# Vejledning om adgangsstyring i forhold til personoplysninger og systemer

| | |
|---|---|
| Organisation | **Databeskyttelsesrådgiverfunktion i Den Storkøbenhavnske Digitaliseringsforening (DSD)** |
| Dokument navn | Vejledning om adgangsstyring i forhold til personoplysninger og systemer v. 1.0 docx |
| Dokument ejer | Daniel Bach og Michael Drews Olsen |
| Senest ændret | 1. marts 2019 |
| Autoriseret af | |
| ISO 27001 og ISO 27002 | 9.1 – Forretningsmæssige krav til adgangsstyring, 9.2 – Administration af brugeradgang |
| GDPR-reference | Artikel 5, stk. 1, litra f – Sikre tilstrækkelig sikkerhed for personoplysninger<br>Artikel 24.1 – Påvise efterlevelse af forordning.<br>Artikel 32, 1 – Sikre passende sikkerhedsniveau for personoplysninger |
| Dataklassifikation | Internt dokument |

| Version nr. | Dato | Revisions forfatter | Beskrivelse |
|---|---|---|---|
| 1.0 | 1. marts 2019 | Daniel Bach, Michael Drews Olsen | Første version |
| | | | |
| | | | |
| | | | |

**Formål**
Datatilsynets tilsynsplan for første halvår 2019 indeholder fokusområdet "autorisation af medarbejdere hos kommunerne". Fokusområdet betyder, at Datatilsynet kommer til at føre tilsyn med, om kommunernes medarbejdere har adgang til flere personoplysninger, end de har arbejdsmæssigt behov for, og om kommunerne fører kontrol hermed.

Det er hensigten med denne vejledning at hjælpe kommunerne i DSD, som er tilsluttet den fælles databeskyttelsesfunktion, i forhold til at sikre og være i stand til at påvise, at medarbejderne ikke har adgang til flere personoplysninger, end de har arbejdsmæssigt behov for. Vejledningen gennemgår de forhold, som er vigtige i forhold til autorisation af medarbejdere og kontrol hermed.

**Omfang:** Alle kommuner i DSD tilsluttet den fælles databeskyttelsesrådgiverfunktion.

## Indhold

## Lovkrav

Det følger af persondataforordningens artikel 32, stk. 1, at kommunen skal gennemføre passende tekniske og organisatoriske sikkerhedsforanstaltninger, der sikrer et passende sikkerhedsniveau for personoplysningerne i kommunen. Det fortolkes af Datatilsynet således, at medarbejdere kun må have adgang til personoplysninger, som der er arbejdsmæssigt behov for.

Det følger af artikel 24, stk. 1, i forordningen, at kommunen skal være i stand til at påvise, at de persondataretlige krav overholdes. Det betyder, at kommunen skal kunne påvise, at medarbejderne kun har adgang til personoplysninger, som der er arbejdsmæssigt behov for.

*Sikkerhedsbekendtgørelse nr. 528 af 15. juni 2000 og ISO 27001*
Persondataforordningen angiver ikke, hvilke sikkerhedsforanstaltninger der er relevante at gennemføre. Den tidligere sikkerhedsbekendtgørelse giver dog nogle gode retningslinjer, og Datatilsynet anbefaler stadig at følge den, selvom den er ophævet som lovmæssigt krav. Kommunen kan derfor lade sig inspirere af den tidligere sikkerhedsbekendtgørelse og den tilhørende vejledning, herunder sikkerhedsforanstaltninger i ISO 27001 og den tilhørende implementeringsvejledning ISO 27002.

## Politik for adgangsstyring

ISO 27001 angiver, at der skal udarbejdes en politik for adgangsstyring. En politik for adgangsstyring giver kommunen mulighed for at administrere brugeradgang til personoplysninger efter på forhånd fastsatte kriterier, som tager hensyn til beskyttelse af personoplysninger i kommunen. En politik for adgangsstyring vil samtidig udgøre rammen for en formel autorisationsordning og -procedure i kommunen (se afsnittet nedenfor).

