NORMEN

Personvernprinsippene (faktaark 57)

Versjon 1.0

11.06.2021

Utarbeidet med støtte fra direktoratet for e-helse

Vedtatt av styringsgruppen for Normen

Dette faktaarket er et støttedokument under Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) som forvaltes av Styringsgruppen for Normen etter Normens forvaltningsmodell. Se mer på www.normen.no

Tema for faktaarket	Dette faktaarket beskriver personvernprinsippene i Personvernforordningens artikkel 5, deres funksjon og hvordan virksomhetene kan jobbe med dem. Formålet med faktaarket er vise hva personvernprinsippene er og hvordan de kan og bør brukes i arbeidet med personvern. Faktaarket har både en teoretisk og praktisk tilnærming og inneholder mange beskrivende eksempler og en eksempelmal for å hjelpe i dette arbeidet.
Dette faktaarket er spesielt relevant for	Målgruppen for faktaarket er den som planlegger, er ansvarlig for eller har fått delegert det daglige ansvaret for en behandling av personopplysninger
Krav i Normen	• Norm for informasjonssikkerhet kapittel 2.2 Dataansvarliges ansvar
Særlig relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk	• Personvernforordningen artikkel 5 Prinsipper for behandling av personopplysninger • Personvernforordningen artikkel 6 Behandlingens lovlighet • Personvernforordningen artikkel 7 Vilkår for samtykke • Personvernforordningen artikkel 9 Behandling av særlige kategorier av personopplysninger • Personvernforordningen artikkel 16 Rett til retting • Personvernforordningen artikkel 17 Rett til sletting («rett til å bli glemt») • Personvernforordningen artikkel 24 Den behandlingsansvarliges ansvar • Personvernforordningen artikkel 32 Sikkerhet ved behandlingen

Innhold

1. Personvernprinsippene

Dataansvarlig må sikre at egen virksomhet opptrer i henhold til personvernprinsippene.[1] Personvernprinsippene stammer fra de generelle personvernreglene i personvernforordningen artikkel 5.[2] Personvernforordningen gjelder både for behandling av personopplysninger som skjer i forbindelse med at det gis helsehjelp og behandling av personopplysninger i andre sammenhenger. Andre sammenhenger vil for eksempel omfatte personaladministrasjon, kvalitetsarbeid og forskning.

Personvernprinsippene består av:

- Prinsippene om lovlighet, rettferdighet og åpenhet
- Prinsippet om formålsbegrensning
- Prinsippet om dataminimering
- Prinsippet om riktighet
- Prinsippet om lagringsbegrensninger
- Prinsippet om integritet og konfidensialitet
- Prinsippet om ansvar

[1] Normen v6.0 Kapittel 2.2 Dataansvarliges ansvar
[2] EUs personvernforordning 2016/679 (personvernforordningen)

I dette faktaarket gis en introduksjon til prinsippenes innhold og eksempler på hvordan de kan påvirke virksomheter i helse- og omsorgssektoren. Eksemplene er i hovedsak knyttet til personvernprinsippene. De ulike eksemplene vil samtidig kunne illustrere både etiske dilemmaer, forskningsprinsipper og andre normer sektoren kjenner godt.

2. Om prinsippene og deres funksjon

Personvernforordningen bygger på noen grunnleggende prinsipper som virksomheten må sørge for å ivareta når den behandler personopplysninger. Personvernforordningen ble utarbeidet både for å sikre at personopplysninger kan utveksles fritt i EU- og EØS-området, men også for å gi de registrerte bedre kontroll over egne opplysninger gjennom flere og tydeligere rettigheter. Sistnevnte må ses i sammenheng med at både retten til vern av privatlivet og beskyttelse av personopplysninger er sentrale menneskerettigheter.

Personvernprinsippene er listet opp i forordningens artikkel 5. Prinsippene gir uttrykk for både grunnleggende hensyn som personvernforordningen skal ivareta, og konkrete krav til hvordan personopplysninger skal behandles. Prinsippene er selvstendige regler som stiller krav til all behandling av personopplysninger. I tillegg skal de brukes i tolkningen av andre bestemmelser i forordningen og personvernbestemmelser i andre lover, herunder lover som regulerer behandling av personopplysninger i helse- og omsorgssektoren.

Prinsippene gjelder ikke utelukkende ved oppstart av nye behandlinger eller utvikling av egne systemer. Prinsippene skal også følges i for eksempel anskaffelsesprosesser, hvor mange andre interesser og prioriteringer ofte kommer tydelig til uttrykk. Ved anskaffelse av et system vil beslutningstakerne måtte veie f. eks. økonomi opp mot formålet med systemet de anskaffer og hvorvidt systemet har funksjonalitet som svarer til formålet og personvernprinsippene. Dette kan f.eks. være systemets robusthet, innebygd personvern, mulighetene man har for å holde opplysningene oppdaterte og riktige (prinsippet om riktighet), korrigere dem ved feil, begrense tilganger, føre logg etc.

Personvernprinsippene harmonerer godt med reglene om forsvarlige og gode helsetjenester, pasientsikkerhet og sikring av tillit til helse- og omsorgssektoren. Ivaretakelse av prinsippet om at personopplysninger skal være riktige, er for eksempel en viktig forutsetning for pasientsikkerheten og at helsepersonellet skal kunne gi forsvarlig helsehjelp. Prinsippet om personopplysningers konfidensialitet harmonerer også godt med helsepersonellets taushetsplikt.[3] I noen tilfeller kan hensynet til personvern og hensynet til pasientsikkerhet, forsvarlig helsehjelp, forskning eller andre formål trekke i forskjellige retninger. Dataansvarlig må da være varsom med å innfortolke en motstrid, og virksomheten må tilstrebe å harmonisere tolkningen av prinsippet med kravet til pasientsikkerhet og forsvarlig helsehjelp. Lykkes ikke dataansvarlig i å harmonisere sin fortolkning av et personvernprinsipp med reglene om forsvarlig helsehjelp og pasientsikkerhet, så bør dataansvarlig søke en avklaring hos veiledende organer på området.

Personvernforordningens fortale uttrykker at «Retten til vern av personopplysninger er ikke en absolutt rettighet; den må ses i sammenheng med den funksjon den har i samfunnet, og

[3] Se Normen v6.0 Kapittel 1.1, 1.2 og 4.2.1

veies mot andre grunnleggende rettigheter i samsvar med forholdsmessighetsprinsippet».[4] Noen ganger må retten til personvern veies opp mot andre sentrale menneskerettigheter som retten til liv og retten til ytringsfrihet.

Personvernprinsippene baserer seg ikke på fastlåste terskler og rammer. I samsvar med prinsippet om ansvarlighet, må dataansvarlig tolke prinsippene og hvilken betydning det enkelte prinsippet får i ulike situasjoner Det må alltid gjøres en avveining mellom hensynet til personvern og hensynet til forsvarlig helsehjelp og pasientsikkerheten, dersom disse hensynene trekker i forskjellig retning. Flere av personvernprinsippene legger også uttrykkelig opp til en fortolkning av hva som er nødvendig for å ivareta formålet med behandlingen av personopplysninger som skal utføres. Der formålet med behandlingen av personopplysninger er å yte forsvarlig helsehjelp og/eller å ivareta pasientsikkerhet, så er det den medisinsk-faglige vurderingen som bør vektlegges i vurderingen av hva som er nødvendig for å ivareta formålet. Dataansvarlig må likevel alltid gjøre en reell vurdering av om man kan oppnå samme effekt ved mindre personverninngripende tiltak.

Personvernprinsippene påvirker hvordan dataansvarlig skal behandle personopplysningene helt fra de samles inn, frem til de slettes eller anonymiseres. I faktaarkets siste avsnitt gis et eksempel på hvordan dataansvarlig vanligvis må ta hensyn til personvernprinsippene ved oppstart av ny behandling av personopplysninger.

