Oplysningsskema vedrørende autorisation og adgangsstyring

Datatilsynet skal informere om, at Datatilsynet er dataansvarlig for behandlingen af de personoplysninger, der indsamles i forbindelse med tilsynsbesøget, herunder i dette oplysningsskema. Oplysningerne vil blive brugt i forbindelse med tilsynsbesøget og vil indgå i Datatilsynets tilsyn med behandling af oplysninger, der er omfattet af databeskyttelsesforordningen og databeskyttelsesloven. Oplysningerne vil endvidere kunne anvendes til statistik. Oplysninger indsamlet i oplysningsskemaet kan tænkes videregivet i forbindelse med anmodninger om aktindsigt efter offentligheds- og/eller forvaltningsloven.

Hvis der er uklarheder omkring spørgsmålene, kan Datatilsynet kontaktes for en afklaring. Datatilsynet opfordrer til, at spørgsmålene i videst muligt omfang besvares i skemaet.

1 Politikker, procedurer, mv.

Datatilsynet anmoder om en kopi af de politikker, procedurer, mv. der:

- angiver krav omkring tildeling af adgangsrettigheder til (autorisation af) brugere eller administrering af brugernes faktiske adgange, og
- som var gældende den 29. januar 2019.

For hvert af de dokumenter, der indsendes til Datatilsynet, bedes der udfyldt en linje i følgende skema:

Dokumentnavn/titel	Filnavn	Afsnit i dokumentet som er relevante ift. autorisation eller brugeradministration	Dokumentet var gyldigt fra den (dd/mm - åååå)	De sidste **to** datoer for, hvornår dokumentet sidst blev revideret (dd/mm - åååå)

2 It-systemer med brugeradministration på rådhuset

Datatilsynet anmoder om, at der i følgende skema angives it-systemer, hvor:

- brugernes adgang administreres på rådhuset,
- der behandles fortrolige eller følsomme personoplysninger[1], og
- kommunen er dataansvarlig for behandlingen.

[1] Læs mere om disse begreber på Datatilsynets hjemmeside: https://www.datatilsynet.dk/generelt-om-databeskyttelse/hvad-er-personoplysninger/

Navn på it-system	Beskriv her hvis der anvendes noget fysisk til login på dette it-system (eksempelvis RFID eller nøglekort)	Direkte adgang fra internettet? (J/N)	De sidste **to** datoer for undersøgelse af, om brugeradgange til dette it-system var aktuelle (dd/mm - åååå)	Resultat af undersøgelserne (eksempelvis at der er fundet 10 adgange, som skulle have været ændret/lukket)

3 It-systemer med brugeradministration uden for rådhuset

Datatilsynet anmoder om, at der i følgende skema angives de it-systemer, hvor:

- brugernes adgang primært administreres uden for rådhuset, eksempelvis på kommuneskoler, plejehjem, borgerservice,
- der behandles fortrolige eller følsomme personoplysninger, og
- kommunen er dataansvarlig for behandlingen.

Navn på it-system	Beskriv her hvis der anvendes noget fysisk til login på dette it-system (eksempelvis RFID eller nøglekort)	Direkte adgang fra internettet? (J/N)	De sidste **to** datoer for undersøgelse af, om brugeradgange til dette it-system var aktuelle (dd/mm - åååå)	Resultat af undersøgelserne (eksempelvis at der er fundet 10 adgange, som skulle have været ændret/lukket)

4 Lister over brugere

Følgende lister skal være i formaterne XLS (Excel) eller CSV (comma-separated values).

Datatilsynet anmoder om et logudtræk fra kommunens primære journalsystem til sagsbehandling (ESDH-system), hvor der behandles fortrolige eller følsomme personoplysninger. Dette logudtræk kan begrænses til at vise:

- Brugernavne (altså bruger-id, og ikke brugerens faktiske navn) der har tilgået it-systemet i perioden 20. januar 2019 til 8. februar 2019 – begge dage inklusiv.
- Datoer for, hvornår de respektive brugernavne tilgik it-systemet.

Datatilsynet anmoder endvidere om en liste, som indeholder:

- navn, brugernavn, afdeling og arbejdsadresse for samtlige brugere af kommunens primære journalsystem (ESDH-system).

Såfremt brugernavne er forskellige i journalsystemet i forhold til i journalsystemets log, udbedes ligeledes en liste, der viser sammenhængen mellem brugernavnene. Det samme gør sig gældende, hvis brugernavnene er forskellige i journalsystemet i forhold til andet sted, hvor brugerens adgang til journalsystemet (også) styres – eksempelvis i Active Directory.

Herudover anmoder Datatilsynet om en beskrivelse af typer af brugernavne, herunder:

- hvordan et typisk brugernavn ser ud,
- hvordan brugernavne, som er tilknyttet ikke-fastansatte (eksempelvis vikarer eller eksterne konsulenter), ser ud, og
- hvordan brugernavne, som ikke er knyttet til en bestemt person (eksempelvis til brug ved kursusdeltagelse eller test), ser ud.

5 Autorisation

Datatilsynet anmoder om følgende anonymiserede eksempler på en tildeling af adgangsrettigheder (autorisation) fra før 29. januar 2019:

a) Et eksempel, der vedrører kommunens primære journalsystem til sagsbehandling.
b) Såfremt der anvendes andre typer autorisation, tre forskellige eksempler fra andre it-systemer, der administreres på rådhuset.
c) Såfremt der anvendes andre typer autorisation, tre forskellige eksempler fra de it-systemer, der administreres uden for rådhuset.

6 Relevante retsregler

Det fremgår af databeskyttelsesforordningens artikel 32, stk. 1, at den dataansvarlige og databehandleren – under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder – skal gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici, herunder bl.a. alt efter hvad der er relevant:

> a) pseudonymisering og kryptering af personoplysninger
> b) evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
> c) evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
> d) en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

Det følger endvidere af forordningens artikel 32, stk. 2, at der ved vurderingen af, hvilket sikkerhedsniveau der er passende, tages der navnlig hensyn til de risici, som behandlingen udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Behandling af personoplysninger skal i øvrigt altid ske i overensstemmelse med de grundlæggende principper i databeskyttelsesforordningens artikel 5.

Det betyder bl.a., at oplysninger skal behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger jf. databeskyttelsesforordningens artikel 5, stk. 1, litra f (»integritet og fortrolighed«).