idet assistenten kan manipuleres, eksempelvis via signaltransmission<sup>38</sup> (f.eks. radio eller tv). Nogle af de kendte metoder til fjernafgivelse af kommandoer til digitale assistenter som for eksempel laser<sup>39</sup> eller ultralydsbølger<sup>40</sup> (uhørlige) kan ikke engang opfattes af menneskets sanser.

112. Brugerautentifikation kan baseres på én eller flere af følgende faktorer: Noget, du kender (f.eks. en adgangskode), noget, du har (f.eks. et chipkort), eller noget, du er (f.eks. stemmebiometri). Et nærmere blik på disse autentifikationsfaktorer i forbindelse med digitale assistenter viser, at:
- ) Autentifikation ved hjælp af noget, brugeren kender, er problematisk. Den hemmelighed, der ville gøre det muligt for brugere at bevise deres identitet, ville skulle siges højt og dermed blive eksponeret til alle i omgivelserne. Assistentens kommunikationskanal er den omgivende luft, en kanaltype, der ikke kan befæstes på den måde, traditionelle kanaler er (f.eks. ved at begrænse adgangen til kanalen eller kryptere dens indhold).
  - ) Autentifikation ved hjælp af noget, brugeren har, ville kræve, at udbyderne af assistenttjenester opretter, distribuerer og forvalter "tokens", der kan bruges som legitimation.
  - ) Autentifikation ved hjælp af noget, brugeren er, indebærer anvendelse af biometriske data med det formål entydigt at identificere en fysisk person (se afsnit 3.7 nedenfor).
113. Assistenters brugerkonti er knyttet til de enheder, hvor tjenesten leveres. Den konto, der bruges til at håndtere assistenten, bruges ofte også til at håndtere andre tjenester. For eksempel kan ejerne af en Android-mobiltelefon og Google Home-højtaler knytte deres Google-konto til begge enheder og gør det sandsynligvis også. De fleste digitale assistenter kræver og tilbyder ikke en identifikations- eller autentifikationsmekanisme, når en enhed, der leverer en assistenttjeneste, kun har én brugerkonto.
114. Hvis der er mere end én brugerkonto tilknyttet enheden, tilbyder nogle assistenter en valgfri grundlæggende adgangskontrol i form af en PIN uden egentlig brugerautentifikation. Andre assistenter har mulighed for at anvende stemmebiometri som identifikationsmekanisme.
115. Brugereidentifikation eller -autentifikation er måske ikke nødvendig for at få adgang til alle assistentens tjenester, men for nogle er det nødvendigt. Uden en identifikations- eller autentifikationsmekanisme kan enhver få adgang til andre brugeres data og ændre eller slette dem efter behag. For eksempel kan enhver, der er fysisk tæt på en intelligent højtaler, slette andre brugeres playlister fra musikstreamingtjenesten, kommandoer fra kommandohistorikken og kontakter fra kontaktlisten.

---

<sup>38</sup> 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, De Forenede Arabiske Emirater, 2018, s. 1-6, doi: 10.1109/GLOCOM.2018.8647762.

<sup>39</sup> Jf. for eksempel <https://lightcommands.com>

<sup>40</sup> Jf. for eksempel <https://surfingattack.github.io>

116. De fleste assistenter har blind tillid til deres lokale netværk. Enhver kompromitteret enhed i samme netværk kan ændre den intelligente højtalters indstillinger eller give mulighed for at installere malware eller forbinde falske apps/færdigheder med enheden uden brugerens viden eller samtykke.<sup>41</sup>
117. Som al anden software er digitale assistenter også udsat for sikkerhedsrisici. På grund af markedsconcentrationen for digitale assistenter<sup>42</sup> er millioner af brugere af disse assistenter eksponeret for sikkerhedsrisiciene. Som assistenterne i øjeblikket er designet, sender de ikke oplysninger til cloud-tjenesten for talegenkendelse, før aktiveringskommandoen registreres. På grund af sårbarheder i softwaren kan en angriber imidlertid have held til at omgå assistentens opsætning og sikkerhedsforanstaltningerne. Det kan på den måde blive muligt for eksempel at få en kopi af alle data, der sendes til assistent-clouden, og videresende den til en server, der kontrolleres af angriberen.
118. Persondata, der behandles eller udledes lovligt af en assistent, gør det muligt at udarbejde en forholdsvis præcis profil af dens brugere, da assistenten ved eller kan udlede sine brugeres placering, relationer og interesser. Digitale assistenter findes i stigende grad i brugernes hjem og smartphones. Det øger risikoen for masseovervågning og masseprofilering. Sikkerhedsforanstaltningerne til beskyttelse af såvel data under overførsel som lagrede data, i enhederne og i clouden, bør derfor matche disse risici.
119. Den stigende brug af digitale assistenter i kombination med de retshåndhævende myndigheders utilstrækkeligt afbalancerede adgangsrettigheder kan have en afskrækkende virkning, der ville underminere grundlæggende rettigheder som for eksempel ytringsfriheden.
120. Retshåndhævende myndigheder, både i<sup>43</sup> og uden for<sup>44</sup> EU har allerede givet udtryk for deres interesse i at få adgang til de "snippets", som de digitale assistenter registrerer. Adgang til data, der behandles eller udledes af digitale assistenter i EU, bør være i overensstemmelse med EU's eksisterende rammer for databeskyttelse og beskyttelse af personoplysninger. Hvis nogle medlemsstater overvejer at udstede specifik lovgivning, der begrænser de grundlæggende rettigheder til databeskyttelse og beskyttelse af personoplysninger, bør sådanne begrænsninger altid overholde kravet i artikel 23 i databeskyttelsesforordningen.<sup>45</sup>
121. Den menneskelige kontrol af taleoptagelser og tilknyttede data med henblik på at forbedre kvaliteten af assistenttjenester er almindelig praksis for udbydere af digitale assistenter. På grund af den følsomme karakter af de oplysninger, der behandles af disse menneskelige kontrollører, og det forhold, at processen ofte udføres af databehandlere som underleverandører, er det yderst vigtigt, at der iværksættes passende sikkerhedsforanstaltninger.

