RETTEN I GLOSTRUP
DOM

afsagt den 11. maj 2021

Sag BS-19120/2019-GLO

Sagsøger 1
(advokat Eva Tofteberg Persson)

mod

Gladsaxe Kommune
(advokat Anders Valentiner-Branth)

og

Sag BS-22348/2019-GLO

Sagsøger 2
(advokat Eva Tofteberg Persson)

mod

Gladsaxe Kommune
(advokat Anders Valentiner-Branth)

og

Sag BS-49315/2019-GLO

Sagsøger 3

(advokat Eva Tofteberg Persson)

mod

Gladsaxe Kommune
(advokat Anders Valentiner-Branth)

og

Sag BS-51045/2019-GLO

Sagsøger 4
(advokat Eva Tofteberg Persson)

mod

Gladsaxe Kommune
(advokat Anders Valentiner-Branth)

og

Sag BS-51234/2019-GLO

Sagsøger 5
(advokat Eva Tofteberg Persson)

mod

Gladsaxe Kommune
(advokat Anders Valentiner-Branth)

og

Sag BS-51318/2019-GLO

Sagsøger 6
(advokat Eva Tofteberg Persson)

mod

Gladsaxe Kommune
(advokat Anders Valentiner-Branth)

og

Sag BS-51332/2019-GLO

Sagsøger 7
(advokat Eva Tofteberg Persson)

mod

Gladsaxe Kommune
(advokat Anders Valentiner-Branth)

Denne afgørelse er truffet af dommer Hans J. Christensen, dommer Janne Ro-strup Hansen og kst. dommer Pia Blaabjerg Andersen.

Sagernes baggrund
Sagsøger 1's sag er anlagt den 25. april 2019. Sagsøger 2's sag er anlagt den 15. maj 2019. Sagsøger 3's sag er anlagt den 2. november 2019. Sagsøger 4's sag er anlagt den 12. november 2019. Sagsøger 5, Sagsøger 6 og Sagsøger 7's sager er an-lagt den 13. november 2019.

Sagerne, der er forhandlet i forbindelse med hinanden, vedrører personoplys-ninger om 20.620 borgere, herunder de 7 sagsøgere, hvilke personoplysninger indgik i et regneark lagret på en bærbar PC, der blev stjålet fra Gladsaxe Kom-munes rådhus. Sagen omhandler, om kommunens behandling af personoplys-ningerne var lovlig og begrænset til det relevante formål, om oplysningerne var undergivet en tilstrækkelig behandlingssikkerhed, samt om der er hjemmel i databeskyttelsesforordningens artikel 82 til at tilkende sagsøgerne en godtgørel-se for ikke økonomisk skade.

Påstande
BS-19120/2019-GLO
Sagsøger 1 har nedlagt påstand om, at Gladsaxe Kommune skal betale 25.000 kr. med tillæg af procesrente fra den 2. december 2018 til betaling sker.

BS-22348/2019-GLO
Sagsøger 2 har nedlagt påstand om, at Gladsaxe Kommune skal betale 10.000 kr. med tillæg af procesrente fra den 2. december 2018 til betaling sker.

BS-49315/2019-GLO
Sagsøger 3 har nedlagt påstand om, at Gladsaxe Kommune skal beta-le 30.000 kr. med tillæg af procesrente fra den 2. december 2018 til betaling sker.

BS-51045/2019-GLO
Sagsøger 4 har nedlagt påstand om, at Gladsaxe Kommune skal betale 20.000 kr. med tillæg af procesrente fra den 2. december 2018 til betaling sker.

BS-51234/2019-GLO
Sagsøger 5 har nedlagt påstand om, at Gladsaxe Kommune skal be-tale 27.500 kr. med tillæg af procesrente fra den 2. december 2018 til betaling sker.

BS-51318/2019-GLO
Sagsøger 6 har nedlagt påstand om, at Gladsaxe Kommune skal betale 15.000 kr. med tillæg af procesrente fra den 2. december 2018 til beta-ling sker.

BS-51332/2019-GLO
Sagsøger 7 har nedlagt påstand om, at Gladsaxe Kommune skal betale 7.500 kr. med tillæg af procesrente fra den 2. december 2018 til betaling sker.

Sagsøgte, Gladsaxe Kommune, har påstået frifindelse.

Oplysningerne i sagen
Det fremgår af Gladsaxe Kommunes informationssikkerhedshåndbog, revideret i maj 2018:

> "…
> **5 Informationssikkerhedspolitik**
> **5.1 Indledning**
> …
> Målet med informationssikkerheden i Gladsaxe Kommune er, at informationer og informationssystemer skal beskyttes mod uautoriseret eller utilsigtet adgang, anvendelse, videregivelse, driftsforstyrrelse, ændring eller ødelæggelse. Det er samtidig målsætningen, at indsatsen nøje afvejes i forhold til, at kommunen sik-kert og optimalt kan udføre kerneopgaverne over for borgere og virksomheder.
>
> **5.2 Formål**

…
lnformationssikkerheden i Gladsaxe Kommune skal altid leve op til gældende lovgivning og myndighedskrav. Endvidere er følgende indsatsområder særligt i fokus:

- Kommunens it-infrastruktur skal være effektivt beskyttet mod eksterne trus-ler og.
- Oplysninger om borgere og virksomheder som kommunen er i besiddelse af, skal til enhver tid beskyttes mod uberettiget videregivelse som følge af tekni-ske og menneskelige fejl eller forsætlige handlinger.
- God praksis for informationssikkerhed, principper og normer for adfærd i anvendelsen af kommunens informationssystemer skal være klart formulere-de og formidlet til medarbejderne, så uberettiget anvendelse forebygges og undgås.

5.3 Holdninger og principper
Det er Gladsaxe Kommunes politik, at informationssikkerhed bygger på tillid, sund fornuft og ansvarlighed hos kommunens medarbejdere frem for kontrol, overvågning og mistanke. Kommunen ønsker derfor også, at informationssikker-hedspolitikken fungerer adfærdsregulerende snarere end kontrollerende over for de ansatte.
…

6.2 Mobilt udstyr og fjernarbejdspladser
Formålet er at sikre fjernarbejdspladser og brugen af mobilt udstyr.

6.2.1 Politik for mobilt udstyr
Adgangen til mobilt udstyr beskyttes med PIN-kode på mindst 4 tegn, en ad-gangskode eller en anden sikker identifikationsmetode.

Fortrolige oplysninger og følsomme personoplysninger må kun opbevares i ES-DH-system eller fagsystem og må således ikke opbevares på mobile enheder.

Hvis det som led i løsningen af den faglige opgave midlertidigt er nødvendigt at opbevare fortrolige oplysninger eller følsomme personoplysninger på mobilt ud-styr, skal informationerne beskyttes med kryptering. Krypteringsløsningen skal godkendes af Digitaliseringsafdelingen.
…

8.2.1 Klassifikation af information
lnformationssikkerhedskoordinatorerne har ansvar for, at der skabes bevidsthed i organisationen omkring klassifikation af data og informationer, samt hvordan medarbejderne skal håndtere disse alt efter klassifikationen.

Gladsaxe Kommune sondrer mellem følgende klassifikationer:

- **Følsomme personoplysninger** om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering, jf. databeskyttelsesforordningens artikel 9
- **Fortrolige oplysninger** (herunder også fortrolige personoplysninger), der omfatter væsentlig økonomisk eller forvaltningsmæssig information, der kan forårsage væsentlig skade på Gladsaxe Kommunes forvaltning, omdømme eller økonomi såfremt de offentliggøres. Det kan f.eks. være økonomiske da-ta, udbudsmateriale, fortrolige planer, lukkede politiske punkter og oplys-ninger om it-infrastruktur, dvs. oplysninger som er omfattet af tavshedspligt og ikke vil udleveres i tilfælde af aktindsigt. Alle følsomme personoplysnin-ger er også at betragte som fortrolige. Almindelige personoplysninger kan også være fortrolige. Det gælder fx for oplysninger om væsentlige sociale problemer, CPR, andre rent private forhold, økonomi, skat, gæld samt i nog-le tilfælde også informationer om uddannelses- og ansættelsesmæssige for-hold jf. Forvaltningslovens § 27. Personoplysninger vedrørende straffedom-me og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger jf. data-beskyttelsesforordningens artikel 10 betragtes også som fortrolige.
- **Almindelige personoplysninger**, der omfatter væsentlige sociale problemer, andre rent private forhold, økonomi, skat, gæld, sygedage, tjenstlige forhold, familieforhold, bolig, bil, eksamen, ansøgning, CV, ansættelsesdato, stilling, arbejdsområde, arbejdstelefon, navn, adresse, fødselsdato, identificerbare oplysninger, f.eks. navn og adresse, økonomiske forhold, jf. databeskyttelses-forordningens artikel 6 og Forvaltningslovens § 27. Bemærk at almindelige personoplysninger godt kan være fortrolige.
- **Interne oplysninger**, der er oplysninger, som kun er rettet til intern brug i Gladsaxe og som kun medarbejdere har adgang til enten i elektronisk eller analog form. Offentliggørelse vil kun forårsage ubetydelig skade på Gladsaxe Kommunes forvaltning, omdømme eller økonomi.
- **lkke-fortrolige oplysninger**, som ikke er omfattet af ovenstående klassifikationer og i øvrigt er tilgængelige efter offentlighedens regler om aktindsigt.

…

8.3 Mediehåndtering

Formålet er at forhindre uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier.

8.3.1 Styring af bærbare medier

Flytbare lagringsmedier som f.eks. USB-nøgle, ekstern harddisk, CD og lignende må ikke anvendes til lagring eller forsendelse af fortrolige oplysninger eller personlysninger, med mindre disse er krypteret.
Datamedier, herunder også papir, som indeholder andet end offentlig informa-tion, skal opbevares aflåst i perioder, hvor informationen ikke anvendes.

…

11 Fysisk sikring og miljøsikring

11.1 Sikre områder
Formålet er at forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter.

11.1.1 Fysisk perimetersikring
I områder, hvor der opbevares fortrolige eller følsomme personoplysninger, skal der ske en passende sikring af materialet, således at oplysningerne ikke gøres tilgængelige for uvedkommende.

Serverrum, krydsfelter og lignende sikrede områder, hvor der er placeret netværksudstyr, skal holdes aflåst. For serverrum med kritisk informationsbehandlingsudstyr skal der etableres et adgangskontrolsystem, hvor adgangene logges med oplysninger om, hvem der har haft adgang hvornår.

11.1.2 Fysisk adgangskontrol
Sikrede områder skal beskyttes med adgangskontrol, så kun autoriserede perso-ner kan få adgang. Kun personer, der skal udføre rutinemæssige opgaver i områ-derne kan opnå fast autorisation til adgang. Til serverrum kan serviceleverandø-rer (f.eks. elektriker) efter en konkret risikovurdering opnå en fast autorisation til adgang, når dette er betinget af hurtig adgang f.eks. ved driftsnedbrud uden for arbejdstid og lignende.

Adgangsautorisationen skal gennemgås og revurderes mindst en gang årligt.

11.1.3 Sikring af kontorer, lokaler og faciliteter
Der skal være en passende fysisk sikkerhed for kommunens kontorer, lokaler og faciliteter. Kommunens ønske om at fremstå åben over for borgerne skal løbende afvejes mod hensynet til sikring af kommunens informationer.

I områder med borgeradgang samt ubemandede områder skal ledelsen sikre, at uvedkommende ikke får adgang til følsom eller fortrolig information, samt at borgere ikke uforvarende kan aflæse oplysninger fra skærme og lignende.

Der skal anvendes tilstrækkelige alarmsystemer på relevante bygninger og loka-ler
…
11.1.5 Arbejde i sikre områder
Gæster, der ikke har autorisation til adgang til sikrede områder, skal være ledsa-get af autoriseret personale.

11.2 Udstyr
Formålet er at undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen.

11.2.1 Placering og beskyttelse af udstyr
Udstyr skal placeres, så risikoen for skader og uautoriseret adgang minimeres.

Udstyr (f.eks. computere, mobile enheder, skærme og printere), hvor der behand-les eller udskrives følsomme personoplysninger eller fortrolige oplysninger, skal placeres eller indrettes, så informationerne ikke kan ses eller tilgås af uvedkommende. På printere anbefales det, at der benyttes en fortrolig udskriftfunktion, så det kun er muligt at printe ved medarbejderens tilstedeværelse.
…

18.1.3 Privatlivets fred og beskyttelse af personoplysninger
Systemejerne har ansvar for, at der er tilstrækkelig beskyttelse indbygget i it-systemerne, således at personoplysninger er beskyttet i overensstemmelse med lovgivningen. Hvis der foretages behandlinger, der er forbundet med høj risiko som beskrevet i databeskyttelsesforordningens artikel 35, skal der foretages en konsekvensanalyse, inden behandlingen igangsættes.

Endvidere skal det sikres, at anvendelse og udstilling af personoplysninger begrænses efter principperne om "Privacy by design" og "Privacy by default", jf. databeskyttelsesforordningen.

Ledere og medarbejdere har ansvar for, at personoplysninger i analog form (pa-pir) beskyttes og ikke gøres tilgængeligt for uvedkommende.

Alle medarbejdere har ansvar for, at personoplysninger er tilstrækkelige, relevan-te og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de be-handles jf. databeskyttelsesforordningens princip om dataminimering.
…"

Det fremgår af Gladsaxe Kommunes 15 sikkerhedsbud:

"…
Det er afgørende for borgerne som privatpersoner og Gladsaxe Kommune som organisation, at der er styr på informationssikkerheden. Derfor skal alle medarbejdere følge de 15 sikkerhedsbud.
…
1) Du har et medansvar for vores sikkerhed. Følg retningslinjerne for sikkerhed, hold dig orienteret, stil spørgsmål og vær kritisk.
…
4) Sørg for, at pin- eller adgangskode altid er aktiveret på din mobil, iPad eller tablet, så uvedkommende ikke kan få adgang til dine oplysninger, hvis du f.eks. mister enheden.
…
6) Brug kun godkendte journal- eller fagsystemer til at gemme personoplysninger eller andre typer af oplysninger, der er fortrolige. Brug aldrig lokale drev, fællesdrev, usb-nøgler eller eksterne harddiske til disse formål.
…

9) Indhent og del kun personoplysninger, når der er et fagligt behov. Del så lidt som muligt med så få som muligt.

…"

Den 5. december 2018 anmeldte Gladsaxe Kommune til Københavns Vestegns Politi, at der var blevet stjålet 4 bærbare PC´ere fra rådhuset.

På den ene af de 4 bærbare PC´ere var der på et lokaldrev lagret et regneark med oplysninger om 20.620 borgere, herunder de 7 sagsøgere, Sagsøger 1, Sagsøger 2, Sagsøger 3, Sagsøger 4, Sagsøger 5, Sagsøger 6 og Sagsøger 7.

Det fremgår af regnearket, at der for alle de 7 sagsøgere var oplysninger om CPR-nummer, navn og adresse.

Vedrørende Sagsøger 1 var der yderligere i en kolonne med tek-sten "Paragraf sektion" angivelse af § 112, § 138, § 138, § 138, § 83,2, § 83,2 og § 83 a. For hver bestemmelse var der anført startdato og slutdato samt en kolonne med angivelse af "Leverandør navn" , hvor der på 5 linjer fremgik "GLX Vest 4" og på 1 linje fremgik "GLX Rehab Vest" . Der var endvidere i en kolonne med teksten "Ydelsestekst" rækker med angivelse af "Almindelig boligsikring" , og i hver række var der angivelse af periode, beløb, refusionsprocent og kommunal udligning.

Vedrørende Sagsøger 2 var der yderligere i en kolonne med tek-sten "Ydelsestekst" rækker med angivelse af "Almindelig boligsikring" , og i hver række var der angivelse af periode, beløb, refusionsprocent og kommunal udligning.

Vedrørende Sagsøger 3 var der yderligere i en kolonne med teksten "Paragraf sektion" anført "§ 140" med angivelse af startdato, slutdato og "Leve-randørnavn" , hvor der fremgik, "GLX TCG Sundhed og Træning" .

Vedrørende Sagsøger 4 var der yderligere anført, "Institutionsop-hold" , "Fraflytningskommune" med angivelse af kode, tilflytningsdato med an-givelse af dato og "Institution (manuel) Egebo" .

Vedrørende Sagsøger 5 var der yderligere i en kolonne med teksten "Ydelsestekst" rækker med angivelse af "Tilskud til lejere" , og i hver række var der angivelse af periode, beløb, refusionsprocent og kommunal udligning.

Vedrørende Sagsøger 6 var der yderligere i en kolonne med teksten "Paragraf sektion" rækker, hvor der var anført "§ 140" med angivelse af

startdato og slutdato. Under ”Leverandørnavn” fremgik i 3 rækker ”GLX TCG Sundhed og Træning” og i 1 række ”GLX TCG Sundhed og Træning Koordinatorer” .

Vedrørende Sagsøger 7 var der yderligere i udtrækket om ”Alle ydelser” anført ”Nettobeløb 22564” og ”samlet funktion 5.58.82 Ress”

Den 5. december 2018 indberettede Gladsaxe Kommune sagen som en sikkerhedshændelse til Datatilsynet. Det fremgår af indberetningen:

> ”…
> Årsag til hændelsen / hvad er der sket
>
> Beskriv hændelsen
>
> En fil med fortrolige og følsomme personoplysninger er blevet gemt lokalt på en computer. Computeren er efterfølgende blevet stjålet.
>
> Der er i løbet af weekenden d. 30/11-3/12 (mellem arbejdstidsophør fredag og mandag morgen) blevet stjålet flere computere fra 3. sal i fløj 5 på Gladsaxe Rådhus. På en af disse computere var en fil med personoplysninger midlertidigt lag-ret lokalt på pc'ens skrivebord (filen var blevet lagt lokalt d. 28/11) i modstrid med de interne retningslinjer. Data var ikke krypteret. Der er tale om en manuel menneskelig fejl.
>
> I filen sammenkøres en række oplysninger på CPR-niveau for at beregne den mellemkommunale refusion. I datasættet optræder i alt 19.681 unikke CPR-num-re. Nedenfor fremgår den samlede liste, inkl. antal berørte CPR-numre, over de informationer, der er sammenkørt.
> …
> Involveret teknologi
> …
> Personlig computer (fx bærbar, stationer, tablet)
> …
> Konsekvenser
>
> Sandsynlige konsekvenser af hændelsen for hhv. personer, virksomheder og tjenester
>
> Brud på fortrolighed
> …
> - Utilsigtet videregivelse af oplysninger, der er linket til andre oplysninger om de berørte
> - Oplysningerne kan blive misbrugt til andre eller ulovlige formål
> - Andre konsekvenser som følge af brud på fortrolighed
>
> …

Fysisk, materiel eller immateriel skade med betydelige konsekvenser for den be-rørte
- Mistet kontrol over egne oplysninger

…
Uddybende oplysninger
Mulige konsekvenser er angivet ud fra, at kommunen vurderer, at der forment-ligt er tale om et brugstyveri, hvorfor det vurderes som meget lidt sandsynligt, at de nævnte data vil blive misbrugt. Såfremt data bliver delt, vil konsekvenserne for de berørte kunne være mere omfattende.

Håndtering
Foranstaltninger, der er truffet for at håndtere hændelsen og begrænse dets muli-ge skadevirkninger

Foranstaltninger, der er truffet
Tyveriet blev straks meldt til Rådhusets vagter, ligesom der er sket en politian-meldelse af tyveriet. Derudover blev kommunens lT-afdeling gjort opmærksom-me på tyveriet. Endelig er procedurerne for håndtering af denne type filer blevet indskærpet over for afdelingens medarbejdere for at undgå lignende tilfælde i fremtiden.

Foranstaltninger, der foreslås truffet
Gladsaxe Kommune har allerede haft betydeligt fokus på lagring på lokale drev i forbindelse med awareness-arbejdet. Denne sag forventes brugt i awareness-kon-tekst for at vise, hvor alvorlige konsekvenser brud på retningslinjerne kan have.
…"

Den 6. december 2018 sendte Gladsaxe Kommune en uddybende indberetning til Datatilsynet, hvor antallet af berørte CPR-numre blev ændret, ligesom over-sigten over, hvilke data der var omfattet af filen på den stjålne PC, blev korrige-ret. Det fremgår:

"…
I det følgende gennemgås hver af de 19 datakilder, der indgik i den omtalte fil. For hver af disse er angivet typen af datakilde, antal unikke CPR-numre, perio-den som informationerne vedrører og typen af konkrete informationer. Da der er tale om et regneark, er der tale om informationer på et relativt enkelt og overord-net detaljeringsniveau. Nedenstående overskrifter er dækkende for det faktiske indhold. Der indgår således ikke journaltekst i regnearket.

Institutionsophold (fra CPR Web), 2.955 unikke CPR-numre, marts-oktober 2018
- Borgers CPR-nummer
- Navn på borgeren
- Borgers nuværende adresse
- Borgers tidligere adresse
- Til- og fraflytningsdato
- Navnet på den institution, som borgeren har været / er tilknyttet

Ydelser (fra kommunens økonomisystem), 8.031 unikke CPR-numre, oktober 2018
- Borgers CPR-nummer
- Bogførte ydelser (f.eks. særlig tilrettelagt ungdomsuddannelse, hjælpemidler, midlertidige botilbud, kontanthjælp, revalideringsydelse, førtidspension, ressourceforløb og ledighedsydelse)

Ydelse (fra KMD Nexus), 9.023 unikke CPR-numre, øjebliksbillede
- Borgers CPR-nummer
- Navn på borgeren
- Borgers adresse
- Paragraffen som ydelsen er leveret i henhold til (f.eks. §83a, §85, §138 og §140).
- Start- og slutdato for ydelsen
- Opholds-, handle- og betalingskommune
- Leverandørnavn (f.eks. GLX TGC Sundhed og Træning)

Mellemkommunale borgere på beskæftigelsesområdet (manuel liste), 51 unikke CPR-numre, øjebliksbillede
- Borgers CPR-nummer
- Betalingskommune
- Start- og slutdato for ydelsen
- Mellemkommunale krav (beløb)

MAF / KMD Social Opsætning, 239 unikke CPR-numre, 2018 år til dato
- Borgers CPR-nummer
- Kommune
- Mellemkommunale afregnede beløb
- Årsag (f.eks. "6 års regel" og ”Anbragt på institution")

Pensionssager (fra KMD Sag), 1.969 unikke CPR-numre, øjebliksbillede
- Borgers CPR-nummer
- Navn på borgeren
- Status (f.eks. Aktiv, hvilket vil sige borgeren modtager pension på opgørelsestidspunktet)
- Sagstype (f.eks. Førtidspension, Mellemste førtidspension, Højeste førtidspension og Invaliditetsydelse)

Efterværnssager (fra Gladsaxe Tilbudsapplikation), 471 unikke CPR-numre, 2018 år til dato
- Borgers CPR-nummer
- Borgers mors CPR-nummer
- Borgers fars CPR-nummer
- Sagsbehandler
- Status (f.eks. Aktiv og Afsluttet)
- Forældremyndighed (angiver om det er mor eller far, der har forældremyndigheden)

- Sagskategorisering (angiver hvor sagen er registreret, f.eks. Ungeenheden)

Mellemkommunale efterværnssager, 10 unikke CPR-numre, øjebliksbillede
- Borgers CPR-nummer
- Navn på borgeren
- Handlekommune
- Tilsagnsperiode
- Indsats (f.eks. SEL 76.3.2 Kontaktperson)
- Opfølgningsdato

Boligstøtte R127 (Fra Det kommunale boligstøttesystem), 7.923 unikke CPR-numre, april- oktober 2018
- Borgers CPR-nummer
- Opholds- og betalingskommune
- Beløb
- Ydelsestekst (f.eks. Tilskud til lejebetaling i ældrebolig og Tilskud til lejere)

Kontante ydelser / STAR, 373 unikke CPR-numre, 2018 år til dato
- Borgers CPR-nummer
- Ydelsestype (f.eks. Førtidspension, Særlig støtte, Kontanthjælp og Ressourceforløb)
- Udgifter

Ældrebolig (fra KMD Nexus), 56 unikke CPR-numre, øjebliksbillede
- Borgers CPR-nummer
- Ældreboligbevilling (f.eks. Ældrebolig (§§ 105 og 115 stk. 2)

Botilbud (manuel liste), 30 unikke CPR-numre, øjebliksbillede
- Borgers CPR-nummer
- Navn på borgeren
- Tilbudsnavn f.eks. Center for Døve, Taxhus og Præstø)
- Paragraf som tilbuddet er bevilget i henhold til (f.eks. § 108)
- Diagnose (Denne overskrift er misvisende, da der alene er tale om oplysninger om institutionstypen, f.eks. psykisk handicappede. Derimod er der ikke oplysninger om den enkelte borgers konkrete diagnose.)
- Kontonummer i kommunens økonomisystem
- Start- og slutdato for borgers tilknytning til tilbuddet

Plejehjem (manuel liste), 76 unikke CPR-numre, øjebliksbillede
- Borgers CPR-nummer
- Navn på borgeren
- Tilbudsnavn (f.eks. Egegården)
- Betalingskommune
- Start- og slutdato for borgeres ophold på tilbuddet

Plejebolig (manuel liste), 69 unikke CPR-numre, øjebliksbillede
- Borgers CPR-nummer

- Navn på borgeren
- Opholds-, handle- og betalingskommune
- Kontonummer i kommunens økonomisystem
- Paragraf som tilbuddet er bevilget i henhold til (f.eks. §83/192)
- Start- og slutdato for borgers ophold på tilbuddet
- Samlet forbrug

Hjemmehjælp (manuel liste), 34 unikke CPR-numre, øjebliksbillede
- Borgers CPR-nummer
- Navn på borgeren
- Borgers nuværende adresse
- Borgers tidligere adresse
- Ydelse (f.eks. Hjemmehjælp og Træning)
- Kontonummer i kommunens økonomisystem
- Start- og slutdato for ydelsen

§ 117 (manuel liste), 34 unikke CPR-numre, oktober2018
- Borgers CPR-nummer
- Navn på borgeren
- Samlet forbrug
- Antal egenbetalinger

BPA § 96 (fra kommunens økonomisystem), 116 unikke CPR-numre, oktober 2018
- Borgers CPR-nummer
- Kontonummer i kommunens økonomisystem
- Posteringstekst i kommunens økonomisystem
- Beløb
- Bogføringsdato

Mellemkommunale borgere bosiddende i Gladsaxe Kommune (fra CPR-registe-ret), 1.153 unikke CPR-numre, øjebliksbillede
- Borgers CPR-nummer
- Navn på borgeren
- Borgers mors CPR-nummer
- Borgers fars CPR-nummer
- Borgers ægtefælles CPR-nummer
- Stillingsbetegnelse
- Medlemskab af folkekirken
- Fødselsregistreringssted
- Betalingskommune
- Borgers nuværende adresse
- Borgers tidligere adresse
- Datoer for til- og fraflytning

Mellemkommunale borgere bosiddende i andre kommuner (fra CPR-registeret), 326 unikke CPR-numre, øjebliksbillede

- Borgers CPR-nummer
- Bopælskommune
- Betalingskommune
- Bemærkningsfelt

…"

Det fremgår af e-mail af 7. december 2018 fra Person 1, partner hos PwC – Cyber & Informationssikkerhed, til Gladsaxe Kommune:

"…
Jeg fremsender hermed som aftalt min vurdering af risikoen for borgerne hvis deres CPRnr, navn og adresser måske er/eller konkret er blevet eksponeret over for offentligheden, hvorved der er en risiko for at uautoriserede har fået adgang til deres CPRnr, navn og adresse.

