Lagringstid og sletting (faktaark 25)

Versjon 2.0

01.12.2021

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 omhandler lagringstid og sletting av helse- og personopplysninger. Formålet med faktaarket er å gi en oversikt og beskrivelse av kravene knyttet til lagringstid og sletting i personvernforordningen, særlovgivningen for helse- og omsorgssektoren og arkivloven med forskrifter for å bistå virksomheten med å etterleve Normens krav til lagringstid og sletting. Faktaarket omhandler også tilintetgjøring av dokumenter i behandlingsrettet helseregister mv. etter digitalisering og krav til oppbevaring av behandlingsrettet helseregister ved opphør og overdragelse av virksomhet mv.
Dette faktaarket er spesielt relevant for	Målgruppen for faktaarket er virksomheter som behandler helse- og personopplysninger. Faktaarket vil særlig være relevant for personell som har fått delegert det daglige ansvaret for personvern i virksomheten. Både medisinskfaglig kompetanse og arkivfaglig kompetanse vil imidlertid være avgjørende for å gjøre

	nødvendige avveininger knyttet til lagringstid og sletting i virksomheten.
Krav i Normen 6.0	Faktaarket gjelder for følgende kapitler i Normen 6.0 • Kapittel 2.2 Dataansvarliges ansvar • Kapittel 4.2.6 Oppbevaring av helse- og personopplysninger
Relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk	Følgende lov- og forskriftsbestemmelser er spesielt relevante for faktaarket: • Personvernforordningen Artikkel 5.Prinsipper for behandling av personopplysninger bokstav e • Personvernforordningen Artikkel 17 Rett til sletting («rett til å bli glemt») • Pasientjournalloven § 24 Overdragelse eller opphør av virksomhet • Pasientjournalloven § 25 Plikt til bevaring eller sletting • Pasientjournalforskriften §16 Tilintetgjøring av dokumenter mv. etter digitalisering • Pasientjournalforskriften §17 Opphør av virksomhet mv. • Helsepersonelloven § 43 Sletting av journalopplysninger • Arkivlova § 6 Arkivansvaret. • Arkivforskriften § 18 Avlevering og arkivdepot • Riksarkivarens forskrift § 7-29 • Helsearkivforskriften kapittel 2 Spesialisthelsetjenestens plikt til å avlevere pasientarkiv til Norsk helsearkiv, • Helsearkivforskriften §17 Tidspunkt for avlevering av pasientarkivmateriale • Helsearkivforskriften §21 Digitalisering og kassasjon

LAGRINGSTID OG SLETTING

Normen stiller krav om at virksomheten oppbevarer helse- og personopplysninger så lenge det er nødvendig for å oppnå formålene med behandlingen av opplysningene. Med mindre opplysningene deretter skal oppbevares i henhold til nye og legitime formål, skal opplysningene slettes eller anonymiseres. Dette faktaarket gir en oversikt over, og beskrivelse av, kravene om lagringstid og sletting av helse- og personopplysninger. Krav til lagringstid og sletting finnes både i særlovgivningen for helse- og omsorgssektoren og i den generelle personvernforordningen. I tillegg har arkivlovgivningens[1] regler betydning for lagringstid og sletting av helse og personopplysninger.

Videre beskriver faktaarket krav til tilintetgjøring av dokumenter i behandlingsrettet helseregister etter digitalisering og krav til oppbevaring av behandlingsrettet helseregister ved opphør og overdragelse av virksomhet. Slike krav finnes i særlovgivningen for helse- og

[1] I dette faktaarket omfatter arkivlovgivningen arkivlova, arkivforskriften og riksarkivarens forskrift.

omsorgssektoren, samt arkivlovgivningen. Faktaarket gir også veiledning om hvordan virksomheten bør gå frem for å gjennomføre sletting.

