| **IT**  Dato: 19. januar 2021  Sagsbehandler: Eva Maria Minke Andersen  Direkte tlf.: 7376 7001  E-mail: ema@aabenraa.dk |
| --- |

# Beredskabsplan ved større datalæk ved Aabenraa Kommune

Efter indførslen af GDPR i maj 2018 er opmærksomheden på datalæk steget voldsomt, ligesom der er kommet krav om indberetning til Datatilsynet, samt orientering af de berørte parter.

Vi ser indtil nu to typer af læk ved Aabenraa Kommune. Den ene (og mest udbredte) er hvor en sagsbehandler kommer til at sende oplysninger om en borger som fejlagtig sendes til en anden borger. Den anden er systemlæk, hvor fagsystemer udsender fejlagtige eller for mange oplysninger til en borgergruppe. Ud over disse to, er der i andre kommuner set, at der ved en fejl lækkes oplysninger om rigtig mange borger til en eller flere uvedkommende.

I sommeren 2019 oplevede Aabenraa Kommune imidlertid et større datalæk, der efter gennemgribende undersøgelse af ca. 20.000 siders dokumentation udløste orientering af ca. 650 borgere samt tilbagevendende spørgsmål fra Datatilsynet. Forløbet var langt, reaktion fra Datatilsynet, reaktioner fra borgere med trussel om sagsanlæg og krav om erstatning. Erfaringsgrundlaget var lille, hvad skulle man svare borgerne? Hvad var gældende retsgrundlag? hvor skulle man få hjælp fra? Oplevelsen fra pågældende forvaltning var, at man generelt opererede på et usikkert grundlag og uden sikkerhedsnet.

Med baggrund i denne konkrete oplevelse, lægges der derfor op til en Beredskabsplan ved større datalæk, som skal sikre at fremtidige datahændelsessager i Aabenraa Kommune håndteres korrekt og efter ens retningslinjer.

## Definition af større datalæk

Et større datalæk er et læk, hvor mange borgers informationer enten lækkes ud på internettet, eller mange borgers informationer fejlagtig sendes til andre borger eller myndigheder. Jo mere følsomme data jo større kan datalækket betragtes. Det er derfor svært at sætte en grænse. 20 borgers meget følsomme data f.eks. vejet op imod 100 borgers almindelige personoplysninger. Det vil derfor altid være en vurdering fra situation til situation både på antal borgere og de oplysninger, der er lækket.

### Ansvar

Det vil altid være system/dataejer der er ansvarlig for egne systemer/data og dermed også hovedansvarlig for et evt. datalæk. System/dataejer ved Aabenraa Kommune er altid fagchefen for det pågældende system.

### Vurdering af datalæk

Vurdering af lækkets størrelse og dermed også hvorvidt Taskforce skal aktiveres sker i samarbejde mellem vedkommende fagchef, DPO, sikkerhedskoordinator og evt. systemkoordinator.

### Nedsættelse af Taskforce

Vurderes lækket at være stører karakter, nedsættes en taskforce til at hjælpe pågældende fagforvaltning. Taskforcen består minimum af:

* Pågældende fagchef=system og data ejer (ansvarlig for indkaldelse)
* Systemkoordinatoren fra pågældende fagforvaltning
* Sekretariatsbistand fra den pågældende forvaltning (sikre dokumentation)
* DPO= Eva Minke Andersen
* Jurist= Claus Hansen
* Journalist/kommunikation=Kasper Stoof
* Sikkerhedskoordinator=Thomas Veltz Majholt
* Adhoc, driftsleder i IT hvis datalækket skyldes tekniske fejl

Taskforcens opgave er at dække bredt på alle områder, herunder få stoppet lækket og så vidt muligt underrettet de berørte borger, inden 72 timer at få indberettet datalækket til Datatilsynet (DPO-opgave). Afdelingschefen har ansvaret til beslutning om, hvem der foretager kommunikation med de berørte borgere, der evt. vil vende tilbage med spørgsmål/erstatningskrav. Alt efter datalækkets omfang kan der aftales en møderække inden for de første dage.

Informationssikkerhedsudvalget/DDS/SKF orienteres på førstkommende møde.

