Retningslinjer for sletning

Revisionshistorik

Version	Dato	Beskrivelse af ændringer	Udført af	Godkendt af
1.1	27-10-2021	Mindre redaktionelle rettelser	Sikkerhedsrådgiver	Sikkerhedsteam
2.0	26-10-2022	Større ændringer foretaget og tilføjelse af afsnit om drev/mail samt fysisk opbevarede oplysninger	Sikkerhedsrådgiver	Sikkerhedsteam
2.1	18-02-2025	Tilføjelser i flere afsnit	Sikkerhedsrådgiver	Sikkerhedsteam

Formål

Disse retningslinjer har til formål at sikre, at Jammerbugt Kommune sletter personoplysninger efter gældende lovgivning, og at sikre ensartede slettefrister på tværs af organisationen. Retningslinjerne omfatter sletning af alle former for opbevarede personoplysninger, som kommunen har – herunder data opbevaret i it-systemer, på drev eller i mail samt fysisk opbevarede dokumenter indeholdende personoplysninger.

Ifølge databeskyttelsesforordningen skal Jammerbugt Kommune sikre sig, at personoplysninger ikke opbevares i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles (jf. databeskyttelsesforordningens artikel 5, stk. 1, litra e). Det betyder, at data som udgangspunkt skal slettes eller anonymiseres, når personoplysninger ikke længere er nødvendige at opbevare.

Der henvises i øvrigt til retningslinjer for dataklassifikation og -opbevaring, hvori kommunen klassificerer forskellige datatyper, herunder hvor og hvor længe data må opbevares på kommunens it-udstyr.

Hvad er sletning?

Sletning af personoplysninger er en handling, der sikrer, at oplysningerne ikke længere er tilgængelige. Hvis personoplysninger efter sletning fx kan tilgås af systemets administrator, er der ikke tale om en reel sletning. Hvis personoplysninger omvendt reelt set er slettet via operativsystemet, og på disken venter på at blive overskrevet med andre data, er der tale om sletning, da oplysningerne ikke længere med rimelige midler er tilgængelige.

Arkivering og journalisering

En række data er underlagt krav om arkivering, jf. arkivloven. Hvis et system indeholder data, der er omfattet af arkivering, er systemejer ansvarlig for, at de arkivpligtige data arkiveres, inden de slettes. Systemejere kan kontakte kommunens arkivansvarlige for sparring og vejledning i forhold til arkivering.

Arkivering kan foregå løbende, eller der kan arkiveres samlet for en fastsat periode. Datatilsynet har tilkendegivet, at de accepterer en arkivperiode på 5 år – dvs. at der arkiveres fra systemer hvert 5. år, selvom det vil betyde, at personoplysninger gemmes i

op til yderligere 5 år, end det er fastlagt i slettefristen, plus tid til godkendelse af arkiveringen.

Når data er udtaget til arkiv, går der tid, før arkivversionen er godkendt af Rigsarkivet, og data kan slettes i systemet. Der kan dermed gå op til 2 år, før arkiveringen er tilendebragt. Systemejer er forpligtet til løbende at orientere kommunens arkivansvarlige om arkiveringsprocessen.

Det er vigtigt, at data aldrig slettes, før der er foretaget en korrekt arkivering, og at der foreligger skriftlig dokumentation for, at arkivversionen er godkendt af Rigsarkivet.

Alle ansatte skal overholde journaliseringspligten, jf. offentlighedsloven, hvilket vil sige, at ansatte har pligt til at journalisere relevante filer i fx SBSYS eller fagsystemer, inden filerne slettes. Det er vigtigt for at undgå fejl, at ansatte dobbelttjekker, at journaliseringen er foregået korrekt, inden sletningen foretages.

Slettefrister
I it-systemer er systemejeren på baggrund af formålene med behandlinger af personoplysninger ansvarlig for at fastsætte slettefrister for det data, som behandles i løsningen. Ansvaret for at fastsætte slettefrister for personoplysninger, som opbevares fysisk uden for it-systemer, er placeret hos lederen i det fagområde, som primært er ansvarlig for den pågældende proces/arbejdsgang.

Systemejeren kan hente inspiration til fastsættelse af slettefrister på KLE-online.dk. KL har gennem KLE-online noteret anbefalede slettefrister koblet op på emner (KLE-numre). Alle ansatte har via kommunens netværk adgang til KLE-online.dk og kan få inspiration til, hvilke slettefrister man kan opsætte på kommunens sagstyper. Få mere viden herom i 'Vejledning i fastsættelse af slettefrister'.