Flere av de andre bestemmelsene i personvernforordningen gir utfyllende beskrivelser av hvordan prinsippene skal ivaretas. For eksempel er innholdet i prinsippet om lovlighet nærmere beskrevet i artikkel 6. Bestemmelsen definerer at all behandling av personopplysninger må oppfylle kravene til minst ett av behandlingsgrunnlagene som er listet opp i bestemmelsen, for at behandlingen skal være lovlig. Et av behandlingsgrunnlagene er samtykke, og kravene til slike samtykker er nærmere definert i artikkel 7. Prinsippet om åpenhet har gitt utslag i en konkret plikt for dataansvarlig til å gi de registrerte informasjon om hvordan deres personopplysninger behandles. Innholdet i denne plikten fremgår av forordningens artikkel 12 til 14.

Det er også lagt inn flere henvisninger til personvernprinsippene i lovgivning som regulerer behandling av personopplysninger på særskilte områder i helse- og omsorgssektoren. For eksempel henviser helseforskningsloven § 32 til personvernprinsippene i personvernforordningen artikkel 5, og at medisinsk og helsefaglig forskning skal være i samsvar med disse.[5] I tillegg henviser helsepersonelloven § 42 til retten til retting, som er en del av prinsippet om personopplysningers riktighet. I helseregisterloven §§ 23 og 24, finnes regler om informasjon om behandling av personopplysninger i helseregistre, som må ses i sammenheng med prinsippet om åpenhet.

Overholdelse av prinsippene i artikkel 5 skal sørge for at all behandling av personopplysninger er forutsigbar og forholdsmessig for den registrerte.

Ved bruk av databehandlere skal dataansvarlig bare benytte databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i personvernforordningen og vern av den registrertes rettigheter (jf. personvernforordningen art. 28, punkt 1). Databehandler har på sin side et selvstendig ansvar som blant annet innebærer at databehandleren omgående skal underrette den dataansvarlige dersom databehandler/vedkommende mener at en instruks er

[4] Personvernforordningen fortalepunkt 4

[5] Tilsvarende henvisning for ivaretakelse av personvernprinsippene i helseregistre, finnes i helseregisterloven § 6 første ledd.

i strid med forordningen eller andre bestemmelser om vern av personopplysninger (jf. personvernforordningen art. 28, punkt 3, bokstav h).

1.1 PRINSIPPET OM LOVLIG, RETTFERDIG OG ÅPEN BEHANDLING

Prinsippet om lovlighet, rettferdighet og åpenhet har flere sider. For det første krever prinsippet at behandlingen av personopplysninger må være lovlig. At behandlingen må være lovlig innebærer først og fremst at behandlingen av personopplysninger må baseres på minst ett av de rettslige grunnlagene som personvernforordningen lister opp, også kalt behandlingsgrunnlag. Gjelder behandlingen særlige kategorier av personopplysninger, som for eksempel helseopplysninger, så må den også oppfylle noen tilleggskrav. Kravene til lovlighet og hvilke vurderinger virksomheten må gjøre, er beskrevet overordnet i Normen og mer detaljert i et eget faktaark.[6]

Videre må behandlingen være rettferdig og åpen. At behandlingen skal være rettferdig innebærer at sammenhengen mellom behandlingen og formålet som er fastsatt skal være forståelig for den registrerte. Åpenhet innebærer at behandlingen skal være forutsigbar for den registrerte og ikke foregå på en måte som er skjult. I praksis ivaretas åpenhet gjennom personvernforordningen artikkel 12 jf. artikkel 13 og 14, som pålegger virksomheten å gi den registrerte informasjon om hvordan personopplysninger behandles. Slik informasjon gis ofte i personvernerklæringer eller informasjonsskriv.[7]

Prinsippet om åpenhet kommer blant annet til uttrykk i helseforskningsloven § 39, hvor det fremgår at den forskningsansvarlige og prosjektlederen må sikre åpenhet rundt forskningen. Det samme gjelder i helseregisterloven §§ 23 og 24, som regulerer dataansvarlig sin plikt til å gi allmennheten og registrerte informasjon om behandling av personopplysninger i helseregister.

Eksempel 1 - Åpenhet:

Normviksenteret tilbyr behandling for rusavhengighet på vegne av spesialisthelsetjenesten. I forbindelse med behandlingen samler klinikken inn en rekke opplysninger om pasientenes helse, familiære og sosiale forhold. For å ivareta prinsippet om åpenhet, så oppgir klinikken i skjemaet for registrering av nye pasienter, at informasjon om klinikkens behandling av personopplysninger finnes på klinikkens nettside. På nettsiden har klinikken en lett tilgjengelig personvernerklæring, som beskriver hvorfor og hvordan klinikken behandler pasienters personopplysninger, i samsvar med kravene i personvernforordningen artikkel 12 jf. artikkel 13 og 14.

Eksempel 2 – Lovlighet:

NN er innlagt på Normland sykehus for å få gjennomført en operasjon. Etter operasjonen mottar NN fysioterapi. Fysioterapeuten spør NN om hun kan filme

[6] Formål og behandlingsgrunnlag (faktaark 56)

[7] Informasjonsplikten (den registrertes rett til informasjon) er beskrevet i Veileder for rettigheter ved behandling av helse- og personopplysninger kapittel 3 Retten til informasjon om behandling av personopplysninger

behandlingen slik at opptaket kan brukes til opplæring internt. NN sier ja, og skriver under på en samtykkeerklæring, der det står at formålet med behandlingen av personopplysninger er opplæring internt på sykehuset. Et halvt år senere ønsker en av medarbeiderne å bruke filmen til opplæring av studenter som er i praksis på sykehuset. Hvis det er mulig, så ønsker han også å bruke filmen i kveldsundervisningen han holder på en høyskole. Sykehuset har brukt NN sitt samtykke som behandlingsgrunnlag for oppbevaring og fremvisning av filmen under opplæring av ansatte på sykehuset.

Sykehuset gjør en vurdering, og kommer frem til at NN ikke har samtykket til at videoen kan brukes til opplæring utenfor sykehuset, og sykehuset har derfor ikke behandlingsgrunnlag for dette. Sykehuset er imidlertid i tvil om NN sitt samtykke dekker opplæring av studentene som er i praksis på sykehuset. Sykehuset velger derfor å ta kontakt med NN for å innhente et nytt samtykke til både bruk i opplæring av studenter i praksis på sykehuset og undervisningen på høyskolen.

Eksempel 3 – Åpenhet og rettferdighet

Normklinikken gjennomfører et forskningsprosjekt der det ses nærmere på sammenhengen mellom personers kostholdsvaner og alder og kjønn. Deltakerne har blant annet fått informasjon om hvordan deres personopplysninger vil bli behandlet, og at formålet er å påvise sammenheng mellom kostholdsvaner og alder og kjønn. Forskningslederen oppdager etter hvert at det kan være interessant å se nærmere på om etnisk opprinnelse kan få betydning for kostholdsvanene. Han går derfor gjennom alle intervjuer som er gjennomført, og henter ut informasjon om etnisitet der dette finnes. Han legger dette til i analysen, men gjør ingenting overfor deltakerne.

Dette kan være i strid med prinsippet om rettferdig behandling av personopplysninger, fordi behandlingen av opplysninger om deltakernes etnisitet har vært skjult for deltakerne. Som følge av informasjonen deltakerne har fått, må bruken også regnes som utenfor det deltakerne kunne forvente, og behandlingen av personopplysninger har derfor heller ikke vært forutsigbar for deltakerne. I tillegg utgjør den mangelfulle informasjonen om forskningsprosjektets behandling av personopplysninger et brudd på prinsippet om åpenhet. Legg også merke til at behandling av personopplysninger utover det opprinnelige formålet kan utgjøre et brudd på prinsippet om formålsbegrensning. Dette prinsippet er nærmere beskrevet under.