Der indberettes til den interne hændelseslog (evt. vedlægge indberetning til Datatilsynet).

### Orientering af politisk og administrativ organisation

Fagchefen i pågældende fagforvaltning vurderer i samråd med direktøren i fagforvaltningen, hvem der yderligere skal orienteres. Kommunaldirektør/borgmester/fagudvalg/økonomiudvalg/byråd

### Standardbrev til orientering af borgerne

Da de forskellige databrud ikke ligner hinanden kan der ikke bare udformes et standardbrev, der kan bruges ved alle brud, men som **bilag C** i kommentar/bilagsnotatet, vedlægges forskellige anonymiserede udkast til breve der er brugt ved Aabenraa Kommune

### Erstatningskrav

Har borgeren ret til erstatning? Den juridiske vurdering og konklusion herpå er:

*Dette betyder på normal dansk, at der pt. – indtil der kommer en domstolsafgørelse – ikke er hjemmel i § 40 eller artikel 82 til at givet erstatning for en ”ulovlig behandlingsaktivitet.*

*Erstatning for en ”immateriel skade”, datalæk – ulovlig behandlingsaktivitet - vil således skulle gives i medfør af erstatningsansvarslovens § 26.*

*Men, der er pt. ikke afsagt nogen domme – så vidt jeg ved – som har tilkendt erstatning med hjemmel i § 26 på grund af et datalæk som kan karakteriseres som en ulovlig behandlingsaktivitet*.

Hele vurdering er vedlagt som bilag **A** i kommentar/bilagsnotatet

### Er Aabenraa Kommune forsikret?

Forsikringsmægler udtaler:

*Vi er aktuelt ikke bekendt med forsikringsselskaber der vil tilbyde dækningen/Cyber-forsikring til kommuner og/eller regioner, men følger løbende op på mulighederne*

Hele svaret er vedlagt som bilag **B** i kommentar/bilagsnotatet

### Bødekrav fra Datatilsynet

I de fleste europæiske lande kan de nationale datatilsyn selv udstede administrative bøder, men reglerne er anderledes i Estland og Danmark.

Her fungerer det på den måde, at Datatilsynet efter at have belyst og vurderet sagen politianmelder den dataansvarlige. Herefter undersøger politiet, om der er grundlag for at rejse en sigtelse mv., og endelig vil en eventuel bødestraf blive afgjort ved en domstol. Praksis er, at Datatilsynet indstiller en bødestørrelse, men i sidste enden er det en domstolsafgørelse. Der er ikke faldet bøder i danske kommuner endnu, så der er ikke præcedens for bødestørrelse. Dog er der nu indgivet anmeldelse fra Datatilsynet på to sager, nemlig Gladsaxe og Hørsholm med krav om bødestørrelse på henholdsvis 100.000 kr. og 50.000 kr. Begge sager var tyveri af computere, hvor der lå store mængder af personfølsomme data ukrypteret og direkte på harddisken.

# Bilag A, juridisk vurdering

*”Databeskyttelseslovens § 40 har følgende ordlyd:*

***§ 40.****Enhver person, som har lidt materiel eller immateriel skade som følge af en ulovlig behandlingsaktivitet eller enhver anden behandling i strid med denne lov og databeskyttelsesforordningen, har ret til erstatning efter databeskyttelsesforordningens artikel 82.*

*Og artikel 82 følgende ordlyd:*

*Artikel 82* ***Ret til erstatning og erstatningsansvar***

*1. Enhver, som har lidt materiel eller immateriel skade som følge af en overtrædelse af denne forordning, har ret til erstatning for den forvoldte skade fra den dataansvarlige eller databehandleren.*

*Spørgsmålet er herefter hvordan dette skal forstås, idet en forudsætning for erstatning i Danmark normalt kræver et formuetab, medmindre der er en udtrykkelig hjemmel til at få erstatning for et ikke ”økonomisk tab”.*

*Uanset, at § 40 og artikel 82 anvender udtrykket ”immateriel skade” så kommer noten i Karnov frem til følgende, på nuværende tidspunkt gældende konklusion:*