## Anbefalinger

---

<sup>41</sup> Jf. for eksempel 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>

<sup>42</sup> Markedet for digitale assistenter er i øjeblikket delt mellem færre end et dusin tjenesteudbydere.

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

<sup>44</sup> Jf. for eksempel <https://cdt.org/insights/alexa-is-law-enforcement-listening>.

<sup>45</sup> Jf. også Databeskyttelsesrådets retningslinjer 10/2020 om begrænsninger i henhold til artikel 23 i databeskyttelsesforordningen.

122. Designere af digitale assistenter og udviklere af assistent-applikationer bør stille sikre avancerede autentifikationsprocedurer til rådighed for brugerne.
123. Menneskelige kontrollører bør altid modtage de strengt nødvendige pseudonymiserede oplysninger. De retlige aftaler, der regulerer kontrollen, bør udtrykkeligt forbyde enhver behandling, der kan medføre, at den registrerede identificeres.
124. Hvis nødopkald er inkluderet i assistentens tjenester, bør der garanteres en stabil opetid<sup>46</sup>.

### 3.8 Behandling af særlige kategorier af oplysninger

125. Som tidligere nævnt har digitale assistenter adgang til oplysninger af intim karakter, som kan beskyttes i henhold til artikel 9 i databeskyttelsesforordningen (jf. afsnit 3.7.1), som for eksempel biometriske data (jf. afsnit 3.7.2). Designere og udviklere af assistenter skal derfor omhyggeligt fastslå, i hvilke tilfælde behandlingen indebærer særlige kategorier af oplysninger.

#### 3.8.1 Generelle betragtninger ved behandling af særlige kategorier af data

126. Digitale assistenter kan behandle særlige kategorier af oplysninger under forskellige omstændigheder:
  - ) Som led i deres egne tjenester, for eksempel i forbindelse med administration af lægeaftaler i brugeres kalender.
  - ) Når udbydere af assistenter fungerer som grænseflade for tredjepartstjenester, behandler de kommandoernes indhold. Afhængigt af den type tjeneste, brugeren anmoder om, kan udbydere af assistenter behandle særlige kategorier af oplysninger. Et eksempel kan være, når en kvindelig bruger afgiver en kommando til en assistent om at anvende en tredjepartsapp, der skal holde styr på hendes ægløsning.<sup>47</sup>
  - ) Når taledata anvendes til entydigt at identificere brugeren, som beskrevet nedenfor.

#### 3.8.2 Generelle betragtninger ved behandling af biometriske data

127. Nogle digitale assistenter er i stand til entydigt at identificere deres brugere udelukkende på grundlag af disses stemme. Denne proces kaldes stemmegenkendelse. I registreringsfasen for stemmegenkendelse behandler assistenten en brugers stemme med henblik på at skabe en stemmemodel (eller voiceprint). Under normal brug kan assistenten beregne en hvilken som helst brugers stemmemodel og sammenligne den med de registrerede modeller for entydigt at identificere den bruger, der har afgivet kommandoen.

##### Eksempel 11:

En gruppe brugere installerer en digital assistent med henblik på at bruge stemmegenkendelse. Efter at have gjort dette indtaler de deres stemmemodel.

Senere anmoder en bruger assistenten om at få adgang til møderne i brugernes kalender. Da adgang til kalenderen kræver brugeridentifikation, trækker assistenten modellen ud af

<sup>46</sup> Den tid, en enhed eller en tjeneste kan efterlades uden opsyn uden at gå ned eller uden at skulle genstartes i forbindelse med administration eller vedligeholdelse.

<sup>47</sup> Jf. for eksempel et produkt, der findes her: <https://www.amazon.com/Ethan-Fan-Ovulation-Period-Tracker/dp/B07CRLSHKY>



brugerens stemme, beregner dens stemmemodel og tjekker, om den matcher en registreret bruger, og om den pågældende bruger har adgang til kalenderen.