1.2 PRINSIPPET OM FORMÅLSBEGRENSNING

Prinsippet om formålsbegrensning bestemmer at personopplysninger bare skal samles inn og behandles for spesifikke, uttrykkelig angitte og berettigede formål.[8] En rekke av forordningens bestemmelser viser til formålet med behandlingen. Formålet er derfor i stor grad styrende for hvordan personopplysninger kan behandles i det enkelte tilfelle.

[8] Dette gjenspeiles også i helseforskningsloven § 32, hvor det fremgår at «Behandling av helseopplysninger i medisinsk og helsefaglig forskning skal … ha uttrykkelig angitte formål. Helseopplysningene skal være relevante og nødvendige for å nå forskningsprosjektets formål»

Et eksempel i helse- og omsorgssektoren vil være behandlingen av personopplysninger i en pasientjournal. Denne behandlingen reguleres av pasientjournalloven og personvernforordningen. I den nasjonale lovgivningen (pasientjournalloven) er det fastsatt hvilke opplysninger man har anledning til å legge inn i en pasientjournal (dataminimering), til hvilke formål de kan anvendes og regler for hvorvidt og hvordan de kan utleveres eller deles med andre. Opplysninger som ligger i en pasientjournal skal behandles og være tilgjengelige for flere formål, som blant annet omfatter å yte, administrere eller kvalitetssikre helsehjelp. Dette gjelder uavhengig av om pasientjournalsystemet er elektronisk eller i fysiske mapper. Et system kan vanligvis ikke betraktes som *en* behandling, i de fleste tilfeller skal systemer imøtekomme flere legitime formål.

Virksomheten må definere og beskrive formålet før behandlingen starter, og formålet må beskrives konkret og tydelig. Dette vil sørge for at den registrerte forstår hva personopplysningene skal brukes til, og det vil gjøre det lettere for virksomheten å ta stilling til hvilket behandlingsgrunnlag som er aktuelt, hvilke personopplysninger det er nødvendig å samle inn, hvor lenge de skal lagres mv.[9]

Personopplysningene kan i utgangspunktet ikke gjenbrukes for andre formål enn de som virksomheten definerte ved innsamlingen. Personopplysningene kan likevel behandles for nye forenelige formål. I vurderingen av forenelighet skal det blant annet tas hensyn til forbindelsen mellom opprinnelige og nye formål, sammenhengen personopplysningene ble samlet inn i (herunder relasjonen mellom virksomheten og den registrerte, og den registrertes forventninger), personopplysningenes art, mulige konsekvenser av behandlingen og eventuelle garantier for personvernet.[10] De nye formålene kan være forenelige med den opprinnelige behandlingen, hvis de er en naturlig forlengelse av de opprinnelige formålene, og den nye behandlingen ikke medfører større konsekvenser for den registrerte.

Hvis virksomheten ønsker å behandle personopplysningene for nye formål som ikke er forenelige med de opprinnelige, må behandlingen enten være basert på samtykke eller rettslig plikt.

Eksempel 4 – Formålsbegrensning

Normland sykehus behandler personopplysninger om pasienter i pasientjournaler. Sykehuset har definert formålet med behandlingen til oppfyllelse av kravene til journalføring i helsepersonelloven, pasientjournalloven og pasientjournalforskriften. Hvis en av pasientene senere søker jobb på sykehuset, så forbyr blant annet prinsippet om formålsbegrensninger, bruk av opplysningene i pasientjournalen i vurderingen av om kandidaten er egnet til stillingen. Opplysningene i journalen kan imidlertid behandles videre for arkivformål selv om dette ikke ble definert før de ble samlet inn, fordi slike formål regnes som forenelige med de opprinnelige formålene.

Eksempel 5 – Formålsbegrensning

[9] Kravet til definering av formål for behandling av personopplysninger er definert i både Normen kapittel 2-2 Dataansvarliges ansvar og Formål og behandlingsgrunnlag (faktaark 56)
[10] Personvernforordningen artikkel 6 (4) og Skullerud (2019) lovkommentarer til personvernforordningen artikkel 6

Normland apotek er plaget med gjentatte innbruddsforsøk. Apoteket setter derfor opp et overvåkingskamera ved bakdøren som også brukes som personalinngang. Apoteket definerer behandlingen av personopplysningers formål til å være forebygging og oppklaring av innbruddsforsøk og hærverk. De ansatte får informasjon om dette. Noen måneder senere får daglig leder mistanke om at en av de ansatte jukser med timelistene, gjennom å oppgi å ha jobbet fra et tidligere tidspunkt enn det han egentlig har. For å kontrollere når den ansatte egentlig har kommet på jobb, så sjekker daglig leder opptak fra overvåkingskameraet. Dette vil være i strid med prinsippet om formålsbegrensning. Relevante momenter i tolkningen er blant annet at det ikke er noen sammenheng mellom nytt og gammelt formål, maktubalansen mellom arbeidsgiver og den ansatte, at behandlingen er uventet for den ansatte og at mulige konsekvenser kan være at den ansatte mister jobben.

Eksempel 6 – Formålsbegrensning

Normland spesialsykehus for epilepsi samler inn og behandler helse og personopplysninger om pasienter m6d alvorlig epilepsidiagnoser og formålet med behandlingen av helse og personopplysninger er å yte helsehjelp. Etter 3 måneder ved spesialsykehuset har NN nå god anfallskontroll og fått tilpasset nye epilepsimedisin. Ved utskriving til hjemkommunen vil mange ha behov for informasjon om hvordan de skal best tilrettelegge for NN. Helsepersonell kan gi opplysninger til annet samarbeidende personell som deltar i behandlingen av pasient når det er nødvendig for helsehjelpen. Normland spesialsykehus kan derfor sende opplysninger til de som har sammenfallende formål – yte helsehjelp til NN. Prinsippet om formålsbegrensninger hindrer spesialsykehuset å dele personopplysning med f.eks. NNs fotballtrener når han lurer på hvordan de må planlegge treninger ol for N. Personopplysningene vil da brukes til noe som er uforenelig med det opprinnelige formålet. For å overføre opplysninger til treneren må sykehuset innhente samtykke fra NN/ NN's foresatte.

1.3 PRINSIPPET OM DATAMINIMERING

Prinsippet om dataminimering fastslår at personopplysningene som behandles skal være adekvate, relevante og begrenset til det som er nødvendig for å oppnå de formålene som er fastsatt ved innsamling. Prinsippets viktigste side er at mengden personopplysninger skal begrenses til det som er nødvendig for formålet. For hver behandling må det derfor vurderes om formålet kan oppnås med færre personopplysninger eller om formålet kan oppnås uten at den registrerte må være identifiserbar under hele behandlingen. Prinsippet om dataminimering kommer også til uttrykk i helseregisterloven § 6, hvor det fremgår at «Graden av personidentifikasjon» i helseregistre, ikke skal være av et større omfang enn det som er nødvendig for å ivareta formålene med helseregisteret.

Det er viktig å være oppmerksom på at personvernforordningen ikke gir noe endelig svar på hvilke personopplysninger som er nødvendig å behandle. Avhengig av formålet vil det derfor være store forskjeller på hvordan prinsippet slår ut i det enkelte tilfelle.

