Retningslinjer for logning af it-systemer

Revisionshistorik

Version	Dato	Beskrivelse af ændringer	Udført af	Godkendt af
2.0	30-05-2022	Ændring i flere afsnit	Sikkerhedsrådgiver	Sikkerhedsteam
2.1	26-04-2024	Tilføjelse til punkt "Kontrol af log" ift. opfølgning	Sikkerhedsrådgiver	Sikkerhedsteam
2.2	07-05-2025	Tilføjelser i flere afsnit herunder kontrol af administratorer, gennemgang af og kontrol af logdata samt "Proaktive awareness-tiltag"	Sikkerhedsrådgiver	Sikkerhedsteam

Formål

Disse retningslinjer har til formål at sikre, at Jammerbugt Kommune lever op til databeskyttelsesforordningens artikel 32 stk. 1, som pålægger den dataansvarlige at gennemføre passende tekniske og organisatoriske foranstaltninger. Derudover bygger retningslinjerne på den forhenværende sikkerhedsbekendtgørelses § 19, stk. 1, som pålægger offentlige myndigheder at foretage logning af alle anvendelser af personoplysninger.

Der henvises desuden til:

- Retningslinjer for logning af infrastruktur, som målretter sig logning af teknisk data
- Procedure for gennemgang af medarbejderes data herunder logoplysninger

Logning af adgang til IT-ressourcer

I Jammerbugt Kommune logges det hver gang en medarbejder har været inde i et system. Det logges også, hvilke sager/filer den enkelte medarbejder har været inde på, hvis det er systemer eller filer indeholdende personoplysninger. Alle mislykkede adgangsforsøg, anvendelser af data, som indeholder fortrolige eller følsomme personoplysninger samt medarbejdernes brug af hjemmesider via internettet og e-mail registreres via loggen.

Der er udarbejdet en procedure for gennemgang af medarbejderes data herunder logoplysninger. Proceduren anvendes i forbindelse med, at en medarbejder ikke er i stand til at varetage sit arbejde, og at kommunen har brug for at tilgå oplysningerne for at kunne varetage sin myndighedsudøvelse. Det kan også ske i forbindelse med mistanke om en ansats misbrug af adgange, hvor kommunen er nødt til at undersøge sin mistanke via en gennemgang af logs.

Hvad skal logges?

Jammerbugt Kommune arbejder ud fra en risikobaseret tilgang, hvilket vil sige, at kommunen for hver enkelt databehandling vurderer, hvilke tekniske eller organisatoriske sikkerhedsforanstaltninger der er nødvendige for at sikre den pågældende data tilstrækkeligt. Det er således et systems risikovurdering, der skal afgøre, hvorvidt logning og kontrol af log er relevant og tilstrækkelig. Systemejeren er ansvarlig for at vurdere, hvorvidt det er relevant at gennemføre kontrol af log, og sikkerhedsrådgiveren kan bistå med rådgivning herom.

Systemejeren kan fx begrænse eller udelade at udføre kontrol af log ud fra følgende overvejelser:

- Der er ikke oprettet brugere i systemet, hvorfor det heller ikke er muligt at kontrollere brugeres adfærd.
- I nogle systemer har brugerne kun adgang til egne data, dvs. data som de selv har beriget systemet med. Her vurderer kommunen ikke, at det er relevant at føre kontrol af log.
- I nogle systemer findes der en meget begrænset adgang fx via roller, så brugerne kun kan tilgå oplysninger, som er relevant for det arbejde, de bestrider. Her vurderer kommunen, at kontrol af log ikke er relevant. Til gengæld er det meget vigtigt, at systemejer i disse tilfælde har et særligt fokus på procedure for brugerautorisationer og kontrol hermed.
- I nogle systemer besidder brugerne en 'skrankefunktion', hvor de fx får borgerhenvendelser via telefon, mail eller fysisk fremmøde. Brugerne har samtidigt ikke tildelt specifikke sager, men skal kunne tilgå alle oplysninger i systemer, alt efter hvilke borgere der henvender sig til dem. I dette tilfælde vurderer kommunen, at man ikke uden et uforholdsmæssigt stort ressourcetræk vil kunne finde frem til eventuelt misbrug af adgang. Det vil dog altid afhænge af systemejers vurdering ud fra det konkrete system, erfaringer med brug og misbrug i systemet, samt systemets risikovurdering.

Hvis systemejer fravælger kontrol af log for et system, skal vurderingen heraf nedfældes i et skriftligt notat, som journaliseres i SBSYS. Der findes en skabelon hertil på TRYK. Systemejer skal årligt gennem sin revision af risikovurderingen genoverveje beslutningen vedrørende fravalg af kontrol af log, da risikobilledet eller systemet godt kan have ændret sig siden sidst.

Systemejeren har desuden ansvaret for at sikre sig, at niveauet af logning i systemet lever op til nedenstående krav og er anvendelige til at kunne foretage kontroller ud fra.

Logning af adgang
Mislykkede adgangsforsøg logges og registreringerne herom gennemgås periodisk. Digitalisering, IT og Borgerservice har ansvaret for, at denne kontrol gennemføres. Gentagne mislykkede forsøg skal medføre lukning af adgang.