128. I ovennævnte eksempel er genkendelsen af brugerens stemme på grundlag af en stemmemodel ensbetydende med behandling af særlige kategorier af personoplysninger som omhandlet i artikel 9 i databeskyttelsesforordningen (behandling af biometriske data med det formål entydigt at identificere en fysisk person).<sup>48</sup> Behandlingen af biometriske data med det formål at identificere brugeren ifølge eksemplet kræver udtrykkeligt samtykke fra den eller de berørte registrerede (artikel 9, stk. 2, litra a), i databeskyttelsesforordningen). Når dataansvarlige derfor indhenter brugeres samtykke, skal de efterleve betingelserne i artikel 7 og som præciseret i betragtning 32 i databeskyttelsesforordningen og bør tilbyde en alternativ identifikationsmetode til biometri, hvad angår den frivillige karakter af samtykke.
129. Når der anvendes taledata til biometrisk identifikation eller autentifikation, skal de dataansvarlige sikre, at det er gennemsigtigt, hvor der anvendes biometrisk identifikation, og hvordan stemmemodeller (biometriske modeller) opbevares og spredes på tværs af enheder. For at opfylde dette krav om gennemsigtighed anbefaler Databeskyttelsesrådet at besvare følgende spørgsmål:
- ) Aktiverer aktiveringen af stemmeidentifikation på én enhed automatisk denne funktion på alle andre enheder, der anvender samme konto?
  - ) Spredes aktiveringen af stemmeidentifikation via infrastrukturen hos den dataansvarlige for den digitale assistent til enheder, der er ejet af andre brugere?
  - ) Hvor genereres, opbevares og matches biometriske modeller?
  - ) Er biometriske modeller tilgængelige for udbydere og udviklere af assistenter eller andre?
130. Når den registrerede bruger konfigurerer assistenten til at identificere brugernes stemme, vil ikke-registrerede og utilsigtede brugeres stemme også blive behandlet med henblik på entydigt at identificere disse.
131. Registrering af den rigtige brugers stemme indebærer således også en sammenligning af stemmen med stemmen hos andre personer i nærheden af assistenten. Med andre ord kan den talegenkendelsesfunktionalitet, der anvendes i digitale assistenter, kræve, at stemmebiometrien hos personer i husstanden, registreres, således at brugerens stemmekarakteristika kan skelnes fra egenskaberne hos den person, der ønsker at blive genkendt. Biometrisk identifikation kan derfor medføre, at ikke-informerede personer underkastes biometrisk behandling ved at registrere deres stemmemodel og sammenligne den med stemmemodellen for den bruger, der ønsker at blive genkendt.
132. For at undgå en sådan indsamling af biometriske data uden de registreredes viden og samtidig gøre det muligt for en bruger at blive genkendt af assistenten, bør der prioriteres løsninger, der udelukkende er baseret på brugerens data. Konkret betyder dette, at biometrisk genkendelse kun aktiveres ved hver anvendelse på brugerens initiativ og ikke ved en permanent analyse af de stemmer, assistenten hører. De tilstedeværende personer kan for eksempel få et specifikt nøgleord eller spørgsmål med henblik på at få deres samtykke til at udløse biometrisk behandling. Brugeren kan eksempelvis sige "identifikation", eller

assistenten kan spørge, "ønsker du at blive identificeret?", hvorefter assistenten afventer et positivt svar for at aktivere biometrisk behandling.

Eksempel 12:

Hvis brugeren ønsker at installere biometrisk autentifikation med henblik på adgang til visse beskyttede data som for eksempel sin bankkonto, kan den digitale assistent vente med at aktivere brugerverifikationen, til brugeren åbner applikationen, og kontrollere den pågældendes identitet på denne måde.

## Anbefalinger

133. Stemmemodeler bør udelukkende genereres, opbevares og matches på den lokale enhed, ikke på fjernservere.
134. På grund af stemmemodellernes sensitivitet bør standarder som ISO/IEC 24745 og teknikker til beskyttelse af biometriske modeller<sup>49</sup> anvendes omhyggeligt.
135. Udbydere af digitale assistenter, der anvender stemmebaseret biometrisk identifikation, bør:
  - ) Sikre, at identifikationen er tilstrækkeligt præcis til pålideligt at knytte personoplysninger til de rette registrerede.
  - ) Sikre, at pålideligheden er ens for alle brugergrupper, ved at tjekke, at der ikke foreligger væsentlige skævheder for forskellige demografiske grupper.

## 3.9 Dataminimering

136. Dataansvarlige bør minimere mængden af data, der indsamles direkte eller indirekte og indhentes ved behandling og analyse, for eksempel ikke foretage analyse af brugerens stemme eller andre auditive oplysninger med henblik på at udlede oplysninger om brugerens psykiske tilstand, eventuelle sygdom eller livsomstændigheder.
137. Anvende standardindstillinger, der begrænser dataindsamling og/eller databehandling til det minimum, der er nødvendigt for at levere tjenesten.
138. Afhængigt af placering, konteksten for anvendelse samt mikrofonfølsomhed kan assistenten indsamle tredjeparters taledata som en del af baggrundsstøjen ved indsamling af brugernes tale. Selv om baggrundsstøj ikke omfatter taledata, kan den godt omfatte situationsdata, der kan behandles for at udlede oplysninger om emnet (f.eks. placering).

## Anbefalinger

139. Designere af digitale assistenter bør gøre brug af teknologier, der fjerner baggrundsstøj, med henblik på at undgå registrering og behandling af baggrundsstemmer og situationsoplysninger.

---

<sup>49</sup> Jf. for eksempel:

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 og A. K. Jindal, "*Biometric Template Protection Through Adversarial Learning*" 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2019, s. 1-6, doi: 10.1109/ICCE.2019.8661905.

### 3.10 Ansvarlighed

140. Dataansvarlige er i henhold til artikel 7, stk. 1, i databeskyttelsesforordningen forpligtet til at kunne påvise registreredes samtykke for al behandling, der er baseret på samtykke. Taledata kan anvendes til at påvise overholdelse (f.eks. påvise samtykke). Forpligtelsen til opbevaring af disse taledata vil da være bestemt af ansvarlighedskravene i den pågældende specifikke lovgivning.
141. Ved vurderingen af behovet for en konsekvensanalyse vedrørende databeskyttelse har Databeskyttelsesrådet fastsat kriterier<sup>50</sup>, som datatilsynsmyndigheder skal anvende til at udarbejde lister over behandlingsaktiviteter, hvor en konsekvensanalyse er påkrævet, og give eksempler på behandling, der sandsynligvis kræver en konsekvensanalyse. Det er meget sandsynligt, at assistenttjenester falder ind under de kategorier og betingelser, hvor det er fastslået, at de kræver en konsekvensanalyse. Dette omfatter overvejelser om, hvorvidt enheden kan observere, overvåge og kontrollere registrerede eller foretage systematisk overvågning i stort omfang, jf. artikel 35, stk. 3, litra c), anvendelse af "ny teknologi" eller behandling af følsomme oplysninger og oplysninger om sårbare registrerede.
142. Alle dataindsamlings- og behandlingsaktiviteter skal dokumenteres i overensstemmelse med artikel 30 i databeskyttelsesforordningen. Det omfatter al behandling, der involverer taledata.

### Anbefalinger

143. Hvis der skal anvendes talebeskeder til at informere brugerne i henhold til artikel 13, bør de dataansvarlige offentliggøre meddelelser om dette på deres websted, så de er tilgængelige for brugerne og datatilsynsmyndighederne.

### 3.11 Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger

144. Udbydere og udviklere af digitale assistenter bør overveje, om det er nødvendigt at have en registreret bruger for hver af deres funktionaliteter. Det er klart, at det er nødvendigt at have en registreret bruger til at administrere en kalender og en adressebog, men det er ikke lige så klart, at det at foretage et telefonopkald eller en internetsøgning kræver, at assistenten har en registreret bruger.
145. Som standard bør tjenester, der ikke kræver en identificeret bruger, ikke forbinde nogen af assistentens identificerede brugere med kommandoerne. En standardassistent, der efterlever krav om databeskyttelse og beskyttelse af personoplysninger, behandler kun brugeres personoplysninger til at udføre brugernes anmodninger og opbevarer ikke og registrerer ikke eksekverede kommandoer.
146. Nogle enheder kan kun afvikle én assistent, mens andre kan vælge mellem forskellige assistenter. Udbydere af assistenter bør udvikle branchestandarder, der muliggør dataportabilitet i henhold til artikel 20 i databeskyttelsesforordningen.
147. Nogle udbydere af assistenter har hævdet, at deres assistenter ikke kan slette alle brugeres oplysninger, selv når den registrerede anmoder herom. Udbydere af assistenter bør sikre, at alle brugeres data kan slettes på en brugers anmodning i henhold til artikel 17 i databeskyttelsesforordningen.

---

<sup>50</sup> Artikel 29-Gruppens retningslinjer om konsekvensanalyse vedrørende databeskyttelse (DPIA), wp248 rev. 01, godkendt af Databeskyttelsesrådet.

## 4 MEKANISMER TIL UDØVELSE AF REGISTREREDES RETTIGHEDER

148. I henhold til databeskyttelsesforordningen skal dataansvarlige, der leverer assistenttjenester, give alle brugere, registrerede såvel som ikke-registrerede, mulighed for at udøve deres rettigheder som registrerede i databeskyttelsessammenhæng.
149. Udbydere og udviklere af assistenter bør sikre de registreredes kontrol med deres personoplysninger igennem hele databehandlingsperioden, navnlig deres ret til indsigt, berigtigelse, sletning, deres ret til at begrænse behandlingen og, afhængigt af retsgrundlaget for behandlingen, deres ret til dataportabilitet og deres ret til indsigt.
150. Den dataansvarlige bør give oplysninger om den registreredes rettigheder på det tidspunkt, hvor de registrerede tænder en assistent, og senest på det tidspunkt, hvor den første brugers taleanmodning behandles.
151. Eftersom assistenters vigtigste interaktionsmiddel er tale, bør designere af assistenter sikre, at brugere, uanset om de er registrerede eller ej, kan udøve deres rettigheder som registrerede i databeskyttelsessammenhæng ved hjælp af letforståelige talekommandoer. Designere af assistenter samt appudviklere bør, hvis de indgår i løsningen, ved processens afslutning informere brugeren om, at der er taget højde for dennes rettigheder, enten i form af tale eller ved at sende en skriftlig meddelelse til brugerens mobiltelefon, konto eller ethvert andet middel, som brugeren har valgt.
152. Designere af digitale assistenter og appudviklere bør navnlig som minimum implementere specifikke værktøjer, der sikrer en effektiv måde at udøve sådanne rettigheder på. De bør derfor, hvad angår deres enheder, foreslå en måde at udøve registreredes rettigheder på som for eksempel ved at give den registrerede selvbetjeningsværktøjer som et profilstyringssystem.<sup>51</sup> Dette kan smidiggøre effektiv og rettidig håndtering af registreredes rettigheder og gøre det muligt for den dataansvarlige at inkludere identifikationsmekanismen i selvbetjeningsværktøjet.
153. For så vidt angår udøvelsen af de registreredes rettigheder i tilfælde af flere brugere, når en bruger, registreret eller ej, udøver en af sine rettigheder, bør den pågældende gøre dette, uden at det berører andre brugeres rettigheder. Alle brugere, registrerede såvel som ikke-registrerede, kan udøve deres rettigheder, så længe den dataansvarlige stadig behandler oplysningerne. Den dataansvarlige bør indføre en proces, der sikrer, at de registreredes rettigheder udøves.

### 4.1 Ret til indsigt

154. I henhold til artikel 12, stk. 1, i databeskyttelsesforordningen skal kommunikation i henhold til artikel 15 gives skriftligt eller med andre midler, herunder, hvis det er hensigtsmæssigt, elektronisk. For så vidt angår adgang til personoplysninger, der behandles, er det i artikel 15, stk. 3, fastsat, at hvis den registrerede fremsætter anmodningen elektronisk, og medmindre de registrerede anmoder om andet, bør oplysningerne gives i en almindeligt anvendt elektronisk form. Hvad der kan betragtes som en almindeligt anvendt elektronisk form, bør baseres på de registreredes rimelige forventninger og ikke på, hvilket format den

---

<sup>51</sup> Ved profilstyringssystem forstås et sted i assistentsystemet, hvor brugerne til enhver tid kan gemme deres præferencer, foretage ændringer og nemt ændre deres indstillinger for beskyttelse af personoplysninger

dataansvarlige anvender i sin daglige drift. Den registrerede bør ikke være forpligtet til at anskaffe specifik software eller hardware for at få adgang til oplysningerne.

155. Efter anmodning bør dataansvarlige derfor sende en kopi af personoplysninger, og navnlig lyddata (herunder taleoptagelser og -transskriptioner), i et almindeligt format, der kan læses af den registrerede.
156. Når der træffes afgørelse om, hvilken type format oplysningerne i henhold til artikel 15 skal gives i, skal den dataansvarlige være opmærksom på, at formatet bør gøre det muligt at præsentere oplysningerne på en måde, der både er letforståelig og lettilgængelig. Dataansvarlige bør også tilpasse oplysningerne til den specifikke situation for den registrerede, der fremsætter anmodningen.

#### Eksempel 13:

En dataansvarlig, der leverer en assistenttjeneste, modtager fra en bruger både en anmodning om adgang og en anmodning om dataportabilitet. Den dataansvarlige beslutter at give oplysningerne i en pdf-fil i henhold til både artikel 15 og artikel 20. I det tilfælde bør den dataansvarlige ikke anses for at behandle begge anmodninger korrekt. En pdf-fil opfylder teknisk set den dataansvarliges forpligtelser i henhold til artikel 15, men opfylder ikke den dataansvarliges forpligtelser i henhold til artikel 20.<sup>52</sup>

Det skal bemærkes, at den blotte henvisning til brugernes tidligere interaktioner med taleassistenten ikke synes at sætte den dataansvarlige i stand til at opfylde alle sine forpligtelser i henhold til retten til indsigt, da de tilgængelige oplysninger generelt kun udgør en del af de oplysninger, der behandles i forbindelse med leveringen af tjenesten.

157. Retten til indsigt bør ikke bruges til at modvirke/omgå principperne om dataminimering og -opbevaring.

## 4.2 Ret til berigtigelse

158. For at sikre retten til berigtigelse bør brugere, uanset om de er registreret eller ej, til enhver tid kunne administrere og opdatere deres personoplysninger gennem tale direkte fra assistentenheden som beskrevet ovenfor. Desuden bør der implementeres selvbetjeningsværktøjer i enheden eller en applikation for at gøre det nemt for dem at berigtige deres personoplysninger. Brugere bør informeres om opdateringen via tale eller skriftligt.
159. Mere generelt gælder retten til berigtigelse for alle den dataansvarliges udtalelser og inferens<sup>53</sup>, herunder profilering, og størstedelen af oplysningerne bør betragtes som meget subjektive.<sup>54</sup>

<sup>52</sup> WP29-retningslinjerne vedrørende retten til dataportabilitet — godkendt af Databeskyttelsesrådet, s. 18.

<sup>53</sup> At udtalelser og inferens kan betragtes som personoplysninger, er blevet bekræftet af EU-Domstolen, som bemærkede, at udtrykket "alle oplysninger" i definitionen af personoplysninger omfatter oplysninger, der "ikke blot er objektive, men også subjektive i form af udtalelser og vurderinger, forudsat at de "vedrører den registrerede" — sag C-434/16 *Peter Nowak v Data Protection Commissioner* ECLI:EU:C:2017:994 [34].