Det vil for eksempel være forskjell på hvilke personopplysninger det er nødvendig å samle inn om pasienter for å yte helsehjelp, og hvilke personopplysninger det er nødvendig å samle

inn i en ansettelsesprosess. Her er formålene henholdsvis å gi riktig helsehjelp til pasienten og vurdering av jobbsøkerens egnethet. For å sikre riktig helsehjelp, er det ofte nødvendig å hente inn flere personopplysninger enn i ansettelsesprosesser. For eksempel kan innhenting av opplysninger om den registrertes foreldre være nødvendig for å utrede en pasient, men det er neppe nødvendig for å vurdere ansettelse av en jobbsøker.[11]

Eksempel 7 - Dataminimering:

En psykiatripasient blir overført til behandling på et sykehus for å få helsehjelp. Sykehuset ber om å få opplysninger fra den psykiatriske journalen. I et slikt tilfelle kan det være nødvendig ut fra en medisinskfaglig vurdering å samle inn opplysninger om pasientens psykiatriske diagnoser og behandlingsforløp, men vurderingen kan også vise at det ikke er nødvendig å innhente detaljerte opplysninger om pasientens barndom for å gi helsehjelpen. Siden formålet med denne behandlingen av personopplysninger er å gi forsvarlig helsehjelp (som innebærer at pasientsikkerheten må ivaretas), så må prinsippet om dataminimering likevel ikke tolkes så strengt at det kan går ut over forsvarlig helsehjelp.

1.4 PRINSIPPET OM RIKTIGHET

Personvernforordningens prinsipp om riktighet fastslår at personopplysninger skal være korrekte og oppdaterte. Dersom virksomheten oppdager at personopplysninger ikke er korrekte, må de rettes eller slettes på virksomhetens eget initiativ og uten opphold. Den registrerte har i tillegg en rett til å be om retting etter personvernforordningen artikkel 16. Den registrerte har også denne retten når hennes personopplysninger behandles i helseforskning, behandlingsrettede helseregistre og andre helseregistre. I lovgivningen som regulerer disse områdene, er det lagt inn henvisninger til rettigheten i personvernforordningen. Retten til å kreve retting er nærmere beskrevet i en egen veileder til Normen.[12]

Prinsippet om riktighet handler om å sørge for at opplysningene man behandler er riktige og holdes oppdaterte underveis i behandlingen dersom dette er i tråd med formålet de behandles for.

For å etterleve dette prinsippet må virksomheten sette inn tiltak for å sikre personopplysningenes riktighet. Eksempler på tiltak kan være rutiner for å sørge for at registre og pasientjournal holdes oppdatert, å sjekke kontaktlister opp mot folkeregisteret, eller å be pasienter om å bekrefte at kontaktinformasjon er korrekt og fullstendig. En praktisk måte å sikre opplysningenes riktighet på, er å gi registrerte en mulighet til å få innsyn i opplysningene om seg selv, og deretter kunne kreve retting eller sletting. På helsenorge.no har for eksempel pasienter en mulighet til å få innsyn i egne pasientjournaler. Prinsippet bør ses i sammenheng med retten til innsyn i artikkel 15.[13]

[11] Fra dette utgangspunktet kan det tenkes visse unntak, for eksempel i forbindelse med sikkerhetsklarering etter sikkerhetsloven.
[12] Den registrertes rett til sletting er beskrevet i Veileder for rettigheter ved behandling av helse- og personopplysninger kapittel 5 Retten til retting
[13] Se mer om denne rettigheten i Veileder for rettigheter ved behandling av helse- og personopplysninger kapittel 4 Retten til innsyn

Risikoen for at opplysninger blir feil og utdaterte øker dersom helsepersonell har flere systemer å registrere de samme helseopplysninger i. Tiltak for å sikre at dette ikke skjer kan også være et utslag av prinsippet om riktighet.

I likhet med dataminimeringsprinsippet vil dette prinsippet også slå ut forskjellig i enkelte tilfeller. Retten til å kreve retting er begrenset i helse- og omsorgssektoren fordi helsepersonell er underlagt en dokumentasjonsplikt, som skal sikre at visse opplysninger er etterviselige og kontrollerbare. Det er naturligvis av stor betydning at personopplysninger er korrekte når det ytes helsehjelp, men plikten til å rette sammenholdt med dokumentasjonsplikten kan for eksempel innebære at virksomheten må supplere opplysningene med nye, fremfor å erstatte opplysningene. Det vil blant annet være forskjell på tilfeller hvor det dreier seg om rene faktaopplysninger eller om det dreier seg om skjønnsmessige vurderinger.

Eksempel 8 – Personopplysningers riktighet:

NN (38) har bedt om innsyn i sin pasientjournal hos fastlegen. Når NN går gjennom journalen, ser hun at fastlegen har oppført en uriktig opplysning i journalen. I forbindelse med behandling av en betennelse i NNs ankel, har fastlegen ført opp at NN brakk det samme benet da hun var syv år gammel. Dette stemmer ikke, for NN var 37 år gammel da dette skjedde. NN tar kontakt med fastlegen og ber om å få rettet denne opplysningen. For fastlegen er det viktig å dokumentere hvilken informasjon han tok utgangspunkt i da han behandlet betennelsen i ankelen. Han kan derfor ikke erstatte den uriktige opplysningen med den riktige opplysningen. For å ivareta pasientsikkerheten og sikre riktig medisinsk behandling fremover, samt ivareta prinsippet om riktighet, legger fastlegen til en kommentar til oppføringen. Her skriver han at det er en feil i oppføringen, og at pasienten i realiteten var 37 år gammel da bruddet i benet oppsto.

Eksempel 9 – Personopplysningers riktighet:

Kvinneklinikken ved Normsund sykehus behandler til enhver tid en rekke pasienter med magesmerter i sine polikliniske avdelinger. Ettersom magesmerter er et symptom som kan oppstå av mange forskjellige årsaker, og det i mange tilfeller kan være utfordrende å stille en diagnose, velger Normsund sykehus å opprette et internt kvalitetsregister etter Helsepersonellovens §26 for oppfølgingen av disse pasientene. Normsund sykehus definerer formålet som kvalitetssikring av det diagnostiske arbeidet med disse pasientene og sikring av at pasientene er gitt tilstrekkelig oppfølging. I forbindelse med opprettingen av kvalitetsregisteret, så utarbeider sykehuset en integrasjon mellom det elektroniske pasientjournalsystemet og kvalitetsregisteret. Integrasjonen gjør at alle nye pasienter som er aktuelle for registeret automatisk føres opp i registeret, og at pasientjournalen fra pasientens første konsultasjon importeres til registeret. Sykehuset glemmer imidlertid å etablere funksjonalitet som sikrer at kvalitetsregisteret oppdateres etter hvert som pasientjournalen oppdateres. Dette gjør at kvalitetsregisteret mangler informasjon fra senere konsultasjoner og medisinsk behandling som pasienten mottar på klinikken. Personopplysningene i kvalitetsregisteret oppdateres ikke, og de vil i flere tilfeller være ufullstendige eller uriktige. Sykehuset har derfor brutt prinsippet om riktighet. I dette eksempelet går hensynet til pasientsikkerheten hånd i hånd med

personvernprinsippet, ettersom riktige opplysninger også er nødvendig for forsvarlig helsehjelp.

Eksempel 10 – Personopplysningers riktighet

NN ligger klar til MR av lumbalcolumna med kontrast. NN blir forklart at det skal gis kontrast pga. operasjonen han har hatt i ryggen. NN sier at han aldri er operert i ryggen. Det viser seg at henvisningsopplysningene er lagt inn på feil pasient. Henvisningen er skannet inn, og på denne henvisningen er det et annet navn og fødselsnummer. Manglende kontroll i samspill mellom manuelle og teknologiske prosesser fører til feil i pasientjournalen.

Avviket må håndteres, dokumenteres, rapporteres og meldes til tilsynsmyndighetene i tråd med Normsorg sine rutiner og det bør vurderes hvilke tiltak (tekniske/og eller organisatoriske) som skal iverksettes for å lukke avviket og hindre at tilsvarende feil kan skje igjen. Avviket ved Normland kan tyde på at de har utfordringer med kvalitetssikringen av informasjonen de er avhengige av, inkludert personopplysningenes riktighet, og at dette ikke i tilstrekkelig grad har blitt håndtert i form av nye og bedre rutiner.