Konsekvensen for borgerne
Misbrug af CPRnr, navn og adresse kan føre til identitetstyveri, som kan få en økonomisk konsekvens.

Sandsynligheden for at konsekvensen udløses
Det er min vurdering at der i Danmark er en meget lille sandsynlighed for at bor-gere bliver udsat for identitetstyveri. Selvom vores cyber survey viser at der er en stigning i antallet af tilfælde i forhold til sidste år, er det stadig et meget lille an-tal. Det kan skyldes at identitetstyveri kræver at den kriminelle skal udgive sig for at være en anden og dette kræver at de fysisk skal møde op for at få udstedt nye identitetspapirer, hvilket øger risikoen for at de bliver opdaget og identifice-rede. De tilfælde vi kender til vedr. identitetstyveri er når personer har haft en fy-sisk relation i en periode og kender hinanden.

Der har i de seneste år været en lang række sager hvor borgers CPRnr og navn har være eksponeret over for uvedkommende og der har ikke været tilfælde hvor der har medført direkte sager om identitetstyveri.
…"

Ved e-mail af 7. december 2018 orienterede kommunaldirektøren i Gladsaxe Kommune byrådet om sagen, herunder om hvilke oplysninger filen med regne-arket indeholdt, at kommunen havde underrettet Datatilsynet om hændelsen, samt om hvilke tiltag kommunen havde og ville iværksætte for fremover at undgå lignende hændelser.

Den 10. december 2018 orienterede Gladsaxe Kommune de berørte borgere om, at der var stjålet en computer med fortrolige oplysninger. Det fremgår af orien-teringen:

"…

Gladsaxe Kommune har i weekenden mellem uge 48 og 49 fået stjålet fire computere fra rådhuset. Desværre har vi konstateret, at der på én af computerne ved en fejl var blevet gemt et regneark, som indeholdt fortrolige oplysninger om dig og andre borgere. Vi har meldt hændelsen - som vi karakteriserer som et sikker-hedsbrud - til Datatilsynet og tyveriet til Vestegnens Politi.

Karakteren af sikkerhedsbruddet
På baggrund af de konkrete omstændigheder ved tyveriet har vi ikke grund til at tro, at computerne er blevet stjålet med det formål at skaffe sig adgang til Gladsaxe Kommunes oplysninger. Der er sandsynligvis tale om et brugstyveri, hvor indholdet på computeren hurtigt bliver slettet, så computeren kan sælges videre, og oplysningerne dermed ikke bliver tilgængelige.

Det kan dog ikke afvises, at tyven eller andre, som får computeren i hænde, kan finde frem til oplysningerne. I henhold til databeskyttelsesforordningen, som trå-dte i kraft 25. maj 2018, skal vi derfor orientere alle personer, hvis oplysninger fremgår af det nævnte regneark, og derfor orienterer vi også dig.

Oplysningerne på kommunens computere er beskyttet via tekniske og organisatoriske sikkerhedsforanstaltninger. Foranstaltninger, som også beskytter oplysningerne, hvis vi mister vores computere ved tyveri eller ved et hændeligt uheld. I dette tilfælde indeholdt én af disse computere dog undtagelsesvis et regneark med fortrolige oplysninger, som ved en menneskelig fejl var gemt midlertidigt lokalt på computeren.

Informationerne i regnearket var blevet udtrukket med henblik på rutinemæssig økonomisk kontrol, til sikring af korrekt afregning kommunerne i mellem. Det skal for en god ordens skyld nævnes, at denne økonomiske kontrol alene har be-tydning for afregningen kommunerne i mellem, og ikke har betydning for din el-ler andre borgeres konkrete sager, herunder de tilbud eller ydelser, som du even-tuelt er berettiget til at modtage.

Informationerne i regnearket bestod af personnummer, alder, køn og i nogle til-fælde yderligere informationer som adresse, familiære forhold (for eksempel ci-vilstand, forældre og børn), overordnet information om kommunale ydelser m.m. For en gruppe af borgere, der bor på et botilbud, er tilbudstypen oplyst (for eksempel institution for borgere med fysisk handicap). Endelig er der for en min-dre gruppe af borgere informationer om medlemskab af folkekirken.

Relevante foranstaltninger
Gladsaxe Kommune har som nævnt anmeldt tyveriet til politiet

Derudover har Gladsaxe Kommune kontaktet en ekstern it-sikkerhedsekspert for at få en vurdering af de mulige konsekvenser. Vurderingen er, at risikoen for misbrug af dit personnummer er begrænset, da oplysningerne ikke i sig selv er nok til misbrug. Egentligt misbrug af oplysningerne kræver således oftest kode

eller personligt fremmøde, eksempelvis i forbindelse med udstedelse af identitetspapirer.

Du kan selv forebygge eventuelt misbrug af dine oplysninger. Dette kan du læse mere om på borger.dk: https://www.borger.dk/internet-og-sikkerhed

Hvis du har spørgsmål til den konkrete sag, er du velkommen til at kontakte Gladsaxe Kommune på telefonnummer 39 57 50 00. Telefonen er åben mandag til fredag i tidsrummet 09.00-14.00.

Hvis du har spørgsmål til, hvordan Gladsaxe Kommune generelt behandler dine personoplysninger, kan du kontakte vores Databeskyttelsesrådgiver på e-mail: dpo@gladsaxe.dk eller telefonnummer 39 57 69 00. Hvis du skal sende personli-ge, fortrolige eller følsomme oplysninger anbefales det, at du sender en sikker mail. Se nærmere herom i beskrivelsen af databeskyttelsesrådgiveren på gladsaxe.dk.

Vi ser med stor alvor på hændelsen og skal beklage, at vi har mistet fortrolige oplysninger om dig og andre borgere.
…"

Efter anmodninger fra hver af sagsøgerne meddelte Gladsaxe Kommune dem indsigt i de oplysninger om dem hver især, der fremgik af det omhandlede regneark, der var lagret på den stjålne PC.

Gladsaxe Kommunes borgmester orienterede på et byrådsmøde den 19. decem-ber 2018 om sagen. Det fremgår af borgmesterens notat herom af 20. december 2018:

"…
Formålet med regnearket

Lad mig starte med at slå fast, at det ikke er enestående, at medarbejdere i kommunen arbejder med regneark, hvori der indgår store mængde af data om borge-re i kommunen. Det er en forudsætning for at kunne løse de opgaver, som med-arbejdere i vores økonomifunktioner arbejder med, og som bidrager til den stær-ke økonomistyring, som vi har her i Gladsaxe Kommune.

I dette tilfælde var der tale om et regneark, der blev brugt til at lave en obligato-risk kontrol af, om Gladsaxe Kommune får indhentet den korrekte mellemkom-munale refusion - dvs. betalinger til og fra andre kommuner. For at kunne lave denne kontrol er der brug for oplysninger om alle de borgere, der modtager ydel-ser, der potentielt kunne være omfattet af mellemkommunal refusion. Det forkla-rer det store antal af cpr-numre. I 2018 har denne kontrol sikret, at kommunen har indhentet ca. 5,5 mio. kr. som manglede i mellemkommunal refusion.

Desværre er det sådan, at man i det dokumenthåndteringssystem, som kommu-nen har, ikke kan arbejde aktivt med store og komplicerede regneark. Derfor bli-ver man nødt til gemme filerne midlertidigt et andet sted, mens der arbejdes med dem. Medarbejderne ved godt, at de her skal arbejde med filerne på et centralt netværksdrev, hvor de ligger sikkert, indtil de igen kan placeres i dokument-håndteringssystemet. Desværre var der i dette tilfælde et meget uheldigt sam-menfald mellem et tyveri og det forhold, at en medarbejder var kommet til at gemme regnearket et forkert sted om torsdagen - altså umiddelbart før, at com-puteren blev stjålet.

…

Anmeldelse til Datatilsynet og orientering af borgere

Da den pågældende medarbejder mødte på arbejde mandag morgen og opdage-de at pc'en var stjålet, fortalte han straks, at han havde lagt et regneark på pc'en om torsdagen. Forvaltningen gik herefter i gang med at finde ud af, hvad der helt præcist lå i regnearket. Heldigvis lå der en identisk kopi i vores dokumenthånd-teringssystem, så vi kunne identificere og gennemgå indholdet. Onsdag den 5. december foretog forvaltningen en anmeldelse til datatilsynet, som efterfølgende blev præciseret den 6. december. Byrådet blev desuden orienteret den 7. decem-ber.

Forvaltningen brugte herefter tid på at afklare, hvordan borgerne bedst muligt skulle orienteres, og ikke mindst hvordan dette praktisk kunne tilrettelægges. Det er en meget stor opgave at sende breve ud til 20.000 borgere. Målet var at gi-ve en præcis og dækkende beskrivelse, som samtidig redegjorde for den reelle ri-siko, men ikke gjorde de berørte mere bekymrede, end der reelt var grund til. Derfor kontaktede man PriceWaterhouseCoopers (PWC), som overvåger it-kri-minalitet i ind og udland. På baggrund af en lang og grundig snak udarbejdede PWC en vurdering af sikkerhedsrisikoen for hændelsen. PWC vurderede, at risi-koen for, at personoplysninger på den stjålne PC ville blive misbrugt (i værste til-fælde til identitetstyveri), var meget lille. Årsagen til denne vurdering er, at om-stændighederne tyder på, at der er tale om et brugstyveri, hvor PC´en hurtigt vil-le blive renset for data med henblik på videresalg. Samtidig er misbrug af perso-noplysninger i Danmark meget sjældne, da det oftest kræver NemlD eller per-sonligt fremmøde med forevisning af pas eller kørekort. De misbrug i form af identitetstyveri, som finder sted, begås oftest af folk i den nære bekendtskabs-kreds.

…

Oplysninger om medlemskab af folkekirken

Person 2 spørger også til, at der i regnearket i nogle tilfælde fremgik oplysninger om den enkelte borgers tilhørsforhold til Folkekirken.

Et centralt princip i de nye Databeskyttelsesregler er Dataminimering, hvilket på lidt mere let forståeligt dansk betyder, at man kun indhenter de oplysninger, der er relevante for den konkrete opgave man skal løse. Dette har også været ud-gangspunktet for den analyse regnearket har været brugt til.

Men for et mindre antal borgere har et udtræk fra CPR-registret indeholdt oplysninger om medlemskab af folkekirken. Det er naturligvis en fejl, og noget vi blev opmærksomme på tidligt i forløbet, og som vi også har nævnt i anmeldelsen til datatilsynet, ligesom det fremgik af kommunaldirektørens orientering til Byrå-det, at regnearket for et mindre antal borgere omfattede oplysninger, der ikke var relevante for den opgave regnearket bruges til. Jeg kan oplyse, at oplysninger om medlemskab af folkekirken ikke bliver brugt i kontrollen af mellemkommunale betalinger. Og jeg kan også oplyse, at de data vil blive slettet og vil ikke fremgå af det pågældende regneark fremadrettet.
…
En kulturændring
Og så giver sagen naturligvis også anledning til endnu engang at se på, hvor vi kan forbedre sikkerheden, og hvad vi kan lære af den. Vi kan aldrig gardere os mod menneskelige fejl, men vi kan arbejde for, at konsekvenserne af fejl ikke bli-ver så store. Digitaliseringsafdelingen er derfor gået i gang med at kryptere alle nye maskiner og forventer at alle maskiner med Windows 10 vil være krypteret inden jul. Efterfølgende vil alle ældre maskiner enten blive krypteret eller udfa-set. Vi kan også skærpe den fysiske sikkerhed på Rådhuset bedre, så uvedkom-mende får sværere ved at få adgang til computere og kontorer.
…"

Datatilsynet stillede den 11. december 2018 og 3. januar 2019 spørgsmål om sagen til Gladsaxe Kommune.

Det fremgår af bilag 1, kommunens svar af 4. januar 2019 til Datatilsynet:

"…

	Datatilsynets spørgsmål/anmodning	Dataansvarliges svar
1	I anmeldelsen af bruddet på persondatasikkerheden fremgår det, at der er blevet stjålet flere computere. Er der alene tale om en computer, med en enkelt fil, hvor de af bruddet omfattede personoplysninger indgår? I afkræftende fald bedes dette uddybet.	Ja, det er korrekt. Filen, der indeholdt 20620 unikke CPR-numre, lå på én fil på én computer. Filen blev i strid med kommunens retningslinjer lagt på computerens skrivebord torsdag 29. november med henblik på midlertidig lagring.

2	I anmeldelsen fremgår det at filen (et regneark) med personoplysninger ikke er krypteret. Er der i øvrigt anvendt kryptering på computerens harddisk? I bekræftende fald bedes det oplyst: • Hvilken type af kryptering der er tale om. • Om computeren var tændt på det tidspunkt hvor den blev stjålet.	Nej.
3	Er computeren opsat med adgangskontrol? I bekræftende fald bedes det uddybet hvilken form der anvendes, fx brugernavnog password, 2-faktor autentificering, osv.	Ja, computeren er beskyttet med Windows brugernavn og adgangskode. Begge dele skal kendes, før der kan logges ind på computeren. Brugernavnet er unikt og personligt og består af en bogstavkombination sammensat af forbogstaverne fra brugerens fornavn og efternavn. Passwordet overholder standardreglerne for komplekse passwords i Windows. Dvs.: Mindst 8 tegn Må ikke indeholde brugerens fornavn, mellemnavn, efternavne eller brugernavn. Adgangskoden skal indeholde mindst 3 af disse tegn: - Store bogstaver - Små bogstaver - Tal - Specialtegn (som !, $, #, %) Efter 5 mislykkede forsøg spærres for adgang.

4	Af opfølgningen på anmeldelsen fremgår det, at der er rettelser til antallet af personnumre i de forskellige kategorier. Oplyst venligst det endelig e anta l unikke personnumre, der er om fattet af bruddet.	20620
5	Indebærer brudd et på persondatasikkerhede n oply sninger hvis behandling er omfa ttet af databeskyttelsesforord ninge ns artikel 9? I bekræften de fal d bedes den dataansvar lige re degøre for hvilke oplysninge r der e r tale om, samt angive en f ordeling af typen af oplysninger p å det a ntal registrerede, om hvem d en ko nkrete type oplysning behan dles.	Der henvises til bilag 4.
6	Beskriv ven ligst d en fysiske sikkerhed på sted et, hv orfor computeren blev stjålet.	Der henvises til bilag 5 og 5.1. I forhold til den konkrete hændelse blev tyveriet konstateret 03.12.2018 kl. 09.00. Computeren blev stjålet i weekenden d. 30/11-3/12 (mellem arbejdstidsophør fredag og mandag morgen). Der var juletræstænding fredag 30/11, hvorfor der også redegøres for sikkerheden i den kontekst i bilaget. Computeren blev stjålet fra Rådhusets 3. sal, fløj lokale 3525.
7	Var compu teren f astlåst på det sted hvorfra den blev stjålet, fx med wirelås?	Nej.
8	Af opfølgn ingen på anmeldelsen fremgår de t, at al le registrerede vil blive under rettet den 9. december 2018. Er alle regis trerede blevet underrettet om hæn delsen? I bekræften de fald bedes underretningens indho ld angivet. I af-	Vi udsendte et orienteringsbrev til alle berørte den 10. december (bilag 6). Brevet blev sendt med digital post til deres e-boks. Borgere, der er fritaget for digital post, har modtaget et fysisk brev 1-3 dage efter. Ud af de 20620 berørte borgere var

	kræftende fald bedes det oplyst hvorfor underretning endnu ikke har fundet sted.	1392 døde på tidspunktet for udsendelsen af orienteringsbrevet. 53 breve er efterfølgende kommet tilbage, hvilket eks. kan betyde, at borgeren ikke har nogen adresse. Siden udsendelsen af orienteringsbrevet har ca. 1300 borgere kontaktet Gladsaxe Kommune telefonisk eller skriftligt med forskellige spørgsmål. I forlængelse heraf har 429 borgere (pr, 7. december 2019) fået indsigt i hvilke oplysninger der fremgik om netop dem i regnearket. (se bilag 6.1 og 6.2)

…"

Det fremgår af bilag 2, kommunens svar af 4. januar 2019 til Datatilsynet, blandt andet:

"…

	Datatilsynets spørgsmål/anmodning	Dataansvarliges svar
1	Redegør for indholdet af de interne retningslinjer, der refereres til i hændelsesbeskrivelsen, og hvordan disse retningslinjer udmøntes.	Der henvises til nes informationssikkerhedspolitik, håndbog samt de 15 sikkerhedsbud, der alle fremgår som bilag til besvarelsen. Der henvises desuden til redegørelsen om behandlingssikkerhed, hvori udmøntningen også beskrives (Bilag 3).
2	Redegør for med hvilken baggrund, at filen med de følsomme persondata er blevet gemt lokalt på pc'ens skrivebord. a) Hvilket filformat var filen gemt i, og var der anvendt en adgangskode på filen?	At filen var lagret lokalt skyldes en fejl fra medarbejderens side. Lagring af personoplysninger i ikke-krypteret form lokalt på computere er klart i strid med Kommunens regler for informationssikkerhed. a) Der er tale om en excel fil uden adgangskode på selve filen.

3	Redegør for hvilke sikkerhedsforanstaltninger, der blev anvendt lokalt på pc'en herunder bl.a. kompleksitet og længde af password til operativs ystem , og om der blev anvendt BI OS pæssword på pc'en.	Der henvises til besvarelsen af Datatilsynets spørgsmålark af 11. december 2018, spørgsmål nr. 3 (Bilag 1). Det kan desuden oplyses, at der ikke blev anvendt BIOS-password på pc'en.
4	Redegør ve nligst for om Gladsaxe Kommune på bag rund af hændelsen har skæ rpet d e interne retningslinjer, politi kker og procedure udover, hva d der allerede er nævnt. a) Er der de suden taget nye tekniske forans taltni nger i brug på baggrund a f hæn delsen?	De interne retningslinjer vurderes at være tilstrækkeligt klare, og hændelsen er udtryk for et klart brud på de interne retningslinjer. Hændelsen har naturligvis givet anledning til, at man endnu engang har haft fokus på awareness. Bl.a. har den ansvarlige direktør sendt en mail til alle medarbejdere, der har været relevant information på intranet og lign. a) Ja. Der henvises til redegørelsen for kryptering i beskrivelsen af behandlingssikkerhed.

…"

Det fremgår af bila g 4, k ommunens svar af 14. januar 2019 på spørgsmål 5 i bilag nr. 1:

"…
Sikkerhedsbru ddet omfattede følsomme personoplysninger iht. Databeskyttelsesforordninge n art. 9:

<u>Oplysninger o m reli giøs overbevisning:</u>

- For 467 re gistre rede fremgår, hvorvidt de har medlemskab af folkekirken, markeret med e t "F" (medlem) eller "U" (udmeldt).

<u>Helbredsoplys ninge r:</u>

- For 30 reg istrere de som er eller har været bosiddende på et botilbud, er angi-vet tilbud dets m ålgruppe opdelt på psykisk udviklingshæmmede, fysisk handicapp ede, psykisk syge eller sindslidende.

- For 28 reg istrere de er angivet, at leverandøren af de pågældende ydelser er Gladsaxe Komm unes Rusmiddelcenter. Rusmiddelcenteret er et tilbud til

borgere over 30 år, som har brug for hjælp til problemer med alkohol, hash eller stoffer.

I det vedlagte regneark i fanen "TOP botilbud" er vist anonymiserede eksempler på, hvordan oplysningerne med tilbuddets målgruppe fremgår i arket. Oplysnin-gerne fremgår i kolonne "1", som har titlen "Diagnose". Denne overskrift er imid-lertid misvisende, da der alene er tale om oplysninger om institutionstypen/mål-gruppen, f.eks. psykisk udviklingshæmmede. Derimod er der ikke oplysninger om den enkelte borgers konkrete diagnose.
I det vedlagte regneark i fanen "Nexus" er vist anonymiserede eksempler på, hvordan oplysningerne om at leverandøren er Gladsaxe Kommunes Rusmiddel-center er fremgået i arket.

Supplerende bemærkninger

- For flere registrerede er angivet efter hvilken paragraf, de registrerede har modtaget eller modtager ydelser omfattet af den mellemkommunale bereg-ning. Selve lovgrundlaget er dog ikke oplyst i regnearket, og det vil derfor ikke være muligt for udenforstående at udlede det konkrete hjemmelsgrund-lag for ydelsen.

Selv hvis det fulde hjemmelsgrundlag kunne udledes, er det kun i 29 tilfælde, at paragraf henvisningen i sig selv indikerer de bagvedliggende helbredsproblemer. I det vedlagte regneark, fanen "Nexus", er vist anonymiserede eksempler på to af omtalte 29 registreringer, hvor de 28 registreringer er sammenfaldende med de borgere, hvor det fremgår, at leverandøren er Gladsaxe Rusmiddelcenter jf. oven-stående.

På baggrund af den manglende lovhenvisning vurderer Gladsaxe Kommune, at disse registreringer ikke er omfattet af forordningens art. 9.

- For registrerede som har bopæl på en selvejende, privat eller kommunal in-stitution i Gladsaxe Kommune og omfattet af den mellemkommunale bereg-ning, er institutionens navn angivet.

Institutionens navn kan i visse tilfælde indikere, at der er tale om registrerede som har en eller anden form for nedsat funktionsevne eller som af sociale årsager har bopæl på en institution. Der er dog tale om institutioner som henvender sig til en sammensat målgruppe af borgere, og institutionens navn siger i sig selv så-ledes ikke noget konkret om de registreredes fysiske eller psykiske tilstande. I det vedlagte regneark, fanen "Institutionsophold", er vist anonymiserede eksempler på registreringerne i kolonne "N", "Institutionsophold (manuel)".

På denne baggrund vurderer Gladsaxe Kommune, at disse registreringer ikke er omfattet af forordningens art. 9.

I øvrigt bemærkes, at der er tale om offentligt tilgængelige oplysninger, da oplysninger om botilbuddet vil kunne udledes ved et almindeligt opslag på de registreredes adresse i f.eks. Kraks telefonbog.

Der har generelt været bevågenhed om ikke at indhente flere data end nødven-digt til regnearket. Der er dog konstateret undtagelser for dette princip, idet fx oplysninger om medlemskab af folkekirken og fødselsregistreringssted fremgår af arket selvom oplysningerne ikke kan bidrage til at løse kontrolopgaven vedrø-rende mellemkommunale betalinger.
…"

Det fremgår af bilag 5, kommunens svar af 14. januar 2019 på spørgsmål 6 i bi-lag nr. 1:

"…
Svar på spørgsmål nr. 6 i bilag nr. 1
I det følgende beskrives sikringsforhold på Gladsaxe Rådhus, opdelt på Skalsik-ring, Rumsikring samt Vagtservice.

Skalsikring

Rådhusets Hovedindgang, svingdør med elektronisk lås, åben for borgere kl. 10-14, torsdage kl. 10.00-18.00.

Personaleindgange A, B, C, D, E og F, har alle ADK (Automatisk Dør Kontrol) med Salto system og udgangstryk.
Indgang A ved Servicegården har samtaleanlæg til Vagtservice og Kantinekøk-ken, ITV overvågning, bruges tillige til vareindlevering.
Indgang B er tillige Handicapindgang, har samtaleanlæg til Vagtservice, ITV overvågning.
Indgang E er dækket af ITV overvågning fra Indgang A.
Indenfor indgang A, C, D, E, og F, alarmfølere, aktiveres kl. 23.00-05.00.

Flugtvejsdør ved Byrådssal, ADK, ITV overvågning.
Cykelkælderindgang, ADK.
Indgang til kælderarkiv, ADK.
Indgang til mellemgang ved fløj 2 og 3, ADK.

ITV overvågning af bilpark i Servicegården samt ved cykelskur til elcykler med ADK.

Rumsikring

AIA (Automatisk Indbruds Alarm) aktiveres kl. 23.00-05.00 i følgende områ-der/lokaler:

Rådhushallen, Europa mødelokalet, mødelokale 1609, Kantinen Rådhuskælde-ren, Kantinekøkken, Borgerservice, torve områder fløj 4 og 5 etage 2 og 3 samt Vagtcentralen.

ADK, Salto, ved følgende døre:
Etage 0, fløj 4 og 5 (tillige AIA).
Efter personaleindgang B, dør videre til trappeopgang med konstant lås. Dør til mødelokaler i fløj 6, samt fløj 4 og 5.
Dør til Borgerservice, låses kl. 18.00-05.00.
Dør til mellemgang ved mødelokaler i stueetagen, låses kl. 18.00-05.00.
Byrådets arbejdsværelse, Europaværelset, låst konstant.
Fra Rådhushallens trappeopgang, døre ind til fløj 1, 2, 3, 4, 5 og 6, Digitaliserings-afdelingen, Kontor Borgmester og Kommunaldirektør samt kantine-køkken, låses kl. 18.00-05.00.

ITV indendørs: Indgangsdør B, flugtvejsdør ved Byrådssal, Vagtcentral.

Vagtservice sikringsrum i etage 0: ADK, AIA, tågekanon, ITV i lokalet.

Cellesikring

Smartboard i Europaværelset.

Vagtservice

Døgnbemandet Vagtcentral beliggende i forbindelse med Rådhushallen med ud-syn til Borgerservice. I Rådhusets åbningstid, runderende vagt med særlig fokus på Rådhushal og Borgerservice. Vagten servicerer samtaleanlæg ved indgang A og B, sikrer personlig kontakt for adgang. Vagtservice håndterer overfaldstryk fra sagsbehandlere.