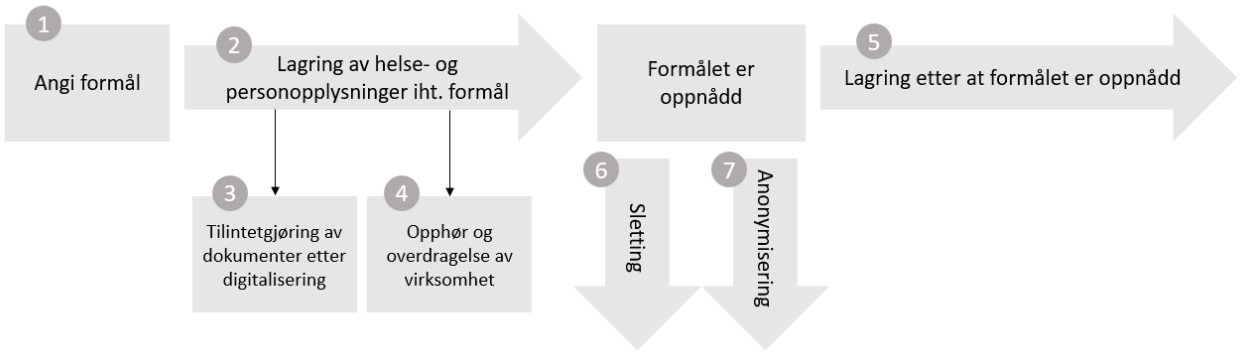
Avgrensning

Virksomheter kan ha en plikt til å slette helse- og personopplysninger både etter eget initiativ, eller etter forespørsel fra den registrerte. Faktaarket er avgrenset mot situasjoner der den registrerte ber om sletting. Hvordan virksomheten skal håndtere disse situasjonene er nærmere beskrevet i eget veiledningsmateriell.[2]

Videre er faktaarket avgrenset mot krav om lagringstid og sletting av helse- og personopplysninger i forskningsprosjekter. Dette omtales nærmere i eget veiledningsmateriell.[3]

Oversikt

Faktaarket er bygget opp etter aktivitetene som gjennomføres gjennom livsløpet til helse- og personopplysninger. Figuren nedenfor illustrerer livsløpet for behandling av helse- og personopplysninger.



Figur 1: Illustrasjon av livsløpet for behandling av helse- og personopplysninger.

[2] Veileder for rettigheter ved behandling av helse- og personopplysninger
[3] Veileder for rettigheter ved behandling av helse- og personopplysninger kapittel 6

OPPBYGNINGEN AV FAKTAARKET ER SOM FØLGER:

1 ANGI FORMÅL

Virksomheten skal alltid definere ett eller flere formål med behandlingen av helse- og personopplysninger før opplysningene samles inn.[4] Dersom virksomheten har en rettslig plikt til å behandle helse- og personopplysninger, vil formålet ofte være fastsatt i loven eller forskriften som plikten fremgår av. For eksempel er det i pasientjournalloven fastsatt at helseopplysninger i en pasientjournal kan benyttes for å yte, administrere, og kvalitetssikre helsehjelp.

Formålet med behandlingen av helse- og personopplysninger er styrende for hvor lenge virksomheten kan lagre opplysningene. Når virksomheten oppnår formålet med behandlingen, så må helse- og personopplysningene i utgangspunktet slettes eller anonymiseres.[5]

Selv om formålet er oppnådd, kan virksomheten i noen tilfeller fortsette å lagre helse- og personopplysninger der virksomheten har nye og legitime formål med behandlingen. Dette gjelder for eksempel dersom

- virksomheten har en rettslig plikt til å fortsette lagringen av helse- og personopplysningene[6], eller
- opplysningene er nødvendig for å oppfylle et nytt formål som er forenlig med det opprinnelige formålet.[7]

2 LAGRING AV HELSE- OG PERSONOPPLYSNINGER IHT. FORMÅL

2.1 BEHANDLINGSRETTET HELSEREGISTER

Helse- og personopplysninger i behandlingsrettet helseregister skal oppbevares til det av hensyn til helsehjelpens karakter ikke lenger antas å bli bruk for dem. Det samme gjelder opplysninger om hvem som har hatt tilgang til eller fått utlevert helseopplysninger som er knyttet til pasientens eller brukerens navn eller fødselsnummer (logger).[8]

Helseopplysninger som kan være nødvendig for å yte helsehjelp til pasienten skal ikke slettes, men behovet må heller ikke fremstå som for hypotetisk.[9] Hvilke helseopplysninger som vil være nødvendig må vurderes konkret i hver enkelt sak. Ved vurderingen vil

[4] Personvernforordningen artikkel 5 nr. 1 bokstav b
[5] Personvernforordningen artikkel 5 nr. 1 bokstav e
[6] Personvernforordningen artikkel 17 nr. nr. 3 bokstav b
[7] Arkivformål i allmennhetens interesse, formål knyttet til vitenskapelig eller historisk forskning eller statistiske formål skal alltid anses som forenelige formål, jf. personvernforordningen artikkel 5 nr. 1 bokstav b.
[8] Normen 6.0 Kapittel 4.2.6.1 Lagringstid ved ytelse av helsehjelp og pasientjournalloven § 25 første ledd. Pasientjournalloven § 25 korresponderer delvis med helsepersonelloven § 43 som regulerer helsepersonellets plikt til å slette personopplysninger. Etter helsepersonelloven § 43 kan helseopplysninger kun slettes dersom det er ubetenkelig ut fra allmenne hensyn, sletting ikke er i strid med arkivloven §§ 9 og 18, og det åpenbart ikke er nødvendig.
[9] Helsedirektoratets rundskriv «Helsepersonelloven med kommentarer» s. 102

medisinskfaglige hensyn være avgjørende. Det er derfor viktig at det er noen med medisinskfaglig kompetanse som gjør avveiningen.

Eksempel 1 – Nødvendige helseopplysninger

NN som er pasient hos fastlege Normland blir henvist til Normberg distriktspsykiatriske senter (Normberg DPS) etter en vurdering av at han kan ha behov for psykisk helsevern. I henvisningsbrevet skriver fastlege Normland utfyllende om NNs bakgrunn, herunder at han «tilhører Romanifolket». Ved avslutningen av behandlingen ved Normberg DPS, skriver overlege Normstad i epikrisen «opprinnelig av Romanifolket» om NN. Epikrisen blir sendt til fastlege Normland. NN reagerer på dette og mener at både fastlege Normland og Normberg DPS ikke har hatt lovlig grunnlag for å behandle opplysninger om hans etniske opprinnelse da disse ikke har vært nødvendig for å yte helsehjelp.

I et slikt tilfelle vil de medisinskfaglige vurderingene til fastlege Normland og Normberg DPS være avgjørende for om helseopplysningene er nødvendige. Eksempelet er basert på en sak fra Personvernnemda[10] hvor det aktuelle distriktspsykiatriske senteret som var påklaget hadde vurdert at opplysningen om etnisitet var relevant for den helsehjelpen som ble gitt i likhet med annen bakgrunnsinformasjon som var beskrevet i henvisningsbrevet. Både Datatilsynet og Personvernnemda uttalte at de er varsomme med å overprøve medisinskfaglige vurderinger av hvilke helseopplysninger som er nødvendig for å yte forsvarlig helsehjelp.

Ved vurdering av oppbevaringstid må virksomheten også vurdere hensynene bak dokumentasjonsplikten, herunder hensynet til at det skal være mulig å føre kontroll med virksomheten i ettertid og hensynet til pasientens mulighet til å fremme erstatningskrav ved skade.[11] På bakgrunn av disse hensynene vil det ofte være grunnlag for å lagre helseopplysninger i behandlingsrettet helseregister over lang tid.

Oppbevaring av logger er nærmere omtalt i eget faktaark.[12]

2.2 FORSKRIFTSREGULERT HELSEREGISTER

Krav om lagringstid for helse- og personopplysninger i forskriftsregulerte helseregistre følger som regel av de enkelte forskriftene som regulerer helseregistrene. Opplysninger i helseregistre skal ofte lagres på ubestemt tid. Dette gjelder for eksempel opplysninger i kreftregisteret[13] og helsearkivregisteret[14].

Dette faktaarket gir ikke en uttømmende beskrivelse av reglene for lagringstid og sletting i forskriftsregulerte helseregistre. Det kan derfor finnes krav til disse som ikke er omtalt her.

[10] PVN-2021-08
[11] Helsedirektoratets rundskriv «Helsepersonelloven med kommentarer» s. 102
[12] Se faktaark 15 om logging og hendelsesregistrering.
[13] Kreftregisterforskriften § 6-1
[14] Helsearkivforskriften § 6

2.3 ANNEN BEHANDLING AV PERSONOPPLYSNINGER

Andre helse- og personopplysninger i virksomheten skal oppbevares så lenge det er nødvendig for formålet som virksomheten har definert før innsamling.[15]

3 TILINTETGJØRING AV DOKUMENTER ETTER DIGITALISERING

Når dokumenter på papir er digitalisert på forsvarlig måte, kan fysiske originaldokumenter tilintetgjøres.[16] Med forsvarlig digitalisert menes at all tekst er lesbar, og at all tekst, alle sider, bilder og figurer er skannet inn. Elektronisk behandlingsrettet helseregister skal gjenspeile originalen.[17]

Skanningen skal utføres uten informasjonstap og oppløsningen skal være på minimum 300 dpi (100 %, RGB, 24 bit dybde, lavest mulig kompresjon).[18]

Virksomheten skal fastsette retningslinjer for å kontrollere at skanningen er utført korrekt og komplett, og at dokumentene er lesbare, før den originale papirversjonen destrueres. Rutinen må beskrive[19]

- ansvar
- hvordan skanningen skal gjennomføres
- hvordan virksomheten skal kvalitetssikre dokumentet som er skannet inn

4 OPPHØR OG OVERDRAGELSE AV VIRKSOMHET

Ved overdragelse eller opphør av virksomhet kan behandlingsrettet helseregister overføres til en annen virksomhet. Pasient/bruker kan motsette seg overføring av sin journal og i stedet kreve at registeret overføres til en annen bestemt virksomhet.[20] Dersom det er praktisk mulig, skal pasienten/brukeren gjøres kjent med denne retten.[21]

Det ovennevnte gjelder ikke ved overføringer grunnet strukturelle endringer i den offentlige helse- og omsorgstjenesten, for eksempel ved virksomhetsoverdragelse av et sykehus fra et

[15] Personvernforordningen artikkel 5 nr. 1 bokstav e og artikkel 17.
[16] Normen 6.0 Kapittel 4.2.6.2 Tilintetgjøring av dokumenter i behandlingsrettet helseregister mv. etter digitalisering, pasientjournalforskriften § 16 og helsearkivforskriften § 21
[17] Normen 6.0 Kapittel 4.2.6.2 Tilintetgjøring av dokumenter i behandlingsrettet helseregister mv. etter digitalisering
[18] Riksarkivarens forskrift § 5-15, jf. § 3-6 nr. 1, jf. pasientjournalforskriften § 16
[19] Riksarkivarens forskrift § 3-6 nr. 2 og Arkivverkets veileder for dokumentasjonskrav for fullelektroniske arkivsystemer
[20] Normen 6.0 Kapittel 4.2.6.3 Behandlingsrettet helseregister ved opphør og overdragelse av virksomhet mv. og pasientjournalloven § 24
[21] Pasientjournalloven § 24

helseforetak til et annet. Ved strukturelle endringer vil pasienten derfor ikke ha rett til å motsette seg overføring.[22]

Hvis det ved overdragelse eller opphør av virksomhet ikke er aktuelt å overføre pasientjournalene til et bestemt helsepersonell eller til en bestemt virksomhet, skal de avleveres til Helsedirektoratet eller det organ direktoratet bestemmer. Helsedirektoratet er dataansvarlig for behandlingen av opplysningene etter at de er avlevert.[23]

Journaler som avleveres oppbevares til det av hensyn til helsehjelpens karakter ikke lenger antas å bli bruk for dem, og kan deretter tilintetgjøres etter samråd med Riksarkivaren eller avleveres til offentlig arkivdepot. Materialet fra spesialisthelsetjenesten skal behandles som bestemt i helsearkivforskriften.[24]

Materialet fra spesialisthelsetjenesten er pasientjournalarkiv om avdøde pasienter. Se punkt 7.1 nedenfor.

5 LAGRING ETTER AT FORMÅLET ER OPPNÅDD

5.1 LAGRING ER NØDVENDIG FOR Å OPPFYLLE VIRKSOMHETENS ARKIVPLIKT

Virksomheten skal fortsette å lagre helse- og personopplysninger etter at formålet er oppnådd dersom opplysningene er underlagt arkivplikt.[25] Alle offentlige organer er underlagt arkivlova med forskrifter[26], og dermed underlagt arkivplikt.[27] Regionale helseforetak og helseforetak regnes som offentlige organer etter arkivlova, og er dermed også underlagt arkivplikt.[28]

Helse- og personopplysninger fra helse- og omsorgstjenesten skal som regel ikke arkiveres før etter at pasienten er død. På dette tidspunktet gjelder ikke personvernforordningens bestemmelser om behandling av personopplysninger da personvernforordningen ikke omfatter døde personer.[29] Særlovgivningen for helse- og omsorgssektoren og arkivlovgivningen har imidlertid bestemmelser som gjelder avdøde personer.

Både offentlige og private virksomheter i spesialisthelsetjenesten skal bevare og avlevere pasientjournalarkivene sine til Norsk Helsearkiv.[30] Pasientjournalarkivene skal avleveres til Norsk Helsearkiv tidligst ti år etter pasientens død[31], alternativt 110 år etter pasientens fødsel.[32]

Fra elektroniske pasientjournaler skal følgende avleveres:[33]

---

[22] Engelschiøn og Vigerust (2021) lovkommentar til pasientjournalloven § 24
[23] Pasientjournalforskriften § 17 første ledd
[24] Pasientjournalforskriften § 17 annet ledd
[25] Pasientjournalloven § 25 annet ledd, helsepersonelloven § 43 og arkivlova med forskrifter
[26] Arkivlova § 5
[27] Arkivlova § 6
[28] Helseforetaksloven § 5 fjerde ledd
[29] Personvernforordningens fortalepunkt 27
[30] Spesialisthelsetjenesteloven § 3-2a og helsearkivforskriften kapittel 2
[31] Helsearkivforskriften § 17
[32] Helsearkivforskriften § 19
[33] Helsearkivforskriften § 11

- Alle opplysninger som registreres i henhold til helsepersonelloven §§ 39 og 40
- Pasientidentifikasjon og all informasjon som kan representeres som tekst, inkludert koder, tall og målte verdier mv.
- Dokumenter som arkivskaper har digitalisert, som en del av den løpende journalføringen eller på et senere tidspunkt

Fra fysisk pasientarkiv skal følgende avleveres:[34]

- Legejournaler og epikriser
- Korrespondanse som er lett tilgjengelig innenfor den enkelte journal
- Dokumentasjon av vedtak om bruk av tvang

Alle virksomheter i spesialisthelsetjenesten skal avlevere alle fysiske pasientjournaler for pasienter som døde før 1. januar 1950 i sin helhet.[35] I tillegg finnes det egne bestemmelser om avlevering av fysisk pasientarkiv for enkelte navngitte virksomheter[36] og fra virksomheter som yter eller har ytet nasjonale eller flerregionale behandlingstjenester[37].

Privatpraktiserende spesialister skal ikke avlevere pasientjournalarkivene sine til Norsk Helsearkiv med mindre Riksarkivaren treffer vedtak om det. Privatpraktiserende spesialister kan kassere[38] pasientjournalarkivene ti år etter pasientens død.[39]

Visse tjenester i den kommunale og fylkeskommunale helse- og omsorgstjenesten skal bevare sine pasient- og journalopplysninger. Dette gjelder helsestasjonstjenester, skolehelsetjenesten og tannhelsetjenesten, samt tjenester innen rusomsorg og psykososial omsorg.[40] Arkivene skal avleveres til kommunalt depot.[41] Med pasient- og journalopplysninger menes all individbasert dokumentasjon som skapes av kommunale og fylkeskommunale tjenester som yter helsehjelp.[42] Kommunen og fylkeskommunen trenger imidlertid ikke å bevare individbaserte opplysninger om vaksiner som er meldt til Nasjonalt vaksinasjonsregister (Sysvak).[43]

Andre tjenester i den kommunale eller fylkeskommune helse- og omsorgstjenesten kan kassere sine pasient- og journalopplysninger minimum 20 år etter pasientens død, alternativt 120 år etter pasientens fødsel.[44]

Riksarkivarens forskrift lister også opp andre sakstyper fra kommunens og fylkeskommunens helse- og omsorgstjeneste som skal bevares.[45] Disse omtales ikke nærmere her.

[34] Helsearkivforskriften § 10
[35] Helsearkivforskriften § 9
[36] Helsearkivforskriften § 7
[37] Helsearkivforskriften § 8
[38] Kassasjon innebærer å destruere arkivmateriale, jf. Ot.prp.nr.77 (1991-1992) s. 5.
[39] Helsearkivforskriften § 12
[40] Riksarkivarens forskrift § 7-29
[41] Arkivforskriften § 18 (2)
[42] Riksarkivarens forskrift § 7-29 nr. 1 bokstav b
[43] Riksarkivarens forskrift § 7-29 nr. 2 bokstav h
[44] Riksarkivarens forskrift § 7-29 nr. 1 bokstav b
[45] Riksarkivarens forskrift § 7-29

5.2 LAGRING ER NØDVENDIG FOR Å OPPFYLLE EN ANNEN RETTSLIG PLIKT, FOR Å UTFØRE EN OPPGAVE I ALLMENNHETENS INTERESSE ELLER FOR Å UTØVE OFFENTLIG MYNDIGHET

Virksomheten skal fortsette å lagre helse- og personopplysninger dersom opplysningene er omfattet av andre oppbevaringsplikter (enn arkivplikt) i lov eller forskrift, eller dersom lagring er nødvendig for å utføre en oppgave i allmennhetens interesse eller for å utøve offentlig myndighet.[46]

5.3 LAGRING ER NØDVENDIG AV HENSYN TIL ALLMENNHETENS INTERESSE PÅ OMRÅDET FOLKEHELSE

Virksomheten kan fortsette å lagre helse- og personopplysninger etter at formålet er oppnådd dersom lagring er nødvendig av hensyn til allmennhetens interesse på området folkehelse.[47] Unntaket gjelder for eksempel når behandlingen av personopplysninger er nødvendig for å bekjempe en epidemi eller pandemi.

5.4 LAGRING ER NØDVENDIG FOR Å OPPNÅ NYE OG FORENLIGE FORMÅL

Virksomheten kan fortsette å lagre helse- og personopplysninger etter at formålet er oppnådd dersom lagring er nødvendig for å oppnå nye formål som er forenlige med det opprinnelige formålet[48]

I vurderingen av forenlighet 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.[49] De nye formålene kan være forenlige 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.

Arkivformål i allmennhetens interesse, formål knyttet til vitenskapelig eller historisk forskning eller statistiske formål skal ikke anses som uforenlig med de opprinnelige formålene.[50] Hva som ligger i disse begrepene, er ikke tydelig definert i personvernforordningen. Behandling av helse- og personopplysninger i helse- og omsorgssektoren er imidlertid ofte regulert av annen lovgivning.

5.5 LAGRING ER NØDVENDIG FOR Å FASTSETTE, GJØRE GJELDENDE ELLER FORSVARE RETTSKRAV

Virksomheten kan fortsette å lagre personopplysninger etter at formålet er oppnådd dersom lagring er nødvendig for å fastsette, gjøre gjeldende eller forsvare rettskrav.[51][52] Unntaket kan

[46] Personvernforordningen artikkel 17 nr. 3 bokstav b
[47] Personvernforordningen artikkel 17 nr. 3 bokstav c
[48] Personvernforordningen artikkel 5 nr. 1 bokstav e
[49] Personvernforordningen artikkel 6 (4) og Skullerud (2019) lovkommentarer til personvernforordningen artikkel 6
[50] Personvernforordningen artikkel 5 nr. 1 bokstav b
[51] Personvernforordningen artikkel 17 nr. 3 bokstav e
[52] Hva som skal regnes som et rettskrav er ikke definert i personvernforordningen. Begrepet er imidlertid også brukt i tvisteloven § 1-3, og tvistelovens forarbeider defineres rettskrav som krav som reguleres av rettsregler.

for eksempel være relevant for virksomhetens behandling av personopplysninger om egne ansatte dersom det oppstår en tvist som gjør det nødvendig å oppbevare opplysninger etter at formålet er oppnådd for å oppklare tvisten.

6 SLETTING NÅR FORMÅLET ER OPPNÅDD

Dersom virksomheten ikke har grunnlag for å oppbevare helse- og personopplysninger etter at formålet er oppnådd, så skal de slettes.[53]

Slettingen skal gjøres på en forsvarlig måte.[54] Det skal brukes en metode som gjør at det ikke er mulig å rekonstruere opplysningene. Det er ikke tilstrekkelig å begrense tilgangen til opplysningene ved hjelp av tilgangsstyring. For å oppfylle sletteplikten må virksomheten slette alle kopier av opplysningene, i utgangspunktet også filer og data i sikkerhetskopier.

Det anbefales[55] å velge et produkt for sletting (også omtalt som sletteverktøy) som er sertifisert[56] i henhold til standarden ISO/IEC 15408 Common Criteria for IT Security Evaluation, herunder evaluert av et uavhengig akkreditert laboratorium. Det vil gi en høyere grad av tillit til at sletteverktøyet fungerer etter hensikten. Se også lister over flere kategorier evaluerte og sertifiserte produkter for sletting og makulering av lagringsmedier i NATOs Information Assurance Product Catalogue (NIAPC)[57].

Sletting av bare utvalgte filer og data i sikkerhetskopier byr på særlige utfordringer, men er mulig. Det forutsetter en løsning for sikkerhetskopiering som kan skaleres, slik at det i nødvendig grad skilles mellom sikkerhetskopiering av ulike typer av filer og data.

For å redusere risikoen knyttet til personvernet ved oppbevaring av helse- og personopplysninger i filer fra sikkerhetskopier, bør virksomheten sørge for at sikkerhetskopiene overskrives regelmessig. Virksomheten bør likevel sørge for at overskriving ikke forhindrer virksomheten fra å oppnå formålet med sikkerhetskopiene.

Å gjennomføre sletting av helse- og personopplysninger kan være en utfordring for mange virksomheter, særlig dersom virksomheten ikke har systemer med funksjonalitet for sletting. Virksomheter som ikke kan gjennomføre sletting bør iverksette andre tiltak for å ivareta personvernet. Tiltak kan for eksempel være skjuling, merking og begrensning av tilgang til opplysninger som skulle vært slettet. Det er viktig å være oppmerksom på at selv om slike tiltak vil kunne ha en risikodempende effekt på personvernet, vil det ikke vil være tilstrekkelig for å oppfylle en sletteplikt. For å kunne etterleve kravene om sletting bør virksomheten derfor undersøke om systemene har funksjonalitet for sletting allerede ved anskaffelse eller utvikling av systemer.[58]

---

[53] Personvernforordningen artikkel 5 nr. 1 bokstav e og artikkel 17, og pasientjournalloven § 25

[54] I Normen 6.0 er det et krav i pkt. 5.3.3 om at lagringsmedier som tas ut av bruk skal slettes forsvarlig. Tilsvarende forsvarlighetskrav kan legges til grunn for sletting av filer og data, også der lagringsmediet ikke tas ut av bruk etterpå.

[55] NSMs grunnprinsipper for IKT-sikkerhet 2.0, tiltak 2.1.3.

[56] Liste over evaluerte og sertifiserte verktøy for sletting finnes under kategorien «Data protection» her: https://www.commoncriteriaportal.org/products/

[57] Se https://www.ia.nato.int/NIAPC

[58] Dette er også fastsatt i NSMs grunnprinsipper for IKT-sikkerhet 2.0, tiltak 2.1.10 bokstav j.

7 ANONYMISERING NÅR FORMÅLET ER OPPNÅDD

Virksomheten kan anonymisere personopplysninger for å unngå å måtte slette opplysningene etter at formålet er oppnådd. Dette gjelder imidlertid ikke i behandlingsrettet helseregister. I behandlingsrettet helseregister skal helse- og personopplysninger slettes.[59]

Personopplysninger anses som anonymiserte når de håndteres eller bearbeides slik at de ikke lenger kan knyttes til en identifisert eller identifiserbar fysisk person.[60]

Virksomheten må være oppmerksom på at anonymisering i seg selv er en behandling av personopplysninger som forutsetter at personvernforordningens krav er oppfylt. Virksomheten står derfor ikke helt fritt til å anonymisere helse- og personopplysninger når de ønsker det.

[59] Ordlyden «slettes» i pasientjournalloven § 25
[60] Personvernforordningen fortalepunkt 26