Logning af anvendelse
Alle anvendelser af data vedrørende enkeltpersoner logges og gemmes i et halvt år og ved særlige behov op til 5 år (gælder ikke dokumenter under udarbejdelse). Den enkelte systemejer har ansvaret for, at denne kontrol gennemføres. Loggen skal indeholde tidspunkt, bruger, anvendelse og personen, som anvendelsen vedrører.

Opbevaring
Data skal opbevares, så kun autoriserede brugere har adgang til dem. Brugergenererede logdata skal være omfattet af en backup-strategi.

Kontrol af log
Systemejere er ansvarlige for at gennemføre stikprøver på loggen mindst to gange årligt for de systemer, hvor dette er vurderet relevant. Ud fra den risikobaserede tilgang og systemets risikovurdering kan systemejer beslutte, hvor ofte det er nødvendigt at

gennemføre stikprøven – fx afhængig af mængden og typen af persondata, der behandles i systemet. Dog skal kontrollen udføres minimum to gange årligt.

Stikprøverne vil have fokus på, om der er medarbejdere, der uden gyldig arbejdsbetinget grund har fremsøgt, læst eller på anden vis tilgået eller anvendt personoplysninger. Det er vigtigt, at proceduren for kontrol af brugere også har fokus på administratorers aktiviteter. Ofte har administratorer udvidede rettigheder, hvilket medfører en højere konsekvens i tilfælde af misbrug hos netop brugere af denne type. Det anbefales derfor, at it-systemer altid har mindst to administratorer, og at disse administratorer kontrollerer hinandens aktiviteter.

Stikprøver vil i praksis foregå ved, at logdata fra en udvalgt periode bliver gennemgået. Systemejer skal kunne dokumentere, hvornår kontrollen er foretaget, og skal destruere logningsfilerne, når disse har udtjent deres formål. Det anbefales som standard, at logningsfilerne destrueres et halvt år, efter stikprøven er udført. Til brug for dokumentation har kommunen udarbejdet en skabelon 'Procedure for kontrol af log', som systemejeren udfylder og journaliserer i SBSYS, hver gang en ny kontrol er foretaget. Skabelonen må ikke indeholde personhenførbare oplysninger om de personer, som er kontrolleret, men fungerer udelukkende som en dokumentation af de gennemførte kontroller.

Hvis en stikprøvekontrol viser, at en eller flere medarbejdere har tilgået personoplysninger i systemet uden at have et arbejdsbetinget behov herfor, skal medarbejderens nærmeste leder underrettes herom. Lederen har pligt til at vurdere og undersøge forholdet nærmere, og hvis lederen mistænker en medarbejder for kriminelle forhold eller alvorlige brud på kommunens interne retningslinjer, skal lederen omgående rette henvendelse til HR-afdelingen, som håndterer sagen derfra. Proceduren herfor er beskrevet nærmere i 'Procedure for gennemgang af medarbejderes data herunder logoplysninger'.

Anden gennemgang af medarbejderes logdata

Kommunen kan i visse situationer have brug for at tilgå medarbejderes personlige oplysninger herunder logs. Det kan ske i forbindelse med, at en medarbejder ikke er i stand til at varetage sit arbejde, og at kommunen har brug for at tilgå logoplysninger for at kunne varetage sin myndighedsudøvelse. Det kan også ske i forbindelse med direkte mistanke om en ansattes misbrug af adgange, hvor kommunen er nødt til at undersøge sin mistanke via en gennemgang af logs. En mistanke kan fx opstå på baggrund af en ekstern henvendelse fra en borger, som mener, at en ansat ved noget, som vedkommende ikke burde, eller ved, at kolleger grundet en ansats kendskab til specifikke personsager mistænker den ansatte for at tilgå flere oplysninger, end vedkommende har et arbejdsbetinget behov for.

Hvis kommunen har behov for at gennemgå en specifik ansattes logdata på baggrund af en af ovennævnte situationer, følges 'Procedure for gennemgang af medarbejderes data herunder logoplysninger'.

Proaktive awareness-tiltag

Som tilføjelse til selve logkontrollen udføres proaktive tiltag i forbindelse med logning i fagsystemer. Tiltagene tjener et primær formål i at have en forebyggende effekt på uberettigede aktiviteter i kommunens fagsystemer samt at informere medarbejdere om

kommunens retningslinjer på området, herunder omfanget af logning og kontrol samt konsekvenser ved misbrug/uberettiget aktivitet i fagsystemer. På denne måde er det kommunens vurdering, at sandsynligheden for uberettiget adfærd og aktivitet, der fx kan føre til sikkerhedsbrud eller andre konsekvenser, bedre kan minimeres.

Konkret informeres medarbejdere i Jammerbugt Kommune gennem generelle awareness-tiltag om, at aktiviteter generelt logges i fagsystemer, hvor det er relevant, og at der føres kontrol med loggen af disse aktiviteter. Derudover har systemejere pligt til at informere brugerne om, at der er i de givende fagsystemer registreres aktiviteter (logges), samt at der føres kontrol med det.