Slettefristerne for data noteres i de relevante behandlingsaktiviteter, hvori behandlingen af de pågældende data indgår. I kommunen registreres slettefrister af GDPR-koordinatorerne i ISMS-systemet OS2Compliance.

Slettefrist for arkivpligtige data
Den reelle slettefrist for persondata, som skal arkiveres, og som behandles i et system, hvorfra der arkiveres hvert 5. år, vil få en slettefrist, der maksimalt vil være:

Fastlagt slettefrist + 5 års arkiv-interval + 2 år til godkendelse = reel slettefrist.

Eksempel:

- Personsager i sundhedsplejen skal gemmes i 10 år, efter sagen er lukket jf. sundhedsloven.
- Der arkiveres fra sundhedsplejens system hvert 5. år.
- En sag kan nå 10 års henlæggelse/afslutning, kort efter der er blevet arkiveret. Der går derfor 5 år, før næste arkivering finder sted.
- Der går op til 2 år, før udtrækket til arkiv er godkendt, og sletning kan gennemføres.

Den reelle slettefrist er i dette tilfælde:

10 års gemmetid, efter sagen er afsluttet
+ maksimalt 5 år indtil næste arkivering

+ maksimalt 2 års arbejdstid til at få godkendt arkivversionen
= 17 år, før data slettes i forhold til data med en 10 års opbevaringsperiode.

I oplysningsskrivelsen til den registrerede skal der derfor stå følgende: 'Vi gemmer dine data i maksimalt 17 år, efter din sag er lukket. Herefter overføres data til arkiv og slettes i kommunen'.

Det er vigtigt, at det altid er den reelle slettefrist, der anføres på oplysningspligten, og ikke den slettefrist, som er fastlagt via særlovgivning eller vejledning i KLE-online. Det er systemejerens ansvar at sikre sig, at slettefristen fremgår af den oplysningspligt, som kommunen har over for den registrerede.

Sletning af data i it-systemer
Systemejeren er, jf. informationssikkerhedspolitikken, ansvarlig for at sikre, at der er fastsat slettefrister for personoplysninger behandlet i it-systemet, at sletning foretages, samt at der gennemføres kontrol af sletning.

Det er systemejers ansvar, at der er udarbejdet dokumentation for slettefrister og beskrivelse af proceduren for sletning for ethvert system, som indeholder personoplysninger. Til dette formål skal systemejer anvende skabelonen 'Sletning af persondata'. Den udfyldte skabelon gemmes som dokumentation i SBSYS, evt. i sagen vedrørende databehandleraftalen for det pågældende system. Der er også udarbejdet en praktisk vejledning til sletning i it-systemer, som fungerer som en tjekliste, når systemejer skal påbegynde processen med implementering af sletning af personoplysninger i et it-system.

Systemejer har pligt til at sikre, at der to gange årligt foretages stikprøvekontroller på, at sletningen sker. Opfølgning på sletning giver en vished om, at de valgte sletteprocedurer virker, og at man som dataansvarlig overholder bestemmelserne fastlagt i databeskyttelsesforordningens artikel 5, stk. 1, litra c-e. Opfølgning vil ligeledes hjælpe med tidligt at identificere personoplysninger, som burde have været slettet, men som mod forventning ikke er blevet det. Kravet om kontrol gælder uanset, om sletningen sker automatisk eller manuelt, og resultaterne af kontrollerne skal noteres i ovennævnte skabelon, så det sikres, at kommunen har den nødvendige skriftlige dokumentation.

Teknisk definition på sletning i it-systemer
Sletning af personoplysninger i et system er en handling, der sikrer, at oplysningerne ikke længere er tilgængelige. Hvis personoplysninger efter sletning fx kan tilgås af systemets administrator, er der ikke tale om en reel sletning. Hvis personoplysninger omvendt reelt set er slettet via operationssystemet, og på disken venter på at blive overskrevet med andre data, er der tale om sletning, da oplysningerne ikke længere med rimelige midler er tilgængelige.

Et system, hvori der behandles personoplysninger, kan typisk opdeles i en database, hvori alle oplysninger er lagret, og en brugerrettet del, hvor oplysninger i databasen kan fremvises og redigeres. Der er således en kobling mellem databasen og den brugerrettede del, og typisk vil oplysningerne fremgå en-til-en. Der kan dog være systemer, der anvender en såkaldt "soft delete", hvor sletning i den brugerrettede del sletter koblingen, men ikke personoplysningen i den bagvedliggende database. Her er der ikke tale om en

reel sletning, da adgang til personoplysningerne stadig er mulig via databasen udenom den brugerrettede del.

