Utfylt sjekkliste for ny behandling av personopplysninger

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

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

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	*Ja, resultatet av vurderingen er dokumentert i organisasjonens protokoll over behandlingsaktiviteter linje 43, 44 og 45.*

	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)[1]	*Les mer om når Normsorg kan bruke de forskjellige behandlingsgrunnlagene i denne rutinen.*[2] *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.*[4]

[1] Formål og behandlingsgrunnlag (faktaark 56)
[2] Dette er en fiktiv rutine
[4] 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)[3].	*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 utarbeidet en rutine for slette- og anonymiseringsprosessene.*

[3] 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.)	
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 også vurdert sannsynligheten for at slike brudd kan oppstå, og hvilke	*ROS-analyse er utarbeidet i samarbeid mellom prosjektet, sikkerhetsarkitekt, representant for leverandøren av den tekniske løsningen og personvernombudet. Se saksnr. 21/1234 for fullstendig vurdering.*

	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?	*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?	*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*

	For mer informasjon om den registrertes rettigheter, se Veileder for rettigheter ved behandling av helse- og personopplysninger[5]	*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.*

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?	

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

	Les mer om behandlingsgrunnlag i helse- og omsorgssektoren i Formål og behandlingsgrunnlag (faktaark 56)[6]	
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):* 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)[7].*	
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?	

[6] Formål og behandlingsgrunnlag (faktaark 56)
[7] Formål og behandlingsgrunnlag (faktaark 56)

	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 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 Veileder for rettigheter ved behandling av helse- og personopplysninger.[8]	

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

Vedlegg til faktaark 57 – Eksempel på utfylt sjekkliste for ny behandling av personopplysninger (ref. eksempel 17)