En politik for adgangsstyring bør afspejle principperne ”need to know” (man får kun adgang til den information, som er nødvendige for at kunne udføre ens arbejdsopgaver) og ”need to use” (man får kun adgang til de netværk, systemer, applikationer mv., som man har behov for, for at kunne udføre sine arbejdsopgaver).

En politik for adgangsstyring bør indeholde følgende:

- Regler for adgangsstyring
- Adgangsrettigheder og -begrænsninger for specifikke brugerroller, hvor detaljeringsgraden og adgangsstyringen skal afspejle, at medarbejderne kun må få adgang til personoplysninger og systemer, som er nødvendige for at medarbejderne kan udføre deres arbejdsopgaver (gælder alle de brugerroller, som kommunen opretter).
- Regler om adskillelse af adgangsstyringsfunktioner (sikre at adgangsansøgning, adgangsautorisation og adgangsadministration ikke varetages af en og samme person)
- Krav til formel autorisation af adgangsansøgninger
- Krav til regelmæssig gennemgang af adgangsrettigheder og sletning af adgangsrettigheder.

## Formel autorisationsordning og -procedure

Sikkerhedsbekendtgørelsen og ISO 27001 angiver, at der skal fastsættes en formel autorisationsordning og -procedure. I forhold til efterlevelse af forordningen er en formel autorisationsordning og -procedure essentiel, fordi kommunen på denne måde kan sikre og påvise, at nyoprettede brugere og

eksisterende brugere ikke har rettigheder til at tilgå personoplysninger og systemer, medmindre sådanne rettigheder aktivt er tildelt den pågældende bruger.

En autorisationsordning bør indeholde dels en procedure for brugeroprettelse og afmelding, dels en procedure for tildeling og tilbagekaldelse af adgangsrettigheder, dels en procedure for justering af adgangsrettigheder for brugere, som får nye funktioner eller stillinger i kommunen, og dels en procedure for spærring eller tilbagekald af rettigheder for brugere, som stopper i kommunen.

Det er vigtigt, at der foretages en vurdering af, hvad der er den enkelte brugers behov, før brugeren tildeles rettigheder til at tilgå personoplysninger og systemer. Det gælder også før, der justeres i brugeres rettigheder. Vurderingen af hvilke personoplysninger og systemer, som en bruger skal have adgang til, bør foretages i sammenspil mellem brugerens nærmeste leder, ejer af systemet og/eller administrator.

Kommunen skal dokumentere, hvilken adgangsrettigheder de forskellige brugere er tildelt, så kommunen kan føre løbende kontrol med autorisationer (se afsnittet herom nedenfor).

En autorisationsordning og -procedure bør indeholde følgende:

- Brug af entydigt bruger-ID'er, hvormed medarbejderen kan forbindes til bruger-ID'et og gøres ansvarlig for sine handlinger
- Spærring eller sletning af brugere, så snart de er stoppet i kommunen
- Regelmæssig identifikation og sletning eller spærring af nedlagte bruger-ID'er
- Beskyttelse mod tildeling af nedlagte bruger-ID'er til nye brugere
- Autorisation fra netværk og ejer af systemet til at bruge systemet
- Separat godkendelse af adgangsrettigheder fra nærmeste leder, fagansvarlig eller dennes repræsentant
- Sikkerhed for at adgangsrettigheder ikke aktiveres, før der foreligger en godkendelse
- Brugerkonti og adgangsrettigheder for kommunens informationssystemer og infrastruktur skal registreres og vedligeholdes centralt
- Justering af adgangsrettigheder for brugere, som har nye funktioner eller stillinger i kommunen
- Regelmæssig gennemgang af adgangsrettigheder
- Særlige retningslinjer for tildeling og tilbagekald af adgangsrettigheder til brugere, som kun har brug for midlertidig adgang (f.eks. udførelse af revision, teknisk vedligehold, fejlretning, driftsovervågning og lign.).