1.5 PRINSIPPET OM LAGRINGSBEGRENSNING

Lagringsbegrensningsprinsippet bestemmer at personopplysninger ikke kan lagres lenger enn det som er nødvendig for formålet. Når formålet er oppnådd må personopplysningene i utgangspunktet slettes eller anonymiseres. Sletting skal skje på dataansvarliges eget initiativ, men den registrerte er også gitt en rett til sletting i artikkel 17.[14]

Personvernforordningen angir ingen konkrete frister for sletting. Dataansvarlig må derfor selv angi slettefrister basert på hva som er nødvendig for formålet med behandlingen. For eksempel vil det sjeldent være nødvendig å oppbevare en skriftlig advarsel til en ansatt lenger enn fem år, når advarselen gjelder mindre alvorlige hendelser som forsentkomming, og dette ikke har gjentatt seg siden.

Virksomheten kan være underlagt dokumentasjonsplikter i andre regelverk som angir konkrete frister, og da er det disse som er avgjørende for hvor lenge personopplysningene skal lagres. Helse- og omsorgsektoren er underlagt flere dokumentasjonsplikter. Helsepersonell har for eksempel plikt til å nedtegne helse- og personopplysninger i pasientjournaler, og hver pasientjournal skal oppbevares så lenge det er bruk for den av hensyn til helsehjelpens karakter.

Selv etter at de opprinnelige formålene er oppnådd kan det være behov for å fortsette lagringen. Prinsippet inneholder derfor flere unntak, herunder regler om at personopplysninger kan lagres lenger for arkiv- eller forskningsformål. Disse unntakene er svært relevante for helsesektoren, som for eksempel i mange tilfeller har plikt til å bevare helse- og personopplysninger etter arkivlovgivningens bestemmelser.

[14] Den registrertes rett til sletting er beskrevet i Veileder for rettigheter ved behandling av helse- og personopplysninger kapittel 6 Retten til sletting

Eksempel 11 - Lagringsbegrensning:

Det bryter ut en pandemi i Normland. Normvik kommune vedtar en midlertidig pandemiforskrift som pålegger alle kommunale etater å utarbeide lister over hvem som har besøkt deres lokaler de siste 14 dagene, for å sikre mulighet til smittesporing dersom det oppstår smitte. Normsjø eldresenter tar derfor i bruk et nytt elektronisk system for besøksregistrering. Formålet med behandlingen av personopplysninger defineres som oppfyllelse av den nye pandemiforskriften. Siden pandemiforskriften kun pålegger lagring av informasjon om besøkende fra de siste 14 dagene, så vil formålet være oppfylt når registreringene blir eldre enn 14 dager. Normsjø eldresenter sikrer derfor at registreringene slettes automatisk når de blir 15 dager gamle.

1.6 PRINSIPPET OM INTEGRITET OG KONFIDENSIALITET

Ifølge prinsippet om integritet og konfidensialitet skal virksomheten sørge for tilstrekkelig sikring av personopplysningene. Det innebærer at virksomheten må sette inn sikkerhetstiltak for å beskytte personopplysninger mot utilsiktet og ulovlig tilgang, ødeleggelse, tap eller endringer.

Prinsippet må ses i sammenheng med de mer utfyllende kravene til sikkerhet i personvernforordningen artikkel 32. Der fremgår det at dataansvarlig må sikre et sikkerhetsnivå som er egnet med hensyn til behandlingen av personopplysninger og risikobildet. Artikkel 32 inneholder også konkrete krav til ivaretakelse av personopplysningers integritet, konfidensialitet og tilgjengelighet. Dette er tre grunnpilarer innen informasjonssikkerhet.[15] I tillegg introduserer artikkel 32 et krav til robusthet, som er et nytt krav sammenlignet med tidligere lovgivning og standarder for informasjonssikkerhet.[16]

I lovgivning som regulerer behandling av personopplysninger på særskilte områder i helse- og omsorgssektoren, refereres det også til kravene til sikkerhet i personvernforordningen artikkel 32. I helseregisterloven § 21 vises det til artikkel 32, før det utdypes at dataansvarlig og databehandler blant annet må sørge for tilgangsstyring, logging og etterfølgende kontroll. Det stilles også krav til kryptering av direkte personidentifiserende kjennetegn ved lagring i forskriftsregulerte helseregistre. I pasientjournalloven § 22 fremgår det at artikkel 32 også gjelder for behandlingsrettede helseregistre, i tillegg til en rekke krav til konkrete sikkerhetstiltak som fremgår i pasientjournalforskriften.

For å sikre konfidensialitet bør virksomheten for eksempel kreve brukerautentisering i elektroniske pasientjournalsystemer. Dette skal hindre at uvedkommende får tilgang til personopplysninger i pasientjournalene. Integriteten kan for eksempel ivaretas gjennom å skille mellom leserettigheter og skriverettigheter i tilgangssikringen og logging av endringer. Til slutt kan tilgjengelighet ivaretas ved utarbeidelse av tydelige rutiner som skal sikre at relevant helsepersonell får tilgang til det de trenger i pasientjournaler for å kunne yte forsvarlig helsehjelp.

[15] Kravet bør ses i sammenheng med øvrige krav i Normen, som i stor grad er utarbeidet for å sikre informasjonsverdiers integritet, konfidensialitet og tilgjengelighet.
[16] Se Normen kapittel 3.2 for mer informasjon om sammenhengen mellom kravene til tilgjengelighet og robusthet

Eksempel 12 – Konfidensialitet

Normsjøklinikken tilbyr behandling til pasienter med alvorlige spiseforstyrrelser. Som følge av et pandemiutbrudd, må klinikken stenge for fysisk oppmøte på poliklinikken. Klinikken har tekniske verktøy som er godt egnet for individuelle konsultasjoner digitalt. Klinikken er imidlertid i tvil om den vil klare å ivareta prinsippet om konfidensialitet og integritet dersom gruppeterapi gjennomføres digitalt. Mange av pasientene har svært godt utbytte av gruppeterapien, og enkelte er svært sårbare for store forandringer i hverdagen. Hensynet til forsvarlig helsehjelp taler derfor for at klinikken bør tilby gruppeterapien digitalt, så lenge poliklinikken er stengt for fysisk oppmøte. Hensynet til ivaretakelsen av personopplysningers integritet og konfidensialitet, taler imidlertid for at klinikken må være varsom med å digitalisere gruppeterapien. Når aktiviteten digitaliseres, blir det vanskelig å sikre at uvedkomne ikke kan skaffe seg tilgang til informasjon som deles under terapien.
Normsjøklinikken har gjort en ROS-analyse, og konkludert med at den tekniske sikkerheten er tilstrekkelig. Klinikken har imidlertid ikke mulighet til å sikre at hver enkelt pasient er alene rent fysisk når han deltar i terapien. Det vil ikke være mulig å kontrollere at ikke uvedkomne oppholder seg nært nok på en pasient, til å kunne fange opp deler av terapien (for eksempel ved at uvedkomne sitter i samme rom som pasienten). Det vil også være vanskelig å fange det opp dersom en pasient velger å ta bilder/film/lydopptak av terapien. Dette kan utfordre konfidensialiteten til helse- og personopplysningene til pasientene. Klinikken kan imidlertid til en viss grad avhjelpe dette med god informasjon til deltagerne, der de blir bevisstgjort på behovet for å beskytte opplysninger om de andre i gruppen. Får å kunne beslutte hvorvidt de skal gjennomføre gruppeterapien digitalt må klinikken gjøre en avveining mellom hensynet til forsvarlig helsehjelp og hvor strengt den skal tolke prinsippet om integritet og konfidensialitet.