*Der synes alt i alt ikke på nuværende tidspunkt at være tilstrækkeligt grundlag for at fastslå, at*godtgørelse*for ikke-økonomisk skade er omfattet af retten til*erstatning*for materiel eller immateriel skade efter art. 82, stk. 1. I hvert fald ikke i medlemsstater som Danmark, hvor der normalt ikke uden særskilt hjemmel er mulighed for erstatning for ikke-økonomisk tab. »Immateriel skade« i forordningens forstand må, i en dansk kontekst, således antageligvis forstås som den almindelige eller rene formueskade, som er lidt som følge af overtrædelse af forordningens bestemmelser, hvilket f.eks. kan være et tab i form af mistet omsætning eller fralæggelse af den retsstridigt indvundne berigelse. Det må således antages – indtil andet måtte følge af praksis – at godtgørelse for tort, der ikke medfører formuetab, også fremover alene kan kræves efter*[*erstatningsansvarslovens § 26*](https://pro.karnovgroup.dk/document/rel/LBKG20181070_P26?src=document)*. Denne forståelse af artikel 82 er udtrykkeligt lagt til grund i forarbejderne til*[*databeskyttelseslovens § 40*](https://pro.karnovgroup.dk/document/rel/L2018502_P40?src=document)*, der gengiver artikel 82.*

*En sådan hjemmel kunne som anført være erstatningsansvarslovens § 26 som har følgende ordlyd:*

***§ 26.****Den, der er ansvarlig for en retsstridig krænkelse af en andens frihed, fred, ære eller person, skal betale den forurettede godtgørelse for tort.*

*Dette betyder på normal dansk, at der pt. – indtil der kommer en domstolsafgørelse – ikke er hjemmel i § 40 eller artikel 82 til at givet erstatning for en ”ulovlig behandlingsaktivitet”.*

*Erstatning for en ”immateriel skade”, datalæk – ulovlig behandlingsaktivitet - vil således skulle gives i medfør af erstatningsansvarslovens § 26.*

*Men, der er pt. ikke afsagt nogen domme – så vidt jeg ved – som har tilkendt erstatning med hjemmel i § 26 på grund af et datalæk som kan karakteriseres som en ulovlig behandlingsaktivitet.*

*Og ja, en borger/virksomhed som vil have erstatning skal rejse en civil sag ved de almindelige domstole”*

# Bilag B, udtalelse fra forsikringsmægler

Jf. vor telefonsamtale d.d. skal det oplyses, at dækning af denne risiko vil kræve en cyber-forsikring.

Jeres erhvervs- og produktansvarsforsikring dækker alene ting- og personskader, medens Jeres professionelle ansvarsforsikring også dækker formuetab, men begrænset til følgende aktiviteter

***Risikobeskrivelse***

*Forsikringen dækker kommunens erstatningsansvar for formuetab i forbindelse med sikredes afgivelse af fejlagtige ejendomsoplysninger og lægeerklæringer.*

*Forsikringen dækker også kommunens erstatningsansvar for formuetab i forbindelse med kommunal rådgivningsvirksomhed, afgørelser (forvaltningsakter), tilsyn og videregivelse af oplysninger ol.*

I de almindelige forsikringsbetingelser for prof. ansvar er der endvidere en undtagelse, som omfatter;

***16.7 IT***

*Erstatningskrav, der skyldes computer virus og manglende forebyggelse af uautoriseret indtrængen i, eller brug af, computersystemer eller computerprogrammer, hvad enten der er tale om sikredes egne systemer, eller systemer, hvorom sikrede har rådgivet.*

Vi er aktuelt ikke bekendt med forsikringsselskaber der vil tilbyde dækningen/Cyber-forsikring til kommuner og/eller regioner, men følger løbende op på mulighederne.

# Bilag C, forskellige forslag til orienteringsbrev

**1.**

**Orientering om videregivelse af personoplysninger**

Aabenraa Kommune beklager at skulle orientere dig om, at dine personoplysninger, herunder særligt dine økonomiske oplysninger, er videregivet til uvedkommende i samme husstand i forbindelse med ansøgning om økonomisk friplads.