Hvis et system driftes af en ekstern leverandør, skal adgangsstyring fremgå af leverandørkontrakten.

## Teknisk adgangskontrol i systemer og logning

Vejledningen til sikkerhedsbekendtgørelsen angiver, at systemer skal være teknisk indrettet således, at brugere skal identificere sig over for systemer for at få adgang. Systemer skal også være indrettet således, at brugerne kun må få adgang til personoplysninger og handlinger i systemer i overensstemmelse med autorisationerne til brugerne. Dette er helt essentielle krav i forhold til efterlevelse af forordningen, fordi der vil være uhindret adgang for kommunens medarbejdere til personoplysninger uden teknisk adgangskontrol i systemer.

Teknisk adgangskontrol i systemer vil normalt være individuel brugeridentifikation med tilhørende password eller multi-faktor autentifikation. Metoden for adgangskontrol skal være proportionel med værdien af de informationer, der beskyttes. Passwords skal være stærke, og medarbejdere må aldrig dele deres passwords med andre.

Sikkerhedsbekendtgørelsen angiver, at systemer skal logge (registrere) alle anvendelser af følsomme personoplysninger. Dette er fortsat et relevant krav i forhold til efterlevelse af forordningen. Logning gør det bl.a. muligt at følge op på afviste adgangsforsøg og om handlinger i systemer (bl.a. anvendelse af personoplysninger) er i overensstemmelse med autorisationer.

## Styring af privilegerede adgangsrettigheder

Privilegerede eller udvidede rettigheder skal forstås som rettigheder, der giver adgang til personoplysninger eller anden data eller funktioner, som er særligt kritiske, medfører øget risiko for personoplysninger eller systemer, og/eller er omfattet af særlige krav efter lovgivning på området.

Kommunen skal være opmærksom på, at tildeling af privilegerede adgangsrettigheder til brugere, indebærer en forhøjet risiko for brud på persondatasikkerhed. Det bør kommunen tage højde for ved fastlæggelse af politik for adgangsstyring, herunder ved etablering af en formel autorisationsordning og -procedure.

Kommunen bør overveje at indarbejde følgende trin politik for adgangsstyring og i autorisationsordning og -procedure:

- Tildeling af privilegerede adgangsrettigheder til brugere ud fra need-to-use princippet og fra gang til gang
- Sikring af at der ikke tildeles privilegerede adgangsrettigheder, før der er tildelt autorisation på baggrund af autorisationsordning og -procedure
- Registrering (dokumentation) af alle tildelte rettigheder
- Der bør defineres krav til udløb af privilegerede adgangsrettigheder
- Privilegerede adgangsrettigheder knyttes til en bruger-ID, som er forskelligt fra de ID-er der anvendes til almindelig behandling. Almindelig behandling bør ikke udføres med privilegeret ID
- Kompetencerne hos brugere med privilegerede adgangsrettigheder bør gennemgås regelmæssigt for at verificere, om de er i overensstemmelse med deres opgaver.
- Ansatte med privilegerede adgangsrettigheder gøres bekendte med deres udvidet ansvar og om overvågningen, som dette eventuelt indebærer.

Systemer skal logge brugere med privilegerede adgangsrettigheder på grund af den øget risiko for personoplysninger og systemer.

På sikkerdigital.dk kan kommunen lade sig inspirere yderligere af vejledende retningslinjer for styring af privilegerede adgangsrettigheder og kontrol hermed[1].

[1] https://sikkerdigital.dk/myndighed/adgangsstyring/privilegerede-rettigheder/

## Løbende kontrol af autorisationer

Sikkerhedsbekendtgørelsen angiver, at det mindst en gang hvert halve år skal sikres, at autoriserede brugere opfylder betingelserne for adgang i forhold til følsomme personoplysninger. I forhold til efterlevelse af forordningen bør kontrol af adgangsrettigheder ikke begrænses til følsomme personoplysninger, men bør udstrækkes til at omfatte alle kategorier af personoplysninger.

