Modenhedstilsyn 2022

Nedslag i 5 udvalgte tendenser

DATATILSYNET

Tag stilling til procedurer for sletning

En organisation 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.

24 organisationer ud af 55 svarer at de i mindre grad eller slet ikke har indført faste procedurer/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.

26 organisationer ud af 55 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).

16 organisationer ud af 55 svarer 'Ja' og 'Delvist – mere end 2/3 gennemført' på spørgsmålet om, hvorvidt de regelmæssigt foretager en sådan gennemgang af eller stikprøve i logfiler for at identificere usædvanlige hændelser.

Adressér risikoen for de registrerede gennem konsekvensanalyse

Kommuner og regioner 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.

20 kommuner ud af 50 svarer 'Ja' eller 'Delvist – mere 2/3 gennemført' på spørgsmålet om, hvorvidt organisationen har lavet konsekvensanalyser for alle behandlinger af personoplysninger, der sandsynligvis indebærer en høj risiko for de registrerede.

Find mere vejledning om emnet her

Rådet for digital sikkerhed har udgivet en vejledning med titlen 'Konsekvensanalyse i praksis', der beskriver, hvordan arbejdet med at udføre konsekvensanalyser kan gøres.

Test IT-beredskabsplaner

Kommuner har en række behandlingsaktiviteter, der er meget afhængige af, at de tilhørende it-systemer er tilgængelige. Derudover råder kommunerne over en stor mængde data, der er vitale for korrekt sagsbehandling. Netop derfor er opdaterede og testede it-beredskabsplaner vigtige. At der foreligger en gennemprøvet plan, kan afbøde konsekvenserne ved et stort angreb eller nedbrud, hvad enten det handler om fortsat at kunne levere ydelser i en periode uden it-understøttelse eller om at genetablere data og systemer efter eksempelvis et ransomware-angreb.

Testen af beredskabsplanen er vigtig, da nogle elementer i en beredskabsplan kan se fornuftige ud på papiret, men i praksis viser sig svære at udføre eller ikke fungerer, som de enkelte elementer var tiltænkt. Dertil kommer, at organisationen kan have overset forhold eller fejlvurderet forhold som værende irrelevante. Netop denne slags uhensigtsmæssigheder vil man ofte kunne afdække gennem øvelser og tests.

22 kommuner ud af 50 svarer 'nej' og 'nej, men det planlægges' på spørgsmålet om, hvorvidt organisationen foretager regelmæssige tests af beredskabsplaner.
Til sammenligning svarer 5 ud 5 regioner 'ja' på samme spørgsmål.

Find mere vejledning om emnet her

Information, råd og anbefalinger til test af beredskabsplaner kan bl.a. findes på sikkerdigital.dk – hvor der også findes en mini-beredskabsplan.