Eksempel 13 – Integritet og konfidensialitet

Normdal kommune driver et bosenter for rusavhengige. Bosenteret tilbyr en kombinasjon av behandling for rusavhengighet og oppfølging innen livsmestring. Ifølge bosenterets rutiner skal det registreres daglig at alle pasienter er gjort rede for. I praksis skjer dette ved at hver avdeling har en pasientliste i excel-format, hvor helsepersonell med særskilt ansvar fører inn klokkeslettet og initialene til den som var i kontakt med pasienten. Listene oppbevares på tilgangsstyrte mapper med særskilte sikkerhetstiltak. Påfølgende dag føres informasjonen inn i pasientens journal og listen slettes.

Når bosenteret ansetter en ny kveldsvikar gjøres det en feil i defineringen av hans rolle i IT-systemene. Han får for vide tilganger, og får blant annet tilgang til pasientlisten med registreringene av når pasientene ble gjort rede for. Kveldsvikaren er ivrig etter å lære, og han åpner diverse mapper og dokumenter for å se om det står noe interessant der som han kan lære noe av. Når behandlende lege kommer på jobb morgenen etter, så ser hun at noen har gjort en endring i pasientlisten og lagret disse kl. 02.14 samme natt. Hun kan se at det er den nye kveldsvikaren som har lagret dokumentet, men hun kan ikke se hvilke endringer som er gjort. Kveldsvikaren beklager og sier at han ikke kan huske å ha endret noe, og at han sikker bare har lagt til et mellomrom et sted.

Denne hendelsen utgjør et brudd på prinsippet om konfidensialitet, fordi opplysningene utilsiktet ble gjort tilgjengelig for en medarbeider i strid med virksomhetens rutiner for tilgangsstyring og uten at medarbeideren hadde et tjenstlig behov. Hendelsen utgjør også et brudd på prinsippet om integritet, fordi bosenteret ikke kan spore om endring av personopplysningene har skjedd, og fordi de ikke har lykkes i å beskytte personopplysningene mot uautoriserte endringer. Behandlende lege må melde hendelsen som et avvik og dette må håndteres umiddelbart i henhold til bosenterets avviksrutiner.

Eksempel 14 – Integritet og konfidensialitet

Normvik Fysioterapi er utsatt for et vellykket nettfiskeangrep, der aktøren som står bak angrepet har lykkes i å trenge inn i virksomhetens IT-systemer. Aktøren har kryptert hele personalarkivet, og logger viser at den også har vært inne i det elektroniske pasientjournalsystemet. Aktøren har imidlertid klart å slette loggene som viser hva den gjorde i pasientjournalsystemet, slik at Normvik Fysioterapi ikke kan se om aktøren har endret noen av opplysningene i systemet.

Hendelsen innebærer brudd på personopplysningers integritet og konfidensialitet. I personalarkivet har det også skjedd et brudd på personopplysningenes tilgjengelighet. Virksomheten har brutt prinsippene om tilgjengelighet og integritet, fordi den ikke har lykkes i å sikre seg mot at personopplysninger blir tilgjengelig for uvedkomne og uautoriserte endringer av personopplysninger.

1.7 PRINSIPPET OM ANSVARLIGHET

I tillegg til prinsippene som er nevnt over inneholder forordningen et prinsipp om ansvarlighet. Prinsippet understreker at virksomheter har et ansvar for å sørge for at de behandler personopplysninger i henhold til regelverket. Prinsippet innebærer i praksis at virksomheten må kunne dokumentere sin egen etterlevelse av regelverket og at personvernet ivaretas til enhver tid.

Virksomheten må sørge for å ha oversikt over hvordan personopplysninger behandles og rutiner for behandling av personopplysninger. I tillegg må virksomheten ha kontrolltiltak som skal sikre at rutiner og ansvar etterleves. Et internkontroll-/styringssystem for personvern kan være en måte å etterleve prinsippet om ansvarlighet på.

Eksempel 15 - Ansvarlighet:

Normsund sykehus arbeider mye med forskning. I flere av forskningsstudiene bruker sykehuset samtykke som behandlingsgrunnlag for behandlingen av personopplysninger som forskningen innebærer. For å sikre at sykehuset alltid oppfyller kravene til bruk av samtykke som behandlingsgrunnlag, og for å dokumentere dette, så utarbeides det en sjekkliste for disse kravene. Sjekklisten inneholder hjelpetekster, og når den er ferdig utfylt skal den sendes til personvernombudet og oppbevares sammen med øvrig dokumentasjon for prosjektet. Sykehuset pålegger alle forskningsrådgiverne å bruke sjekklisten når det utarbeides samtykkeerklæringer for behandling av personopplysninger i forskning. Personvernombudet tar periodiske stikkprøver på forskningsprosjektene, og kontrollerer at sjekklisten er utfylt og at samtykkeerklæringen oppfyller kravene i

personvernforordningen. I tillegg er det beskrevet en prosess for at sykehuset skal evaluere tiltakenes hensiktsmessighet og effekt ved alvorlige hendelser og minst en gang i året.

Eksempel 16 - Ansvarlighet:

Internrevisjonen i Normvik kommune utfører en revisjon knyttet til personvern i helseetaten. Internrevisjonen ber etaten om å legge frem dokumentasjon på hvordan etaten oppfyller kravene til risikovurderinger i personvernforordningen artikkel 32. Helseetaten legger frem dokumentasjon som viser noen halvferdige ROS-analyser som ble utarbeidet for tre år siden. Andre revisjonsbevis viser at ROS-analysene ble ferdigstilt og fulgt opp. Etaten forteller at kommunaldirektøren aksepterte restrisikoen i analysene, men dette ble ikke dokumentert. Dokumentasjonen fra ROS-analysene har ikke blitt oppdatert etter det. Internrevisjonen konkluderer med at kommunen oppfyller kravet til å utføre risikovurderinger etter personvernforordningen artikkel 32. Internrevisjonen konkluderer med at etaten imidlertid har brutt prinsippet om ansvarlighet, ettersom ROS-analysene ikke fullt ut er dokumenterte, og kommunaldirektørens aksept av restrisikoen ikke er dokumentert.

3. Hvordan bør dataansvarlig arbeide med personvernprinsippene?

Personvernprinsippene påvirker hvordan dataansvarlig skal håndtere personopplysninger gjennom hele «livsløpet» til personopplysningene, fra tidspunktet for innsamling til opplysningene slettes eller anonymiseres. Hvordan dataansvarlig skal arbeide med å ivareta prinsippene må ses i sammenheng med kravet til å etablere egnede tekniske og organisatoriske tiltak som sikrer og påviser at behandling skjer i samsvar med personvernforordningen, i personvernforordningen artikkel 24 nr. 1. Når virksomheten vurderer hvilke tiltak som er egnede, må den ta hensyn til behandlingen av personopplysningers art, omfang, formål, sammenhengen den utføres i og risikoen for registrertes rettigheter og friheter. Dette innebærer at tiltakene bør være proporsjonale med hvor inngripende behandlingen av personopplysninger er for de registrerte og risikoen for at de ikke får oppfylt sine rettigheter og friheter.

Flere av prinsippene krever at dataansvarlig gjør noen vurderinger før personopplysninger kan samles inn. Dette kan gjøres på mange måter. Her viser vi et eksempel på hvordan en virksomhet kan ivareta prinsippene:

Eksempel 17 – Etterlevelse av personvernprinsippene ved oppstart av ny behandling av personopplysninger:

Ayan jobber som personvernrådgiver i den ideelle organisasjonen Normsorg. Hun bistår organisasjonen i et prosjekt der det skal opprettes et digitalt chatterom for ungdom som ønsker å snakke med en helsesykepleier. Normsorg kan bare identifisere ungdommene hvis de ber leverandøren av den tekniske løsningen om

tilgang til IP-adressen til den enkelte ungdommen (som lagres hos leverandøren en kort periode), eller hvis ungdommen etter eget initiativ velger å oppgi identifiserende opplysninger i chatten.