Når lagringsmedier som harddiske og USB-medier, der har været anvendt til behandling af personoplysninger, bortskaffes, er det vigtigt, at lagrede personoplysninger slettes forsvarligt, så oplysningerne ikke kan komme uvedkommende i hænde. Tidligere datamedier, som skal kasseres, afleveres hos Digitalisering, It og Borgerservice, som sørger for en standardiseret og sikker sletning af indholdet.

Mange systemer indeholdende personoplysninger understøtter logning af de handlinger, der udføres i systemet, herunder sletning af oplysninger. Systemejeren skal være opmærksom på, hvorvidt disse logs i sig selv indeholder personoplysninger og evt. tage stilling til slettefrister for logoplysningerne.

Data på drev og i mail
Kommunen har en slettefrist på maksimalt 30 dage for følsomme og fortrolige oplysninger på alle midlertidige opbevaringsplaceringer, hvilket omfatter alle drev, Microsoft OneDrive, Microsoft Outlook, Microsoft Teams, Microsoft SharePoint og PC-skrivebord. Følsomme og fortrolige oplysninger dækker både over følsomme forretningsoplysninger samt følsomme og fortrolige personoplysninger.

Almindelige personoplysninger samt alle øvrige oplysninger må opbevares på midlertidige opbevaringsplaceringer, indtil det ikke længere er relevant at gemme, og/eller at sagen er afsluttet, hvorefter filerne evt. journaliseres i fagsystem og slettes.

Det er den enkelte medarbejders ansvar løbende at slette filer indeholdende personoplysninger på egne drev (fx OneDrive) og i egen mailindbakke (Outlook), samt at sikre overholdelse af ovennævnte slettefrist på maksimalt 30 dage.

Alle ledere er ansvarlige for at sikre, at der i egne afdelinger følges op på, at hver enkelt medarbejder overholder reglerne. På samme vis er det den enkelte leders ansvar at sikre, at der ryddes op i fællesfiler i afdelingen. Det anbefales, at afdelinger udarbejder skriftlige procedurer for sletning, samt man med jævne mellemrum orienterer medarbejdere om procedurerne.

Data på PC
Alle filer i mappen ”Overførsler” bliver automatisk slettet efter 30 dage for at mindske pladsforbruget og for at nedsætte risikoen for, at medarbejderen har dokumenter eller andre filer indeholdende følsomme eller fortrolige oplysninger lokalt opbevaret på PC’en.

Papirkurven på kommunens PC’er bliver automatisk slettet fra enheden efter 30 dage efter, at brugeren har slettet filen.

Fysisk opbevarede oplysninger
Det anbefales, at personoplysninger så vidt muligt kun opbevares digitalt på de it-løsninger, kommunen stiller til rådighed. Dette vurderes både som værende mere sikkert samt som værende ressourcebesparende sammenlignet med udgifter til print. Hvis man lokalt ønsker at printe og opbevare fysiske dokumenter indeholdende personoplysninger, skal nedenstående retningslinjer overholdes.

Fysiske dokumenter indeholdende personoplysninger må opbevares, indtil medarbejderen vurderer, at det ikke længere er relevant at gemme dokumenterne i papirform, så længe de er låst inde, fx i en skuffe, et skab eller på et kontor. Det er den nærmeste leders ansvar, at der stilles aflåsningsmuligheder til rådighed for medarbejdere med behov for fysik opbevaring af dokumenter indeholdende personoplysninger. Her er det vigtigt at være opmærksom på, at kun medarbejdere med et arbejdsbetinget behov for at kunne tilgå de pågældende oplysninger skal have adgang til de opbevarede dokumenter.

Det er nærmeste leders ansvar at fastsætte slettefrister for fysisk opbevarede oplysninger i egen afdeling, dvs. at fastlægge, hvor længe oplysninger må gemmes fysisk. Det er medarbejderens eget ansvar løbende at sikre, at dokumenter skal destrueres i overensstemmelse med de fastsatte slettefrister, herunder at sikre, at relevante informationer eventuelt indscannes og journaliseres i it-systemer inden destruktion. Dokumenter indeholdende personoplysninger skal makuleres inden kassation. Den nærmeste leder er ligeledes forpligtet til at sikre, at ovenstående regler til enhver tid overholdes, herunder at der med jævne mellemrum udføres kontroller heraf. Det anbefales, at afdelinger udarbejder skriftlige procedurer for sletning, som nyansatte præsenteres for, samt lederen med jævne mellemrum orienterer medarbejdere om procedurerne.