Kommunen skal etablere en kontrolproces i forhold til autorisationer. Det vil normalt kræve, at der tilgår relevant information fra f.eks. HR-afdeling eller fra brugerens nærmeste leder til ejer af systemer og/eller administrator, når der sker ændringer i brugernes behov (f.eks. ved nye funktioner eller ny stilling i kommunen), eller når brugeren stopper i kommunen.

Løbende kontrol af autorisationer kan f.eks. gennemføres ved at sammenholde oprettede brugere med oversigter over kommunens medarbejdere, sammenholde tildelte adgangsrettigheder med brugernes aktuelle stillinger eller funktioner i kommunen og gennemgå brugeraktivitet for oprettede brugere.

Kontrol af adgangsrettigheder skal dokumenteres med henblik på, at kommunen kan påvise efterlevelse af forordningen.

Kommunen bør tage følgende i betragtning ved etablering af en kontrolproces:

- Gennemgang af brugeres adgangsrettigheder med jævne mellemrum (minimum en gang hvert halve år) og efter ændringer (nye funktioner eller stillinger) og ved ansættelsesophør
- Gennemgang og tildeling af adgangsrettigheder på ny ved flytning af en funktion til en anden i kommunen
- Autorisationer til privilegerede adgangsrettigheder bør gennemgås hyppigere (minimum hver tredje måned) for at sikre, at deres rettigheder er relevante og autoriserede
- Privilegerede bruger konti, der ikke kan spores til en fysisk medarbejder, bør kontrolleres og passwords bør udskiftes regelmæssigt.

### Praktiske eksempler

**Begrænsninger for specifikke brugerroller:**
Risikoen for uautoriseret adgang kan mindskes ved begrænsning af brugerroller blandt andet ved at opdele adgangen efter, hvad den enkelte mere specifikt har behov for, og/eller begrænse den enkeltes muligheder for behandling (læse, anvende, ændre, udtrække, samkøre, slette m.v.) specielt når antallet af personer, har adgang til en (stor) mængde (følsomme) oplysninger.

**Logning af tilgang til personoplysninger:**
Uautoriseret adgang til personoplysninger kan spores ved logning af behandling af personoplysninger (for at kunne finde ud af, hvem der gør hvad, og om der er uvedkommende på netværket), kombineret med kontrol af, om en konkret tilgang til oplysningerne har været inden for reglerne for tilgang.

# Bilag Standardinformation i vejledninger fra databeskyttelsesrådgiverfunktionen i DSD

**Relevante definitioner:**

**»dataansvarlig«**: en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger. I DSD-kommuner kalder vi denne rolle for [Fagansvarlig].

**»fagansvarlig«**: en fagansvarlig har ledelsesansvaret for et område, et center, eller en forvaltning i kommunen. En fagansvarlig har det overordnende ledelsesansvar for behandlingsaktiviteter (behandlingen af personoplysninger) inden for det pågældende område, center eller forvaltning. En fagansvarlig refererer til den administrative direktion i kommunen.

**»databehandler«**: en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne

**»fagcentre«**: en kommune er opdelt i forskellige enheder med fokus på et specifikt pligtområde. Disse enheder kaldes også fagcentre, afdelinger, forvaltninger eller centre. Et fagcenter har en eller flere [fagansvarlig], der bærer rollen som dataansvarlige.

**Officielle kilder:**

| |
|---|
| Datatilsynet |
| Persondataforordningen |
| Databeskyttelsesloven |
| Sikkerhedsbekendtgørelsens §§ 11, 12, 16,17 og 19 |
| Vejledning til sikkerhedsbekendtgørelsen |
| ISO 27001 og ISO 27002 |