Normsorg har utarbeidet en sjekkliste for oppstart av ny behandling av personopplysninger. Sjekklisten skal brukes ved oppstart av nye behandlingsaktiviteter eller endring av eksisterende behandlingsaktiviteter, der Normsorg har vurdert at den selv er dataansvarlig. Aktivitetene i sjekklisten må utføres før Normsorg kan starte behandlingen av personopplysninger. Dette skal sikre at organisasjonen dokumenterer sin egen etterlevelse av alle prinsippene, i samsvar med kravene i prinsippet om ansvarlighet. Normsorg har allerede registrert og dokumentert de nødvendige kjerneopplysningene om behandlingen som skal fremgå av protokollen, jf. Personvernforordningen art. 30.

Ayan fyller ut sjekklisten slik (Ayans svar i kursiv):

Sjekkliste for ny behandling av personopplysninger hvor Normsorg er dataansvarlig

Navn på utfyller: Ayan Karlsen		**Dato: 12.02.2021**
Kravnr.	**Aktivitet**	**Svar**
1	Formålsbegrensning Hva er formålet med den nye behandlingen av personopplysninger? Husk at alle formål må være spesifikke, uttrykkelig angitte og berettigede formål.	*Formålet er å tilby ungdom generell rådgivning knyttet til fysisk og psykisk helse, i form av et lavterskeltilbud.*
2	Dataminimering Har du sikret at det kun vil bli samlet inn personopplysninger som det er nødvendig å behandle for å ivareta formålene med behandlingen? Husk å vurdere hvor høy detaljeringsgrad opplysningene må ha for å oppfylle formålet.	*Ja, resultatet av vurderingen er dokumentert i organisasjonens protokoll over behandlingsaktiviteter linje 43, 44 og 45.*
3 a)	Behandlingens lovlighet etter artikkel 6 Hva er behandlingsgrunnlaget for behandlingen av personopplysninger?	*Les mer om når Normsorg kan bruke de forskjellige*

	Les mer om behandlingsgrunnlag i helse- og omsorgssektoren i Formål og behandlingsgrunnlag (faktaark 56).[17]	*behandlingsgrunnlagene i denne rutinen.*[18] *Normsorg har vurdert at samtykke er behandlingsgrunnlaget for innsamling av brukernes personopplysninger, bruken av dem i vurderinger og lagring en kort periode etter samtalen.* *Dersom det gis råd som utløser helsepersonellets dokumentasjonsplikt, eller det oppstår hendelser som utløser helsepersonellets opplysningsplikt eller andre lagringsplikter som følger av lov/forskrift, er behandlingsgrunnlaget oppfyllelse av en rettslig plikt. Aktuelle bestemmelser er dokumentert i organisasjonens protokoll over behandlingsaktiviteter linje 43, 44 og 45.* *Logging av hvem som har besvart henvendelser, når dette skjedde og overordnet tema, har behandlingsgrunnlag i Normsorgs berettigede interesse i å styre egen virksomhet.*
3 b)	Behandlingens lovlighet etter artikkel 9 Dette punktet må bare fylles ut hvis behandlingen av personopplysninger vil omfatte særlige kategorier av personopplysninger *(*for eksempel	*Les mer om når Normsorg kan bruke de forskjellige behandlingsgrunnlagene i denne rutinen.*[20]

[17] Formål og behandlingsgrunnlag (faktaark 56)
[18] Dette er en fiktiv rutine
[20] Dette er en fiktiv rutine

	helseopplysninger eller opplysninger om fagforeningsmedlemskap): Hvilket unntak i personvernforordningen artikkel 9 nr. 2 oppfyller behandlingen av personopplysninger? Les mer om behandlingsgrunnlag i helse- og omsorgssektoren i Formål og behandlingsgrunnlag (faktaark 56)[19].	*Behandlingen vil omfatte helseopplysninger. Normsorg har vurdert at behandlingen faller inn under unntaket om ytelse av helsehjelp i personvernforordningen artikkel 9 nr. 2 bokstav h.*
4	Formålsbegrensning Dette punktet må bare fylles ut hvis Normsorg skal "gjenbruke" personopplysninger som tidligere er samlet inn for et annet formål:	-
4 a)	Har du sikret at den nye behandlingen av personopplysningene er forenelig med formålene som opplysningene først ble samlet inn til?	*Ikke aktuelt.*
4 b)	Hvis den nye behandlingen av personopplysningene *ikke* er forenelig med formålene som opplysningene først ble samlet inn til: Er behandlingen basert på den registrertes samtykke eller oppfyllelse av en rettslig plikt som Normsorg er underlagt? Husk henvisning til den aktuelle bestemmelsen ved bruk av «rettslig plikt».	*Ikke aktuelt.*
5	Lagringsbegrensning Har du vurdert hvor lenge det er nødvendig å oppbevare personopplysningene, og har du sikret at det er utarbeidet frister eller kriterier	*Ja, dette er dokumentert i organisasjonens protokoll over behandlingsaktiviteter linje 43, 44 og 45. Det er også*

[19] Formål og behandlingsgrunnlag (faktaark 56)

	for når personopplysningene skal slettes eller anonymiseres? (Husk at anonymisering er en behandling av personopplysninger som også må oppfylle kravene til behandling av personopplysninger.)	*utarbeidet en rutine for slette- og anonymiseringsprosessene.*
6	Åpenhet Har du sikret at den registrerte vil få informasjon om behandlingen av personopplysninger i samsvar med kravene i personvernforordningen artikkel 12 til 14?	*Ja, dette er beskrevet i Normsorgs generelle personvernerklæring som det linkes til i «footer» på nettsiden. Ved start av chattetjenesten henvises brukeren også til personvernerklæringen (med link) for mer informasjon om hvordan Normsorg behandler personopplysninger.*
7	Åpenhet og rettferdighet Har du husket å vurdere om det er behov for å implementere flere tiltak for å ivareta prinsippene om åpenhet og rettferdighet? Dette kan være aktuelt hvis behandlingen er uventet eller inngripende for den registrerte. F.eks. kan det være aktuelt ved overvåking, kontrolltiltak overfor ansatte eller bruk av ny profilering til å ta beslutninger.	*Det er snakk om sårbare registrerte og beskyttelsesverdige personopplysninger, men ikke spesielt uventet eller inngripende behandling av personopplysninger. Den registrerte velger også selv hvilke opplysninger som Normsorg skal få tilgang til utover IP-adresse. Ytterligere åpenhetstiltak anses ikke nødvendig.*
8	Riktighet Har du vurdert om det er behov for å etablere tiltak som sikrer at personopplysningene alltid er korrekte og oppdaterte?	*Personopplysninger om brukere av tjenesten lagres kun en kort tidsperiode. Det er ikke identifisert behov for løpende oppdatering eller kvalitetssikring av personopplysninger.*
9 a)	Informasjonssikkerhet (Konfidensialitet og integritet) Har du vurdert hvilke trusler og sårbarheter som kan medføre brudd på personopplysningenes konfidensialitet, integritet eller tilgjengelighet? Har du	*ROS-analyse er utarbeidet i samarbeid mellom prosjektet, sikkerhetsarkitekt, representant for leverandøren av den tekniske løsningen og personvernombudet. Se saksnr.*