<sup>54</sup> Getting Data Subject Rights Right, A submission to the EDPB from data protection academics, november 2019.

### 4.3 Ret til sletning

160. Brugere, såvel registrerede som ikke-registrerede, bør til enhver tid kunne slette oplysninger om dem via tale fra assistenten eller via et selvbetjeningsværktøj, der er integreret i enhver enhed, der er forbundet med assistenten. Personoplysninger kan slettes af en registreret lige så let, som de afgives. Som følge af de iboende vanskeligheder med at anonymisere taledata samt de mange forskellige typer persondata, der indsamles fra, observeres hos og udledes om den registrerede<sup>55</sup>, kan retten til sletning i denne forbindelse næppe tilgodeses ved at anonymisere personlige datasæt. Da databeskyttelsesforordningen er teknologineutral, og teknologien udvikler sig hurtigt, er det dog ikke udelukket, at retten til sletning kan gøres effektiv gennem anonymisering.
161. Uden en tredjepartsskærm eller muligheden for at vise gemte data (f.eks. en mobilapplikation eller en tablet) er det i nogle tilfælde vanskeligt at få en forhåndsvisning af de registrerede spor med henblik på at vurdere anvisningernes relevans. Sammen med taleassistenten bør der leveres et dashboard (eller en applikation), der for at gøre brugen nemmere er bredt tilgængelig for brugere, med henblik på at slette anmodningshistorikken og tilpasse værktøjet til brugerens behov.<sup>56</sup>
162. I forbindelse med al databehandling og navnlig når registrerede, der er registrerede i datasammenhæng, giver samtykke til, at taleoptagelserne transskriberes og anvendes af udbyderen til at forbedre dennes tjenester, bør udbydere af assistenter efter anmodning fra brugeren kunne slette den oprindelige taleoptagelse samt enhver tilhørende transskription af personoplysningerne.
163. Den dataansvarlige bør sikre, at der ikke foretages behandling, efter at retten til sletning er udøvet. Med hensyn til tidligere foranstaltninger kan retten til sletning navnlig være underlagt visse juridiske og tekniske begrænsninger.

#### Eksempel 14:

Hvis en bruger forud for anmodningen om sletning har foretaget et onlinekøb ved hjælp af sin assistent, kan udbyderen af assistenten slette taleoptagelsen vedrørende onlinekøbet og sikre, at den ikke anvendes i fremtiden. Købet gælder dog stadig, og det gør den stemmestyrede ordre eller den skriftlige transskription, der behandles af e-handelswebstedet, også (her er undtagelsen baseret på e-handelswebstedets retlige forpligtelse).

Og tilsvarende hvis brugeren inden anmodningen om sletning har tilføjet et bestemt stykke musik til sin playliste ved hjælp af sin assistent, kan udbyderen af assistenten på samme måde slette den mundtlige anmodning, men ikke de tidligere konsekvenser af en sådan anmodning (sletningen påvirker ikke brugerens playliste).

164. På baggrund af ovenstående bør dataansvarlige, hvis de samme personoplysninger behandles med henblik på forskellige behandlingsformål, tolke anmodninger om sletning som et klart signal om at standse behandlingen af oplysningerne til alle formål, for hvilke der ikke foreligger en retlig undtagelse.

<sup>55</sup> Artikel 29-Gruppens udtalelse 05/2014 om anonymiseringsteknikker, vedtaget den 10. april 2014.

<sup>56</sup> "Assistants vocaux et enceintes connectées, l'impact de la voix sur l'offre et les usages culturels et médias", det franske "Conseil Supérieur de l'Audiovisuel", maj 2019.

I henhold til betingelserne i artikel 21, stk. 1, i databeskyttelsesforordningen bør oplysninger, der behandles på grundlag af assistentudbydernes legitime interesser, ikke udgøre en undtagelse fra retten til sletning, navnlig fordi registrerede ikke med rimelighed forventer yderligere behandling af deres personoplysninger.

#### 4.4 Ret til dataportabilitet

165. Den databehandling, som assistentudbyderne foretager, hører under dataportabilitet, da behandlingen hovedsagelig er baseret på den registreredes samtykke (i henhold til artikel 6, stk. 1, litra a), eller artikel 9, stk. 2, litra a), når det drejer sig om særlige kategorier af personoplysninger) eller på en kontrakt, som den registrerede er part i i henhold til artikel 6, stk. 1, litra b).
166. I praksis bør retten til dataportabilitet gøre det nemmere at skifte mellem forskellige assistentudbydere. I tilfælde af assistenter, der især anvendes i et digitalt miljø, og registreredes tale optages i en applikation eller på en platform, bør retten til dataportabilitet gives for alle personoplysninger, der afgives af den registrerede. Desuden bør den dataansvarlige give brugerne mulighed for at hente deres personoplysninger direkte fra deres brugerområde som et selvbetjeningsværktøj. Brugere bør også kunne udøve denne ret gennem talekommandoer.
167. Udbydere og udviklere af assistenter bør sikre de registrerede omfattende kontrol over de personoplysninger, der vedrører disse, med henblik på at give dem mulighed for at overføre personoplysninger fra én udbyder af assistenter til en anden. Dataregistrerede bør derfor modtage de personoplysninger, de har afgivet til den dataansvarlige, i et struktureret, almindeligt anvendt og maskinlæsbart format samt fra midler<sup>57</sup>, der bidrager til at besvare anmodninger om dataportabilitet (f.eks. downloadværktøjer og programmeringsgrænseflader til program)<sup>58</sup>. Som anført i retningslinjerne vedrørende retten til dataportabilitet bør den dataansvarlige i tilfælde af omfattende eller kompleks indsamling af personoplysninger, hvilket kan være tilfældet her, give en oversigt "*i en kortfattet, gennemsigtig, letforståelig og lettilgængelig form og i et klart og enkelt sprog*" (jf. artikel 12, stk. 1, i databeskyttelsesforordningen) på en sådan måde, at registrerede altid har klare oplysninger om, hvilke data de skal downloade eller videregive til en anden dataansvarlig i forbindelse med

---

<sup>57</sup> Jf. til illustration Artikel 29-Gruppens ræsonnement i retningslinjerne vedrørende retten til dataportabilitet — godkendt af Databeskyttelsesrådet, s. 16:

*"På et teknisk plan bør dataansvarlige undersøge og vurdere to forskellige og supplerende måder at stille oplysninger, som kan gøres til genstand for dataportabilitet, til rådighed for de registrerede eller andre dataansvarlige på:*

*- direkte transmission af det samlede datasæt af data, der kan gøres til genstand for dataportabilitet (eller en række uddrag af dele af det samlede datasæt)*

*- et automatisk værktøj, der gør det muligt at udtrække relevante data.*

*Den anden metode kan foretrækkes af dataansvarlige i tilfælde, hvor der er tale om komplekse og store datasæt, da det giver mulighed for at udtrække en hvilken som helst del af datasættet, som er relevant for den registrerede i forbindelse med den pågældendes anmodning, kan bidrage til at begrænse risikoen og eventuelt gøre det muligt at anvende datasynkroniseringsmekanismer (for eksempel i forbindelse med løbende kommunikation mellem dataansvarlige). Det kan være en bedre måde til at sikre, at den "nye" dataansvarlige overholder reglerne, og vil udgøre god praksis med hensyn til at begrænse risiciene for datasikkerheden fra den oprindelige dataansvarliges side".*

<sup>58</sup> I den henseende: Artikel 29-Gruppens retningslinjer vedrørende retten til dataportabilitet — godkendt af Databeskyttelsesrådet, s. 1.

et givet formål. Registrerede bør for eksempel være i stand til at anvende softwareapplikationer til nemt at identificere, genkende og behandle specifikke data fra dem.

168. Denne ret bør navnlig gøre det muligt for brugeren til personlig brug at hente de oplysninger, som den pågældende har afgivet ved hjælp af sin stemme (f.eks. historik over taleinteraktioner) og inden for rammerne af oprettelsen af sin brugerkonto (f.eks. efternavn og fornavn), til personlig brug.
169. Med henblik på fuld anvendelse af denne ret for registrerede i forbindelse med et digitalt indre marked bør designere af assistenter samt appudviklere navnlig udvikle fælles maskinlæsbare formater, der sikrer dataformatets indbyrdes kompatibilitet mellem assistentsystemer<sup>59</sup>, herunder standardformater for taledata. Teknologier bør struktureres med henblik på at sikre, at behandlede personoplysninger, herunder taledata, nemt og i fuldt omfang kan genbruges af den nye dataansvarlige.<sup>60</sup>
170. Hvad angår formatet, bør udbydere af assistenter levere personoplysninger ved hjælp af almindeligt anvendte åbne formater (f.eks. mp3, wav, csv, gsm osv.) sammen med egnede metadata, der anvendes til at beskrive betydningen af udvekslede oplysninger præcist.<sup>61</sup>

## 5 BILAG: AUTOMATISK TALEGENKENDELSE, TALESYNTese OG BEHANDLING AF NATURLIGT SPROG

171. Som følge af det teoretiske grundlag for signalbehandling, navnlig Claude Shannons informations- og prøvetagningsteorier, er automatisk talebehandling blevet et grundlæggende element i ingeniørvidenskaberne. I krydsfeltet mellem fysik (akustik, bølgeudbredelse), anvendt matematik (modellering, statistik), computervidenskab (algoritmer, læringsteknikker) og humaniora (perception, ræsonnement) er talebehandling hurtigt blevet opdelt i en lang række studieemner: identifikation og kontrol af den talende, automatisk talegenkendelse, talesyntese, følelsesdetektion osv. I løbet af de seneste omkring femten år har disciplinen som helhed gjort meget store fremskridt, hvilket en række faktorer bidrager til: forbedrede metoder, stor stigning i databehandlingskapaciteten og større mængder tilgængelige data.

### 5.1 Automatisk talegenkendelse (ASR)

172. Automatisk talegenkendelse (også kaldet tale til tekst) omfattede tidligere tre adskilte faser, der havde til formål at: 1) fastslå ved hjælp af en akustisk model, hvilke fonemer der blev sagt; 2) fastslå ved hjælp af en fonetikordbog, hvilke ord der blev sagt; 3) transskribere rækkefølgen af ord (sætning), der med størst sandsynlighed blev sagt, ved hjælp af en sprogmodel. I dag,

---

<sup>59</sup> I den henseende: betragtning 68 i databeskyttelsesforordningen; WP29-retningslinjerne vedrørende retten til dataportabilitet — godkendt af Databeskyttelsesrådet, s. 17.

<sup>60</sup> "I den henseende opfordrer betragtning 68 dataansvarlige til at udvikle indbyrdes kompatible formater, der muliggør dataportabilitet, men uden at de dataansvarlige forpligtes til at indføre eller vedligeholde behandlingssystemer, der er teknisk kompatible. Databeskyttelsesforordningen forbyder imidlertid dataansvarlige at etablere hindringer for overførslen" — WP29-retningslinjerne vedrørende retten til dataportabilitet — godkendt af Databeskyttelsesrådet, s. 5.

<sup>61</sup> Databeskyttelsesrådet opfordrer kraftigt til samarbejde mellem interessenter fra branchen og brancheorganisationer med henblik på sammen at udvikle et fælles sæt af indbyrdes kompatible standarder og formater for på den måde at opfylde kravene til retten til dataportabilitet.



hvor der er gjort fremskridt med dyb læring (en maskinlæringsteknik), tilbyder mange systemer komplet automatisk talegenkendelse. Her behøver man ikke gennemføre kompleks træning af tre forskellige modeller, og samtidig opnås større effektivitet med hensyn til resultater og behandlingstid. Næsten alle større digitale aktører tilbyder nu egne ASR-implementeringer, der nemt kan anvendes af API-systemer, men der findes også open source-systemer (f.eks. DeepSpeech<sup>62</sup> eller Kaldi<sup>63</sup>).

## 5.2 Behandling af naturligt sprog (NLP)

173. Behandling af naturligt sprog er et tværfagligt felt, der omfatter lingvistik, datalogi og kunstig intelligens, og som har til formål at udvikle værktøjer til behandling af naturligt sprog til en lang række applikationer. Forsknings- og anvendelsesområderne er talrige: syntaktisk analyse, maskinoversættelse, automatisk tekstgenerering og -opsummering, stavekontrol, systemer til besvarelse af spørgsmål, tekstmining, navngiven enhedsgenkendelse, sentimentanalyse osv. Konkret er formålet med NLP at give computere mulighed for at læse, forstå og udlede betydning af menneskelige sprog. Udviklingen af NLP-applikationer er en udfordring, fordi computerværktøjer traditionelt kræver, at mennesker interagerer med dem i et programmeringssprog, der er formelt, dvs. præcist, utvetydigt og stærkt struktureret. Den menneskelige tale er imidlertid ikke altid præcis. Den er ofte tvetydig, og den sproglige struktur kan afhænge af mange komplekse variabler, herunder slang, regionale dialekter og social kontekst.
174. Syntaks og semantisk analyse er to hovedteknikker, der anvendes sammen med NLP. Syntaks er kombinationen af ord i en sætning for at give grammatisk mening. NLP anvender syntaks til at vurdere betydningen af et sprog baseret på grammatiske regler. De anvendte syntaksteknikker omfatter parsing (grammatisk analyse af en sætning), ordsegmentering (der opdeler et stort stykke tekst i enheder), sætningsbrydning (der placerer sætningsgrænser i store tekster), morfologisk segmentering (der opdeler ord i grupper) og stemming (der opdeler bøjede ord i rodformer). Semantik indebærer brug og betydning bag ord. NLP anvender algoritmer til at forstå sætningers betydning og struktur. Teknikker, som NLP anvender sammen med semantik, omfatter disambiguering af ordbetydninger (som udleder betydningen af et ord baseret på kontekst), navngiven enhedsgenkendelse (som bestemmer ord, der kan kategoriseres i grupper) og generering af naturligt sprog (som anvender en database til at bestemme semantikken bag ord). Mens tidligere tilgange til NLP omfattede regelbaserede metoder, hvor simple maskinlæringsalgoritmer fik besked om, hvilke ord og sætninger der skulle søges efter i en tekst, og blev fodret med konkrete svar, når disse ordforbindelser dukkede op, er de nuværende NLP-metoder baseret på dyb læring, en type kunstig intelligens, der undersøger og anvender mønstre i data til at forbedre et programs forståelse.

## 5.3 Talesyntese

175. Talesyntese er kunstig produktion af menneskelig tale. Talesyntese er hovedsagelig blevet implementeret ved sammenkædning af taleenheder, der opbevares i en database. Denne teknik består i, at man blandt alle en aktørs optagelser, der tidligere er transskriberet til fonemer, stavelser og ord, vælger de lydblokke, der svarer til de ord, man ønsker assistenten skal sige, og samler dem en efter en med henblik på at danne en forståelig sætning med naturligt diktion. Alternativt kan en talesynthesizer inkorporere en model af stemmekanalen og

---

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

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

andre karakteristika ved menneskelig tale med henblik på at modellere parametrene for tale som for eksempel intonation, rytme og klang ved hjælp af generative statistiske modeller (f.eks. WaveNet<sup>64</sup>, Tacotron<sup>65</sup> eller DeepVoice<sup>66</sup>) og skabe et fuldstændigt syntetisk taleoutput.

---

<sup>64</sup> 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>

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

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