Tilsyn med kommunernes modenhed

i forhold til grundlæggende behandlingssikkerhed 2024

Datatilsynet har afsluttet skriftlige tilsyn med behandlingssikkerheden i 48 kommuner. Resultatet indikerer, at der på visse områder fortsat er udfordringer, som kræver mere opmærksomhed blandt kommunerne.

Tilsynet viser bl.a., at der fortsat er behov for øget fokus på:

- Procedurer for sletning
- Foranstaltninger som skal sikre, at der ikke sker utilsigtet deling af personoplysninger i forbindelse med udgående mails
- Rettighedsstyring
- Konsekvensanalyse
- Domænesikkerhed

Datatilsynet har på baggrund af resultaterne lavet målrettet vejledning vedrørende nedslag i fem udvalgte tendenser, som findes på de følgende sider.

Tag stilling til procedurer for sletning

En dataansvarlig skal sikre sig, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles. Det vil sige, at man ikke må behandle personoplysninger længere end nødvendigt. Det er et grundlæggende princip, som skal mindske risikoen for misbrug af overflødige oplysninger til skade for de registrerede, f.eks. ved datalæk, ransomware-angreb og andre situationer, hvor data uberettiget bliver tilgået.

Som dataansvarlig bør man derfor sikre sig, at der er taget stilling til, hvilke procedurer der skal følges, når personoplysninger skal slettes fra behandlingssystemer.

17 kommuner ud af de 48 svarer 'ja' eller 'Delvist – mere 2/3 gennemført' til at have indført faste procedure/rutiner for rutinemæssig sletning af personoplysninger.

Find mere vejledning om emnet her

Læs mere om sletning på Datatilsynets hjemmeside.

Arbejder du inden for det kommunale område, kan du læse mere om sletning på KL Emnesystematik (KLE), der er en struktureret oversigt over alle kommunale aktiviteter.

Reducer risikoen for at personoplysninger sendes forkert

Hovedparten af de brud på persondatasikkerheden, som anmeldes til Datatilsynet, vedrører situationer, hvor "rigtige" personoplysninger sendes til en "forkert" modtager, typisk en e-mailadresse, eller hvor der bliver vedhæftet et dokument med "forkerte" oplysninger til den "rigtige" modtager. For at reducere forekomsten af denne type af brud kan den dataansvarlige indføre forskellige foranstaltninger. Det kan eksempelvis være scanning af alle udgående mails for f.eks. personnumre og/eller fravalg af funktionen "autoudfyld" ved indtastning af mailadresser. Det kan også være sikring af, at det indtastede cpr-nummer eller den indtastede mailadresse svarer til den person, der måtte være registreret på en borgers sag.

25 kommuner ud af de 48 svarer 'ja' eller 'Delvist – mere 2/3 gennemført' til spørgsmålet om, hvorvidt de foretager scanning af udgående e-mails for at undgå utilsigtet forsendelse af personoplysninger.

Kontrollér adgang til oplysninger

Selvom brugere (f.eks. medarbejdere) har fået tildelt brugeradgang/rettigheder til et it-system, er det ikke ensbetydende med, at de frit kan anvende personoplysninger i it-systemet. For at opdage et eventuelt misbrug af oplysninger kan det være nødvendigt løbende at foretage en form for kontrol af brugernes adfærd. En sådan kontrol kan også virke præventivt, hvis brugerne er klar over, at et eventuelt misbrug vil kunne opdages.

For at undgå utilsigtede adgange til personoplysninger bør den dataansvarlige desuden have fokus på styring af brugeres adgangsrettigheder. Fejl i rettighedsstyring kan f.eks. opstå via brugerfejl (f.eks. kopiering af eksisterende adgangsrettigheder ved nyoprettelse) og pga. manglende handling (f.eks. manglende opdatering af rettigheder ved ændringer i organisationen).

15 kommuner ud af de 48 svarer 'ja' eller 'Delvist – mere 2/3 gennemført' til spørgsmålet om, hvorvidt de regelmæssigt foretager en gennemgang af eller stikprøve i logfiler for at identificere usædvanlige hændelser.

Mere vejledning om emnet

Læs om foranstaltningerne i Datatilsynets katalog over sikkerhedsforanstaltninger, som også henviser til Datatilsynets praksis på området.

- Logning af brugernes anvendelser af personoplysninger
- Stikprøver i log over brugernes anvendelser af personoplysninger
- Centraliseret rettighedsstyring
- Awareness

Adressér risikoen for de registrerede gennem konsekvensanalyse

Kommuner er dataansvarlige for en række behandlingsaktiviteter, hvor der kan være en høj risiko for de registrerede. Den type af behandlingsaktiviteter kan give anledning til, at der skal udarbejdes en konsekvensanalyse for de registreredes rettigheder.

Konsekvensanalysen skal sikre, at behandlingsaktiviteter og formål med behandlingen beskrives på systematisk vis, og at den dataansvarlige foretager en vurdering af, om behandlingsaktiviteterne er nødvendige og står i rimeligt forhold til formålene. Konsekvensanalysen skal samtidig sikre, at den dataansvarlige både foretager en vurdering af risiciene for de registreredes rettigheder og frihedsrettigheder og får beskrevet de foranstaltninger, der påtænkes for at imødegå de risici.

13 kommuner ud af de 48 svarer 'ja' eller 'Delvist – mere 2/3 gennemført' til spørgsmålet om, hvorvidt de har lavet konsekvensanalyser for alle behandlinger af personoplysninger, der sandsynligvis indebærer en høj risiko for de registrerede.

Mere vejledning om emnet

På Datatilsynets hjemmeside er der forskelligt materiale om konsekvensanalyser, herunder vejledninger og skabeloner til gennemførelse af konsekvensanalyser.
Rådet for digital sikkerhed har også udgivet en vejledning med titlen 'Konsekvensanalyse i praksis', der beskriver, hvordan arbejdet med at udføre konsekvensanalyser kan gøres.

Husk domænesikkerheden

For at minimere risikoen ved, at kommuners mailadresse bliver anvendt til IT-kriminalitet, bør der anvendes DANE for alle indgående mailgateways. Det skal tydeliggøre overfor afsendere, at der anvendes kryptering. Derved kan risikoen for fremsendelse af ukrypterede e-mails reduceres.

14 kommuner ud af de 48 svarer 'ja' til spørgsmålet om, hvorvidt de anvender DANE på alle indgående mailgateways.

Mere vejledning om emnet

På hjemmesiden Sikker på nettet kan du finde mere materiale og informationer om domænesikkerhed og Dane.