	også vurdert sannsynligheten for at slike brudd kan oppstå, og hvilke konsekvenser det vil ha for de registrertes rettigheter og friheter?	*21/1234 for fullstendig vurdering.*
9 b)	Informasjonssikkerhet (Konfidensialitet og integritet) I lys av vurderingen i punkt 10 a), har du etablert sikkerhetstiltak som sikrer et sikkerhetsnivå som er innenfor det det organisasjonen har akseptert?	*Etablerte tiltak er dokumentert i ROS-analysen i saksnr. 21/1234. Se også beslutning fra ledergruppen om aksept av restrisikoen.*
10 a)	Personvernkonsekvenser Har du vurdert hvilke personvernkonsekvenser behandlingen kan gi, og om behandlingen kan medføre en høy risiko for de registrertes rettigheter og friheter?	*Behandlingen gjelder et stort antall sårbare registrerte (barn og unge) og beskyttelsesverdige personopplysninger (herunder helseopplysninger). Den oppfyller artikkel 29-gruppens kriterier for når det er behov for DPIA. Normsorg har konkludert med at det er sannsynlig at behandlingen kan medføre en høy risiko for de registrertes rettigheter og friheter, se saksnr. 21/1234 for fullstendig vurdering.*
10 b)	Personvernkonsekvenser Hvis du har vurdert at behandlingen vil medføre høy risiko for de registrertes rettigheter og friheter, har du gjennomført en personvernkonsekvensvurdering (DPIA)?	*Normsorg har gjennomført en DPIA, og ledelsen har godkjent denne. se saksnr. 21/1234 for fullstendig vurdering og ledelsens aksept.*
11	Ansvarlighet Har du husket å vurdere om det er behov for å utarbeide tiltak for å håndtere identifiserte risikoer underveis i behandlingen?	*Ja, sikkerhetstiltak er definert i ROS-analysen i saksnr. 21/1234. For å dempe risikoer knyttet til personvernkonsekvenser utarbeides et kurs for nye ansatte og en retningslinje for hvordan henvendelser via*

		chatten skal besvares og håndteres.
12	Den registrertes rettigheter Har du sikret at det vil være mulig å oppfylle registrertes forespørsler om håndheving av rettigheter, i den grad disse gjelder? For mer informasjon om den registrertes rettigheter, se Veileder for rettigheter ved behandling av helse- og personopplysninger.[21]	*Brukernes personopplysninger anonymiseres enten umiddelbart eller kort tid etter at samtalen er avsluttet, så det vil sjeldent være aktuelt.* *Henvendelser som kommer inn mens det fortsatt behandles personopplysninger vil kunne imøtekommes og besvares. Ungdommene er informert om at lagringsperioden er svært kort/opplysningene anonymiseres kort tid etter at samtalen er avsluttet.* *For ansattes opplysninger, vil ivaretakelse av rettighetene skje i samsvar med Normsorgs generelle rutine for ivaretakelse av registrertes rettigheter.*

Ayan lagrer sjekklisten i Normsorgs saksbehandlingssystem, slik at den er tilgjengelig for senere oppdateringer, vurderinger og kontrollaktiviteter.

[21] Veileder for rettigheter ved behandling av helse- og personopplysninger:

Vedlegg til faktaark om personvernprinsippene – Skjema for ivaretakelse av personvernprinsippene ved oppstart av ny behandling av personopplysninger

Kravnr.	Aktivitet:	Svar:
1	Formålsbegrensning Hva er formålet med den nye behandlingen av personopplysninger? Husk at alle formål må være spesifikke, uttrykkelig angitte og berettigede formål.	
2	Dataminimering Har du sikret at det kun vil bli samlet inn personopplysninger som det er nødvendig å behandle for å ivareta formålene med behandlingen? *Husk å vurdere hvor høy detaljeringsgrad opplysningene må ha for å oppfylle formålet*	
3 a)	Behandlingens lovlighet etter artikkel 6 Hva er behandlingsgrunnlaget for behandlingen av personopplysninger? *Les mer om behandlingsgrunnlag i helse- og omsorgssektoren* i Formål og behandlingsgrunnlag (faktaark 56)[22]	
3 b)	Behandlingens lovlighet etter artikkel 9 Dette punktet må bare fylles ut hvis behandlingen av personopplysninger vil omfatte særlige kategorier av personopplysninger *(for eksempel helseopplysninger eller opplysninger om fagforeningsmedlemskap):*	

[22] Formål og behandlingsgrunnlag (faktaark 56)

	Hvilket unntak i personvernforordningen artikkel 9 nr. 2 oppfyller behandlingen av personopplysninger? *Les mer om behandlingsgrunnlag i helse- og omsorgssektoren i Formål og behandlingsgrunnlag (faktaark 56)[23].*	
4	Formålsbegrensning Dette punktet må bare fylles ut hvis Normsorg skal "gjenbruke" personopplysninger som tidligere er samlet inn for et annet formål:	
4 a)	Har du sikret at den nye behandlingen av personopplysningene er forenelig med formålene som opplysningene først ble samlet inn til?	
4 b)	Hvis den nye behandlingen av personopplysningene *ikke* er forenelig med formålene som opplysningene først ble samlet inn til: Er behandlingen basert på den registrertes samtykke eller oppfyllelse av en rettslig plikt som Normsorg er underlagt? Husk henvisning til den aktuelle bestemmelsen ved bruk av «rettslig plikt»	
5	Lagringsbegrensning Har du vurdert hvor lenge det er nødvendig å oppbevare personopplysningene, og har du sikret at det er utarbeidet frister eller kriterier for når personopplysningene skal slettes eller anonymiseres? Husk at en anonymiseringprosess er en behandling av personopplysninger som	

[23] Formål og behandlingsgrunnlag (faktaark 56)

	også må oppfylle kravene til behandling av personopplysninger.	
6	Åpenhet Har du sikret at den registrerte vil få informasjon om behandlingen av personopplysninger i samsvar med kravene i personvernforordningen artikkel 12 til 14?	
7	Åpenhet og rettferdighet Har du husket å vurdere om det er behov for å implementere flere tiltak for å ivareta prinsippene om åpenhet og rettferdighet? Dette kan være aktuelt hvis behandlingen er uventet eller inngripende for den registrerte. F.eks. kan det være aktuelt ved overvåking, kontrolltiltak overfor ansatte eller bruk av ny profilering til å ta beslutninger.	
8	Riktighet Har du vurdert om det er behov for å etablere tiltak som sikrer at personopplysningene alltid er korrekte og oppdaterte?	
9 a)	Informasjonssikkerhet (Konfidensialitet og integritet) Har du vurdert hvilke trusler og sårbarheter som kan medføre brudd på personopplysningenes konfidensialitet, integritet eller tilgjengelighet? Har du også vurdert sannsynligheten for at slike brudd kan oppstå, og hvilke konsekvenser det vil ha for de registrertes rettigheter og friheter?	
9 b)	Informasjonssikkerhet (Konfidensialitet og integritet) I lys av vurderingen i punkt 10 a), har du etablert sikkerhetstiltak som sikrer et	

	sikkerhetsnivå som er innenfor det det organisasjonen har akseptert?	
10 a)	Personvernkonsekvenser Har du vurdert hvilke personvernkonsekvenser behandlingen kan gi, og om behandlingen kan medføre en høy risiko for de registrertes rettigheter og friheter?	
10 b)	Personvernkonsekvenser Hvis du har vurdert at behandlingen vil medføre høy risiko for de registrertes rettigheter og friheter, har du gjennomført en personvernkonsekvensvurdering (DPIA)?	
11	Ansvarlighet Har du husket å vurdere om det er behov for å utarbeide tiltak for å håndtere identifiserte risikoer underveis i behandlingen?	
12	Den registrertes rettigheter Har du sikret at det vil være mulig å oppfylle registrertes forespørsler om håndheving av rettigheter, i den grad disse gjelder? For mer informasjon om den registrertes rettigheter, se denne veilederen.[24]	

[24] Veileder for rettigheter ved behandling av helse- og personopplysninger: