Helsedirektoratet

Dato:
13.09.2021

# Veileder i personvern for organisasjonene i DIGI-UNG

## Innhold

Helsedirektoratet

# 1. Om håndboken og personvernregelverket

## 1.1. Om DIGI-UNG-programmet og håndboken

Formålet med DIGI-UNG-programmet er å samordne tilbudet av digitale informasjons- og hjelpetjenester som er relevante for ungdom på tvers av sektorer. Dagens fragmenterte tilbud skal samordnes i et økosystem. De digitale tjenestene som formidles skal leveres av offentlige aktører som for eksempel Helsedirektoratet, Barne-, Ungdoms- og familiedirektoratet, Direktoratet for e-Helse, Utdanningsdirektoratet, Politidirektoratet, Arbeids- og velferdsdirektoratet, Klima- og miljødirektoratet, Forsvaret og Kommunesektorens organisasjon, men også av frivillige aktører.

Det finnes per dags dato over 20 chattjenester i DIGI-UNG nettverket. Noen bemannes av frivillige mens andre har ansatte som svarer på chathenvendelser fra ungdom. De som svarer på chat har ulik kompetanse, blant annet svarer noen som likepersoner og andre som fagpersoner. Felles for mange av organisasjonene er at de må orientere seg i et komplisert landskap hvor anonymitet, personvern, taushetsplikt og melde- og avvergelsesplikt, er sentralt. For å bistå organisasjonene i DIGI-UNG nettverket med problemstillinger knyttet til personvern, har Helsedirektoratet utarbeidet en håndbok i personvern og chat.

Håndboken er ikke uttømmende når det gjelder rettigheter og plikter som kan følge av personvernregelverket, men tar for seg sentrale temaer som vil være relevant for chat-tjenester rettet mot barn og unge. Det er viktig at den enkelte organisasjon setter seg inn i håndboken, og vurderer chattetjenestene i lys av anbefalingene og rådene i veilederen.

## 1.2. Om personvernregelverket

20. juni 2018 fikk Norge et nytt personvernregelverk som er en direkte følge av EUs personvernforordning (GDPR). Personvernforordningen etterfølger den tidligere norske personvernlovgivningen, og den skjerper kravene til virksomheters behandling av personopplysninger på flere områder. GDPR er i norsk rett inntatt gjennom en henvisningsbestemmelse i Personopplysningsloven. Personopplysningsloven og GDPR vil i håndboken samlet bli omtalt som personvernregelverket.

Formålet med personvernregelverket er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger, og skal bidra til at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn. Sentralt er det enkelte menneskets krav på respekt for egen integritet og privatlivets fred. Personvern er derfor nært knyttet til enkeltindividers rett til privatliv, selvbestemmelse og selvutfoldelse.

Det er Helsedirektoratets oppfatning at samfunnet generelt, men også barn og unge spesielt, stiller større krav til åpenhet og profesjonalitet i virksomhetens behandling av personopplysninger. Godt personvern vil ikke bare bidra til bedre etterlevelse av regelverket, men skaper også større tillit til tjenestene som behandler personopplysninger.

## 2. Personvern for barn og unge

Barn og unge har samme krav på personvern som voksne. I FNs barnekonvensjon fremgår det at alle barn har rett til privatliv.

Etter personvernregelverket har barn et særskilt krav på beskyttelse. Begrunnelsen er at barn kan være mindre bevisste på hva behandling av personopplysninger innebærer, konsekvenser av behandlingen, og rettighetene de har. Datatilsynet skriver på sin nettside at for tjenester som retter seg mot unge må man *"tenke ekstra nøye gjennom hvilke data som samles inn, hvordan dataene brukes, hvordan dataene beskyttes, og hvordan tjenestene kan gi informasjon som er forståelig og tilpasset målgruppen".*[1] Det sistnevnte er særlig viktig for at unge skal forstå hva behandlingen av personopplysninger innebærer, og konsekvenser av handlinger på digitale plattformer.

Et annet viktig aspekt er at kravene til informasjonssikkerhet skjerpes når barns personopplysninger behandles. Den som behandler opplysningene, må derfor ha iverksatt både tekniske og organisatoriske tiltak som sørger for at barns personopplysninger har et tilstrekkelig beskyttelsesnivå.

## 3. Noen grunnleggende personvernprinsipper

Personvernregelverket er et nokså omfattende regelverk, men felles for reglene er at de bygger behandlingen av personopplysninger på noen grunnleggende prinsipper. Personvernprinsippene er beskrevet i personvernforordningens artikkel 5. Alle som behandler personopplysninger må opptre i samsvar med prinsippene.

I denne håndboken fremhever vi seks prinsipper som er særlig relevante: *lovlighet* og *åpenhet, formålsbegrensning, dataminimering*, *lagringsbegrensning* og *integritet,* samt *konfidensialitet*.

*Lovlighet og åpenhet*
Ingen har lov til å behandle personopplysninger uten at det finnes et rettslig grunnlag for den behandlingen en virksomhet ønsker å gjøre, se også håndbokens pkt. 6.[2] Personvernforordningen lister opp en rekke behandlingsgrunnlag i art. 6 og 9. Et slikt grunnlag kan være en lovpålagt plikt, samtykke fra data subjektet, avtale eller berettiget interesse m.m. Virksomheten må selv vurdere lovligheten av behandlingen før den starter. Prinsippet om åpenhet betyr at behandlingen skal være forutsigbar for den opplysningene gjelder, og at det gis tilstrekkelig med informasjon.

*Formålsbegrensning*
Personopplysninger skal kun behandles for spesifikke, uttrykkelige, angitte og legitime formål. Det innebærer at virksomheten må ha et tydelig og definert formål med innhentingen av personopplysningene.

*Dataminimering*
Prinsippet kan ses i sammenheng med prinsippet om formål ovenfor, og innebærer at virksomheten skal begrense behandlingen av personopplysninger til et minimum - det som er nødvendig og relevant.

---

[1] Digitale tjenester og forbrukeres personopplysninger | Datatilsynet
[2] I loven omtalt som et *behandlingsgrunnlag*,

*Lagringsbegrensning*
Personopplysninger skal slettes eller anonymiseres når de ikke lengre er nødvendige for formålet de ble samlet inn for. Virksomheten bør ha tiltak som sikrer dette ved å ha rutiner og systemer for sletting. Se mer om lagring og sletting i pkt. 8.

*Integritet* og *konfidensialitet*
Integriteten og konfidensialiteten til personopplysningene skal beskyttes. Konfidensialiteten knytter seg til at opplysningene ikke blir kjent for uvedkommende, og integriteten handler om at opplysningene ikke blir endret utilsiktet. Det innebærer ikke bare å få på plass tilstrekkelig informasjonssikkerhet mot eksterne trusler, men også å ha gode interne systemer og rutiner. Et eksempel er rutiner for tilgangskontroll slik at kun personer med tjenstlig behov har tilgang til opplysningene.

# 4. Hva er en personopplysning?

Personvernregelverket gjelder ved "behandling av personopplysninger". En personopplysning er opplysninger og vurderinger som kan knyttes til en enkeltperson og er i regelverket definert som *"enhver opplysning om en identifisert eller identifiserbar fysisk person; en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres (…)".*

Typisk vil personopplysninger være kontaktopplysninger som navn, adresse og mobilnr., men omfatter i praksis alle typer opplysninger som kan bidra til å identifisere en enkeltperson, enten direkte eller indirekte. Ved siden av forannevnte eksempler kan en personopplysning eksempelvis være informasjon om en sinnstilstand, adferdsmønstre, slik som hvilke butikker du går i, tv-serier du ser på m.m. En nettidentifikator, slik som en IP-adresse, regnes som en personopplysning.

Loven definerer også særlig kategori av opplysninger (sensitive personopplysninger) som det skal mer til å kunne behandle enn andre opplysninger. Det gjelder bl.a. helseopplysninger, opplysninger om religion, seksuell legning, politisk oppfatning, m.m.[3]

I tillegg må det skje en «*behandling*» av personopplysninger. I loven er behandling definert som *"enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, for eksempel innsamling, registrering, strukturering, lagring (…)».*

## 2.1. Når behandles personopplysninger i chat?

Organisasjonene i DIGI-UNG-programmet må gjøre egne vurderinger av om chatten den enkelte organisasjon tilbyr *"behandler personopplysninger".* Noen typetilfeller kan likevel tenkes:

*Eksempel 1:*
Hvis bruker av tjenesten må oppgi kontaktinformasjon i predefinert felt før oppstart av chat, f.eks. navn, epost, mobilnr., m.m.

[3] Retningslinjer for bruk av videoenheter | Datatilsynet

*Eksempel 2:*
Ved lagring av IP-adresse. IP-adresse[4] regnes i utgangspunktet som en personopplysning ettersom det er en nettidentifikator som kan bidra til identifisering.

*Eksempel 3:*
Hvis bruker av tjenesten oppgir personopplysninger i chatsamtalen. Det kan f.eks. være at bruker av tjenesten oppgir navn, adresse, mobilnr. eller annen informasjon som er egnet til å identifisere personen.

*Eksempel 4:*
Personopplysninger er som nevnt tidligere også informasjon som indirekte kan bidra til å identifisere bruker av tjenesten. Isolert sett vil ikke opplysninger om kjønn, alder m.m. være identifiserende, men hvis denne informasjonen kan sammenstilles med annen informasjon i chatdialogen, kan det være at opplysningene samlet sett er egnet til å identifisere vedkommende. I slike tilfeller vil det skje en behandling av personopplysninger.

Ved behandling av personopplysninger må virksomheten forholde seg til, og etterleve kravene i personvernregelverket. De aller fleste kravene i personvernregelverket er rettet mot den som loven omtaler som behandlingsansvarlig.

## 5. Ansvarsplassering - *behandlingsansvarlig* og *databehandler*

Personvernregelverket skiller mellom rollen som *behandlingsansvarlig* og *databehandler*.[5] Rollen har betydning for hvilket ansvar virksomheten har etter regelverket. Det er den som er behandlingsansvarlig som er pålagt hovedvekten av pliktene. Før virksomheten skal behandle personopplysninger er det viktig å avklare hvilken rolle virksomheten har.

Det er den behandlingsansvarlige som *bestemmer* over personopplysningene, mens databehandleren opptrer *på vegne* av den behandlingsansvarlige.

En databehandler vil normalt ikke ha et eget rettslig grunnlag eller formål for å behandle personopplysningene, og en databehandler kan i utgangspunktet ikke bestemme selv hvordan opplysningene skal behandles ettersom en databehandler kun skal behandle personopplysningene etter *instruks* fra den behandlingsansvarlige. Instruks gis normalt i en databehandleravtale eller på annen skriftlig måte.

En databehandlersituasjon foreligger typisk i de tilfeller der den behandlingsansvarlige setter ut hele eller deler av arbeidet (behandlingen av personopplysninger) til en annen virksomhet, som den behandlingsansvarlige kunne gjort selv. Eksempler på typiske databehandlere er driftsleverandører av IT-tjenester, skytjenesteleverandører, leverandører av HR-tjenester eller regnskapssystemer.

For organisasjonene i DIGI-UNG-programmet må rollene vurderes ved bruk av samarbeidspartnere og tekniske underleverandører. Selv om Helsedirektoratet ikke har vurdert dette konkret for hver

[4] Dynamisk IP-adresse regnes som en personopplysning. Se mer om dette her: Dynamiske IP-adresser | Datatilsynet
[5] I helsesektoren benyttes begrepet *dataansvarlig* istedenfor *behandlingsansvarlig*. Det skyldes at begrepet behandlingsansvarlig ikke skal forveksles med den som yter helsehjelp.

enkelt organisasjon, er det mest nærliggende at organisasjonen som tilbyr chat er behandlingsansvarlig.

### 5.1. Databehandleravtale

Når en databehandler behandler personopplysninger på vegne av en behandlingsansvarlig skal behandlingen være underlagt en databehandleravtale, jf. personvernforordningen artikkel 28. Databehandleravtalen vil utgjøre *behandlingsgrunnlaget* til databehandler. Det er behandlingsansvarlig som har plikten til å få på plass en databehandleravtale.

Personvernforordningen artikkel 28 stiller en rekke krav til innholdet i en databehandleravtale. Eksempelvis skal avtalen blant annet regulere hensikten med og varigheten av behandlingen, behandlingens formål og art, typen av personopplysninger, kategorier av registrerte, samt den behandlingsansvarliges rettigheter og plikter.

Hensikten med en slik avtale er å sette en klar ramme for hvordan databehandleren kan behandle personopplysninger og sørge for at dette skjer i samsvar med regelverket. Ansvaret for at vilkårene i en slik avtale etterlever personvernregelverket ligger hos den behandlingsansvarlige.

### 5.2. Sjekkliste:

- Har virksomheten definert hvilken rolle den har etter regelverket i forbindelse med tilbud om chat?
- Er det inngått nødvendig databehandleravtale med leverandør?

## 6. Behandlingsgrunnlag

All behandling av personopplysninger skal ha et lovlig grunnlag, jf. prinsippet om lovlighet nevnt i pkt. 4. Personvernforordningen bruker uttrykket *behandlingsgrunnlag* og lister opp flere mulige grunnlag i forordningens artikkel 6. Eksempler på mulige grunnlag er nødvendigheten av å oppfylle en avtale, den registrerte har samtykket til behandlingen, eller behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse. Før behandlingen av personopplysninger starter må virksomheten ha identifisert om det finnes et behandlingsgrunnlag.

I denne håndboken går vi nærmere inn på kravene til samtykke som ett av flere behandlingsgrunnlag. Den enkelte virksomhet må selv vurdere om dette er et egnet behandlingsgrunnlag for chatten som tilbys.

### 6.1. Bruk av samtykke overfor barn og unge

Hovedregelen er at barn som er fylt 15 år kan samtykke til innhenting og bruk av egne personopplysninger. For barn under 15 år må foreldrene samtykke på vegne av barnet. Det finnes imidlertid unntak fra denne hovedregelen. Ett unntak er ved bruk av nettjenester og apper, såkalte informasjonssamfunnstjenester. I Norge er aldersgrensen for å kunne samtykke til slike tjenester satt til 13 år. Det er Helsedirektoratets oppfatning at chattene som tilbys gjennom DIGI-UNG programmet som et utgangspunkt må vurderes som informasjonssamfunnstjenester.

Det kan være greit å være klar over at særlige kategorier av personopplysninger (slik som helseopplysninger m.m.) som hovedregel bare kan innhentes etter samtykke fra foreldre frem til barnet er fylt 18 år. Her finnes det imidlertid også unntak, bl.a. i helselovgivningen.

En særskilt problemstilling er hva som kan være et egnet behandlingsgrunnlag for de under 13 år som ikke har samtykkekompetanse. Et mulig grunnlag kan være virksomhetens "berettigede interesse". I en nylig veileder fra det Britiske Datatilsynet om online-tjenester rettet mot barn er berettiget interesse fremhevet som et mulig behandlingsgrunnlag for tjenester rettet mot barn på digitale flater. Om virksomheten har en "berettiget interesse" beror på en interesseavveining som må dokumenteres. Datatilsynet viser her hvilke hensyn som skal legges vekt på i vurderingen: Behandlingsgrunnlag | Datatilsynet.

Et annet behandlingsgrunnlag som er relevant er lov. Melde- og avvergelsesplikten er aktuelle lovgrunnlag der man ikke har innhentet samtykke. Det er imidlertid viktig å være klar over at det først er når melde- eller avvergelsesplikten utløses, at det vil kunne utgjøre er grunnlag for behandling av personopplysninger.

#### *6.1.1. Krav til utforming av samtykke*

Personvernforordningen stiller særskilte krav til hva som er et gyldig samtykke. Det må være frivillig, informert, spesifikt, utvetydig, gitt gjennom en aktiv handling, dokumenterbart og mulig å trekke tilbake like lett som det ble gitt. Det stilles med andre ord nokså strenge krav til hvordan et samtykke skal være utformet.

Samtykket må være frivillig. Et samtykke vil ikke være frivillig dersom bruker av tjenesten ikke har reell valgfrihet, eller ikke er i stand til å nekte å gi eller trekke tilbake et avgitt samtykke uten at det er til skade for vedkommende. Den behandlingsansvarlige bør kunne påvise at bruker av tjenesten har samtykket til behandling, helst i form av en samtykkeerklæring. Forhåndsutarbeidede samtykkeerklæringer bør være utarbeidet i lett og forståelig form, være skrevet med enkelt språk, og ikke inneholde urimelige vilkår.

Bruker av tjenesten må også vite spesifikt hva man samtykker til. En forespørsel om samtykke må vise hvem den behandlingsansvarlige er, formålet for hver enkelt behandling som virksomheten ber om samtykke til, og hvilke personopplysninger som samles inn. I tillegg må forespørselen inneholde informasjon om retten til å trekke tilbake samtykke, informasjon om eventuelle automatiserte avgjørelser og informasjon om risiko og tiltak ved eventuell overføring utenfor EU/EØS-området.

Samtykket er bare gyldig dersom formålet for behandling er klart og presist formulert. Dersom en samtykkeerklæring bare retter seg mot et spesifikt formål, kan man ikke bruke personopplysningene til annet enn dette.

Selve samtykket har ingen formkrav, og kan være muntlig eller skriftlig. Det er imidlertid lite praktisk med muntlig samtykke dersom man skal kunne dokumentere at samtykke er avgitt. Et gyldig samtykke forutsetter en aktiv handling fra bruker av tjenesten. Den aktive handlingen kan for eksempel være å klikke på en knapp eller skrive under på et skjema. Passivitet, stillhet eller bokser som er avhaket på forhånd utgjør ikke gyldig samtykke.

Til enhver tid skal bruker av tjenesten ha rett til å trekke sitt samtykke, og den behandlingsansvarlige må sørge for at denne retten er ivaretatt. Det skal være like enkelt å trekke tilbake som å gi samtykke. Likevel betyr ikke det at samtykke må kunne trekkes tilbake på nøyaktig samme måte som det opprinnelig ble gitt. Før samtykke gis må den enkelte få informasjon om retten til å trekke samtykke tilbake. Normalt vil konsekvensene av å trekke tilbake samtykke være at virksomheten må slette de lagrede opplysningene.

Samtykket må være dokumenterbart, men virksomheten må også kunne dokumentere at alle lovens krav til samtykke er oppfylt. Hvordan dette skal gjøres er opp til virksomheten, men er som regel hensiktsmessig å dokumentere gjennom en samtykkeerklæring.

### 6.1.2. Eksempler på samtykkeerklæringer i chat:

Nedenfor har Helsedirektoratet utarbeidet to eksempler på hvordan en samtykkeerklæring kan utformes ved innhenting av samtykke.

Samtykke 1 (IP-adresse og chatdialog)

*Når du bruker denne chatten vil IP-adressen din bli lagret i [X timer] før den slettes. Grunnen til det er at i tilfelle det skjer noe veldig alvorlig med deg, for eksempel at ditt liv eller helse står i fare, så kan vi tilkalle hjelp. Innholdet i chatsamtalen vil lagres i [X timer] for kvalitetssikring. Det vil ikke bli samlet inn andre opplysninger om deg.*

*Det er frivillig å samtykke, og du kan når som helst trekke ditt samtykke tilbake ved å sende en melding i chatten. Hvis liv eller helse står i fare vil vi likevel kunne tilkalle hjelp.*

*Jeg godtar [avkrysningsboks]*

*Her finner du mer informasjon om hvordan [navn på organisasjonen] behandler opplysninger om deg: [lenke personvernerklæring/privacy policy].*

Samtykke 2 (kun samtalelogg)

*Når du bruker denne chatten vil innholdet i chatsamtalen lagres i [X timer] for kvalitetssikring. Det vil ikke bli samlet inn andre opplysninger om deg.*

*Det er frivillig å samtykke, og du kan når som helst trekke ditt samtykke tilbake ved å sende en melding i chatten. Hvis liv eller helse står i fare vil vi likevel kunne tilkalle hjelp.*

*Jeg godtar [avkrysningsboks]*

*Her finner du mer informasjon om hvordan [navn på organisasjonen] behandler opplysninger om deg: [lenke personvernerklæring/privacy policy].*

I personvernerklæringen (som det henvises til) kan det kort forklares hva samtykke er og hva som menes med IP-adresse.

Om samtykke:

*Norsk lov stiller krav om at det må innhentes spesiell tillatelse (samtykke) for å lagre personopplysninger. Før du begynner å chatte med oss vil vi derfor be om din tillatelse til å lagre internettadressen (IP-adresse) og chatsamtalen.*

Om IP-adresse:

*I starten av chatten blir din internettadresse (IP-adresse) lagret hos oss. Internettadressen kan brukes til å identifisere mobilen eller PCen din, og kan derfor brukes til å identifisere deg. Dette kalles derfor en personopplysning.*

### 6.2. Sjekkliste:

- Er behandlingsgrunnlag fastsatt før behandlingen av personopplysningen starter?
- Er behandlingsgrunnlaget dokumentert? F.eks. dokumentert gjennom en samtykkeerklæring.

## 7. Personvernerklæring

Personopplysninger skal behandles på en åpen og gjennomsiktig måte, jf. prinsippet om åpenhet pkt. 3. Informasjonsplikten er regulert i GDPR art. 12, 13 og 14. Bruker av tjenesten har rett til informasjon fra den behandlingsansvarlige, både dersom personopplysningene er samlet inn fra bruker selv og dersom de er samlet inn fra andre kilder. I forbindelse med tilbud om chat vil personopplysninger normalt innhentes direkte fra bruker. En samtykkeerklæring og en personvernerklæring er to forskjellige til. Et samtykke skal ivareta kravet om rettslig grunnlag for behandlingen, mens personvernerklæring skal ivareta kravet til åpenhet og informasjon.

Informasjonsplikten er viktig for å sikre åpenhet og for å danne grunnlaget for at bruker av tjenesten skal kunne utøve sine rettigheter.

Den behandlingsansvarlige skal gi informasjon om både virksomheten, behandlingen og om forholdet til andre virksomheter. Det skal blant annet gis informasjon om:

- Kontaktinformasjon til virksomheten og et eventuelt personvernombud
- Hvem som er behandlingsansvarlig
- Hvilke personopplysninger som behandles (og eventuelt hvilke kategorier)
- Hvilke formål personopplysningene behandles for
- Det rettslige grunnlaget for behandlingen
- Hvordan personopplysningene samles inn
- Hvor lenge personopplysningene lagres
- Hvilke rettigheter den registrerte har og hvordan disse kan utøves
- Hvem personopplysningene deles med og eventuelt utleveres til
- Hvorvidt personopplysninger overføres til land utenfor EU/EØS, og hvordan bestemmelsene i GDPR kapittel V er oppfylt.

Informasjon skal gis på en kortfattet, åpen, forståelig og lett tilgjengelig måte og på et klart og enkelt språk. Språket må tilpasses til den målgruppen som informasjonen retter seg mot. Dette innebærer blant annet at vage formuleringer bør unngås, at god struktur bør være på plass og at informasjonen som gis må være adskilt fra annen informasjon (for eksempel brukervilkår). Det skal være enkelt for bruker av tjenesten å finne informasjonen og forstå den.

Personvernforordningen beskriver ikke hvordan informasjon skal gis, men utgangspunktet er at informasjonen skal gis skriftlig. Det er vanlig å gi informasjon gjennom en såkalt personvernerklæring. Denne personvernerklæringen kan ligge lett tilgjengelig, eksempelvis på virksomhetens nettside.

### 7.1. Sjekkliste:

- Gir virksomheten informasjon til bruker av tjenesten på en kortfattet, åpen, forståelig og lett tilgjengelig måte og med et klart og enkelt språk? F.eks. gjennom en personvernerklæring.

## 8. Lagring og sletting

Personopplysninger skal slettes eller anonymiseres når de ikke lengre er nødvendige for formålet de ble samlet inn for, jf. prinsippet om lagringsbegrensning pkt. 3.

Det finnes ingen "standardperiode" for oppbevaring og sletting etter personvernregelverket, noe som betyr at det er den enkelte virksomhet som må vurdere hvor lenge personopplysningene skal lagres, og når de skal slettes. Lovens slettekrav er rettet mot den enkelte opplysning, og ikke mot det dokumentet eller systemet som opplysningen finnes i.

Spørsmålet om hvorvidt en personopplysning som skal slettes må ses i sammenheng med formålet med behandlingen. Det vil si at når formålet med behandlingen av opplysningene er nådd, skal opplysningene slettes. Dette må vurderes konkret av den enkelte virksomhet.

Det er virksomhetens ansvar å sørge for å ha systemer og rutiner som sikrer at sletting blir gjennomført. For organisasjonene i DIGI-UNG-programmet vil det bl.a. kunne omfatte rutiner for oppbevaring og sletting av IP-adresse og chatsamtaler som inneholder personopplysninger. Et alternativ til å slette hele chatlogger er å anonymisere innholdet slik at vedkommende ikke kan identifiseres. I slike tilfeller står man friere til å bruke innholdet til andre formål.

### 8.1. Sjekkliste:

- Har virksomhetene rutiner som sørger for sletting eller anonymisering av personopplysninger når det ikke lenger er nødvendig for formålet de ble samlet inn for?

## 9. Registrertes rettigheter[6]

Enkeltpersonen som de lagrede personopplysningene kan knyttes til (bruker av tjenesten) har en rekke rettigheter etter personvernregelverket. Disse rettighetene er samlet i personvernforordningen kapittel 3.

Den behandlingsansvarlige må legge til rette for mottakelse, håndtering og oppfyllelse av henvendelser fra bruker av tjenesten om utøvelse av sine rettigheter. Bruker av tjenesten skal få informasjon om tiltak som er truffet på grunnlag av en anmodning om utøvelse av rettigheter uten ugrunnet opphold, og som hovedregel senest innen én måned.

Tre særlig relevante rettigheter er: *retting, sletting og innsyn.*

*Retting*

Etter GDPR art. 16 har bruker av tjenesten rett til å kreve at uriktige eller ufullstendige personopplysninger blir rettet eller supplert uten ugrunnet opphold. Bruker av tjenesten må kunne sannsynliggjøre at de aktuelle personopplysningene er uriktige eller ufullstendige og hva som er korrekt.

*Sletting*

Retten til sletting følger av GDPR art. 17, og innebærer at bruker av tjenesten kan kreve at personopplysningene blir slettet uten ugrunnet opphold i enkelte opplistede tilfeller:

[6] «Den registrerte» er uttrykket loven bruker om den som de lagrede personopplysningene kan knyttes til.

- Dersom personopplysningene ikke lenger er nødvendige for formålet som de ble samlet inn eller behandlet for (formålet er nådd).
- Dersom den behandlingsansvarlige behandler personopplysninger på bakgrunn av samtykke, og den registrerte trekker tilbake samtykket.
- Dersom bruker av tjenesten protesterer mot behandlingen.
- Dersom personopplysningene har blitt behandlet ulovlig.

Det oppstilles imidlertid også enkelte unntak fra retten til sletting. Noen relevante unntak er:

- For å oppfylle en rettslig forpliktelse, for eksempel avvergelsesplikt ved fare for liv og helse eller meldeplikt til barnevernet,
- For å utføre en oppgave i allmennhetens interesse (eksempelvis folkehelse) eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt.

*Innsyn*

Rett til innsyn følger av GDPR art. 15. Bruker av tjenesten har rett til å spørre virksomheten om hvorfor personopplysningene er lagret, hvordan de behandles og hvilke opplysninger som er lagret. Bruker av tjenesten kan for eksempel stille spørsmål om hva som er formålet med behandlingen av personopplysninger og hvor lenge de lagres eller hvem opplysningene utleveres til. I tillegg kan bruker av tjenesten be om å få en kopi av alle personopplysningene sine, og dette gjelder også elektroniske spor og metadata.

En virksomhet kan i visse tilfeller nekte innsyn, blant annet dersom:

- Det er nødvendig å holde opplysningene hemmelige av hensyn til forebygging og etterforskning av straffbare handlinger.
- Det ikke er hensiktsmessig at bruker av tjenesten får kjennskap til opplysningene av hensyn til helse eller forholdet til pårørende.
- Opplysningene er omfattet av lovfestet taushetsplikt.

Dersom virksomheten mener at et av unntakene får anvendelse skal bruker av tjenesten få skriftlig begrunnelse senest innen én måned med klar og presis informasjon om hvilket unntak som er relevant.

### 9.1. Sjekkliste:

- Gir virksomheten bruker av tjenesten informasjon på en forståelig måte om sine rettigheter og hvordan personopplysningene behandles? F.eks. i en personvernerklæring jf. punkt 7?
- Har virksomheten lagt til rette for tekniske og organisatoriske tiltak slik at bruker av tjenesten kan få innfridd sine rettigheter?

## 10. Overføring av personopplysninger til utlandet

GDPR gjelder innenfor EU/EØS-området, dvs. alle EU-land og Island, Liechtenstein og Norge. Ved overføring av personopplysninger til et land etablert utenfor EU/EØS-området gjelder spesielle krav for overføringen. I praksis innebærer det at virksomheten må sørge for at personopplysningene har det samme beskyttelsesnivået i utlandet som det ellers har innenfor EØS-området.

Sommeren 2020 kom EU-domstolen med en avgjørelse (såkalte Schrems II-avgjørelsen) som gjør det vanskeligere å overføre personopplysninger ut av EU/EØS. I tillegg til å ha et overføringsgrunnlag, må virksomheten undersøke om beskyttelsesnivået som vil oppnås i praksis, faktisk er tilsvarende som i EØS. Her er det blant annet særlig viktig å undersøke om det finnes overvåkingslover eller andre lover som gir myndighetene i tredjeland uforholdsmessig stor adgang til dataene.[7] Hvis det er omstendigheter i mottakerlandet som senker beskyttelsesnivået (overvåkningslover, m.m.) kan det være nødvendig å iverksette ytterligere tiltak (tekniske, juridiske, organisatoriske).

Det er virksomheten som er behandlingsansvarlig som har ansvaret med å sørge for at personopplysningene behandles (lagres) i henhold til regelverket, og at det ikke skjer overføringer av personopplysninger til utlandet som ikke er forenlig med GDPR.

Praktiske situasjoner hvor det kan skje en overføring av personopplysninger er hvis virksomheten benytter underleverandører (databehandlere) som har servere med datalagring i utlandet (utenfor EU/EØS). Et annet eksempel kan være at virksomheten har et driftssenter i Norge, men har en serviceavtale med en leverandør i utlandet for (eks. for feilretting og programvareoppgraderinger) som dermed får tilgang til infrastrukturen og dataene i Norge.

Sjekkliste:

- Har virksomheten oversikt over hvor virksomheten lagrer personopplysninger geografisk?
- Har virksomheten rutiner/strategi for datalagring?
- Sørger virksomheten at det ikke skjer overføring av personopplysninger til utlandet som er uforenlig med GDPR?

# 11. Informasjonssikkerhet – risikovurderinger

## 11.1. Overordnet vurdering av personvernkonsekvenser

Personvernregelverket stiller krav til informasjonssikkerhet. Både behandlingsansvarlig og databehandler skal gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med tanke på den konkrete risikoen ved virksomhetens behandling av personopplysninger. Dette følger av GDPR art. 32.

For å avklare hvilke tiltak som er nødvendige må det foretas en overordnet vurdering av personvernkonsekvenser. Det innebærer en vurdering av sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter (ROS-analyse).

For valg av tiltak kan det i tillegg til denne vurderingen tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i.

Aktuelle tiltak er normalt:

- Tekniske tiltak (f.eks. kryptering) for å sikre vedvarende fortrolighet, integritet, tilgjengelighet og robusthet i it-systemer;
- Tekniske og organisatoriske tiltak for tilgangsstyring; sikre at kun personer med tjenstlig behov[8] har tilgang til personopplysningene

[7] Spørsmål og svar om nye regler for overføring av personopplysninger til land utenfor EØS | Datatilsynet

[8] Det som er nødvendig for at en ansatt/frivillig skal utføre jobben sin.

- Opplæring av medarbeidere, bl.a. i forhold til krav om ivaretakelse av taushetsplikt, informasjonssikkerhet og personvern.
- Pseudonymisering eller anonymisering av personopplysninger der dette er hensiktsmessig;

Den enkelte virksomheten må vurdere hvilke tiltak som er hensiktsmessige for å sikre tilstrekkelig informasjonssikkerhet. Det bør alltid opprettes en prosedyre for regelmessig testing, analysering og vurdering av hvor effektive de tekniske og organisatoriske sikkerhetstiltak er.

### 11.2. Konkret vurdering av personvernkonsekvenser (DPIA)

Dersom det er trolig at en type behandling vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet. Dette følger av GDPR art. 35, og omtales som en DPIA. Høy risiko for personvernet kan oppstå når det behandles personopplysninger om barn og unge.

Datatilsynet gir på sine nettsider veiledning om i hvilke situasjoner det er nødvendig å gjennomføre en DPIA.[9] Første steget i en DPIA er å vurdere nødvendigheten av å gjennomføre en slik konsekvensanalyse og dokumentere denne vurderingen.

### 11.3. Sjekkliste:

- Er det gjennomført en overordnet risikovurdering av personvernkonsekvenser?
- Er det implementert nødvendige tiltak for å ivareta informasjonssikkerheten?
- Er nødvendigheten av en DPIA vurdert?
- Velger behandlingsansvarlig leverandører som er i stand til å levere tjenester som oppfyller lovbestemte krav og krav i personvernregelverket?

## 12. Avvikshåndtering – varsling til Datatilsynet

Skjer det et brudd på personopplysningssikkerheten (personvernbrudd), skal dette varsles til Datatilsynet. Det er behandlingsansvarlig som har ansvaret for å melde et avvik til Datatilsynet. Meldingen skal være skriftlig, men Datatilsynet kan varsles først på telefon dersom det er viktig at Datatilsynet blir raskt kjent med avviket. Eksempelvis dersom avviket kan medføre at Datatilsynet blir varslet av andre aktører om det samme.

Det er en *uautorisert utlevering* som skal meldes til Datatilsynet (innen 72 timer). En uautorisert utlevering av personopplysninger er når personopplysninger behandlingsansvarlig har ansvaret for befinner, seg utenfor behandlingsansvarliges kontroll. Utleveringen kan være tilsiktet eller utilsiktet. Virksomheten (behandlingsansvarlig) må selv vurdere om det er skjedd et brudd på personopplysningssikkerheten.

### 12.4 Eksempler på uautorisert utlevering

- Forsendelsesfeil

a) Personopplysninger er sendt til feil mottaker per post eller per e-post.

[9] Vurdering av personvernkonsekvenser (DPIA) | Datatilsynet

b) Digitale forsendelser som avslører andres e-postadresser i en kontekst hvor mottakeren skal beskyttes.
c) Forsendelser til riktig mottaker, men som ved en feil også inneholder personopplysninger om andre.

- Hacking eller datainnbrudd

Hacking eller datainnbrudd har resultert i at personopplysninger er hentet ut av virksomhetens datasystem, eller det er sannsynlig at dette har skjedd. Eksempelvis at en tredjepart har fått tilgang til behandlingsansvarliges kunderegister.

- Snoking gjennomført av egne ansatte

Snoking i personopplysninger gjennomført av egne ansatte betraktes å være en uautorisert utlevering dersom den ansatte har ervervet opplysninger til egne private formål. Det samme gjelder der handlingen er utført av oppdragstakere eller frivillige som utfører arbeid på vegne av behandlingsansvarlig. Behandlingsansvarlig har da hatt manglende kontroll over egne opplysninger.

- Mangler ved tilgangsstyring

Mangelfull tilgangsstyring har resultert i at uvedkommende, utenfor virksomheten, har fått tilgang til beskyttelsesverdig informasjon.

- Feilpublisering på internett

Publisering av feil personer på internett, eksempelvis manglende anonymisering av personer.

- Fysisk innbrudd

Eksempelvis har digitale og/eller papirdokumenter med personopplysninger kommet på avveie.

### 15.5 Hva skal en avviksmelding inneholde?

En avviksmelding til Datatilsynet skal inneholde;

- Beskrivelse av avviket

a) Hva har skjedd?
b) Hvor skjedde det?
c) Hvordan oppstod avviket?

- Konsekvenser

Utredning av mulige konsekvenser for de berørte (de som har fått sine personopplysninger utlevert).

- Tiltak

Gi en beskrivelse av iverksatte og planlagte tiltak for å forhindre at avviket skal skje igjen og hva som er gjort for å redusere avvikets potensielle skadevirkning.

- Informasjon

Gi en forklaring på hvorvidt de berørte har blitt informert om den uautoriserte utleveringen, eventuelt hvorfor de ikke har blitt informert.

Hvordan melde avvik?

Brudd på personopplysningssikkerheten kan meldes til Datatilsynet via Altinn.

Se under for mer informasjon på Datatilsynets nettsider om melding av avvik;
https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvikshandtering/melde-avvik-til-datatilsynet/

### 15.6. Rutiner for varsling

Når det foreligger et personvernbrudd, skal mye skje på en gang. Det skal innhentes informasjon, undersøkes hva som er skjedd, vurdere om det skal varsles mv. Gode prosedyrer/rutiner vil være viktig å kunne støtte seg på i denne prosessen. Dette er ikke et selvstendig krav etter regelverket, men det anbefales å ha rutiner for hvordan dette skal håndteres.

Det kan også være hensiktsmessig å ha rutiner for hvordan varsle personvernbrudd internt. Det vil kunne sikre at alle hendelser blir rapportert til riktig person/beslutningstaker i organisasjonen og at det blir gjort en riktig vurdering av om hendelsen krever at Datatilsynet varsles.

### 12.1. Sjekkliste

- Har virksomheten rutiner for avvikshåndtering, herunder:
    - Rutine for hvordan avvik skal rapporteres internt?
    - Avklart hvem i virksomheten som vurderer om hendelsen skal rapporteres til Datatilsynet? Ofte er denne rollen tildelt sikkerhetsansvarlig.
    - Rutine for å melde avviket til Datatilsynet?

## 13. Oppsummert og overordnet sjekkliste

Nedenfor følger en enkel og overordnet sjekkliste:

- Har virksomheten gjort en vurdering av om det behandles personopplysninger i chatten som tilbys?
- Hvis konklusjonen er ja:
    - Har vi dokumentert et gyldig behandlingsgrunnlag? F.eks. samtykke eller annet relevant grunnlag?
    - Gir vi god nok informasjon om behandlingen til bruker av tjenesten f.eks. i en personvernerklæring?
    - Er ansvarsforholdene vurdert? Er det eksempelvis vurdert hvem som har ansvaret for at behandlingen møter kravene i regelverket? Inkludert inngått nødvendig databehandleravtale med leverandør?
    - Er nødvendige risikovurderinger gjennomført? Har vi på denne bakgrunn gjennomført tilstrekkelige tiltak for å ivareta informasjonssikkerheten?
    - Har vi etablert gode systemer og rutiner for oppbevaring og sletting av personopplysninger?