Videregivelsen er sket i IT-systemet KMD Institution, som bruges til behandling af sager om økonomisk friplads, hvor systemet har sendt dit navn, adresse, fødselsdato og indkomst til alle i husstanden, som indgik i beregningsgrundlaget.

Den uberettigede videregivelse betyder, at din samlever/registrerede partner/ægtefælle har modtaget dine økonomiske personoplysninger i forbindelse med ansøgningen om økonomisk friplads, selvom denne anden person ikke har del i forældremyndigheden, hvorfor denne person må betragtes som uvedkommende.

Aabenraa Kommune vil gerne gøre opmærksom på, at der ikke er sket en fejl her i kommunen, men at der er tale om en fejl ved forsendelser i KMD Institution.

I Aabenraa Kommune er 35 borgeres data videregivet til uvedkommende i samme husstand i perioden 12. april 2017 til 1. februar 2019.

Leverandøren KMD oplyser over for Aabenraa Kommune, at KMD ved en opdatering af systemet den 8. februar 2019 har sikret, at oplysningerne fremadrettet kun sendes til forældremyndighedsindehavere.

Hvis der er spørgsmål til denne orientering, er du velkommen til at kontakte undertegnede eller xxxx på tlf.xxxx.

Venlig hilsen

**2.**

**Dine personoplysninger har været tilgængelige for andre**

Vi skal her informere dig om, at dine personoplysninger i en periode fra 3. august 2018 til 5. april 2019 har været tilgængelige for uvedkommende.

Det drejer sig helt konkret om dit cpr-nr. og billeder af sår fra før 2006, som vi har registreret i vores IT-system. Vi har ingen informationer om, at dine oplysninger skulle være blevet misbrugt.

Vi er kede af fejlen og beklager, at det er sket.

**Hvad er der sket?**

Som du sikkert ved, opbevarer vi i vores IT-systemer oplysninger om dig, der er relevante i forhold til hjælp, som du får fra Aabenraa Kommune. Ved en fejl har nogle af de personoplysninger været tilgængelige for andre hos en af Aabenraa Kommunes tidligere IT-leverandører. Leverandøren har nu udbedret fejlen. De oplysninger, som har været tilgængelige for andre, stammer fra et IT-system, som vi i Aabenraa Kommune benyttede frem til 2017. Vi benytter ikke længere IT-systemet.

**Hvad betyder det for dig?**

Der er ingen tegn på, at dine personoplysninger er blevet misbrugt eller at andre på nuværende tidspunkt har dine personoplysninger.

**Hvis du har spørgsmål**

Hvis du har spørgsmål til dette brev, er du velkommen til at kontakte undertegnede.

Venlig hilsen

**3.**

**Dine personoplysninger har været tilgængelige for andre**

Vi skal her informere dig om, at dine personoplysninger i en kort periode fra 10. – 17. april 2019 har været tilgængelige for uvedkommende.

Vi har ingen informationer om, at dine oplysninger skulle være blevet misbrugt, men informerer dig her for en god ordens skyld alligevel om, hvad der er sket.

Det drejer sig helt konkret om dit cpr-nummer og derudover kan det være f.eks. oversigter over hjælpemidler, medicin eller lign. oplysninger, som vi har registreret i vores IT-system.

Vi er kede af fejlen og beklager, at det er sket.

**Hvad er der sket?**

Uvedkommende har desværre skaffet sig adgang til et internt IT-supportsystem hos en af vores leverandører. I det system har personoplysninger været tilgængelige for andre. Leverandøren har løst problemet. Der er alene tale om et IT-supportsystem, der indeholder meget få personoplysninger. Der har ikke været adgang til det IT-system, som vi benytter til at opbevare de oplysninger om dig, der er relevante i forhold til hjælp, som du får fra Aabenraa Kommune.

**Hvad betyder det for dig?**

Vi har ingen informationer om, at dine personoplysninger er blevet misbrugt eller at andre på nuværende tidspunkt har dine personoplysninger.

**Hvis du har spørgsmål**

Hvis du har spørgsmål til dette brev, er du velkommen til at kontakte undertegnede.

Venlig hilsen