Særlige forhold under den årlige Juletræstænding kl. 17.00-18.00

Hovedindgang og gammel Rådhusindgang åbnes kl. 15.30 for klargøring til ar-rangement for personale og optrædende.
Stationær vagt i Rådhushallen med generelt opsyn, står udenfor under Borg-mestertalen.
Begge indgange lukkes ca. kl. 18.30.
D. 30. november var døren fra Hallens trappeopgang, etage 2, til fløj 4 og 5 defekt og blev ikke låst kl. 18.00.
…"

Datatilsynet stillede den 18. januar 2019 yderligere spørgsmål til Gladsaxe Kommune. Det fremgår af spørgsmål 10 med besvarelse af 21. januar 2019:

"…

10	Af Gladsaxe Kommunes pressemeddelelse af 11. december 2018 fremgår: *"I denne sag er der alene tale om tyveri af en computer og ikke, at oplysninger har været tilgængelige for en bredere offentlighed. Derfor er harddisken og dermed oplysningerne efter al sand synlighed blevet slettet med henblik på videresalg af computeren. Selv i de tilfælde, hvor cpr-numre har været lækket til en større kreds, har der ikke været tilfælde af misbrug af cprnumre".*	Ad a) Kommunen har vurderet, at det forekommer usandsynligt, at nogle vil stjæle en kommunal computer med datatyveri for øje, idet udefrakommende ikke vil vide, at der lå de pågældende data på maskinen. En bærbar computer af den type og alder, der er stjålet, repræsenterer en væsentlig salgsværdi, hvorfor kommunen finder det mest sandsynligt, at tyveriet er sket med henblik på videresalg af computeren. Computeren vil ikke kunne bruges, som den er, da den vil være beskyttet af et password fastsat af kommunen. Der skal derfor laves en fuldstændig reinstallation af computeren, før den kan anvendes. I den forbindelse vil alt indhold på computeren blive slettet. Ad b) Vurderingen bygger bl.a. på den vurdering, vi har fået fra Person 1 PWC I Partner - Cyber & informationssikkerhed — se vedlagte bilag.
1.	a. Gladsaxe Kommune bedes oplyse, hvilken vurdering der ligger til grund for at udtale, at "oplysningerne efter al sandsynlighed [er] blevet slettet med henblik på videresalg af computeren". b. Gladsaxe Kommune bedes samtidig redegøre for, hvad der menes med "Selv i de tilfælde, hvor cpr-numre har været lækket til en større kreds, har der ikke været tilfælde af misbrug af cprnumre".	

…"

Datatilsynet anmeldte den 10. marts 2020 Gladsaxe Kommune til politiet. Det fremgår af anmeldelsen:

"…

Politianmeldelse af Glad saxe Kommune for overtrædelse af databeskyttelsesforordningens ar tikel 32 , stk. 1

Datatilsynet skal hermed anmelde

Gladsaxe Komm une

…

for:

overtrædelse af databeskyttelsesforordningens artikel 32, stk. 1, jf. databeskyt-telseslovens § 41, stk. 1, nr. 1, jf. stk. 3, jf. stk. 6, jf. databeskyttelsesforordnin-gens artikel 83, stk. 2, og stk. 4, litra a, jf. stk. 9,
ved i perioden fra forud for den 30. november 2018 ikke at have overholdt sin forpligtelse som dataansvarlig til at gennemføre tekniske og organisatoriske for-anstaltninger, der passede til risiciene af varierende sandsynlighed og alvor for de registreredes rettigheder, idet Gladsaxe Kommune ikke havde sørget for at kryptere kommunens computere, hvilket medførte et utilstrækkeligt sikkerheds-niveau og tillige havde den konsekvens, at et sikkerhedsbrud medførte en unø-dig høj risiko for de registrerede, idet en medarbejder den 28. november 2018 - i strid med kommunens interne retningslinjer placerede et regneark med perso-noplysninger om 20.620 borgere, herunder oplysninger af følsom karakter og op-lysninger om personnumre på en af kommunens bærbare computere, hvilken computer i perioden fra den 30. november til den 3. december 2018 blev stjålet fra 3. sal, fløj 5, lokale 3525 i Gladsaxe Rådhus, Rådhus Alle 7 i Søborg.
…

3 Datatilsynets vurdering af sagen

3.1 Behandlingssikkerhed

Af databeskyttelsesforordningens artikel 32, stk. 1, fremgår, at den dataansvarli-ge skal gennemføre tekniske og organisatoriske foranstaltninger, der passer til ri-siciene af varierende sandsynlighed og alvor for de registreredes rettigheder.

Der påhviler således den dataansvarlige en pligt til at identificere de risici, den dataansvarliges behandling udgør for de registrerede og til at sikre, at der indfø-res passende sikkerhedsforanstaltninger, der beskytter de registrerede mod disse risici.

Gladsaxe Kommunes computere var alene beskyttet med Windows brugernavn og adgangskode. Computerne var ikke beskyttet med kryptering.

Gladsaxe Kommune har en politik om, at personoplysninger alene må gemmes i journal- eller fagsystemer. Denne politik har været kommunikeret tydeligt ud til kommunens medarbejdere.

En medarbejder gemte alligevel et regneark med personoplysninger på et lokalt drev på en af kommunens computere, som efterfølgende blev stjålet fra rådhuset.

Kravene om et passende sikkerhedsniveau i artikel 32 indebærer, at Gladsaxe Kommune har pligt til at sikre, at de personoplysninger, som behandles af kom-munens ansatte, ikke kommer til uvedkommendes kendskab.

Det er Datatilsynets klare opfattelse, at Gladsaxe Kommune ikke har levet op til kravene om et passende sikkerhedsniveau i databeskyttelsesforordningens arti-kel 32.

Datatilsynet har ved sin vurdering lagt vægt på, at kommunens computere ikke har været beskyttet med kryptering.

Gladsaxe Kommune har i sin redegørelse for behandlingssikkerhed anført, at risikoen for, at kommunens retningslinjer om, at behandling af personoplysninger uden for godkendte journal- og fagsystemer ikke følges af medarbejderne, er vur-deret som forholdsvis lav.

Endvidere har Gladsaxe Kommune i sin redegørelse anført, at kommunen har vurderet, at det var mere væsentligt at beskytte systemer, hvor medarbejderne er blevet instrueret i at gemme oplysninger, snarere end de steder, hvor medarbej-derne ikke bør gemme oplysninger.

Det er Datatilsynets opfattelse, at Gladsaxe Kommunes vurdering af risikoen for, at oplysninger kom til uvedkommendes kendskab var for lav. Det er i den forbin-delse Datatilsynets opfattelse, at særligt kommunens vurdering af at medarbej-derne ikke følger kommunens retningslinjer er åbenbar for lav. En dataansvarlig må påregne, at ikke alle ansatte til enhver tid følger interne retningslinjer.

Datatilsynet har i sin vurdering heraf lagt vægt på, at medarbejdere - i to sager om anmeldte brud på persondatasikkerheden - i strid med kommunens retnings-linjer har placeret filer med personoplysninger på bærbare computeres harddisk, og at medarbejderen i nærværende sag har gjort dette med overlæg.

Datatilsynet skal endvidere påpege, at Gladsaxe Kommunes generelle risikovur-dering i relation til tyveri eller bortkomst af kommunens computere også har væ-ret for lav.

Ved denne vurdering har Datatilsynet lagt vægt på den generelle risiko for tyve-ri, de åbne adgangsforhold, der er på et rådhus og på, at medarbejderne kan bort-tage arbejdscomputere fra arbejdspladsen. Tilsynet har endvidere lagt vægt på, at Gladsaxe Kommune tidligere har oplevet sikkerhedsbrud under lignende om-stændigheder.

Det er almen viden blandt de, der beskæftiger sig professionelt med IT, at det er simpelt at tilgå de filer, der er gemt på computeren, når en computers harddisk ikke er krypteret, f.eks. ved at flytte harddisken til en anden computer. Ved at flytte harddisken til en anden computer, kan man komme uden om både den tek-niske sikkerhedsforanstaltning, der består af Windows brugernavn og adgangs-kode, samt eventuelle adgangskoder opsat i computerens BIOS…

Hertil kommer, at det er tilsynets vurdering, at stjålne mobile enheder i almin-delighed i højere grad end tidligere bliver gennemgået for personoplysninger, som f.eks. kreditkortoplysninger og personnumre, inden disse bortskaffes f.eks. ved videresalg. Dette skyldes til dels det voksende undergrundsmarked, hvor disse typer oplysninger kan videresælges, og dels den øgede digitalisering af samfun-

det i almindelighed, hvormed mulighederne for udnyttelse af personoplysninger vokser.

Kryptering af personoplysninger er en almindeligt anerkendt sikkerhedsforan-staltning, der endda er specifikt nævnt som eksempel på en teknisk foranstalt-ning i artikel 32, stk. 1, litra a.

Henset til de risici for borgerne der knytter sig til kommunens behandling af per-sonoplysninger, er det Datatilsynets opfattelse, at det er særdeles uforsigtigt, at Gladsaxe Kommune ikke havde beskyttet sine computere med kryptering.

Ved denne vurdering har tilsynet lagt vægt på, at en kommune behandler meget store mængder af personoplysninger om kommunens borgere, herunder oplys-ninger af følsom karakter. En borger har ikke mulighed for at fravælge kommu-nens behandling af oplysninger om vedkommende, og kommunen har derfor et stort ansvar for at beskytte borgerne mod, at disse oplysninger kommer til uved-kommendes kendskab.

Efter en samlet vurdering er det således Datatilsynets opfattelse, at Gladsaxe Kommune ikke har været sig sit ansvar bevidst og gennemført passende tekniske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er for de registreredes rettigheder, og at der er tale om en alvorlig overtrædelse af data-beskyttelsesforordningens artikel 32.

Advokatfirma har i sin skrivelse (bilag 10) under pkt. 2.1. an-ført, at der i Datatilsynets vurdering bør lægges vægt på, at oplysningerne er bortkommet ved udefrakommende kriminelles handlinger, og at kommunen er uden skyld i den handling, der indebar, at oplysningerne er bortkommet. I skri-velsen er der under pkt. 3.2 endvidere anført, at strafansvar efter straffelovens § 27, stk. 1, forudsætter, at der er begået en overtrædelse, der kan tilregnes perso-ner tilknyttet kommunen eller kommunen som sådan. Advokatfirma har frem-hævet, at det forhold, at oplysningerne er bortkommet, ikke skyldes den pågæl-dende kommunale medarbejders fejl, som bestod i at gemme personoplysninger lokalt på sin computer, men derimod skyldes tyveri af computeren, som kommu-nen ikke er ansvarlig for.

Datatilsynet skal hertil bemærke, at artikel 32 omhandler de sikkerhedsforan-staltninger den dataansvarlige (Gladsaxe Kommune) skal gennemføre for at sikre et passende sikkerhedsniveau i forhold til de risici for de registreredes rettighe-der, som behandlingen udgør. Disse risici indebærer den ikke usandsynlige risi-ko, at kommunens interne retningslinjer ikke i alle tilfælde rent faktisk følges af medarbejderne, ligesom de også indebærer udefrakommende omstændigheder, som eksempelvis hacking, tyveri, eller at en medarbejder glemmer en computer et offentligt sted, i hvilke situationer kryptering af computerens harddisk ville have været en passende og nødvendig teknisk foranstaltning. Det, der således kan tilregnes kommunen er, at kommunen ikke har opfyldt sine retlige forpligtel-ser i medfør af artikel 32. I den forbindelse skal det præciseres, at sikkerheds-

bruddet blot er et udtryk for nogle af de mulige konsekvenser den utilstrækkeli-ge sikkerhed medfører. Den utilstrækkelige sikkerhed udgør en høj risiko for alle de registrerede, som kommunen behandler oplysninger om.

3.2 Valg af sanktion

Advokatfirma har endelig anført, at grovheden af overtrædel-sen ikke berettiger til en politianmeldelse og har i den forbindelse bl.a. henvist til, at *"det følger af de almindelige bemærkninger til databeskyttelses/oven, at det ikke er en forudsætning, at der pålægges bøde ved alle overtrædelser af databeskyttelsesforordningen og loven. Sagens konkrete momenter kan således trække i en formildende retning. Dette betyder, at der ikke nødvendigvis skal komme en bestemt reaktion, herunder en bøde, ved overtrædelser af forordningen og loven. Tilsynsmyndigheden kan således - alt efter om-stændighederne - beslutte, at en overtrædelse i første omgang sanktioneres med et påbud, og at der først, hvis påbuddet overtrædes, skrides til bødeforelæg efter lovforslagets § 42 eller til politianmeldelse. I valget af sanktion kan tilsynsmyndigheden således f.eks. lægge vægt på,* om *der er tale om en forsætlig eller uagtsom overtrædelse, overtrædelsens karak-ter, alvor og varighed eller eventuelle relevante tidligere overtrædelser, jf. momenterne opregnet* i *artikel 83, stk. 2."*

I den forbindelse skal det oplyses, at Datatilsynet altid foretager en konkret vur-dering af sagens grovhed ved vurderingen af hvilken sanktion, der efter tilsynets opfattelse er den korrekte.

Datatilsynet har ved vurderingen af sanktion lagt vægt på, at Gladsaxe Kommu-ne behandler meget store mængder af fortrolige og følsomme oplysninger. Tilsy-net har endvidere lagt vægt på, at der er tale om manglende implementering af en generel foranstaltning, og at Gladsaxe Kommune tidligere har oplevet sikker-hedsbrud under lignende omstændigheder. Det er således Datatilsynets opfattel-se, at der er tale om en meget alvorlig overtrædelse, der skal sanktioneres med bøde.
…"

Københavns Vestegns Politi sigtede den 30. marts 2020 Gladsaxe Kommune i overensstemmelse med den anmeldelse, der var modtaget fra Datatilsynet.

Sagsøgernes advokat skrev den 25. marts 2019 på vegne af Sagsøger 1, den 16. april 2019 på vegne af Sagsøger 2, den 10. oktober 2019 på vegne af Sagsøger 3, den 26. april 2019 på vegne af Sagsøger 4, den 20. maj 2019 på vegne af Sagsøger 5, den 16. april 2019 på vegne af Sagsøger 6 og den 26. april 2019 på vegne af Sagsøger 7 til Gladsaxe Kommune med krav om erstatning, der skulle forrentes fra weekenden mellem uge 48 og 49 2018, subsidiært blev der afgivet rentepå-krav.

Gladsaxe Kommune afviste kravene.

Det fremgår om Sagsøger 3's sag, BS-49315/2019-GLO, at der den 11. marts 2019 blev bestilt nyt nøglekort til hendes NemID. Det fremgår blandt an-det videre af hendes NemID oplysninger, at der den 12. marts 2019 blev udstedt nyt nøglenummer. Den 18. marts 2019 blev der fra Sagsøger 3's konto overført henholdsvis 50.000 kr. og 45.000 kr. til andre konti. Sagsøger 3's bank har dækket beløbene. Det fremgår videre af hendes NemID op-lysninger, at brugeren den 18. marts 2020 ikke kunne autentificeres på grund af forkert adgangskode, hvorefter adgangskoden blev spærret med meddelelse til en mailadresse. Det fremgår af oplysninger fra Sagsøger 3's mobiltele-fonselskab, at skift af hendes SIM-kort blev igangsat den 18. marts 2019 efter en telefonisk henvendelse, hvor personen, der ringede, formodes at være blevet verificeret ved oplysning om kundenummer eller CPR-nummer.

Det fremgår om Sagsøger 4's sag, BS-51045/2019-GLO, at der ved op-slag på institutionen Egebos hjemmeside, www.ege-bo.dk, fremgår, at institu-tionen er et unikt, psykosocialt rehabiliteringstilbud, der henvender sig til per-soner over 18 år med psykisk funktionsnedsættelse, ofte med en diagnose in-denfor skizofrenispektret.

Det fremgår om Sagsøger 5's sag, BS 51234/2019-GLO, at hendes Ne-mID af sikkerhedsmæssige årsager blev spærret af Nets den 26. august 2020. Det fremgår af Nets´ brev af 28. august 2020, at baggrunden for spærringen var en mistanke om, at hun havde været udsat for et vellykket phising-angreb, og at it-kriminelle dermed havde fået adgang til hendes bruger-id, adgangskode og nøglerne på hendes nøglekort. Det er oplyst, at hun har navne- og adressebe-skyttelse.

Retsgrundlaget

Af Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personop-lysninger og om fri udveksling af sådanne oplysninger og om ophævelse af di-rektiv 95/46/EF (generel forordning om databeskyttelse) fremgår blandt andet:

> ” EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —
>
> under henvisning til traktaten om Den Europæiske Unions funktionsmåde, sær-lig artikel 16,
>
> under henvisning til forslag fra Europa-Kommissionen,
>
> efter fremsendelse af udkast til lovgivningsmæssig retsakt til de nationale parla-menter,

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg ([1]),

under henvisning til udtalelse fra Regionsudvalget ([2]),

efter den almindelige lovgivningsprocedure ([3]), og

ud fra følgende betragtninger:

(1) Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger er en grundlæggende rettighed. I artikel 8, stk. 1, i Den Europæi-ske Unions charter om grundlæggende rettigheder (»chartret«) og i artikel 16, stk. 1, i traktaten om Den Europæiske Unions funktionsmåde (TEUF) fastsættes det, at enhver har ret til beskyttelse af personoplysninger, der vedrører den pågældende.

(2) Principperne og reglerne for beskyttelse af fysiske personer i forbindelse med behandling af deres personoplysninger bør, uanset deres nationalitet eller bopæl, respektere deres grundlæggende rettigheder og frihedsrettig-heder, navnlig deres ret til beskyttelse af personoplysninger. Denne for-ordning har til formål at bidrage til skabelsen af et område med frihed, sikkerhed og retfærdighed samt en økonomisk union og til økonomiske og sociale fremskridt, styrkelse af og konvergens mellem økonomierne in-den for det indre marked og fysiske personers velfærd.

…

(4) Behandling af personoplysninger bør have til formål at tjene menneske-heden. Retten til beskyttelse af personoplysninger er ikke en absolut ret; den skal ses i sammenhæng med sin funktion i samfundet og afvejes i for-hold til andre grundlæggende rettigheder i overensstemmelse med pro-portionalitetsprincippet. Denne forordning overholder alle de grundlæg-gende rettigheder og følger de frihedsrettigheder og principper, der aner-kendes i chartret som forankret i traktaterne, navnlig respekten for pri-vatliv og familieliv, hjem og kommunikation, beskyttelsen af personop-lysninger, retten til at tænke frit, til samvittigheds- og religionsfrihed, yt-rings- og informationsfrihed, frihed til at oprette og drive egen virksom-hed, adgang til effektive retsmidler og til en retfærdig rettergang og kul-turel, religiøs og sproglig mangfoldighed.

…

(7) Denne udvikling kræver en stærk og mere sammenhængende databe-skyttelsesramme i Unionen, som understøttes af effektiv håndhævelse, fordi det er vigtigt at skabe den tillid, der gør det muligt, at den digitale økonomi kan udvikle sig på det indre marked. Fysiske personer bør ha-ve kontrol over deres personoplysninger. Sikkerheden både retligt og praktisk bør styrkes for fysiske personer, erhvervsdrivende og offentlige myndigheder.

…

(10) For at sikre et ensartet og højt niveau for beskyttelse af fysiske personer og for at fjerne hindringerne for udveksling af personoplysninger inden for Unionen bør beskyttelsesniveauet for fysiske personers rettigheder og frihedsrettigheder i forbindelse med behandling af sådanne oplysnin-ger være ensartet i alle medlemsstater. Det bør sikres, at reglerne for be-skyttelse af fysiske personers grundlæggende rettigheder og frihedsret-tigheder i forbindelse med behandling af personoplysninger anvendes konsekvent og ensartet overalt i Unionen. I forbindelse med behandling af personoplysninger for at overholde en retlig forpligtelse eller for at udføre en opgave i samfundets interesse, eller som henhører under of-fentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt, bør medlemsstaterne kunne opretholde eller indføre nationale bestem-melser for yderligere at præcisere anvendelsen af denne forordnings be-stemmelser. Sammen med generel og horisontal lovgivning om databe-skyttelse til gennemførelse af direktiv 95/46/EF har medlemsstaterne fle-re sektorspecifikke love på områder, hvor der er behov for mere speci-fikke bestemmelser. Denne forordning indeholder også en manøvremar-gen, så medlemsstaterne kan præcisere reglerne heri, herunder for be-handling af særlige kategorier af personoplysninger (»følsomme oplys-ninger«). Denne forordning udelukker således ikke, at medlemsstaternes nationale ret fastlægger omstændighederne i forbindelse med specifikke databehandlingssituationer, herunder mere præcis fastlæggelse af de forhold, hvorunder behandling af personoplysninger er lovlig.

…

(35) Helbredsoplysninger bør omfatte alle personoplysninger om den registre-redes helbredstilstand, som giver oplysninger om den registreredes tidli-gere, nuværende eller fremtidige fysiske eller mentale helbredstilstand. Dette omfatter oplysninger om den fysiske person indsamlet i løbet af re-gistreringen af denne med henblik på eller under levering af sundhedsy-delser, jf. Europa-Parlamentets og Rådets direktiv 2011/24/EU [(9)], til den fysiske person; et nummer, symbol eller særligt mærke, der tildeles en fy-sisk person for entydigt at identificere den fysiske person til sundhedsfor-mål; oplysninger, der hidrører fra prøver eller undersøgelser af en legem-sdel eller legemlig substans, herunder fra genetiske data og biologiske prøver; og enhver oplysning om f.eks. en sygdom, et handicap, en syg-domsrisiko, en sygehistorie, en sundhedsfaglig behandling eller den regi-streredes fysiologiske eller biomedicinske tilstand uafhængigt af kilden hertil, f.eks. fra en læge eller anden sundhedsperson, et hospital, medi-cinsk udstyr eller in vitro-diagnostik.

…

(39) Enhver behandling af personoplysninger bør være lovlig og rimelig. Det bør være gennemsigtigt for de pågældende fysiske personer, at perso-noplysninger, der vedrører dem, indsamles, anvendes, tilgås eller på an-den vis behandles, og i hvilket omfang personoplysningerne behandles eller vil blive behandlet. Princippet om gennemsigtighed tilsiger, at en-

hver information og kommunikation vedrørende behandling af disse personoplysninger er lettilgængelig og letforståelig, og at der benyttes et klart og enkelt sprog. Dette princip vedrører navnlig oplysningen til de registrerede om den dataansvarliges identitet og formålene med den på-gældende behandling samt yderligere oplysninger for at sikre en rimelig og gennemsigtig behandling for de berørte fysiske personer og deres ret til at få bekræftelse og meddelelse om de personoplysninger vedrørende dem, der behandles. Fysiske personer bør gøres bekendt med risici, reg-ler, garantier og rettigheder i forbindelse med behandling af personop-lysninger og med, hvordan de skal udøve deres rettigheder i forbindelse med en sådan behandling. Især bør de specifikke formål med behandlin-gen af personoplysninger være udtrykkelige og legitime og fastlagt, når personoplysningerne indsamles. Personoplysningerne bør være til-strækkelige, relevante og begrænset til, hvad der er nødvendigt i for-hold til formålene med deres behandling. Dette kræver navnlig, at det sikres, at perioden for opbevaring af personoplysningerne ikke er læn-gere end strengt nødvendigt. Personoplysninger bør kun behandles, hvis formålet med behandlingen ikke med rimelighed kan opfyldes på anden måde. For at sikre, at personoplysninger ikke opbevares i længere tid end nødvendigt, bør den dataansvarlige indføre tidsfrister for slet-ning eller periodisk gennemgang. Der bør træffes enhver rimelig foran-staltning for at sikre, at personoplysninger, som er urigtige, berigtiges eller slettes. Personoplysninger bør behandles på en måde, der garante-rer tilstrækkelig sikkerhed og fortrolighed, herunder for at hindre uau-toriseret adgang til eller anvendelse af personoplysninger eller af det udstyr, der anvendes til behandlingen.

…

(74) Der bør fastsættes bestemmelser om den dataansvarliges ansvar, herun-der erstatningsansvar, for enhver behandling af personoplysninger, der foretages af den dataansvarlige eller på den dataansvarliges vegne. Den dataansvarlige bør navnlig have pligt til at gennemføre passende og ef-fektive foranstaltninger og til at påvise, at behandlingsaktiviteter over-holder denne forordning, herunder foranstaltningernes effektivitet. Dis-se foranstaltninger bør tage højde for behandlingens karakter, omfang, sammenhæng og formål og risikoen for fysiske personers rettigheder og frihedsrettigheder.

(75) Risiciene for fysiske personers rettigheder og frihedsrettigheder, af varie-rende sandsynlighed og alvor, kan opstå som følge af behandling af per-sonoplysninger, der kan føre til fysisk, materiel eller immateriel skade, navnlig hvis behandlingen kan give anledning til forskelsbehandling, identitetstyveri eller -svig, finansielle tab, skade på omdømme, tab af for-trolighed for personoplysninger, der er omfattet af tavshedspligt, uautori-seret ophævelse af pseudonymisering eller andre betydelige økonomiske eller sociale konsekvenser; hvis de registrerede kan blive berøvet deres rettigheder og frihedsrettigheder eller forhindret i at udøve kontrol med deres personoplysninger; hvis der behandles personoplysninger, der viser

race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold, og behandling af genetiske data, helbredsoplysninger eller oplysninger om seksuelle forhold eller straffedom-me og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger; hvis personlige forhold evalueres, navnlig analyse eller forudsigelse af forhold vedrørende indsats på arbejdspladsen, økonomisk situation, helbred, personlige præferencer eller interesser, pålidelighed eller adfærd eller geo-grafisk position eller bevægelser, med henblik på at oprette eller anvende personlige profiler; hvis der behandles personoplysninger om sårbare fy-siske personer, navnlig børn; eller hvis behandlingen omfatter en stor mængde personoplysninger og berører et stort antal registrerede

…

(83) For at opretholde sikkerheden og hindre behandling i strid med denne forordning bør den dataansvarlige eller databehandleren vurdere de risici, som en behandling indebærer, og gennemføre foranstaltninger, der kan begrænse disse risici, som f.eks. kryptering. Disse foranstaltninger bør under hensyntagen til det aktuelle tekniske niveau og implementeringsomkostningerne sikre et tilstrækkeligt sikkerhedsniveau, herunder fortrolighed, i forhold til risiciene og karakteren af de personoplysninger, der skal beskyttes. Ved vurderingen af datasikkerhedsrisikoen bør der tages hensyn til de risici, som behandling af personoplysninger indebærer, såsom hændelig eller ulovlig tilintetgørelse, tab, ændring eller uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet, og som navnlig kan føre til fysisk, materiel eller immateriel skade.

…

(85) Et brud på persondatasikkerheden kan, hvis det ikke håndteres på en passende og rettidig måde, påføre fysiske personer fysisk, materiel eller immateriel skade, såsom tab af kontrol over deres personoplysninger eller begrænsning af deres rettigheder, forskelsbehandling, identitetstyveri eller -svig, finansielle tab, uautoriseret ophævelse af pseudonymisering, skade på omdømme, tab af fortrolighed for oplysninger, der er omfattet af tavshedspligt, eller andre betydelige økonomiske eller sociale konsekvenser for den berørte fysiske person. Så snart den dataansvarlige bliver bekendt med, at der er sket et brud på persondatasikkerheden, bør vedkommende derfor anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed uden unødig forsinkelse og om muligt senest 72 timer efter, at denne er blevet bekendt med det, medmindre den dataansvarlige i overensstemmelse med ansvarlighedsprincippet kan påvise, at bruddet på persondatasikkerheden sandsynligvis ikke indebærer risiko for fysiske personers rettigheder eller frihedsrettigheder. Hvis en sådan anmeldelse ikke kan ske inden for 72 timer, bør den ledsages af en begrundelse for forsinkelsen, og oplysningerne kan indgives trinvis uden unødig yderligere forsinkelse.

…

(146) Den dataansvarlige eller databehandleren bør yde erstatning for enhver skade, som en person måtte lide som følge af behandling, der overtræder denne forordning. Den dataansvarlige eller databehandleren bør være fri-taget for erstatningsansvar, hvis den pågældende beviser ikke at være an-svarlig for den forvoldte skade. Begrebet »skade« bør fortolkes bredt i ly-set af retspraksis ved Domstolen, således at det fuldt ud afspejler formåle-ne for denne forordning. Dette berører ikke eventuelle erstatningskrav for skade som følge af overtrædelse af andre bestemmelser i EU-retten eller medlemsstaternes nationale ret. Behandling, der overtræder denne for-ordning, omfatter også behandling, der overtræder delegerede retsakter og gennemførelsesretsakter vedtaget i henhold til denne forordning og til medlemsstaternes nationale ret, der præciserer bestemmelserne i denne forordning. Registrerede bør have fuld erstatning for den skade, som de har lidt. Hvis dataansvarlige eller databehandlere er involveret i den sam-me behandling, bør den enkelte dataansvarlige eller databehandler hæfte for hele erstatningen. Hvis de imidlertid er inddraget i den samme retssag i overensstemmelse med medlemsstaternes nationale ret, kan erstatning fordeles i henhold til den enkelte dataansvarliges eller databehandlers an-svar for den skade, der er forvoldt af behandlingen, forudsat at der sikres fuld erstatning til den registrerede, som har lidt skaden. Enhver dataansvarlig eller databehandler, der har betalt fuld erstatning, kan efter-følgende gøre regres mod andre dataansvarlige eller databehandlere, der er involveret i samme behandling.

…

KAPITEL I
Generelle bestemmelser

Artikel 1

Genstand og formål

1. I denne forordning fastsættes regler om beskyttelse af fysiske personer i for-bindelse med behandling af personoplysninger og regler om fri udveksling af personoplysninger.

2. Denne forordning beskytter fysiske personers grundlæggende rettigheder og frihedsrettigheder, navnlig deres ret til beskyttelse af personoplysninger.

3. Den frie udveksling af personoplysninger i Unionen må hverken indskrænkes eller forbydes af grunde, der vedrører beskyttelse af fysiske personer i forbindel-se med behandling af personoplysninger.

…

KAPITEL II
Principper

Artikel 5

Principper for behandling af personoplysninger

1. Personoplysninger skal:

a) behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede (»lovlighed, rimelighed og gennemsigtighed«)

b) indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål; viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, skal ikke anses for at være uforenelig med de oprindelige formål (»formålsbegrænsning«)

c) være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles (»dataminimering«)

d) være korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, straks slettes eller berigtiges (»rigtighed«)

e) opbevares på en sådan måde, 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; personoplysninger kan opbevares i længere tidsrum, hvis personoplysningerne alene behandles til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, under forudsætning af, at der implementeres passende tekniske og organisatoriske foranstaltninger, som denne forordning kræver for at sikre den registreredes rettigheder og frihedsrettigheder (»opbevaringsbegrænsning«)

f) 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 (»integritet og fortrolighed«).

2. Den dataansvarlige er ansvarlig for og skal kunne påvise, at stk. 1 overholdes (»ansvarlighed«).

…

Artikel 32

Behandlingssikkerhed

1. 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 gennemfører den dataansvarlige og databe-

handleren 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.

2. Ved vurderingen af, hvilket sikkerhedsniveau der er passende, tages der navnlig hensyn til de risici, som behandling 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.

3. Overholdelse af en godkendt adfærdskodeks som omhandlet i artikel 40 eller en godkendt certificeringsmekanisme som omhandlet i artikel 42 kan bruges som et element til at påvise overholdelse af kravene i nærværende artikels stk. 1.

4. Den dataansvarlige og databehandleren tager skridt til at sikre, at enhver fysisk person, der udfører arbejde for den dataansvarlige eller databehandleren, og som får adgang til personoplysninger, kun behandler disse efter instruks fra den dataansvarlige, medmindre behandling kræves i henhold til EU-retten eller medlemsstaternes nationale ret.

…

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.

2. Enhver dataansvarlig, der er involveret i behandling, hæfter for den skade, der er forvoldt af behandling, der overtræder denne forordning. En databehandler hæfter kun for den skade, der er forvoldt af behandling, hvis pågældende ikke har opfyldt forpligtelser i denne forordning, der er rettet specifikt mod databehandlere, eller hvis pågældende har undladt at følge eller handlet i strid med den dataansvarliges lovlige instrukser.

3. En dataansvarlig eller databehandler er fritaget for erstatningsansvar i henhold til stk. 2, hvis det bevises, at den pågældende ikke er skyld i den begivenhed, der medførte skaden.

4. Hvis mere end én dataansvarlig eller databehandler eller både en dataansvarlig og en databehandler er involveret i den samme behandling, og hvis de i henhold til stk. 2 og 3 er ansvarlige for skader, der er forvoldt af behandling, hæfter de solidarisk for hele skaden for at sikre fuld erstatning til den registrerede.

5. Hvis en dataansvarlig eller en databehandler i overensstemmelse med stk. 4 har betalt fuld erstatning for den forvoldte skade, har den pågældende dataansvarlige eller databehandler ret til at kræve den del af erstatningen, der svarer til andres del af ansvaret for skaden, tilbage fra de andre dataansvarlige eller databehandlere, der er involveret i den samme behandling, i overensstemmelse med betingelserne i stk. 2.

6. Retssager med henblik på udøvelse af retten til at modtage erstatning anlægges ved de domstole, der er kompetente i henhold til national ret i den medlemsstat, der er omhandlet i artikel 79, stk. 2.

…"

Af kommissionens forslag af 25. januar 2012 til EUROPA-PARLAMENTETS OG RÅDETS FORORDNING om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (generel forordning om databeskyttelse) /* COM/2012/011 final - 2012/0011 (COD) fremgår blandt andet

"…

3.4.8. KAPITEL VIII - KLAGEADGANG, ANSVAR OG SANKTIONER

…

Artikel 77 omhandler retten til erstatning og ansvar. Den er baseret på artikel 23 i direktiv 95/46/EF, udvider retten til erstatning for den forvoldte skade fra registerførere og præciserer ansvaret for fælles registeransvarlige og fælles registerførere.

…

(118) Personer, der lider skade som følge af en ulovlig behandling, bør have ret til erstatning fra den registeransvarlige eller registerføreren. Denne kan fritages for erstatningsansvar, hvis det bevises, at han ikke er skyld i den forvoldte skade, navnlig hvis der kan henvises til en fejl fra den registreredes side eller et tilfælde af force majeure.

…

Artikel 77 Ret til erstatning og erstatningsansvar

1. Enhver, som har lidt skade som følge af en ulovlig behandling eller enhver anden handling, der er uforenelig med denne forordning, har ret til erstatning for den forvoldte skade fra den registeransvarlige eller registerføreren.

..."

Af lov nr. 502 af 23. maj 2018 – Databeskyttelsesloven – fremgår blandt andet:

> "…
> *§ 1*
> Loven supplerer og gennemfører Europa-Parlamentets og Rådets forordning nr. 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordningen), jf. bilag 1 til denne lov.
>
> …
> *§ 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."

Af lovforslaget til Databeskyttelsesloven, LFF 2017-10-25 nr. 68, fremgår blandt andet:

> "…
> *Til § 40*
>
> Bestemmelsen er en ordret gennemførelse af forordningens artikel 82, stk. 1. Som det fremgår af betænkningen, side 917, udvider forordningsbestemmelsen gældende ret, ved at databehandleren også kan være erstatningsansvarlig. Derudover præciserer bestemmelsen ordlydsmæssigt, at der er ret til erstatning for materiel og immateriel skade, hvilket dog - som det fremgår samme sted i betænkningen - må antages at svare til gældende ret.
>
> Derudover fastsætter forordningens artikel 82, stk. 2 og 3, at der fortsat gælder et præsumptionsansvar.
>
> Det præciseres i forordningens artikel 82, stk. 4 og 5, at såfremt der er flere erstatningsansvarlige, hæfter de solidarisk med mulighed for regres.
>
> Der henvises om forordningens artikel 82 i det hele til betænkningen, side 910-918.
>
> Der henvises i øvrigt til afsnit 2.8. i lovforslagets almindelige bemærkninger.
>
> …"

Af betænkning nr. 1565/2017 om Databeskyttelsesforordningen (2016/679) fremgår blandt andet:

> "…

1.7. Betænkningens retlige status

Betænkningens analyser er baseret på eksisterende retskilder. Betænkningen vil således ikke stå alene som fortolkningsbidrag *fremover*.

Hvor retstilstanden ikke kan anses for entydig, indeholder betænkningen i vidt omfang forslag til *mulige løsninger.*

Det må forventes, at fortolkningen af forordningen på flere punkter i de kom-mende år vil blive udviklet gennem praksis fra bl.a. det med forordningen nyop-rettede Europæiske Databeskyttelsesråd, EU-Domstolen, de danske domstole og Datatilsynet.

Den nuværende retstilstand er f.eks. baseret på meget få domme, og det må for-ventes, at der fremover vil komme flere domme fra bl.a. EU-Domstolen.

I det omfang, der kommer bindende afgørelser fra EU-Domstolen, nationale domstole, Databeskyttelsesrådet og den uafhængige tilsynsmyndighed mv., skal betænkningens analyser naturligvis læses i lyset af den nye praksis.

…

9.6. Ret til erstatning og erstatningsansvar, artikel 82

9.6.1. Præsentation

Databeskyttelsesforordningens artikel 82 , stk. 1 og 2, fastsætter regler om retten til erstatning og om dataansvarliges og databehandleres erstatningsansvar.

Derudover fastsætter forordningens artikel 82, stk. 3-6, et præsumptionsansvar (culpa med omvendt bevisbyrde), solidarisk hæftelse, såfremt der er mere end én dataansvarlig eller databehandler, hvornår udbetalt erstatning kan kræves tilba-gebetalt fra andre involverede (regression), samt hvor en erstatningssag skal an-lægges.

9.6.2. Gældende ret

9.6.2.1. Databeskyttelsesdirektivet

Det følger af artikel 23, stk. 1, i databeskyttelsesdirektivets, at medlemsstaterne fastsætter regler om, at enhver, som har lidt skade, som følge af en ulovlig be-handling eller anden behandling, der er uforenelig med de nationale bestemmel-ser, der vedtages til gennemførelse af dette direktiv, har ret til erstatning for den forvoldte skade fra den dataansvarlige.

Det følger af direktivets artikel 23, stk. 2, at den dataansvarlige helt eller delvist kan fritages for erstatningsansvar for skade, hvis han beviser, at han ikke er skyld i den begivenhed, der medførte skaden.

Af direktivets præambelbetragtning nr. 55 følger det, at personer, som lider ska-de som følge af en ulovlig behandling, skal have ret til erstatning fra den dataansvarlige, og at der skal iværksættes sanktioner over for såvel privatretlige som offentlige personer, der overtræder nationale bestemmelser vedtaget med henblik på gennemførelsen af dette direktiv.

9.6.2.2. EU-retlig retspraksis

EU-Domstolen har i en række sager fortolket begrebet "skade" , herunder hvor-vidt og i hvilke situationer begrebet, foruden økonomisk skade, også omfatter ik-ke-økonomisk skade.

I sag C-168/00, Leitner, dom af 12. marts 2002, havde en person købt en pakkerej-se og blev i forbindelse med afholdelsen af denne syg med symptomer på salmo-nellaforgiftning.

EU-Domstolen udtalte i præmis 19, at [pakkerejse]direktivets[note 872] artikel 5, stk. 2, 1. afsnit, forpligter medlemsstaterne til at træffe de nødvendige foranstaltnin-ger til at sikre, at rejsearrangøren erstatter "de skader, der påføres forbrugeren som følge af manglende eller mangelfuld opfyldelse af kontrakten" .

EU-Domstolen udtalte endvidere i præmis 21, at det imidlertid står fast, at hvis der inden for pakkerejseområdet i visse medlemsstater var en forpligtelse til at erstatte ikke-økonomiske skader, og der ikke var en sådan forpligtelse i andre medlemsstater, ville dette medføre væsentlige konkurrenceforvridninger, da der
- som Kommissionen også anførte i sagen - ofte konstateres ikke-økonomiske skader inden for dette område.

EU-Domstolen udtalte endelig i præmis 23 bl.a., at selv om artikel 5, stk. 2, 1. af-snit, begrænser sig til generelt at henvise til begrebet "skader" , skal det bemær-kes, at idet artikel 5, stk. 2, 4. afsnit, fastsætter muligheden for, at medlemsstater-ne for så vidt angår andre skader end legemlige skader kan tillade, at erstatnin-gen begrænses i henhold til kontrakten under forudsætning af, at begrænsningen ikke er urimelig, anerkender direktivet stiltiende et krav på godtgørelse for andre skader end legemlige skader, herunder ikke-økonomisk skade.

I sag C-277/12, Drozdovs, dom af 24. oktober 2013, omkom sagsøgers forældre i et trafikuheld, hvilket medførte at sagsøger anmodede forsikringsselskabets om og her fik udbetalt en erstatning, hvis størrelse sagsøger var uenig i.

EU-Domstolen udtalte i præmis 38, at det, henset til de forskellige sprogversioner af andet direktivs[note 873] artikel 1, stk. 1, og tredje direktivs[note 874] artikel 1, stk. 1, samt de tre ovennævnte direktivers beskyttelsesformål, måtte fastslås, at omfattet af begrebet "personskade" var ethvert tab, i det omfang der blev foreskrevet en erstatning herfor i medfør af den forsikredes erstatningsansvar i henhold til de *nationale* bestemmelser, der fandt anvendelse på tvisten, som følge af en krænkel-se af personens integritet, hvilket omfattede såvel fysiske som psykiske lidelser.

EU-Domstolen udtalte endvidere i præmis 40, at da de forskellige sprogversioner af andet direktivs artikel 1, stk. 1, i det væsentlige anvender begreberne såvel "legemsskade" som "personskade" , må man henholde sig til den almindelige opbygning af og formålet med disse bestemmelser og direktivet. Det bemærkes her ved, at disse begreber supplerer begrebet "materiel skade" , og at de nævnte bestemmelser og direktivet navnlig tilsigter at styrke beskyttelse af ofrene. Herefter må der anlægges den brede fortolkning af de nævnte begreber, som er anført i denne doms præmis 38.

EU-Domstolen udtalte ydermere i præmis 41, at det heraf [af det brede skadesbegreb] følger, at immaterielle skader, for hvilke der foreskrives en erstatning i medfør af den forsikredes erstatningsansvar i henhold til de *nationale* bestemmel-ser, der finder anvendelse på tvisten, er blandt de skader, som der skal betales er-statning for i overensstemmelse med første, andet og tredje direktiv.

EU-Domstolen udtalte endelig i præmis 44, at eftersom skadesbegrebet i første direktivs[note 875] artikel 1, nr. 2, ikke var yderligere begrænset, var der desuden, i modsætning til hvad den lettiske og litauiske regering havde anført, intet grund-lag for at antage, at visse skader, såsom immaterielle skader, i det omfang der skulle betales erstatning herfor i henhold til de *nationale* bestemmelser om erstatningsansvar, som fandt anvendelse, skulle udelukkes fra dette begreb. Af første direktivs artikel 1, nr. 2, fremgår det, at skadelidte er enhver person, der har ret til erstatning for skade forvoldt af et køretøj.

Det samme følger af C-22/12, Hassová, afgjort af EU-Domstolen samme dag, 24. oktober 2013. Derudover er samme fortolkning anlagt i sag C-371/12, Petillo, dom af 23. januar 2014, hvor sagsøger blev påkørt, hvilket medførte legemsbeskadigel-se.

EU-Domstolen synes ikke at have en konsekvent linje i fortolkningen af begrebet "skade" . Af domspraksis kan det således umiddelbart både udledes, at der af pakkerejsedirektivets skadesbegreb kan fortolkes et krav på godtgørelse for ikke-økonomisk skade, og at EU-Domstolen ved nyere praksis alene, ud af de direkti-ver, der regulerer ansvarsforsikring for motorkøretøjer, fortolker skadesbegrebet til at inkludere et krav om godtgørelse for ikke-økonomisk skade, hvis dette føl-ger af de nationale bestemmelser.

9.6.2.3. EU-lovgivningspraksis om begreberne erstatning og godtgørelse

Begrebet "erstatning" er bl.a. reguleret i artikel 13 i direktiv om håndhævelse af intellektuelle rettigheder[note 876] , der har overskriften erstatning.

Af artikel 13, stk. 1, fremgår det, at medlemsstaterne sikrer, at de kompetente retslige myndigheder på begæring af den forurettede pålægger den krænkende part, der vidste eller med rimelighed burde vide, at hans aktiviteter medførte en

sådan krænkelse, at betale rettighedshaveren en erstatning, der står i rimeligt for-hold til det tab, denne har lidt som følge af krænkelsen.

Når de retslige myndigheder fastsætter erstatningen,

a) skal de tage hensyn til alle relevante aspekter, såsom negative økonomiske konsekvenser, herunder tabt fortjeneste, som den forurettede har lidt, den krænkende parts uberettigede fortjeneste, og, når det er hensigtsmæssigt, andre ele-menter end de økonomiske, f.eks. den ikke-økonomiske skade, rettighedshaveren har lidt som følge af krænkelsen

b) eller de kan, som et alternativ til litra a), når det er hensigtsmæssigt, fastsætte erstatningen til et fast beløb på grundlag af elementer, der som minimum svarer til størrelsen af de gebyrer eller afgifter, som den krænkende part skulle have be-talt, hvis han havde anmodet om tilladelse til at anvende den pågældende intel-lektuelle ejendomsrettighed.

Ligebehandlingsdirektivets (direktiv 2006/54/EF) artikel 18 bærer overskriften "erstatning eller godtgørelse" . I den engelske sprogversion bærer artikel 18 overskriften "compensation or reparation" . Af direktivets artikel 18, 1. pkt., følger det, at medlemsstaterne i deres nationale retsorden indfører de nødvendige be-stemmelser for at sikre en reel og effektiv erstatning eller godtgørelse efter med-lemsstatens afgørelse for tab og skader, der er påført en person som følge af en forskelsbehandling på grundlag af køn, således at det har en præventiv virkning og står i et rimeligt forhold til det tab, den pågældende har lidt.

Af ligebehandlingsdirektivets præambelbetragtning nr. 33, fremgår det bl.a., at EU-Domstolen klart har fastslået, at for, at princippet om ligebehandling kan væ-re effektivt, skal den erstatning, der tildeles i tilfælde af overtrædelse, være tilstrækkelig i forhold til det tab, den pågældende har lidt.

…

9.6.3. Databeskyttelsesforordningen

Det fremgår af begrundelsen til forslaget til databeskyttelsesforordningen , at forordningens artikel 82 (som var en del af artikel 77 i forslaget) udvider retten til erstatning for den forvoldte skade fra dataansvarlige og databehandlere og præciserer ansvaret for solidarisk hæftelse og regression.[note 894]

Det følger af forordningens præambelbetragtning nr. 147, at når forordningen indeholder specifikke kompetenceregler, navnlig for så vidt angår sager om ad-gang til retsmidler, herunder erstatning, mod en dataansvarlig eller databehandler, bør de almindelige kompetenceregler i Europa-Parlamentets og Rådets forordning (EU) nr. 1215/2012 ikke berøre anvendelsen af sådanne specifikke regler.

9.6.3.1. Databeskyttelsesforordningens artikel 82, stk. 1

Det følger af forordningens artikel 82, stk. 1, at 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.

Forordningens artikel 82, stk. 1, ses i vidt omfang at videreføre retten til erstat-ning i direktivets artikel 23.

Det følger bl.a. af præambelbetragtning nr. 146, at begrebet "skade" bør fortolkes bredt i lyset af retspraksis ved Domstolen, således at det fuldt ud afspejler formålene for denne forordning. Det fremgår endvidere af betragtningen, at dette ikke berører eventuelle erstatningskrav for skade som følge af overtrædelse af andre bestemmelser i EU-retten eller medlemsstaternes nationale ret, at behandling, der overtræder denne forordning, også omfatter behandling, der overtræder delege-rede retsakter og gennemførelsesretsakter vedtaget i henhold til denne forord-ning og til medlemsstaternes nationale ret, der præciserer bestemmelserne i den-ne forordning, og at registrerede bør have fuld erstatning for den skade, som de har lidt.

Det fremgår nu eksplicit i forordningen, at der skal gælde et erstatningsansvar for *materiel* eller *immateriel* skade, hvor direktivet alene nævner *skade.* Materiel skade er, som nævnt ovenfor, allerede omfattet af persondatalovens § 69 , hvis et økonomisk tab kan konstateres. Derudover må immateriel skade også anses for at være omfattet af persondatalovens § 69 , i de tilfælde, hvor et økonomisk tab kan konstateres, hvilket efter omstændighederne kan være et tab i form af mistet omsætning, jf. U 2007.1603 S, refereret ovenfor. Dette kunne eksempelvis være tilfældet ved en uberettiget offentliggørelse af personoplysninger, som er en immateriel skade, der kan medføre erstatning, hvis der kan dokumenteres at være lidt et økonomisk tab, herunder et omsætningstab.

Det følger ikke nærmere af ordlyden af artikel 82, stk. 1, hvad der må forstås ved begreberne materiel eller immateriel skade. Det følger dog, at begrebet "skade" , i lyset af retspraksis ved EU-Domstolen, skal fortolkes bredt, således at det afspej-ler formålene i forordningen. På området for pakkerejser har EU-Domstolen for-tolket begrebet "skade" til også at omfatte godtgørelse for ikke-økonomisk skade. EU-Domstolen har dog i nyere praksis ved udmåling af erstatning i forbindelse med trafikuheld fortolket dette til alene at gælde i det omfang, der blev foreskre-vet en erstatning herfor i medfør af den forsikredes erstatningsansvar i henhold til de nationale bestemmelser, der fandt anvendelse på tvisten, jf. den refererede retspraksis fra EU-Domstolen. Det fremstår ikke klart, hvad der må forstås ved en bred fortolkning af begrebet "skade" i EU-Domstolens praksis, jf. præambel-betragtning nr. 146, herunder om der efter artikel 82, stk. 1, skal kunne tilkendes en "erstatning" for ikke-økonomisk skade, såfremt der i national ret er foreskre-vet en erstatning herfor.

EU-lovgiver er heller ikke konsekvent i anvendelsen af henholdsvis begreberne "erstatning" og "godtgørelse" , ligesom der heller ikke kan konstateres konsistens i brugen af begreberne "materiel/immateriel skade" og "økonomisk/ikke-økono-

misk skade" . Dette ses bl.a. afspejlet i de to direktiver, der er gengivet ovenfor. I ligebehandlingsdirektivet ses der at være en klar sondring mellem erstatning på den ene side og godtgørelse på den anden. I direktivet om intellektuel ejendoms-ret følger det derimod, at et af de aspekter, der skal tages hensyn til under udmå-ling af *erstatning,* hvis det er hensigtsmæssigt, er andre elementer end de økono-miske, f.eks. den ikke-økonomiske skade, rettighedshaveren har lidt som følge af krænkelsen.

Databeskyttelsesforordningens formål følger af artikel 1, stk. 2 og 3. Af artikel 1, stk. 2, følger det, at forordningen beskytter fysiske personers grundlæggende ret-tigheder og frihedsrettigheder, navnlig deres ret til beskyttelse af personoplys-ninger. Af artikel 1, stk. 3, følger det, at den frie udveksling af personoplysninger i EU hverken må indskrænkes eller forbydes af grunde, der vedrører beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger.

Forordningens artikel 82, stk. 1, var i artikel 77, stk. 1, i Kommissionens oprinde-lige forslag, affattet på følgende måde: "Enhver, som har lidt skade som følge af en ulovlig behandling eller enhver anden handling, der er uforenelig med denne forordning, har ret til erstatning for den forvoldte skade fra den [dataansvarlige] eller [databehandleren]" . Derudover var præambelbetragtning nr. 118, 1. pkt., (den nuværende betragtning nr. 146) affattet således: "Personer, der lider skade som følge af en ulovlig behandling, bør have ret til erstatning fra den [dataansvarlige] eller [databehandleren]" .

Artikel 29-gruppen har om det oprindelige forordningsforslags artikel 77 bl.a. udtalt, at arbejdsgruppen finder det nødvendigt at afklare (i en betragtning), at ordet "skade" ikke kun henviser til materiel skade, men også omfatter andre for-mer for skade (immateriel skade).

I Europa-Parlamentets betænkning af 21. november 2013 fra udvalget om Borger-nes Rettigheder og Retlige og Indre Anliggender blev der foreslået ændringer til forordningsforslagets præambelbetragtning nr. 118 og artikel 77, stk. 1. Til be-tragtning nr. 118 ønskedes der indsat personer, der lider skade, *uanset om den er økonomisk eller ej.* Til artikel 77, stk. 1, ønskedes der indsat "enhver, som har lidt skade, *herunder ikke-økonomisk skade* …"

Af Rådets generelle indstilling af 11. juni 2015 nævnes det i indledningen, at Rå-det har ønsket at modificere bl.a. præambelbetragtning nr. 118 og artikel 77. Præambelbetragtning nr. 118, der i al væsentlighed kan genfindes i den endelige forordnings præambelbetragtning nr. 146, blev af Rådet affattet på ny og lyder således: "Personer, der lider skade som følge af en behandling, der ikke er i over-ensstemmelse med denne forordning, bør have ret til erstatning fra den dataansvarlige eller databehandleren. Denne bør fritages for erstatningsansvar, hvis det bevises, at den pågældende ikke på nogen måde er skyld i den forvoldte skade (…) Begrebet "skade" skal fortolkes bredt i lyset af retspraksis ved den Eu-ropæiske Unions Domstol, således at det fuldt ud afspejler målene for denne for-ordning" . Artikel 77, stk. 1, der i al væsentlighed kan genfindes i den nuværende

artikel 82, stk. 1, blev også affattet på ny og lyder således: "Enhver, som har lidt materiel eller immateriel skade som følge af en behandling, der ikke er i overens-stemmelse med denne forordning, har ret til erstatning for den forvoldte skade fra den dataansvarlige eller databehandleren."

Det må af det oplistede hændelsesforløb kunne udledes, at Rådet ikke ønskede, at der skulle henvises til ikke-økonomisk skade, hvilket EU-lovgiver som sådan endte med at følge.

Forordningens artikel 82 bærer overskriften "ret til erstatning og erstatnings-ansvar" . I den engelske version bærer artikel 82 overskriften "right to compensa-tion and liability" , ligesom det også var tilfældet i ligebehandlingsdirektivets ar-tikel 18, hvor "erstatning" i den engelske sprogversion er "compensation" . Deru-dover fastsætter forordningen ikke i artikel 82, stk. 1, de nærmere betingelser for at fastslå erstatningsansvaret og den deraf følgende erstatningssum, i modsæt-ning til området for administrative bøder, jf. forordningens artikel 83, stk. 1-6, hvor forordningen er meget udtrykkelig i forhold til bødestørrelserne.

Endelig sondres der efter dansk erstatningsret overordnet set mellem integri-tetskrænkelser (materiel skade) og ikke-integritetskrænkelser (immateriel skade). Derefter sondres der for begge skadestyper mellem økonomisk og ikke-økono-misk skade, da der som udgangspunkt, efter dansk ret, alene kan opnås erstat-ning for *økonomisk* skade (der dog godt kan være immateriel, f.eks. et omsæt-ningstab), jf. gengivelsen af gældende ret ovenfor. Dette taler imod, at der alene ud fra forskellen mellem direktivets artikel 23 om "skade" og forordningens arti-kel 82, stk. 1, om "materiel eller immateriel skade" kan udledes, at det med for-ordningen er tiltænkt, at der også skal gives erstatning for ikke-økonomisk skade efter artikel 82, i hvert fald ikke i situationer, hvor der nationalt ikke er tradition for at give erstatning for ikke-økonomiske tab.

På det foreliggende grundlag, herunder med den foreliggende praksis fra EU-Domstolen og EU-lovgiver, er der således ikke tilstrækkeligt grundlag for at fast-slå, at *godtgørelse* for ikke-økonomisk skade er omfattet af retten til *erstatning* for materiel eller immateriel skade efter artikel 82, stk. 1. I hvert fald ikke, hvis der i en medlemsstat ikke normalt uden særskilt hjemmel er mulighed for erstatning for ikke-økonomisk tab. Immateriel skade i forordningens forstand må, i en dansk kontekst, 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 retsstri-digt indvundne berigelse.

Derudover fremgår det i øvrigt bl.a. af forordningens præambelbetragtning nr. 75, at risiciene for fysiske personers rettigheder og frihedsrettigheder, af varieren-de sandsynlighed og alvor, kan opstå som følge af behandling af personoplysnin-ger, der kan føre til fysisk, materiel eller immateriel skade, navnlig hvis behand-lingen kan give anledning til forskelsbehandling, identitetstyveri eller -svig, fi-nansielle tab, skade på omdømme, tab af fortrolighed for personoplysninger, der

er omfattet af tavshedspligt, uautoriseret ophævelse af pseudonymisering eller andre betydelige økonomiske eller sociale konsekvenser, hvilke eksempler i øv-rigt også peger i retningen af, at der med artikel 82 alene er tiltænkt erstatning for økonomisk skade.

Forordningens artikel 82, stk. 1, ændrer ikke på den mulighed, der eksisterer efter dansk ret, til i visse tilfælde, at udbetale godtgørelse for tort i medfør af erstatningsansvarslovens § 26 for en ikke-økonomisk skade. En sådan bestemmelse må anses for at være en sanktion efter forordningens artikel 84, der er med til at sikre forordningens effektive efterlevelse. For nærmere om forordningens artikel 84 henvises til afsnit 9.11. om sanktioner.

Artikel 82, stk. 1, udvider gældende ret ved at også databehandlere kan være erstatningsansvarlige.

9.6.3.2. Databeskyttelsesforordningens artikel 82, stk. 2

Det følger af forordningens artikel 82, stk. 2, 1. pkt., at enhver dataansvarlig, der er involveret i behandling, hæfter for den skade, der er forvoldt af behandling, der overtræder denne forordning.

Bestemmelsen er i vidt omfang en videreførelse af ordlyden af direktivets artikel 23, og persondatalovens § 69 . Dog forudsættes det i bestemmelsen med ordet *enhver,* at der kan forekomme situationer, hvor flere dataansvarlige er involveret i behandling, og som dermed også kan være erstatningsansvarlige.

Af forordningens artikel 82, stk. 2, 2. pkt., følger det, at en databehandler kun hæfter for den skade, der er forvoldt af behandling, hvis pågældende ikke har opfyldt forpligtelser i denne forordning, der er rettet specifikt mod databehand-lere, eller hvis pågældende har undladt at følge eller handlet i strid med den dataansvarliges lovlige instrukser.

Det følger af direktivets artikel 23 og af persondatalovens § 69 , at det alene er for den dataansvarlige, at der heri kan findes et ansvarsgrundlag. Det bemærkes dog, at en databehandler kan være erstatningsansvarlig efter en culpanorm. Det er dermed nyt i forhold til gældende ret, at ansvarsgrundlaget for en databe-handler under nærmere fastlagte omstændigheder - navnlig hvis databehandle-ren ikke overholder de forpligtelser, som følger af forordningen - er reguleret af forordningens artikel 82, stk. 2. Dette kan f.eks. være tilfældet, hvis databehand-leren uden godkendelse fra den dataansvarlige gør brug af en anden databe-handler, jf. forordningens artikel 28, stk. 2.

9.6.3.3. Databeskyttelsesforordningens artikel 82, stk. 3

Det følger af forordningens artikel 82, stk. 3, at en dataansvarlig eller databe-handler er fritaget for erstatningsansvar i henhold til stk. 2, hvis det bevises, at den pågældende ikke er skyld i den begivenhed, der medførte skaden.

> Af præambelbetragtning nr. 146, præciseres det bl.a., at det er den dataansvarlige eller databehandleren der må bevise, at den pågældende ikke er ansvarlig for den forvoldte skade.
>
> Persondatalovens § 69 præciserer hvilke momenter, der er relevante for en vurdering af, om den dataansvarlige har handlet culpøst. I persondataloven forud-sættes det, at vurderingen af, om den dataansvarlige har handlet erstatningspå-dragende skal ske på baggrund af en kutyme betragtning om, hvad der alminde-ligvis må kræves af en dataansvarlig.
>
> Det fastsættes ikke i forordningens artikel 82, hvilke momenter der er væsentlige i vurderingen af, om den dataansvarlige eller databehandleren har et ansvar for den skade, som den registrerede er blevet påført. Af den grund må det antages, at en vurdering af skyldsspørgsmålet, der fastsættes på baggrund af en kutyme betragtning, ikke er i uoverensstemmelse med forordningens artikel 82, og vil kunne opretholdes.
>
> Det i bestemmelsen fastsatte præsumptionsansvar, følger allerede af direktivets artikel 23, stk. 2, hvorfor der er tale om en videreførelse af gældende ret.
>
> …"

Forklaringer
Der er afgivet partsforklaringer af Sagsøger 6, Sagsøger 3, Sagsøger 4 og Sagsøger 1 samt vidneforkla-ring af Vidne.

Sagsøger 6 har forklaret, at hun hørte om datalækket, da hun modtog en meddelelse i sin e-Boks fra kommunen. Hun fik et chok. Hun og hendes samlever talte om, hvad hun skulle gøre. De blev enige om, at hun skul-le se tiden an.

Hun er hysterisk med IT-sikkerhed og passer meget på. Hun udleverer ikke si-ne oplysninger til nogen. Hun tænkte, at det ikke kunne ske for hende, at kom-munen havde mistet oplysninger om hende. Hun følte sig krænket. Hun havde betroet kommunen sit personnummer, og pludselig var der andre, der havde det. Hvis hun ikke havde været nede med nakken i forvejen på det tidspunkt, var hun kommet det. På daværende tidspunkt var hun i et hårdt forløb omkring en pensionsansøgning. Det var en meget voldsom oplevelse for hende oven i det at høre, at kommunen havde forlagt hendes personnummer.

Sagen har gjort hende meget bekymret og nervøs. Hun har således siden da dagligt eller hver anden dag kontrolleret sin bankkonto for at se, om der er ube-rettigede overførsler. Hun er også forsigtig med telefonopkald fra numre, hun ikke kender. Hun føler, at hun "kigger sig over skulderen" i det daglige. Hun

tænker ligeledes over, hvis der holder en bil på gaden, hun ikke kender. Når det ringer på dørtelefonen, bliver hun nervøs. Sådan havde hun det ikke før data-lækket, der har gjort hende bange, ked af det, mistroisk og opfarende. Det har været krænkende. Det, hun har været udsat for, er en stor stressfaktor.

Det vil være en rimelig løsning på sagen, at hun og andre involverede, der er blevet krænket, får en godtgørelse som et plaster på såret.

Sagsøger 4 har forklaret, at han første gang hørte om datalækket via Facebook, hvor det fremgik, at der var sket noget. Der var en Facebook-gruppe for stjålne data, der var ret tidligt ude med oplysningen om den mistede PC. Han tænkte over, hvad sandsynligheden var for, at hans data var involveret.

Han modtog efterfølgende et brev fra kommunen i sin e-Boks og tænkte, at han så var en af dem, der havde fået sine data lækket. Han googlede, hvad man skulle gøre i en sådan situation og blev bekendt med, at man blandt andet skul-le gå ind på Borger.dk og sætte kryds i et felt om kreditværdighed. Det gjorde han, og det viste sig senere at medføre nogle problemer. Det kan godt være, at der også stod noget om det i kommunens brev. Han gjorde det også, fordi han havde hørt historier om, hvad der kunne ske for personer, der havde fået stjålet deres data.

Efterfølgende tænkte han over, hvorfor det var sket, og hvorfor kommunen ikke havde passet bedre på dataene. Fra sit arbejde havde han selv fået indskærpet ikke at gemme data på et lokalt drev. Senere hørte han noget om, at tyveriet var sket i forbindelse med en juletræsfejring. Han havde tænkt, at kommunen burde have passet bedre på og i det mindste have aflåst deres lokaler. Det gjor-de ham gal, at kommunen ikke havde passet bedre på.

Efter at han modtog kommunens meddelelse, skrev han tilbage til kommunen via e-Boks og modtog efterfølgende et svar. Han ringede også til kommunen og bad om yderligere aktindsigt. Han talte med en kvinde, der forsøgte at tale ham fra at søge om at få udleveret yderligere oplysninger. Hun gav udtryk for, at det ville være et meget stort arbejde. Han tænkte også, at hun forsøgte at bagatelli-sere det, der var sket. Han sad tilbage med en ”nå” følelse. Set i bakspejlet følte han sig ikke hørt, men det gjorde ikke noget større indtryk.

Han var blevet overrasket over, at han var registreret som boende på ”Egebo” og ”Institutionsophold” . Han havde ikke hørt om registreringen tidligere. Han havde spurgt ind til det over for den kvindelige medarbejder fra kommunen, som han havde talt i telefon med. Hun havde svaret, at det var normalt at blive registreret sådan, når man var flyttet til kommunen. Efterfølgende har han tænkt, at hun nok troede, at han var tilknyttet institutionen Egebo, selvom det ikke passede. Han kender ikke så meget til Egebo, men han ved, det er et be-

handlingssted. På daværende tidspunkt var han jobsøgende, og hvis nogen la-vede baggrundscheck på ham, kunne det give problemer, hvis han stod som til-knyttet en institution som Egebo. Dette kunne medføre afvisning af sikkerheds-godkendelse, og i øvrigt var det krænkende, at han stod forkert registreret.

I sin fritid er han involveret i politik og stiller op til kommunalvalget, hvorfor det også i den henseende vil være problematisk, hvis nogen tror, at han bor el-ler har boet på institution. Han undrer sig over, hvordan det kan lade sig gøre, at han fejlagtigt blev registreret som tilknyttet institutionen.

Han er involveret i sagen for at få fastslået, at det ikke er i orden, at der var regi-streret oplysninger om ham, der ikke passede. Det er ikke for at få penge. Sagen kan også være med til at få strammet op på kommunens datasikkerhed, så til-svarende sager undgås. De, der har haft et økonomisk tab, bør også blive kom-penseret.

Sagsøger 3 har forklaret, at hun nok hørte om sagen første gang, da hun modtog kommunens brev i sin e-Boks. Hun blev chokeret og tænkte, at så var hun en af dem, det drejede sig om. Hun læste, at kommunen mente, at det ikke var sket for at begå noget kriminelt med oplysningerne. Det stolede hun på og blev beroliget. Hun forstod også brevet sådan, at der var taget hånd om det.

I marts 2019 var hun sygemeldt med rygsmerter. Den 18. marts 2019 havde hun ligget på sofaen med smerter, da hendes telefon ringede. Hun besvarede opkal-det, men der blev ikke sagt noget. Der var bare nogle lyde, hun ikke forstod. Det var sket i alt tre gange. Hun havde besvaret to af opkaldene.

Derefter modtog hun en sms fra sit teleselskab, hvori der blev spurgt til, om hun var tilfreds med betjeningen. Hun undrede sig over beskeden, da hun ikke havde ringet til dem. Hun reagerede ikke på beskeden, da hun tænkte, det var en fejl, at hun havde fået den tilsendt.

Efterfølgende modtog hun en mail om, at hun havde gjort noget for mange gan-ge med sit NemID, der derfor var blevet spærret. Hun tænkte, at hun ikke hav-de gjort noget og ikke skulle gøre noget. Lidt efter modtog hun en ny mail. Vist mails af 18. marts 2019 fra Nets, bilag 7 og 8, bekræftede hun, at det var de nævnte mails, hun havde modtaget. Der stod, hun ikke skulle gøre noget, og derfor reagerede hun ikke.

Lidt efter mistede hendes mobiltelefon signal. Der var ikke noget galt med den, og hun tænkte, om der var gået noget galt med betalingen af telefonregningen. Da hun var alene hjemme, blev hun utryg. Hun tog hjem til sine forældre og ringede til teleselskabet fra deres telefon. Teleselskabet oplyste, at hun havde

kontaktet dem dagen før for at få et nyt sim-kort. Det var den 19. marts 2019, hun fandt ud af det.

Medarbejderen i teleselskabet sagde, at hun troede, at hun havde været udsat for noget, og det begyndte at gå op hende, hvad der var sket. Det gik op for hende, at hun var blevet udsat for identitetstyveri. Det havde åbenbart været nok for dem, der gjorde det, at have hendes navn, personnummer og telefon-nummer til at få skiftet sim-kort. Hun tænkte, at det var sket på grund af de op-lysninger om hende, som kommunen havde mistet.

Hun blev vejledt om at gå på Borger.dk og oprette sig med kreditvarsel. Det kunne hun imidlertid ikke, da hendes NemID var spærret. Hun blev fra borger-service henvist til politiet, der spurgte, om hun var blevet bestjålet noget. Hun kom derfor til at tænke på sin bank og bankkonti. Politiet henviste hende til at kontakte banken. Hun kontaktede sin bank, der oplyste, at der var overført hen-holdsvis 50.000 kr. og 45.000 fra hendes konto. Hun blev chokeret og gik helt i sort. Da hun var i kontakt med banken, var der ingen, der forstod den situation, hun var i. Der var ingen i banken, der var hjælpsomme. Hun følte, banken men-te, det var hendes egen sag, som hun måtte tage med politiet. Hun fik heldigvis hjælp af sin mor, og efter et trægt forløb blev det afklaret, at hun kunne gøre indsigelse over for hævningerne. Banken dækkede herefter tabet, og banken op-lyste, at det ville være hendes penge efter et år.

Efter hun havde talt med banken, orienterede hun politiet om hævningerne. Hun skulle hele tiden handle og reagere, og det ramte hende på en frygtelig og hård måde. Det var et meget svært og chokerende forløb, og hun følte ikke, der var nogen, der hjalp hende. Hun skulle klare det hele selv.

Hun havde tidligere tillid til, at de, der havde med IT at gøre, havde styr på det, men det havde de ikke. Det har sagen med den mistede PC med blandt andet oplysningerne om hende vist.

Hun tænkte i første omgang ikke på at kontakte kommunen, der et par måne-der før havde skrevet til hende om de mistede oplysninger. Efterfølgende skulle hun bestille nyt NemID og var i den forbindelse i kontakt med kommunen. Hun talte med en medarbejder i kommunen, der ikke var særlig behjælpelig. Hun blev henvist til Herlev Kommune, hvilket hun ikke forstod, når hun nu bo-ede i Gladsaxe Kommune. Det gjorde hende vred og irriteret, at hun selv skulle gøre det hele.

Der var taget penge fra hende en mandag, men det lykkedes hende først om onsdagen at få registreret et kreditvarsel. Det var fordi, hun ikke havde et Ne-mID, der fungerede. Denne forsinkelse var meget stressende for hende, da det

gav gerningsmændene tid til at gøre mere skade. Hun frygtede, der ville ske alt muligt i mellemtiden.

Hendes postkasse hænger udenfor, og efterfølgende har hun tænkt, at nogen har kunnet fiske breve op af hendes postkasse. Banken sagde, at hun havde to nøglekort, men det havde hun ikke, så en anden må have bestilt et ekstra nøglekort i hendes navn og have fisket det op fra hendes postkasse. Det er noget, hun efterfølgende har kunnet stykke sammen.

Sagen har gjort hende nervøs. Hvis hun modtager opkald fra numre, hun ikke kender, gør det hende usikker. Hun tænker over, om det, at nogen ringer, er tilstrækkeligt til, at de uberettiget kan få adgang til hendes oplysninger og gøre noget, de ikke må. På grund af sagen og de lækkede oplysninger, er hun i konstant forsvarsberedskab og kontrollerer sin bankkonto og mails ofte. Det er forsvarsmekanismer, der træder i kraft, når der sker noget uventet. Hvis nogen skal ringe til hende, spørger hun til det nummer, de vil ringe fra, så hun kan være forberedt. Tidligere følte hun sig tryg, hvis hun havde sin telefon, sit nøg-lekort og betalingskort, men det gør hun ikke længere.

Hun har aldrig sendt sine personlige oplysninger til uvedkommende. Hun har altid været meget forsigtig. Når hun har sendt noget til kommunen, har det væ-ret over en sikker forbindelse. Hun har aldrig oplyst sit bankkontonummer til nogen, der har ringet til hende. Hun har ikke tidligere oplevet noget som det, der er sket i denne sag. Det har været underligt, at nogen kan udgive sig for at være hende og stjæle hendes identitet.

En rimelig udgang på sagen handler for hende om at styrke den sikkerhed i forhold til kommunens behandling af personoplysninger, man som borger har krav på. Alle begår fejl, men der hviler et ansvar på kommunen, når de behand-ler sådanne oplysninger, og forløbet har medført, at hendes oplysninger nu er lagt ud. Hun ved ikke, om der kommer til at ske mere, og det gør, at hun hele ti-den er på vagt og ikke kan slappe af. Det kræver energi hele tiden at skulle for-holde sig til det.

Hun forventede, at hendes oplysninger var i trygge hænder. Det var de ikke, og hun fik ingen hjælp af kommunen til at løse de problemer, der opstod. Hun vil håbe, at der kan afsættes penge til at hjælpe dem, der bliver udsat for noget tilsvarende.

Sagsøger 1 har forklaret, at hun hørte om tyveriet af kommu-nens computer i en gruppe på Facebook. Da hun fik en meddelelse fra kommu-nen i sin e-Boks, blev hun opmærksom på, at hendes oplysninger var involve-ret. Det gjorde hende forskrækket og frustreret. Hun havde det ikke så godt i

forvejen, og hun syntes, det var væmmeligt. Hun havde fortalt kommunen nog-le ting i fortrolighed, og nu var de oplysninger forsvundet.

Hun ringede til kommunen, der sagde, der ikke rigtig var sket noget. Hun rin-gede for at høre, om hun skulle gøre noget. Hun fik at vide, at hun ikke skulle gøre noget. Hun følte ikke, hun fik hjælp. Hun var bange for, hvad der kunne ske og frygtede, det ville vælte ind med rudekuverter. Hun magtede ikke at for-holde sig til det. Hun ved stadig ikke, om der kan ske noget som følge af sagen og frygter, at hendes bankkonto pludselig kan blive tømt.

Efterfølgende er hun blevet nervøs for at åbne sin postkasse og sin netbank. Sa-gen sidder hele tiden i baghovedet - også i dag, selvom hun ikke længere tæn-ker over sagen dagligt. Der er tidligere forsvundet computere fra kommunen, og hun ved nu ikke, hvilke af hendes oplysninger, der er forsvundet. Hun har været i kontakt med kommunen i forbindelse med et længere sygeforløb, og hun har i den forbindelse fortalt meget private ting, som hun ikke vil have ud til andre. Det er krænkende for hende, at oplysninger om hendes private for-hold er kommet ud til andre.

Da hun ringede til kommunen, følte hun ikke, at hun blev hørt. Hun har ikke fået en undskyldning fra kommunen ud over det, der står i den meddelelse, de sendte til hende.

Sagen bør føre til, at kommunen ændrer deres procedurer, så det ikke sker igen. Hun ved ikke, om ændrede procedurer vil gøre hende mere tryg, da skaden nu er sket. Hun synes, kommunen bør stramme op. Det har været en frygtelig og chokerende oplevelse at blive udsat for.

Vidne har forklaret, at hun arbejder i Arbejdernes Landsbank, hvor Sagsøger 3 er kunde. Vidnet er filialsupporter og arbejder med "fraud" . Hun har overtaget sagen med Sagsøger 3.

Det fremgår af bankens oplysninger, at banken blev kontaktet den 11. marts 2019 af en person, der udgav sig for at være Sagsøger 3. Personen bestilte et nyt nøglekort. Nøglekortet blev sendt til Sagsøger 3's adresse. Den 18. marts 2019 ringede en person igen og bestilte en aktiveringskode til nøglekortet, der skulle aktiveres. Aktiveringskoden blev sendt med sms til kundens mo-bilnummer den 18. marts 2019. Samme dag kl. 15.15 og 15.17 blev der overført henholdsvis 50.000 kr. og 45.000 kr. fra kundens konto. Overførslerne blev god-kendt med nøglekort og sms. Posteringsoversigten den 20. marts 2019 viser de nævnte overførsler. Det var ikke køb, som anført på kontoudtoget, men over-førsler. Den ene overførsel var til en konto i Danske Bank og den anden til en konto i Arbejdernes Landsbank.

Det fremgår af bankens noter, at Sagsøger 3 ringede den 20. marts 2019, og sagen blev sat i gang. Der blev sendt spærring af beløbene til de to andre konti, men pengene var hævet umiddelbart efter overførslerne. Det viser, at de, der gjorde det, var klar og ventede på at hæve pengene eller videreføre dem.

Når en kunde henvender sig som Sagsøger 3 og oplyser om uberettigede overførsler, spørges kunden ud om opbevaring af NemID, personnummer og andre forhold. Det er bankens opfattelse, at Sagsøger 3 har behandlet sine oplysninger og koder korrekt. Derfor har banken også dækket Sagsøger 3's tab.

Når sagen er færdigbehandlet i banken, anmeldes sagen til politiet. Sagen ver-serer stadig hos politiet, og sagen er åben i banken, der har udlagt de 95.000 kr. til dækning af Sagsøger 3's tab. Straffesagen forventes behandlet i retten i oktober 2021. De 95.000 kr., der er overført af banken til Sagsøger 3 til dækning af hendes tab, er hendes penge og vil ikke blive krævet tilbage.

Vidnet har i det sidste års tid ikke set, at nogen har overtaget en kundes mo-bilnummer. Denne type uberettigede overførsler sker typisk ved ”phising” , hvor de kriminelle får adgang til kundens netbank og derefter går ind og æn-drer kundes telefonnummer til et andet telefonnummer, som den kriminelle kontrollerer.

Hun kan ikke svare på, hvordan banken konkret sikrer sig, at det er rette kun-de, der ringer op, når en kunde retter henvendelse. Hun ved dog, at banken al-tid spørger efter personnummer for at kunne slå kunden op. Hun ved ikke, hvad der konkret blev spurgt om ved de henvendelser, hvor en person udgav sig for at være Sagsøger 3.

Parternes synspunkter
For **sagsøgerne** er der i det væsentlige procederet i overensstemmelse med på-standsdokument af 23. februar 2021, hvoraf fremgår blandt andet:

> ”…
> **Anbringender**
>
> **1. Den stedfundne behandling af personoplysninger**
> ***1.1 Begreber***
> ***1.1.a Begrebet ”behandling”***
>
> Ifølge Persondataforordningens art. 4, nr. 2, omfatter begrebet ”behand-ling” ”enhver aktivitet eller række af aktiviteter — med eller uden brug af automatisk behandling — som personoplysninger eller en samling af per-sonoplysninger gøres til genstand for, f.eks. indsamling, registrering, orga-

nisering, systematisering, opbevaring, tilpasning, [] brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring []" (mine understregninger).

På den baggrund gøres det for det første af sagsøgerne gældende, at der er tale om "behandling" af oplysninger i Persondataforordningens forstand.

Parterne er tilsyneladende enige om, at dette kan lægges til grund af ret-ten.

1.1.b Begrebet "personoplysninger"

Begrebet "personoplysninger" omfatter "enhver form for information om en identificeret eller identificerbar fysisk person" , f.eks. "et navn [eller] identifikationsnummer" , jf. Persondataforordningens art. 4, nr. 1.

Persondataforordningen opdeler personoplysningerne i tre (fire) grupper:

1) "Almindelige personoplysninger" (Persondataforordningens art. 6 og Databeskyttelseslovens 6),
2) "Følsomme personoplysninger" (Persondataforordningens art. 9 og Databeskyttelseslovens § 7), samt
3) Oplysninger om straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger (Persondataforordningens art. 10 og Databeskyttelseslovens § 8).

   Desuden er der en særlig type personoplysninger, som er selvstændigt reguleret i Databeskyttelsesloven (og kun her):

4) CPR-numre (Databeskyttelseslovens § 11, jf. Persondataforordningens art. 87).

"Almindelige personoplysninger" i den første kategori omfatter alle oplysninger, der ikke er klassificeret som særlige kategorier af oplysninger (følsomme personoplysninger), f.eks. identifikationsoplysninger som navn og adresse samt mere personlige oplysninger om økonomi, tjenstlige forhold, familie- og boligforhold mv.

"Følsomme personoplysninger" i den anden kategori er f.eks. oplysninger om etnisk oprindelse, religiøs eller filosofisk overbevisning samt helbredsoplysninger. Følsomme personoplysninger er udtrykkelig afgrænset i Per-

sondataforordningens art. 9, og adgangen til at behandle sådanne oplysninger er snævrere end ved almindelige personoplysninger.

Den tredje kategori rummer oplysninger om straffedomme og lovovertrædelser. Hvis det ud fra en oplysning blot kan udledes, at en person har begået noget strafbart (f.eks. fordi vedkommende har adresse i et fængsel), er der tale om en sådan art. 10-oplysning. Sådanne oplysninger om straf-bare forhold må ikke behandles i den offentlige forvaltning, medmindre det er nødvendigt for varetagelsen af myndighedens opgaver, og der gæl-der endnu strengere regler for videregivelsen.

Behandlingen af CPR-numre er ikke reguleret af Persondataforordningen, men har sin helt egen klassificering i Databeskyttelseslovens § 11 (smh.m. Persondataforordningens art. 87).

Således henhører behandlingen af CPR-numre ikke direkte til en af de tre ovennævnte kategorier 1)-3) i Persondataforordningen, men hos Datatilsynet sidestiller man tilsyneladende behandlingen af CPR-numre med behandlingen af oplysninger om straffedomme og lovovertrædelser, hvilket kan udledes af Datatilsynets hjemmeside (…).

På den baggrund gøres det for det andet gældende, at der er tale om "behandling af personoplysninger" i Persondataforordningens forstand (hvil-ket der – formentlig – også er enighed om).

1.2 Behandlingens lovlighed
1.2.a Oplysningernes art

Spørgsmålet er herefter, om der er tale om ***lovlig*** eller ***ulovlig*** behandling af personoplysninger.

Ifølge Kommunen selv, indeholder det i sagen omhandlede dokument for det første 20.620 unikke CPRnumre.

For så vidt angår de fleste af disse 20.620 unikke CPR-numre er der desuden tale om identifikationsoplysninger som navn og adresse.

For mange borgeres vedkommende er der tillige tale om oplysninger om modtagelse af offentlige ydelser (pension, revalideringsydelse, kontanthjælp, førtidspension, boligstøtte, ressourceforløb, hjælpemidler, botilbud etc.).

Desuden indeholder dokumentet oplysninger om 467 borgeres medlem-skab af folkekirken samt oplysninger om fødselsregistreringssted (hvilket – for nogens vedkommende – må være sammenfaldende med oplysninger om etnisk oprindelse), altså klart "følsomme personoplysninger" (art. 9).

Endelig indeholder dokumentet – implicitte eller eksplicitte – helbredsoplysninger samt (for så vist angår 28 borgere) f.eks. oplysninger om modtagelse af ydelser fra Kommunens Rusmiddelcenter. I visse tilfælde er det – under kolonne I, som har titlen "diagnose" - præciseret, hvilken institutionstype, borgerne modtager hjælp fra eller borgerens "målgruppe" , f.eks. "psykisk udviklingshæmmede" . Der er således her tillige tale om så-danne af art. 9 omfattede "følsomme personoplysninger" .

For så vidt angår de af søgsmålet omfattede 7 borgere, kan det med henvisning til hjælpebilag 1 lægges til grund, at de alle har fået behandlet "almindelige personoplysninger" i Persondataforordningens art. 6's forstand (navne og adresser).

Desuden har de alle 7 fået behandlet deres CPR-numre, hvilket er en klart skærpende omstændighed, jf. Persondataforordningens art. 10, Databeskyttelseslovens § 11 ...

4 af sagsøgerne - Sagsøger 1, Sagsøger 3, Sagsøger 4 og Sagsøger 6 – har derudover fået be-handlet "følsomme personoplysninger" i Persondataforordningens art. 9's forstand (jf. Databeskyttelseslovens § 7), idet de har fået behandlet oplys-ninger om deres helbred.

Sagsøger 1 har fået behandlet flere forskellige helbredsop-lysninger, og ingen læser kan være i tvivl om navnlig hendes helbreds-mæssige situation.

Sagsøger 4 skiller sig ud derved, at det – fejlagtigt – er registreret (og behandlet) hos Gladsaxe Kommune, at han er (eller har været) bosid-dende på institutionen "Egebo" . Egebo er et behandlingssted for menne-sker over 18 år "med psykisk funktionsnedsættelse, ofte med en diagnose indenfor skizofrenispektret" (…). Her er der altså tale om behandling af en klart urigtig og meget alvorlig oplysning om Sagsøger 4's psykiske hel-bred.

Endelig kan det lægges til grund, at den stedfundne behandling allerede har haft helt håndgribelige – og alvorlige – konsekvenser for to af de 7 sagsøgere – Sagsøger 3 og Sagsøger 5 – som begge

har været udsat for identitetstyveri/databedrageri. Sagsøger 3 har i den anledning tilmed fået stjålet kr. 95.000 fra sin bankkonto i Arbejdernes Landsbank (som Arbejdernes Landsbank dog nu har valgt at erstatte).

For Sagsøger 5 har dette direkte bevis for, at også oplysningerne på den i sagen omhandlede liste fra Gladsaxe Kommune (i lighed med computeren selv) er kommet i kriminelle hænder, været yderligere belastende, da Sagsøger 5 er en af borgerne på listen med adressebeskyttelse.

1.2.b Dataminimering – art. 5, stk. 1, litra c

Ifølge Persondataforordningen skal personoplysninger altid være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles (her: kontrol af beregning af mellemkommu-nal refusion). Princippet om "dataminimering" følger af Persondataforordningens art. 5, stk. 1, litra c, og indebærer, at personoplysninger kun bør behandles, hvis formålet med behandlingen ikke med rimelighed kan opfyldes på anden måde. Dataminimering bygger på et proportionalitetsprincip, hvori ligger, at der ikke må indsamles flere personoplysninger end nødvendigt.

Det er Gladsaxe Kommune, som skal dokumentere, 1) at Kommunen har foretaget en tilstrækkelig konkret vurdering af, hvilke oplysninger der var nødvendige at indsamle i det i sagen omhandlede dokument, og 2) at alle de indsamlede oplysninger var nødvendige for at opfylde formålet med at foretage kontrol af beregningen af mellemkommunal refusion.

Når man som dataansvarlig behandler personoplysninger, skal man overveje, om behandlingen af de enkelte oplysninger er nødvendig, herunder om der indsamles for mange oplysninger i forhold til formålet, eller om formålet kan opnås ved mindre indgribende behandlingsformer. Man bør i den forbindelse overveje, om formålet f.eks. kan opnås ved brug af anonymiserede eller pseudonymiserede data, eller om omfanget af behandlingen kan begrænses på anden vis.

På baggrund af det ovenfor anførte, gøres det af sagsøger gældende, at Gladsaxe Kommune ikke har foretaget en tilstrækkelig konkret vurdering af, hvilke oplysninger, der var nødvendige at indsamle i det i sagen omhandlede dokument.

Videre gøres det gældende, at det i sagen omhandlede dokument indehol-der personoplysninger, som ikke var nødvendige for at foretage kontrol af beregningen af mellemkommunal refusion, f.eks. oplysninger om med-

lemskab af folkekirken og oplysninger om fødselsregistreringssted (hvil-ket – for nogens vedkommende – må være sammenfaldende med etnisk oprindelse). Med angivelsen af CPR-numrene kan man i øvrigt også argumentere for, at borgernes navne og adresser ikke var nødvendige at anføre i regnearket.

Kommunen har altså foretaget en hel unødvendig behandling af personoplysninger, som tilmed kan kategoriseres som "følsomme oplysninger" i henhold til art. 9 (og evt. art. 10).

Desuden indeholder dokumentet personoplysninger, som ikke var nødvendige i den form, hvori de er gengivet, for den pågældende opgave; således kunne formålet f.eks. være opnået ved brug af anonymiserede eller pseudonymiserede data.

Det gøres på den baggrund af sagsøger gældende, at de i sagen omhandle-de personoplysninger er blevet behandlet i strid med Persondataforord-ningens art. 5, stk. 1, litra c.

1.2.c Opbevaringen af personoplysningerne – art. 5, stk. 1, litra a

Tilbage er herefter spørgsmålet om, hvorvidt der også er sket en overtræ-delse af Persondataforordningen (en ulovlig behandlingsaktivitet), der-ved, at oversigten er blevet opbevaret på en sådan måde, at den er kom-met i hænderne på en eller flere udenforstående kriminelle.

Ifølge Persondataforordningens art. 5, stk. 1, litra a, skal personoplysnin-ger behandles "lovligt [og] rimeligt" . Personoplysninger skal derudover "opbevares på en sådan måde, 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" , ligesom personop-lysninger skal "behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautori-seret eller ulovlig behandling og mod hændeligt tab, [] under anvendelse af passende tekniske eller organisatoriske foranstaltninger (mine under-stregninger), jf. art. 5, stk. 1, litra e og f.

Der foreligger et brud på datasikkerheden, når en hændelse "fører til hæn-delig eller ulovlig [] tab, [] uautoriseret videregivelse af eller adgang til personoplysninger" (mine understregninger), jf. art. 4, nr. 12.

Det er i præamblen således netop præciseret, at også det hændelige tab af personoplysninger er omfattet af bestemmelsen.

På den baggrund kan det lægges til grund, at de i sagen omhandlede personoplysninger tillige er blevet behandlet i strid med Persondataforordningens art. 5, stk. 1, litra e og f – og altså ulovligt - da de er opbevaret på skrivebordet på en ukrypteret, bærbar computer, der har været placeret på en sådan måde, at udenforstående kunne skaffe sig adgang til den uden brug af destruktive indgreb, herunder at der foreligger et brud på datasik-kerheden i Persondataforordningens forstand.

2. Hjemmelsgrundlaget for godtgørelse ved ikke-økonomisk skade
2.1 Persondataforordningens art. 82
2.1.a Indledning

Ifølge Persondataforordningens art. 82, stk. 1 har "enhver, som har lidt materiel eller immateriel skade som følge af en overtrædelse af [Persondataforordningen], [] ret til erstatning for den forvoldte skade fra den dataansvarlige eller databehandleren."

Persondataforordningen afløste persondatadirektivet fra 1995 (Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger) (i det følgende "Persondatadirektivet").

Af Persondatadirektivet art. 23, stk. 1 hed det:

" Medlemsstaterne fastsætter bestemmelser om, at enhver, som har lidt skade som følge af en ulovlig behandling eller enhver anden handling, der er uforenelig med de nationale bestemmelser, der vedtages til gennemførelse af dette direktiv, har ret til erstatning for den forvoldte skade []."

Efter almindelig opfattelse i dansk ret, omfattede bestemmelsen kun økonomisk skade (formuetab), og sager om ikke-økonomisk skade blev behandlet på grundlag af Erstatningsansvarslovens § 26.

Persondatadirektivet art. 23, stk. 1 blev i øvrigt implementeret i dansk ret ved § 69 i Persondataloven (Lov 2000-05-31 nr. 429 om behandling af personoplysninger). Formodningen er, at hovedparten af sager vedrørende persondatabehandling vedrører immateriel og ikke-økonomisk skade (som ikke nødvendigvis er sammenfaldende begreber, jf. nedenfor), hvor-for § 69 sandsynligvis aldrig har været anvendt.

Det således helt afgørende nye ved Persondataforordningens art. 82, stk. 1, er, at det nu er præciseret, at der også er hjemmel til, at "immateriel ska-de" kan give anledning til erstatning.

Det bemærkes, at det danske begreb "immateriel skade" ikke (nødvendigvis) er synonymt med begrebet "ikke-økonomisk skade" , da en immateriel skade godt kan føre til et økonomisk tab. Ud fra en streng ordlydsfortolkning alene kan det altså ikke nødvendigvis udledes, at art. 82, stk. 1, omfatter krav på "ikkeøkonomisk skade" . På den anden side, er det en kendsgerning, at man ved Persondataforordningens tilblivelse anvendte begreberne "immateriel skade" og "ikke-økonomisk skade" i flæng, jf. pkt. 2.1.b.

Begrebet "skade" skal, ifølge Persondataforordningens præambel (betragtning 146), da også fortolkes bredt;

Heraf følger det, at "Den dataansvarlige eller databehandleren bør yde erstatning for enhver skade, som en person måtte lide som følge af behandling, der overtræder denne forordning. [] Begrebet »skade« bør fortolkes bredt i lyset af retspraksis ved Domstolen, således at det fuldt ud afspejler formålene for denne forordning. [] Registrerede bør have fuld erstatning for den skade, som de har lidt " (mine understregninger).

2.1.b Tilblivelsen af art. 82 – Lovgivningsarbejdet i EU

Det første udkast fra EU-Kommissionen til en Forordningstekst er fra den 25. januar 2012.

I dette udkast er retten til erstatning fastslået i art. 77 – som er forløberen for den nuværende art. 82 – hvori det hedder:

" Enhver, som har lidt skade som følge af en ulovlig behandling eller enhver anden handling, der er uforenelig med denne forordning, har ret til erstatning for den forvoldte skade fra den registeransvarlige eller registerføreren."

Ordlyden i art. 77 blev siden ændret til følgende

" Enhver, som har lidt skade, herunder ikkeøkonomisk skade, som følge af en ulov-lig behandling eller enhver anden handling, der er uforenelig med denne forord-ning, har ret til erstatning for den forvoldte skade fra den dataansvarlige eller da-tabehandleren" (min understregning).

Der henvises til Den Europæiske Unions Tidende C 378/399-C 378/492 af 12. marts 2014 (ændring 186).

Siden blev bestemmelsen så flyttet til art. 82 og præciseret således:

" 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" (min understregning).

Der er intet i forarbejderne som kan indikere, at der ikke dermed var tale om en ***præcisering*** af det i (den daværende) art. 77 anførte, og Gladsaxe Kommune har da heller ikke kunne henvise til, ***hvor*** det skulle fremgå, at man med ordlydsændringen til allersidst i lovgivningsarbejdet pludselige skulle have sigtet mod en ganske betydelig begrænsning af anvendelses-området for bestemmelsen om "ret til erstatning og erstatningsansvar" (som vi i dag finder i art. 82), og noget sådanne bestrides. Tværtimod hen-viser Gladsaxe Kommune i sit svarskrift blot til den danske betænkning (betænkning nr. 1565/2017) "hvor det omtalte forløb ved Persondatafor-ordningens tilblivelse er gennemgået" .

Af sagsøger gøres det imidlertid gældende, at der ikke er juridisk grund-lag for visse af ræsonnementerne vedr. art. 82 i betænkning nr. 1565/2017, hvilket en gennemgang af forarbejderne også afslører.

Tværtimod gøres det af sagsøgerne gældende, at forarbejderne netop do-kumenterer, at begreberne "ikke-økonomisk skade" og "immateriel ska-de" – helt konkret – skal fortolkes synonymt.

Det kan lægges til grund, at der endnu ikke findes EU-domme vedr. Per-sondataforordningens art. 82, stk. 1, men EU-lovgiver selv (EU-Kommis-sionen) har allerede beskrevet beskyttelsen i art. 82 således som den var tiltænkt på EU-Kommissionens officielle hjemmeside.

Beskrivelsen af art. 82 fra lovgiver selv kan sidestilles med lovbemærknin-ger, og er som følger:

"Individuals can claim compensation if a company or an organisation infringed the General Data Protection Regulation (GDPR) and they have suffered material damages, such as financial loss or non-material damages, such as reputational loss or psychological distress . The GDPR ensures they will be provided with compen-sation, regardless of the number of organisations involved in the processing of their data. Compensation can be claimed directly from the organisation or before the competent national courts. Proceedings are brought before the courts of the

EU Member State where the controller or processor has an establishment or where the citizen claiming compensation lives (habitual residence)" (mine understreg-ninger).

…

Allerede på den baggrund må evt. antagelser vedr. rækkevidden af art. 82, stk. 1 fra en kontorfuldmægtig i et dansk ministerium i forbindelse med implementeringen af Persondataforordningen i dansk ret, således som sådanne evt. antagelser har fundet plads i Betænkning nr.1565/2017, synes at have begrænset værdi.

2.1.c Persondataforordningen formål mm.

I Persondataforordningens præambel er det da også flere steder forudsat, at Persondataforordningen beskytter mod ikke-økonomisk tab, og således savner det enhver mening, hvis ikke også art. 82, stk. 1 skulle omfatte sådanne skader;

I præamblens betragtning 75 hedder det f.eks.:

" Risiciene for fysiske personers rettigheder og frihedsrettigheder, af varierende sandsynlighed og alvor, kan opstå som følge af behandling af personoplysninger,
der kan føre til fysisk, materiel eller immateriel skade, navnlig hvis behandlingen kan give anledning til forskelsbehandling, identitetstyveri eller -svig, finansielle tab, skade på omdømme, tab af fortrolighed for personoplysninger, der er omfattet af tavshedspligt, uautoriseret ophævelse af pseudonymisering eller andre betydeli-ge økonomiske eller sociale konsekvenser ; hvis de registrerede kan blive berøvet de-res rettigheder og frihedsrettigheder eller forhindret i at udøve kontrol med deres personoplysninger ; [] hvis der behandles personoplysninger om sårbare fysiske personer , navnlig børn; eller hvis behandlingen omfatter en stor mængde perso-noplysninger og berører et stort antal registrerede " (mine understregninger).

I præamblens betragtning 85 hedder det tilsvarende:

" Et brud på persondatasikkerheden kan, hvis det ikke håndteres på en passende og rettidig måde, påføre fysiske personer fysisk, materiel eller immateriel skade, så-som tab af kontrol over deres personoplysninger eller begrænsning af deres rettig-heder, forskelsbehandling, identitetstyveri eller -svig, finansielle tab, uautoriseret ophævelse af pseudonymisering, skade på omdømme, tab af fortrolighed for oplys-ninger, der er omfattet af tavshedspligt , eller andre betydelige økonomiske eller so-ciale konsekvenser for den berørte fysiske person. Så

snart den dataansvarlige bli-ver bekendt med, at der er sket et brud på persondatasikkerheden, bør vedkommen-

de derfor anmelde bruddet på persondatasikkerheden til den kompetente tilsyns-myndighed uden unødig forsinkelse og om muligt senest 72 timer efter, at denne er blevet bekendt med det, medmindre den dataansvarlige i overensstemmelse med ansvarlighedsprincippet kan påvise, at bruddet på persondatasikkerheden sand-synligvis ikke indebærer risiko for fysiske personers rettigheder eller frihedsrettig-heder " (mine understregninger).

I præamblens betragtning 86 hedder det videre:

" Den dataansvarlige bør underrette den registrerede om et brud på persondatasik-kerheden uden unødig forsinkelse, når dette brud på persondatasikkerheden sand-synligvis vil indebære en høj risiko for den fysiske persons rettigheder og friheds-rettigheder " (min understregning).

Også i præamblens betragtning 10, 75, 76, 81, 84, 89 og 91 (ikke udtøm-mende) omtales "rettigheder og frihedsrettigheder" i øvrigt som af hinan-den uafhængige begreber.

Der henvises videre til præamblens betragtning 146:

" Den dataansvarlige eller databehandleren bør yde erstatning for enhver skade, som en person måtte lide som følge af behandling , der overtræder denne forord-ning" (min understregning" .

Det er helt afgørende, at denne betragtning 146 tager sit udgangspunkt i betragtning 118 i et af de første udkast til forordningstekst (jf. Den Euro-pæiske Unions Tidende C 378/399-C 378/492 af 12. marts 2014), som var af-fattet således:

" Personer, der lider skade, uanset om den er økonomisk eller ej, som følge af en ulovlig behandlingsaktivitet, bør have ret til erstatning fra den dataansvarlige el-ler databehandleren, som kun kan fritages for erstatningsansvar, hvis denne kan bevise, at han ikke er skyld i den forvoldte skade []" (min understregning).

2.1.d Retspraksis

Sammenfattende kan det med henvisning til sagsøgernes materialesam-ling konstateres, at det – siden appeldomstolens afgørelse i sag A2/2014/0403 (Vidal-Hall v Google Inc (CA)) – i Storbritannien er fast an-taget, at brud på datasikkerheden, både i henhold til at. 23 (1) i det dagæl-dende EU-direktiv 96/46/EC men også GDPR art. 82 (1), kan betinge krav om godtgørelse for ikke-økonomisk tab ("non-pecuniary loss" /"non-pecu-niary damage").

Et tilsvarende billede begynder at tegne sig i de øvrige medlemsstater, hvor de første nationale domme er begyndt at komme vedr. Persondata-forordningens art. 82, stk. 1. Også her fastslås det, at borgere, der – som her – har været udsat for brud på datasikkerheden, er berettiget til godtgø-relse, hvis de har "suffered distress as a result of being the victim of the data breach" , altså ikke-økonomisk tab.

Helt generelt – og også i andre sammenhænge – anerkendes godtgørelse for ikke-økonomisk tab da også, hvilket illustreres med dom af 14. februar 2012 i sag 7094/06 fra Den Europæiske Menneskerettighedsdomstol, som tilkender en borger i Holland Euro 9.000 "in respect of non-pecuniary da-mage" .

Det vil således ikke være overensstemmende med retspraksis i de øvrige medlemslande, hvis retten i Glostrup ikke – helt principielt – anerkender, at der er hjemmel i Persondataforordningens art. 82 (1) og/eller Databe-skyttelseslovens § 40 til at tilkende de forurettede borgere i Gladsaxe Kommune tortgodtgørelse, altså godtgørelse for ikke-økonomisk skade, for det forhold, at deres personlige og fortrolige oplysninger er blevet be-handlet på en sådan måde, at det var muligt for uvedkommende kriminel-le at skaffe sig adgange til oplysningerne.
…
2.1.e Sammenfatning

Af sagsøgerne gøres det med henvisning til ovenstående gældende, at der er hjemmel i Persondataforordningens art. 82, stk. 1 (evt. Databeskyttelses-lovens § 40) til at kræve godtgørelse for ikke-økonomisk tab, jf. også pro-fessor Henrik Udsen i UfR 2020B.226:

" Det må således lægges til grund, at art. 82 omfatter retten til at kræve godtgørel-se for ikke-økonomisk skade. Dette resultat er også lagt til grund i de første natio-nale retsafgørelser om art. 82 fra Tyskland, Østrig og Holland" .

Det er en grundlæggende forudsætning for at tildele tortgodtgørelse efter Erstatningsansvarslovens § 26, at der foreligger en krænkelse af en vis grovhed.

" Udgangspunktet efter art. 82 er et andet. Efter denne bestemmelse skal vurderin-gen tage udgangspunkt i, om der er sket en overtrædelse af forordningen, dvs. om der er sket en ulovlig behandling af personoplysninger" , jf. professor Henrik Udsen i UfR 2020B.226.

Af sagsøgerne gøres det gældende, at Gladsaxe Kommune utvivlsomt har behandlet sagsøgernes personoplysninger i strid med Persondataforordningen (og Persondataloven).

Ifølge professor Udsen er der *" grund til at tro, at art. 82 vil "sænke barren" for, hvornår en persondatakrænkelse kan udløse godtgørelse, uden at det dog på nuværende tidspunkt er muligt nærmere at angive, hvor art. 82 placerer denne barre"* .

Af sagsøgerne gøres det med henvisning til ovenstående gældende, at art. 82, stk. 1 tillige dækker tab af kontrol med personoplysninger – navnlig sådanne, som er fortrolige, jf. betragtning 75 og 85.

Det er en skærpende omstændighed, at der er behandlet personoplysnin-ger om sårbare fysiske personer, og behandlingen har omfattet "en stor mængde personoplysninger og berører et stort antal registrerede" (jf. be-tragtning 75).

En sådan udvidelse af de registreredes rettigheder harmonerer med Persondataforordningens formål, som er at "sikre et ensartet og højt niveau for beskyttelse af fysiske personer" (jf. præamblens nr. 10) samt "styrke og præcisere de registreredes rettigheder og de forpligtelser, der påhviler dem, der behandler og træffer afgørelse om behandling af personoplys-ninger" . I den forbindelse nævnes i øvrigt, at formålet med Persondatafor-ordningen er at give "beføjelser til at føre tilsyn med og sikre overholdelse af reglerne om beskyttelse af personoplysninger og indføre tilsvarende sanktioner ved overtrædelser (jf. præamblens nr. 11).

Med Persondataforordningen er der således tiltænkt en betydelig udvidel-se af beskyttelsen af registrerede, hvilket i øvrigt også afspejler sig i de eksorbitante administrative bøder, som tilsynsmyndighederne har hjem-mel til at pålægge (op til Euro 20 mio. eller 4 % af virksomhedens samlede, årlige globale omsætning), jf. Persondataforordningens art. 83, stk. 5.

2.2 Databeskyttelseslovens § 40

Lov 2018-05-23 nr. 502 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger (mm.) (i det følgende: "Databeskyttelsesloven") indeholder i § 40 en (nærmest) ordret gengivelse af art. 82, stk. 1.

Således hedder det i bestemmelsen:

" Enhver person, som har lidt materiel eller immateriel skade som følge af en ulov-lig behandlingsaktivitet eller enhver anden behandling i strid med denne lov og Persondataforordningen, har ret til erstatning efter Persondataforordningens arti-kel 82."

I bemærkningerne til § 40 anføres i øvrigt, at bestemmelsen er indsat for at skabe klarhed og af hensyn til retssikkerheden, men bestemmelsen har da også en selvstændig betydning i sådanne situationer, hvor der sker overtrædelse af nationale særbestemmelser i Databeskyttelsesloven – f.eks. ved behandling af CPRnumre (jf. Databeskyttelseslovens § 11) – da denne behandling dermed også omfattes af art. 82.

Med henvisning til det allerede under pkt. 2.1 anførte (jf. ovenfor) må det nødvendigvis således også med henvisning til § 40 lægges til grund, at sagsøgerne med det stedfundne databrud har lidt immateriel skade og derfor er berettiget til godtgørelse.

2.3 Erstatningsansvarslovens § 26

Også i Erstatningsansvarslovens § 26 er der en selvstændig hjemmel til at tilkende en forurettet godtgørelse for tort i tilfælde af en retsstridig krænkelse af vedkommendes frihed, fred, ære eller person.

Tort defineres som en krænkelse af en persons eget værd og omdømme.

Det er ikke en betingelse, at krænkelsen er strafbar, men tilstrækkeligt, at der foreligger en culpøs krænkelse af en vis grovhed, jf. også det under pkt. 2.1.e anførte (ovenfor).

Det er allerede af domstolene fastslået, at uberettiget videregivelse af følsomme oplysninger – og således også personoplysninger – kan danne grundlag for godtgørelse i henhold til Erstatningsansvarslovens § 26.

2.4 Ansvarsgrundlag

Det er utvivlsomt Gladsaxe Kommune, som har udarbejdet det i sagen omhandlede regneark, herunder behandlet oplysningerne om de 20.620 – fuldstændig sagesløse – borgere.

Gladsaxe Kommune har (foruden selve behandlingen, som også var ulov-lig, bl.a. med henvisning til, at Gladsaxe Kommune ikke har overholdt princippet om "dataminimering) begået - min. - 4 forskellige fejl, og dette har betinget, at databruddet kunne finde sted.

Med de 4 begåede fejl, som Gladsaxe Kommune selv har anerkendt over for Datatilsynet, synes det paradoksalt, at Gladsaxe Kommune nu over for domstolene hævder, at kommunen skulle være "uden skyld" i oplysningernes bortkomst.

Det gøres af sagsøgerne gældende, at der tværtimod er tale om grov skødesløshed.

Det er en skærpende omstændighed, at databruddet er sket hos en offent-lig myndighed – en kommune – 1) da der netop her er tale om tvungen registrering af personoplysninger, 2) da borgerne er fuldstændig sagesløse og helt uden skyld i det passerede og 3) da kommunen har udvist grov sløseri i en række forskellige sager (min. 8 i perioden 25. maj 2018 til 5. fe-bruar 2019, …) omkring personoplysninger. Det gøres gældende, at den offentlige forvaltning har en udvidet forpligtelse til at behandle personop-lysninger med varsomhed, herunder sikre sig mod sløseri og misbrug.

Der er ikke tale om et hændeligt uheld men – tværtimod – et brud på datasikkerheden, som helt åbenbart kunne været undgået.

Endelig er det en skærpende omstændighed, at der i det i sagen omhand-lede regneark var personoplysninger – herunder følsomme oplysninger i henhold til art. 9 - omkring 20.620 borgere, herunder personoplysninger, som var åbenbart irrelevante for opgaven med at kontrollere beregningen af mellemkommunal refusion.

Af sagsøgerne gøres det gældende, at det stedfundne brud på Persondataforordningen er så alvorligt – individuelt set for hver af borgerne i søgsmålet og kollektivt, idet behandlingen har ramt så mange borgere på én gang – at der er hjemmel i art. 82, stk. 1 (evt. Persondatalovens § 40) til at tilkende sagsøgerne godtgørelse.

Af sagsøgerne gøres det gældende, at art. 82, stk. 1 er baseret på et skærpet ansvarsgrundlag. Det er ikke klart, om ansvarsgrundlaget er et objektivt ansvar eller et præsumptionsansvar (culpa med omvendt bevisbyrde).

I betænkning 1565/2017 og forarbejderne til Databeskyttelsesloven lægges til grund, at bestemmelsen er baseret på et præsumptionsansvar, hvilket harmonerer med Persondataforordningens art. 82, stk. 3 (som dog kun henviser til art. 82, stk. 2).

I føromtalte artikel af professor Henrik Udsen i UfR 2020B.226 hedder det da også:

" Udover den, måske navnlig fremtidige, potentielle påvirkning af godtgørelsesni-veau og godtgørelseskriterier vil anvendelsen af art. 82 ændre ansvarsgrundlaget. EAL § 26 er som beskrevet ovenfor baseret på et culpaansvar, hvorimod art. 82 er baseret på et skærpet ansvarsgrundlag. Det er ikke klart, om ansvarsgrundlaget efter art. 82 er et objektivt ansvar eller et præsumptionsansvar (culpa med om-vendt bevisbyrde)."

Det kan således lægges til grund, at Gladsaxe Kommune som minimum må løfte bevisbyrden for, at Gladsaxe Kommune er uden skyld i den begi-venhed, der medførte skaden.

Med de "indrømmelser" , som Gladsaxe Kommune selv har givet over for Datatilsynet i forhold til det passerede, synes det åbenbart, at Gladsaxe Kommune ikke over for domstolene kan løfte bevisbyrden for, at kommu-nen skulle være uden skyld i det passerede. Et sådant argument savner ganske simpelthen mening.

Således er Gladsaxe Kommune da nu også politianmeldt af Datatilsynet, og indstillet til en bøde, stor kr. 100.000, ...

2.5 Konklusion

Af sagsøgerne gøres det på baggrund af ovenstående gældende, at der i Persondataforordningens art. 82, stk. 1 og/eller Databeskyttelseslovens § 40 principielt set er hjemmel til at tilkende de forurettede borgere i Gladsaxe Kommune godtgørelse for den ikke-økonomiske skade, borger-ne har lidt ved deres ufrivillige tab af kontrol over egne personoplysnin-ger og tab af fortrolighed for oplysninger, der utvivlsomt er omfattet af kommunens tavshedspligt (smh.m. Persondataforordningens betragtning 85).

Det er en skærpende omstændighed, at databruddet er sket hos en offent-lig myndighed og i øvrigt at denne offentlige myndighed har udvist grov forsømmelse ved behandlingen af oplysningerne om et meget stort antal borgere samt – endelig – at der er tale om gentagelsestilfælde. Desuden skal der lægges vægt på, at visse af borgerne da også efterfølgende har op-levet identitetstyveri/databedrageri.

Der er ikke tale om et hændeligt uheld men – tværtimod – et brud på data-sikkerheden, som helt åbenbart kunne været undgået.

Det gøres gældende, at den offentlige forvaltning har en udvidet forplig-telse til at behandle personoplysninger med varsomhed, herunder sikre sig mod sløseri og misbrug.

3. Godtgørelsesniveauet

Med henvisning til de ovenstående betragtninger, jf. navnlig pkt. 2.4, gø-res det gældende, at borgerne hver især skal tilkendes en godtgørelse, som skal fastsættes skønsmæssigt på baggrund af arten og omfanget af ved-kommendes oplysninger i regnearket.

Der skal desuden tages højde for, om borgeren har adressebeskyttelse og om det stedfundne databrud de facto har haft konsekvenser.

Der er i medlemsstaterne – navnlig i Tyskland og England – afsagt en ræk-ke domme vedr. Persondataforordningens art. 82, stk. 1, og godtgørelses-niveauet ligger typisk på ca. Euro 300 - 5.000.

Ingen af dommene vedrører dog en situation, som synes så alvorlig, som tilfældet er her, hvor 20.620 borgere er blevet berøvet deres kontrol med personoplysninger – også følsomme personoplysninger – som følge af grov skødesløshed hos en kommunal myndighed.

I nærværende sag er det desuden en skærpende omstændighed, at de om-fattede borgere ikke på noget tidspunkt kan få vished for, at faren for mis-brug ikke længere er tilstede.

På den baggrund bør retten ikke udvise forsigtighed med godtgørelsernes størrelse.

Ifølge professor Udsen i UfR 2020B.226 må danske domstole overveje om det godtgørelsesniveau og de godtgørelseskriterier, der følger af den hidti-dige retspraksis efter Erstatningsansvarslovens § 26, kan overføres til art. 82, hvis art. 82 også omfatter godtgørelse; "Dette kan ikke antages at være tilfældet, selvom art. 82 efterlader et ganske stort rum for fortolkning og udfyldning."
…"

For **Gladsaxe Kommune** er der i det væsentlige procederet i overensstemmelse med sammenfattende processkrift af 11. marts 2021, hvoraf fremgår blandt an-det:

"…

3. Anbringender

3.1. Overordnede synspunkter

Gladsaxe Kommune ser med stor alvor på, at man på den anførte måde har mistet fortrolige oplysninger om sagsøgerne og andre borgere, og kommunen har beklaget hændelsen over for de pågældende. Ud fra en juridisk vurdering er det imidlertid vores opfattelse, at kommunen ikke har pådraget sig et ansvar, der berettiger sagsøgerne til erstatning eller godtgørelse.

I den forbindelse er det vores overordnede synspunkter,

- at bortkomsten af oplysningerne om sagsøgerne ikke er sket som følge af ulovlig behandling af oplysninger i kommunen, jf. nærmere herom pkt. 3.2 og pkt. 3.3,

- at oplysningerne i stedet må antages at være bortkommet ved udefrakommendes uretmæssige – og formodentlig kriminelle – handlinger, og at kommunen således er uden skyld i oplysningernes bortkomst og ikke har pådraget sig et ansvar i forhold til sagsøgerne, jf. nærmere herom pkt. 3.4,

- at databeskyttelsesforordningens artikel 82 ikke giver sagsøgerne ret til erstatning, idet kommunen som anført er uden skyld i en eventuel skade, og idet artikel 82 alene omfatter erstatning for økonomisk skade, således at sagsøgerne, som ikke har påvist at have lidt noget økonomisk tab, også af den grund ikke har noget krav mod kommunen efter artikel 82 og dermed heller ikke efter databeskyttelseslovens § 40, jf. nærmere pkt. 3.5 og pkt. 3.6, og

- at kommunen ikke er ansvarlig for en retsstridig krænkelse, der giver sagsøgerne ret til godtgørelse efter erstatningsansvarslovens § 26, stk. 1, jf. nærmere pkt. 3.7.

3.2. Bortkomsten skyldes ikke ulovlig behandling af oplysninger i kommunen

De oplysninger om sagsøgerne, som indgår i det regneark, der fandtes på en af de formodentlig stjålne computere, er personoplysninger og dermed omfattet af databeskyttelsesforordningens og databeskyttelseslovens anvendelsesområde.

Regnearket var som nævnt ovenfor blevet udarbejdet med henblik på at sikre korrekt mellemkommunal refusion, og den behandling af oplysnin-ger om sagsøgerne, som kommunens udarbejdelse og anvendelse af reg-nearket udgør, har efter vores opfattelse været lovlig.

Der henvises herved blandt andet til artikel 6, stk. 1, litra e, i databeskyt-telsesforordningen om behandling, som er nødvendig af hensyn til udfø-relse af en opgave i samfundets interesse, eller som henhører under offent-lig myndighedsudøvelse, som den dataansvarlige har fået pålagt (…). Be-stemmelsen har et bredt anvendelsesområde, der giver offentlige myndig-heder vid adgang til at behandle personoplysninger som led i varetagelsen af deres opgaver. I den forbindelse kan der henvises til betænkning nr. 1565/2017 "Databeskyttelsesforordningen (2016/679) – og de retlige ram-mer for dansk lovgivning" , hvor der blandt andet er anført følgende (be-tænkningen, side 137-138 …):

"Det kan […] ikke antages at være hensigten med forordningen at begræn-se offentlige myndigheders mulighed for at behandle personoplysninger.

[…]

Forordningen må i det hele taget også kunne udgøre hjemmel, når offentli-ge myndigheder indhenter oplysninger i overensstemmelse med official-maksimen, jf. artikel 6, stk. 1, litra e."

Særligt når det gælder behandling af oplysning om cpr-nummer, kan der henvises til databeskyttelseslovens § 11, stk. 1, hvorefter offentlige myn-digheder kan behandle oplysninger om personnummer med henblik på entydig identifikation eller som journalnummer (…).

Endvidere kan der særligt i forhold til oplysninger, der må anses for hel-bredsoplysninger i forordningens forstand, henvises til forordningens arti-kel 9, stk. 2, litra f, og databeskyttelseslovens § 7, stk. 1, hvorefter der er hjemmel til at behandle blandt andet helbredsoplysninger, hvis det er nødvendigt for, at et retskrav kan fastlægges (…). Det bemærkes herved, at kommunen er enig i, at visse af oplysningerne om Sagsøger 1, Sagsøger 3, Sagsøger 6 og Sagsøger 7 må anses for helbredsoplysninger, således som dette udtryk i forordnin-gens artikel 9 må forstås. Det gælder, uanset at oplysningerne ikke inde-holder nogen konkret information om, hvilken sygdom eller hvilket han-dicap f.eks. Sagsøger 1 måtte have. Også behandlingen af helbredsoplysninger har været lovlig, idet oplysningerne for det første er indgået i en sagsbehandling, hvor der blandt andet har skullet tages stil-

ling til, hvilke krav de pågældende sagsøgere ville have på ydelser mv. ef-ter lovgivningen, og for det andet er indgået i den efterfølgende behand-ling, hvor man har skullet fastlægge kommunens krav på mellemkommu-nal refusion.

Der kan i den forbindelse henvises til betænkning nr. 1565/2017 "Databe-skyttelsesforordningen (2016/679) – og de retlige rammer for dansk lovgiv-ning" , hvor det er omtalt, at den nævnte bestemmelse i forordningen – li-gesom det daværende databeskyttelsesdirektiv og den daværende person-datalov – blandt andet giver offentlige myndigheder hjemmel til som led i varetagelsen af deres myndighedsopgaver at behandle helbredsoplysnin-ger og andre følsomme personoplysninger, hvis det sker for, at et retskrav kan fastslås mv. I betænkningen er således blandt andet anført følgende (betænkningen, side 213 …):

"Det fremgår af forordningens artikel 9, stk. 2, litra f, at behandling af føl-somme oplysninger er lovlig, hvis behandling er nødvendig, for at rets-krav kan fastlægges, gøres gældende eller forsvares, eller når domstole handler i deres egenskab af domstol.

Bestemmelsen i forordningens artikel 9, stk. 2, litra f, svarer efter ordlyden til bestemmelsen i databeskyttelsesdirektivets artikel 8, stk. 2, litra e, 2. led, og persondatalovens § 7, stk. 2, nr. 4.

Det fremgår af præambelbetragtning nr. 52, at en fravigelse desuden bør gøre det muligt at behandle sådanne personoplysninger, hvis det er nød-vendigt, for at retskrav kan fastslås, gøres gældende eller forsvares, uanset om det er i forbindelse med en retssag eller en administrativ eller uden-retslig procedure.

Som tidligere anført følger det af gældende ret, at den situation, at be-handling af oplysninger om den registrerede er nødvendig for, at den dataansvarlige kan afgøre, om den registrerede har et retskrav, er omfattet af bestemmelsen bl.a. vil være tilfældet med hensyn til offentlige myndig-heders behandling af oplysninger som led i myndighedsudøvelse.

På baggrund af en ordlydsfortolkning af bestemmelsen ses der ikke at væ-re holdepunkter for, at bestemmelsen ikke længere skulle finde anvendel-se i forbindelse med offentlige myndigheders myndighedsudøvelse. Det fremhæves endda i præambelbetragtning nr. 52, at bestemmelsen vil finde anvendelse i disse situationer, idet det fremgår, at bestemmelsen kan an-vendes, hvis det er nødvendigt, for at et retskrav kan fastslås i forbindelse med *administrativ procedure.* Bestemmelsens anvendelse i forbindelse med

offentlig myndighedsudøvelse ses derfor at være i overensstemmelse med gældende ret. Forordningens artikel 9, stk. 2, litra f, kan således anvendes på offentlig afgørelsesvirksomhed. Det vil endvidere ikke være udelukket, at bestemmelsen kan anvendes inden for faktisk forvaltningsvirksomhed, hvis dette sker for, at et retskrav kan fastlægges, gøres gældende eller forsvares…"]

Som eksempel på, at der vil være databeskyttelsesretlig hjemmel til at behandle personoplysninger i tilfælde, hvor det er nødvendigt for en tilstrækkelig sagsoplysning (officialmaksimen), kan også nævnes U 2017.1294 H (…), hvor Højesteret fandt, at en kommune i forbindelse med en påtænkt afgørelse om at standse udbetalinger af refusion af sygedag-penge til en arbejdsgiver var berettiget til som led i partshøring af arbejds-giveren at videregive nogle helbredsoplysninger om den sygemeldte med-arbejder. Kommunen havde som udgangspunkt pligt til at partshøre over oplysningerne i medfør af forvaltningslovens § 19, stk. 1, og videregivel-sen af helbredsoplysningerne var derfor berettiget og ikke i strid med reg-lerne i forvaltningsloven og den daværende persondatalov.

Højesteret har den 4. december 2020 (…) også haft anledning til at tage stilling til en sag, hvor en myndighed (Patienterstatningen) havde indret-tet sin praksis (om erstatning for patientskader) på en sådan måde, at de først tog stilling til, om der var et ansvarsgrundlag, og kun hvis det var til-fældet, tog de også stilling til opgørelsen af et eventuelt tab. Kammeradvo-katen gjorde på den baggrund gældende, at myndigheden i den indleden-de sagsbehandling ikke var berettiget til at behandle de oplysninger, der belyste tabet, hvilket i givet fald også i den konkrete sag ville have den po-sitive sidegevinst, at myndighedernes pligt til at betale renter blev ud-skudt.

Højesteret skar imidlertid igennem og fastslog, at myndigheden havde ret til at behandle oplysningerne også på et tidligere tidspunkt og uanset den med rette valgte praksis, og at dette bl.a. ikke var i strid med det databeskyttelsesretlige dataminimeringsprincip. Det er vores vurdering også på baggrund af Højesterets dom, at myndighederne har en vid adgang til at behandle personoplysninger, når blot dette må anses for sagligt og nødvendigt.

Der kan som eksempel også henvises til Datatilsynets afgørelse af 25. oktober 2019 (…), hvor en borger klagede over, at en kommune behandlede oplysninger om borgeren med en såkaldt "type-ahead" -funktion på kommunens hjemmeside (det vil sige en funktion, der automatisk kommer med bestemte søgeforslag). Datatilsynet fandt ikke grundlag for at tilside-

sætte kommunens vurdering af, at behandlingen kunne ske inden for rammerne af forordningens artikel 6, stk. 1, litra e. Der blev herved lagt vægt på, at søgefunktionen skulle understøtte overholdelsen af den almindelige vejledningspligt over for borgerne, sådan at behandlingen var nødvendig af hensyn til kommunens myndighedsudøvelse.

På den anførte baggrund er det vores opfattelse, at udarbejdelsen og anvendelsen af de pågældende oplysninger om sagsøgerne i regnearket har været fuldt lovlig, og at der således ikke har været foretaget en ulovlig og uhjemlet behandling fra kommunens side. Det har derimod været nødvendigt og sagligt for kommunen at udarbejde regnearket til brug for udførelsen af en vigtig opgave.

Der har således ikke været tale om ulovlig behandlingsaktivitet, og kommunen bestrider derfor også, at filen skulle være bortkommet som følge af ulovlig behandlingsaktivitet til eventuel skade for sagsøgerne.

3.3. Nærmere om den lovlige behandling af personoplysninger til brug for mellemkommunal refusion

Som nævnt er behandlingen af personoplysninger i regnearket sket for at kunne kontrollere mellemkommunal refusion, og kommunen har i den forbindelse foretaget konkrete og nærmere overvejelser af, hvilke oplysninger der kan anses for nødvendige for at varetage den pågældende op-gave (…).

Der har dermed som anført i Gladsaxe Kommunes notat af 14. januar 2019 (…) generelt været bevågenhed om ikke at indhente flere personoplysnin-ger end nødvendigt til regnearket. Det vil sige, at kommunen har foretaget en konkret vurdering af, hvilke personoplysninger det var nødvendigt at behandle i den pågældende sammenhæng.

Dog fremgår det også af notatet, at kommunen ved en gennemgang har konstateret enkelte afvigelser fra dette princip om ikke at indhente flere personoplysninger end nødvendigt til regnearket, idet oplysninger om medlemskab af folkekirken og fødselsregistreringssted i forhold til visse borgere indgår i arket, selv om sådanne oplysninger ikke kan bidrage til at løse kontrolopgaven vedrørende mellemkommunale betalinger. Dette har imidlertid ingen betydning i forhold til de syv sager, som retten i nærværende sag skal tage stilling til.

Disse forhold må således anses for at være uden betydning i disse syv sa-ger, allerede fordi det bortkomne regneark ikke i relation til disse sagsøge-

re indeholdt oplysninger om medlemskab af folkekirken og/eller fødsels-registreringssted. Endvidere skal det for god ordens skyld bemærkes, at spørgsmålet i sagen er, om kommunen er ansvarlig for, at oplysningerne om sagsøgerne i regnearket er bortkommet, og om kommunen som følge heraf skal betale erstatning eller godtgørelse til sagsøgerne. Et herfra for-skelligt spørgsmål om, hvorvidt kommunens behandling af oplysninger i regnearket har været nødvendig i enhver henseende, er derfor efter Gladsaxe Kommunes opfattelse ikke afgørende for sagen.

Det kan konstateres, at sagsøgerne alligevel i påstandsdokumentet … gør en del ud af denne problemstilling, herunder i forhold til at problematise-re, at fødselsregistreringssted efter omstændighederne kan være en følsom oplysning i visse tilfælde. Dette er imidlertid en hypotetisk diskussion i forhold til de konkrete sager, som retten i nærværende sag skal tage stil-ling til.

Det skal desuden nævnes, at det fremgår af Gladsaxe Kommunes svar af 21. januar 2019 til Datatilsynet (…), at kontrol af, om der er sket korrekt re-gistrering af den enkelte borger, ikke kan ske uden brug af cpr-nummeret i regnearket, idet opgaven netop består i blandt andet at sikre, at betalings-kommuneforhold bliver korrekt registreret i cpr-registeret. Allerede derfor bestrides det, at formålet med behandlingen af de pågældende oplysnin-ger kunne været opnået ved brug af anonymiserede eller pseudonymisere-de oplysninger. I øvrigt bestrides det mere generelt, at databeskyttelsesfor-ordningen i et tilfælde som det foreliggende, hvor der er tale om en for-valtningsmæssig opgave, der kræver konkret og sikker identifikation af involverede borgere (kontrol af refusion i de pågældende sager) – og ikke f.eks. en opgave af videnskabelig eller statistisk karakter – skulle indebære krav om anonymisering eller pseudonymisering af den karakter, som der tilsyneladende bliver lagt op til i replikken. Dette underbygges også af da-tabeskyttelseslovens § 11, stk. 1, der fastsætter, at offentlige myndigheder kan behandle oplysninger om personnummer med henblik på entydig identifikation eller som journalnummer.

Det bestrides også, at den foreliggende sag kan sammenlignes med sagen omtalt i Datatilsynets udtalelse af 16. maj 2019 (…), hvor tilsynet udtalte alvorlig kritik af, at Fredericia Gymnasium i forbindelse med anvendelse af et program, som skulle overvåge elevernes computeraktivitet for at modvirke eksamenssnyd, ikke i tilstrækkelig grad havde redegjort for, at behandlingen af indsamlede oplysninger var tilstrækkelig, relevant og be-grænset til, hvad der var nødvendigt i forhold til formålet. Datatilsynet be-mærkede også, at sagen efterlod et indtryk af, at gymnasiet ikke havde været bevidst om omfanget af behandlingen og måden, hvorpå elevernes

personoplysninger blev behandlet ved brug af det pågældende program. Endvidere stod det ikke klart, hvorvidt gymnasiet faktisk havde overvejet, om brugen af programmet kunne ske inden for rammerne af de databeskyttelsesretlige regler. Som det således fremgår, indgik der i den omtalte sag, som vedrørte generel overvågning af de pågældendes computeraktivitet, og som i øvrigt slet ikke angik spørgsmålet om muligt ansvar over for de registrerede, helt andre forhold end i den foreliggende sag.

Sammenfattende er det Gladsaxe Kommunes opfattelse, at udarbejdelsen af regnearket og anvendelsen af de pågældende oplysninger om sagsøger-ne i regnearket har været lovlig og ikke har været i strid med forordnin-gen, herunder dataminimeringsprincippet i forordningens artikel 5.

3.4. Bortkomsten skyldes udefrakommendes uretmæssige – og formodentlig kriminelle – handlinger

I stedet for ulovlig behandlingsaktivitet er der tale om, at der i kommunen er sket et sikkerhedsbrud, derved at oplysningerne i regnearket – i strid med kommunens egne retningslinjer – var blevet gemt lokalt på en bærbar computer af den pågældende medarbejder.

Uanset at der var tale om en midlertidig lagring og om et tilfælde, der beroede på en menneskelig fejl, er der således i den pågældende situation ik-ke levet op til de krav, der efter kommunens egne retningslinjer stilles til behandlingssikkerhed. Det gælder også, selv om der var opsat en person-lig adgangskode på den pågældende computer, sådan at der ikke var no-gen umiddelbar tilgængelighed til computerens indhold uden indtastning af brugernavn og adgangskode.

I nærværende sammenhæng er det afgørende imidlertid, at bortkomsten ikke er sket ved en ulovlig behandling af personoplysninger i kommunen eller i øvrigt ved en handling, der kan henføres til kommunen og dens medarbejdere. Højesteret har i U 2019.3990 H (…) også fundet, at en person som udgangspunkt ikke bliver erstatningsansvarlig ved at undlade at foretage en handling, som kunne have forhindret eller begrænset en skade, som er forvoldt af en anden.

Det må således lægges til grund, at de fire computere er bortkommet ved udefrakommendes uretmæssige – og formodentlig kriminelle – handlin-ger, og det er i den forbindelse efter kommunens opfattelse mest sandsyn-ligt, at de fire bærbare computere og dermed den nævnte fil er bortkom-met ved et tyveri om aftenen den 3. december 2018, hvor der som nævnt var udvidet adgang til rådhuset i forbindelse med juletræstænding. Det

har i den forbindelse efterfølgende vist sig, at der på tidspunktet for de pågældende computeres bortkomst var en defekt lås på en dør ved rådhushallens trappeopgang, og at den eller de ansvarlige for det formodede ty-veri kan have skaffet sig adgang gennem denne dør.

Det forhold, at de pågældende oplysninger eventuelt kan være kommet uvedkommende i hænde, må dermed antages at bero på, at personer, hvis handlinger kommunen ikke er ansvarlig for, uretmæssigt og ved en krimi-nel handling har sat sig i besiddelse af de pågældende computere. Herved adskiller den foreliggende sag sig på det grundlæggende plan fra tilfælde, hvor det kan være relevant at rejse krav om erstatning eller godtgørelse over for den, som er ansvarlig for ulovlig behandling af personoplysnin-ger eller anden retsstridig disposition.

Allerede som følge heraf er det vores opfattelse, at der ikke er grundlag for et krav om erstatning eller godtgørelse i denne sag.

Herudover er der en række andre forhold, der efter vores opfattelse er med til at begrunde, at sagsøgerne ikke bør have medhold i det fremsatte krav. Dette er uddybende behandlet i de følgende afsnit særligt om databeskyttelsesforordningens artikel 82 og databeskyttelseslovens § 40 (pkt. 3.5 og pkt. 3.6) samt erstatningsansvarslovens § 26, stk. 1 (pkt. 3.7).

3.5. Særligt om databeskyttelsesforordningens artikel 82 og databeskyttelseslovens § 40

3.5.1. De relevante bestemmelser

Efter databeskyttelsesforordningen artikel 82 har enhver, som har lidt materiel eller immateriel skade som følge af en overtrædelse af forordningen, ret til erstatning hos den dataansvarlige eller databehandleren (…). Bestemmelsen fastsætter nærmere, at enhver dataansvarlig, der er involveret i behandling, hæfter for den skade, der er forvoldt af behandling, der overtræder forordningen, jf. artikel 82, stk. 2. Om ansvarsgrundlaget gælder, at vedkommende alene er fritaget for erstatningsansvar, hvis det bevises, at den pågældende ikke er skyld i den begivenhed, der medførte skaden, jf. artikel 82, stk. 3.

Databeskyttelseslovens § 40 fastsætter, at 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 (…).

Det er vores opfattelse, at sagsøgerne ikke har ret til erstatning efter artikel 82 og dermed heller ikke efter databeskyttelseslovens § 40. For det første foreligger der således ikke det fornødne ansvarsgrundlag, jf. pkt. 5.3.2 umiddelbart nedenfor, og for den andet giver artikel 82 alene ret til erstatning for økonomisk skade, jf. pkt. 5.3.3. nedenfor.

5.2. Ikke det fornødne ansvarsgrundlag

Når den pågældende fil med regnearket på computeren er bortkommet, skyldes det således som allerede omtalt, at personer, hvis handlinger kommunen ikke er ansvarlig for, må antages uretmæssigt og ved en kriminel handling at have sat sig i besiddelse af de pågældende computere, ligesom det bestrides, at der er tale om ulovlig behandlingsaktivitet, som følge af hvilken filen skulle være bortkommet til eventuel skade for sagsøgerne. Det vil sige, at kommunen ikke som anført i artikel 82, stk. 2, har været "involveret i behandling" , hvor der muligvis kan være sket skade "for-voldt af behandling" af de pågældende oplysninger, og at kommunen er uden skyld i den handling, der kan have medført en eventuel skade i for-bindelse med, at oplysningerne måtte komme uvedkommende i hænde, jf. artikel 82, stk. 3.

Under disse omstændigheder kan det efter vores opfattelse heller ikke føre til et ansvar for kommunen efter artikel 82, at en medarbejder i strid med kommunens egne retningslinjer havde lagret regnearket ukrypteret på den bærbare computer. Det bemærkes herved også, at det forhold, at regnear-ket var lagret ukrypteret, ikke var ensbetydende med, at det pågældende regneark "lå frit fremme" eller på nogen måde var umiddelbart tilgænge-lig for uvedkommende. Tværtimod var der som anført opsat en personlig adgangskode på den pågældende computer. Desuden var computeren placeret i et lokale på rådhuset uden adgang for uvedkommende – sådan at det som ligeledes anført i stedet kan skyldes en defekt lås, at den eller de formodede tyve rent faktisk skaffede sig adgang til lokalet.

Det kan efter vores opfattelse heller ikke føre til et ansvar efter artikel 82, at kommunen ikke havde krypteret harddisken i kommunens computere, herunder i den omhandlede computer, sådan at det ikke ville være teknisk muligt for en medarbejder at lagre personoplysninger ukrypteret på en computer.

Vi skal i den forbindelse mere generelt bemærke, at der efter vores opfattelse ikke er grundlag for at antage, at der efter databeskyttelsesforordningen skulle gælde et absolut krav om at anvende kryptering i forbindelse med enhver elektronisk behandling af personoplysninger. Allerede af ord-

lyden af databeskyttelsesforordningens artikel 32 følger det således, at der ikke kan opstilles et sådant absolut krav (…), ligesom der i forarbejderne til databeskyttelsesloven er angivet en "værktøjskasse" med eksempler på, hvilke sikkerhedsforanstaltninger der kan være relevante (…), og som anført i den juridiske litteratur indebærer det, at "det er en konkret vurde-ring, hvilket sikkerhedsniveau, der er det rette" , jf. Kristian Korfits Nielsen og Anders Lotterup i Databeskyttelsesforordningen og databeskyttelseslo-ven med kommentarer (1. udgave 2020, side 639) (…).

Herudover kan der henvises til, at Digitaliseringsstyrelsen og Center for Cybersikkerhed har bestemt, at der på det statslige område gælder et krav om kryptering af harddiske (…). Kravet er imidlertid ikke absolut og ufravigeligt, og det pågældende krav er desuden som nævnt afgrænset til at omfatte det statslige område og at gælde fra den 1. januar 2020. Der er derfor ikke noget grundlag for at antage, at der for kommuner i 2018 skul-le have været noget krav om kryptering af harddiske.

Se også KL´s GDPR-benspænd, hvor Datatilsynet (…) som svar på, om fysiske dokumenter med personoplysninger skal låses inde i f.eks. et skab, anfører, at personoplysninger ikke bør lige frit fremme. Hvis der er almindelig adgang for borgere, skal dokumenterne gennem væk. Derimod må en medarbejder hos en kommune ifølge Datatilsynet gerne lade dokumen-ter ligge på reolen, når vedkommende går hjem, forudsat at der ikke er almindelig adgang til det pågældende kontor. Men hvordan hænger det så sammen med, at der skulle gælde en strafsanktioneret og ubetinget pligt til at kryptere sine harddiske, også når der som i denne sag var tale om computere, der lå i et lokale, hvortil der ikke var almindelig adgang. Som allerede nævnt var der en skalsikring på rådhuset, og det var sandsynlig-vis en defekt dørlås, der gjorde den ulovlige indtrængen i forbindelse med tyveriet mulig.

I øvrigt kan oplyses, at det netop anførte er baggrunden for, at Gladsaxe Kommune ikke har kunnet erkende sig skyldig i den sigtelse, som er rejst mod kommunen, og som er kort omtalt i pkt. 2.1 ovenfor. Som den pågældende sigtelse er formuleret, er den således udtryk for den opfattelse, at selve det forhold, at det har været teknisk muligt for medarbejdere hos kommunen at lagre personoplysninger ukrypteret f.eks. "på skrivebordet" på en bærbar computer, ville udgøre en overtrædelse af forordningens ar-tikel 32.

Sammenfattende er det herefter vores opfattelse, at der ikke er noget ansvarsgrundlag efter artikel 82.

5.3.3. Omfatter alene økonomisk skade

Herudover gøres det gældende, at artikel 82 alene giver ret til erstatning for økonomisk skade – enten materiel eller immateriel økonomisk skade.

Under databeskyttelsesforordningens tilblivelse blev det således i Europa-Parlamentets betænkning foreslået at indsætte formuleringer i forordnin-gens præambel og i bestemmelsen om civilretligt ansvar, hvor det blev ud-trykkeligt fastsat, at retten til at opnå kompensation for "skade" også om-fatter "ikke-økonomisk skade" . Imidlertid tog Rådet disse formuleringer ud af forordningen i forbindelse med dens endelige vedtagelse. Det skete med en bemærkning i Rådets indstilling om, at begrebet skade skal fortol-kes bredt i lyset af retspraksis ved EU-Domstolen, således at det fuldt ud afspejler formålene med denne forordning, jf. også præambelbetragtning 146 i den endelige forordning (…).

Der kan i den forbindelse henvises til betænkning nr. 1565/2017 "Databe-skyttelsesforordningen (2016/679) – og de retlige rammer for dansk lovgiv-ning" , hvor det omtalte forløb ved forordningens tilblivelse er gennemgå-et, og hvor der herefter konkluderes følgende (betænkningen, side 911 …):

På det foreliggende grundlag, herunder med den foreliggende retspraksis fra EU- Domstolen og EU-lovgiver, er der således ikke tilstrækkeligt grundlag for at fastslå, at *godtgørelse* for ikke-økonomisk skade er omfattet af retten til *erstatning* for materiel eller immateriel skade efter artikel 82, stk. 1. I hvert fald ikke, hvis der i en medlemsstat ikke normalt uden sær-skilt hjemmel er mulighed for erstatning for ikke-økonomisk tab. Immate-riel skade i forordningens forstand må, i en dansk kontekst, 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 ind-vundne berigelse."

Det bestrides, at der med den omtalte ændring under forordningens tilbli-velse alene var tale om en "præcisering" uden væsentlig indholdsmæssig betydning. Desuden bestrides det, at udtrykket "ikke-økonomisk skade" er synonymt med "immateriel skade" , der er omfattet af artikel 82 og dens ordlyd. Der kan herved blandt andet henvises til den nævnte betænkning, hvor der er anført følgende (betænkningen, side 902 f. …):

"Der skelnes traditionelt i dansk erstatningsret mellem integritetskrænkel-ser (også benævnt materiel skade) og ikke-integritetskrænkelser (også be-nævnt immateriel skade), jf. A. Vinding Kruse, Erstatningsretten, 5. udga-

ve, 1989, s. 85. Ved integritetskrænkelser forstås skader forvoldt med fysiske midler på det menneskelige legeme eller på ting, dyr eller fast ejen-dom. Alle andre skader henføres til området for ikke-integritetskrænkel-ser. Sondringen går altså på, om skaden er fysisk eller ikke-fysisk forvoldt. Ikke-integritetskrænkelser omfatter således både krænkelser af forfatter- og kunstnerrettigheder, patenter, varemærker mv., retsstridig adfærd un-der erhvervsudøvelse, såsom utilbørlig markedsføring i øvrigt (økonomisk skade) samt krænkelser af privatlivets fred, æreskrænkelser, navnekræn-kelser osv. (ikke-økonomisk skade). Der er en række fællestræk ved ikke-integritetskrænkelser, som i større eller mindre grad går igen hos de fleste af dem. Krænkelserne vil oftere resultere i ikke-økonomiske skader end ved integritetskrænkelser. Hvis der derimod foreligger en økonomisk ska-de, vil denne ofte være betydeligt vanskeligere at dokumentere størrelsen af, end hvor det drejer sig om integritetskrænkelser."

Som det fremgår, er immateriel skade og ikke-økonomisk skade ikke synonyme begreber. Immateriel skade er således anden skade end materiel skade, der omfatter skade på mennesker, dyr, fast ejendom eller ting. Lige-som materiel skade kan immateriel skade som anført medføre krænkelser af både økonomisk karakter og ikke-økonomisk karakter.

Det bestrides, at forordningens formål og præambelbetragtninger kan føre til en antagelse om, at artikel 82 – uanset det ovenfor anførte – giver ret til erstatning for ikke-økonomisk skade.

Desuden bestrides det, at det, der er anført om artikel 82 på Europa-Kommissionens hjemmeside (…), kan føre til en sådan antagelse i den foreliggende sag. Dette følger allerede af, at informationen på den pågældende hjemmeside ikke har nogen retskildemæssig status. Når der i sagsøgernes påstandsdokument (…) er anført, at Europa-Kommissionen er lovgiver, og at beskrivelsen på hjemmesiden udfærdiget af Europa- Kommissionen derfor må sidestilles med lovbemærkninger, er det forkert.

Selv hvis man antog, at hjemmesidens information kunne tillægges betydning, ville dette imidlertid ikke føre til, at det ud fra hjemmesiden kan sluttes, at ikke-økonomisk skade er omfattet af bestemmelsen. De eksempler, der angives på hjemmesiden, vedrører således tab af ens gode navn og psykisk belastning, hvilket er eksempler på immateriel skade, der efter omstændighederne også kan medføre et økonomisk tab – f.eks. i form af mistet indtjening efter at have været udsat for uberettigede injurier eller tabt arbejdsfortjeneste ved sygdom på grund af psykisk belastning.

Datatilsynet har på sin hjemmeside svaret følgende om, hvornår man kan få erstatning, hvis ens oplysninger er blevet behandlet i strid med de databeskyttelsesretlige regler (…): "Hvis du har lidt et økonomisk tab ved en behandling, der er sket i strid med databeskyttelsesreglerne, kan det være, at du har ret til erstatning.

Økonomisk tab som følge af overtrædelser af databeskyttelsesreglerne kan bl.a. forekomme ved ukorrekt databehandling i forbindelse med kreditoplysning, e- handel og i ansættelsessituationer."

Herudover kan der henvises til Kristian Korfits Nielsen og Anders Lot-terup i Databeskyttelsesforordningen og databeskyttelsesloven med kom-mentarer (1. udgave, 2020, side 922-923), hvor der er anført blandt andet følgende (…):

"Det er et væsentlig spørgsmål, hvad der ligger i, at der kan kræves erstatning for *materiel* eller *immateriel* skade […]

På baggrund af en grundig gennemgang af retskildegrundlaget, herunder den foreliggende retspraksis fra EU-Domstolen og EU-lovgiver, konklude-res det i bet. 1565/2017, side 910-914, at der ikke er tilstrækkeligt grundlag for at fastslå, at godtgørelse for ikke-økonomisk skade er omfattet af retten til erstatning for materiel eller immateriel skade efter artikel 82, stk. 1. I hvert fald ikke, hvis der i en medlemsstat ikke normalt uden særskilt hjemmel er mulighed for erstatning for ikke-økonomisk tab. Immateriel skade i forordningens forstand må, i en dansk kontekst, antageligvis for-stås som den almindelige eller rene formueskade, som er lidt som følge af overtrædelse af forordningens bestemmelser, hvilket som nævnt f.eks. kan være tab i form af mistet omsætning eller fralæggelse af den retsstridigt indvundne berigelse.

Artikel 82, stk. 1, ændrer ikke på den mulighed, der eksisterer efter dansk ret, til i visse tilfælde at tilkende godtgørelse for tort i medfør af erstatningsansvarslovens § 26 for en ikke-økonomisk skade. En sådan bestemmelse må anses for at være en sanktion efter artikel 84, der er med til at sikre forordningens effektive efterlevelse."

Det anførte af Henrik Udsen i U 2020B.226 (…) kan ikke føre til et andet resultat.

Da databeskyttelsesforordningens artikel 82 således alene omfatter erstatning for økonomisk skade, og da sagsøgerne ikke har påvist at have lidt

noget økonomisk tab, har de også af den grund ikke ret til erstatning efter artikel 82 – og dermed heller ikke efter databeskyttelseslovens § 40.

Endelig gøres det gældende, at det, der er nærmere anført nedenfor i pkt. 3.7 i forhold til erstatningsansvarslovens § 26, stk. 1, ligeledes er med til ud over det ovenfor anførte at begrunde, at der i forhold til artikel 82 og § 40 ikke foreligger en skade, som Gladsaxe Kommune er ansvarlig for.

3.6. Retsafgørelser fra andre lande samt fra Den Europæiske Menneskerettighedsdomstol

I et supplerende processkrift af 11. december 2019 har sagsøger omtalt en række afgørelser, som er truffet i andre lande eller af Den Europæiske Menneskerettighedsdomstol, og som efter sagsøgers opfattelse støtter sagsøgers påstand og anbringender.

Hertil bemærkes, at det som ovenfor anført er Gladsaxe Kommunes opfattelse, at databeskyttelsesforordningens artikel 82 alene omfatter erstatning for økonomisk skade, og at databeskyttelseslovens § 40 dermed også er begrænset til at omfatte erstatning for økonomisk skade. Dette skal ses i lyset af, at Rådet forud for sin endelige vedtagelse af forordningen ændrede udkastet til artikel 82 sådan, at man tog en formulering om, at ”skade” også omfattede ”ikke-økonomisk skade” , ud af bestemmelsen.

Det fremgår i øvrigt ikke – og kan derfor heller ikke fastslås – hvilken sammenhæng de afgørelser, der er omtalt i sagsøgers supplerende processkrift, eventuelt måtte have med f.eks. indholdet af national ret i de berør-te lande – herunder om alternativet til at anse artikel 82 for også at omfatte ikke økonomisk skade eventuelt ville være, at der i databeskyttelsesretlige sammenhænge aldrig kunne bestå en ret til godtgørelse for ikke økono-misk skade i disse lande i sager af den pågældende karakter. I nærværen-de sag gøres det som bekendt ikke gældende af Gladsaxe Kommune, at overtrædelse af databeskyttelsesretlige regler i Danmark aldrig kan med-føre krav om godtgørelse for ikke økonomisk skade. Det gøres som anført nedenfor i pkt. 3.7 i stedet gældende, at en sådan ret efter omstændighederne kan følge af erstatningsansvarslovens § 26, stk. 1. Desuden gøres det i pkt. 3.7 gældende, at de konkrete betingelser for at opnå godtgørelse ef-ter erstatningsansvarslovens § 26, stk. 1, ikke er opfyldt i nærværende sag.

I øvrigt bemærkes det, at der også kan være en række afgørende konkrete forskelle mellem de pågældende afgørelser og nærværende sag. Nogle af afgørelserne vedrører således f.eks. tilfælde, hvor den dataansvarlige egenhændigt har været skyld i eller forårsaget den belastning, som den re-

gistrerede kan have været udsat for – herunder i form af forsætlig mis-brug. Herudover må det antages, at det har haft betydning i sagerne, at den registrerede har været udsat for en belastning, som efter en konkret vurdering af dens karakter og omfang er blevet anset for at berettige til godtgørelse.

I det omfang nogle af de omhandlede afgørelser kan være udtryk for en anden retsopfattelse end den, som kommunen har givet udtryk for, følger det af det anførte, at Gladsaxe Kommune ikke er enig heri. I øvrigt gælder det generelt for de omtalte afgørelser, at de – med undtagelse af en dom fra Den Europæiske Menneskerettighedsdomstol – er truffet af domstole eller øvrige nationale myndigheder i andre EU-lande. Sådanne nationale afgørelser kan efter Gladsaxe Kommunes opfattelse ikke i sig selv udgøre nogen retskilde i dansk ret.

Om de enkelte sager bemærkes desuden følgende:

Dommen i sagen Vidal-Hall mod Google (...):

I den pågældende sag foretog den britiske domstol blandt andet en fortolkning af artikel 23 i det dagældende databeskyttelsesdirektiv, der efterfølgende er afløst af databeskyttelsesforordningen. Det vil sige, at der var tale om fortolkning af en bestemmelse, som ikke længere gælder, og som dermed heller ikke er relevant i nærværende sammenhæng. Den relevante EU-bestemmelse i nærværende sag er således databeskyttelsesforordningens artikel 82. Gladsaxe Kommune gør som tidligere anført gældende, at denne bestemmelse alene omfatter økonomisk skade, og at dette blandt andet skal ses i lyset af bestemmelsens tilblivelseshistorie, hvor Rådet in-den den endelige vedtagelse tog en formulering om, at ikke økonomisk skade også var omfattet, ud af bestemmelsen.

I øvrigt skal det nævnes, at antagelsen i den pågældende britiske dom om, at artikel 23 i det dagældende databeskyttelsesdirektiv også omfattede ik-ke økonomisk skade, ikke svarer til, hvad der må anses for at være lagt til grund blandt andet af den danske lovgivningsmagt. Der kan herved blandt andet henvises til betænkning nr. 1565/2017 "Databeskyttelsesfor-ordningen (2016/679) – og de retlige rammer for dansk lovgivning" , hvor der mere sammenfattende er anført blandt andet følgende om den dagæl-dende persondatalovs § 69 – en bestemmelse, der skulle gennemføre di-rektivets artikel 23 i dansk ret (betænkningen, side 900-901 …):

"Persondatalovens § 69, der er den nationale udmøntning af databeskyttelsesdirektivets artikel 23, fastsætter, at den dataansvarlige skal erstatte

skade, der er forvoldt ved behandling i strid med bestemmelserne i denne lov, medmindre det godtgøres, at skaden ikke kunne have været afværget ved den agtpågivenhed og omhu, der må kræves i forbindelse med be-handling af oplysninger.

Selv om det ikke klart følger af bemærkningerne til persondatalovens § 69, er der meget der taler for, at bestemmelsen alene dækker økonomisk ska-de. Justitsministeriet har bl.a. i de almindelige bemærkninger til lovforslag nr. L 162 af 28. februar 2007 om udvidelse af adgangen til tv-overvågning og styrkelse af retsbeskyttelsen ved behandling af personoplysninger i for-bindelse med tv- overvågning anført, at godtgørelse for krænkelse af lovens regler om beskyttelse af den registreredes personlige integritet, der ikke har medført et formuetab, falder uden for persondatalovens § 69. I stedet må et sådant krav i givet fald gøres gældende efter den almindelige regel om godtgørelse i erstatningsansvarslovens § 26.

Det bemærkes dog, at Registerudvalget i betænkning nr. 1345 anførte, at såvel økonomisk som ikke økonomisk skade er omfattet af persondata-lovens § 69. Det følger dog af bemærkningerne til persondataloven, at be-stemmelsen ikke – ud over fastsættelse af præsumptionsansvar – indebæ-rer andre ændringer i dansk rets almindelige erstatningsretlige regler. Det må i den forbindelse antages, at der også er tænkt på erstatningsbetingel-sen om, at der skal være lidt et *økonomisk* tab.

[…]

Derudover følger det af persondataloven med kommentarer, at godtgørel-se for tort i anledning af en krænkelse af lovens regler om beskyttelse af den registreredes personlige integritet, der ikke medfører formuetab, alene kan kræves i det omfang, at lovgivningen i øvrigt giver adgang hertil. Det vil i praksis sige i medfør af erstatningsansvarslovens § 26 (…).”

På den anførte baggrund må det antages at være lagt til grund af lovgiv-ningsmagten i Danmark, at den dagældende persondatalov, der gennem-førte persondatadirektivet i dansk ret, alene gav krav på erstatning for økonomisk skade, og at erstatning for ikke økonomisk skade må afhænge af, om betingelserne i dansk rets almindelige bestemmelse om tortgodtgø-relse i erstatningsansvarslovens § 26, stk. 1, er opfyldt.

Dommen i sagen Halliday mod Creation Consumer Finance (...):

I denne sag fremgår det af dommens oplysninger, at der blev tilkendt et beløb for lidelse, smerte mv. (”distress”) på grundlag af nationale, britiske

lovregler, hvorefter der blandt andet var ret til en sådan godtgørelse, hvis vedkommende havde lidt skade (”damage”). Dommen ses allerede derfor efter Gladsaxe Kommunes opfattelse ikke at have betydning ved en fortolkning af blandt andet databeskyttelsesforordningens artikel 82.

Dommene i sagerne mod det østrigske postvæsen (Österreichische Post AG) og mod et hollandsk agentur for arbejdsmarkedsforsikring (UWV) (...):

I disse domme afsagt af lokale/regionale domstole i henholdsvis Østrig og Holland er der efter det oplyste i medfør af databeskyttelsesforordningens artikel 82 tilkendt godtgørelse for ”uhåndgribelig modgang” og ”ikke-økonomisk tab” . Den ene dom er ifølge sagsøger vist nok anket.

Gladsaxe Kommune er som tidligere anført ikke enig i, at databeskyttelsesforordningens artikel 82 omfatter ikke økonomisk skade.

I øvrigt fremgår det ikke umiddelbart, hvorvidt der i forbindelse med de pågældende dommes fortolkning af databeskyttelsesforordningens artikel 82 er foretaget samme omfattende gennemgang af blandt andet bestem-melsens tilblivelseshistorie, sådan som det er sket f.eks. i betænkning nr. 1565/2017 ”Databeskyttelsesforordningen (2016/679) – og de retlige ram-mer for dansk lovgivning” , hvor konklusionen som tidligere omtalt er en anden. Det fremgår som omtalt ovenfor heller ikke – og kan derfor heller ikke fastslås – hvilken sammenhæng dommene eventuelt måtte have med f.eks. indholdet af national ret i de berørte lande – herunder om alternati-vet til at anse artikel 82 for også at omfatte ikke økonomisk skade eventu-elt ville være, at der i databeskyttelsesretlige sammenhænge aldrig kunne bestå en ret til godtgørelse for ikke økonomisk skade i disse lande i sager af den pågældende karakter. I nærværende sag gøres det som bekendt ik-ke gældende af Gladsaxe Kommune, at overtrædelse af databeskyttelses-retlige regler aldrig kan medføre krav om godtgørelse for ikke økonomisk skade. Det gøres som nævnt i stedet gældende, at en sådan ret efter omstændighederne kan følge af erstatningsansvarslovens § 26, stk. 1, men at de konkrete betingelser for at opnå godtgørelse efter denne bestemmelse ikke er opfyldt i nærværende sag, jf. nærmere pkt. 3.7 nedenfor.

Den Europæiske Menneskerettighedsdomstols dom af 14. februar 2012 (Romet mod Nederlandene) (...):

Om denne dom bemærkes, at Gladsaxe Kommune er enig i, at krænkelse af Den Europæiske Menneskerettighedskonvention efter omstændighe-derne kan føre til godtgørelse for tort mv.

I dansk ret er det fastslået, at hjemlen til en sådan godtgørelse sædvanlig-vis vil være princippet i erstatningsansvarslovens § 26, stk. 1, sammen-holdt med konventionens artikel 13, jf. f.eks. U 2019.4010 H (…). Det vil si-ge, at der skal foretages en konkret vurdering af, om betingelserne for tort-godtgørelse i medfør af erstatningsansvarslovens § 26, stk. 1 – eller prin-cippet i denne bestemmelse – er opfyldt i det enkelte tilfælde. Som tidlige-re anført er det Gladsaxe Kommunes opfattelse, at disse betingelser ikke er opfyldt i denne sag.

Sager ved det britiske datatilsyn om British Airways og Marriott:

I disse sager har det britiske datatilsyn efter det oplyste udtrykt en hensigt om at ville udstede meget høje administrative bøder til henholdsvis British Airways og Marriott. Der er i begge sager tilsyneladende tale om, at ude-frakommende har kunnet opnå uretmæssig adgang til de pågældende virksomheders datasystemer indeholdende kundeoplysninger mv.

I sagen om British Airways har det britiske datatilsyn (ICO) blandt andet anført i pressemeddelelse af 8. juli 2019:

”The ICO’s investigation has found that a variety of information was com-promised by poor security arrangements at the company, including log in, payment card, and travel booking details as well name and address infor-mation.”

Det britiske datatilsyn har i sagen om Marriott blandt andet anført følgen-de i pressemeddelelsen af 9. juli 2019:

”The ICO’s investigation found that Marriott failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems.”

Gladsaxe Kommune er på den baggrund ikke enig i, at det oplyste om dis-se sager skulle være udtryk for en retsopfattelse, der ville indebære, at det i nærværende sag er uden betydning, at oplysningerne er bortkommet ved udefrakommendes uretmæssige – og formodentlig kriminelle – handlin-ger. Kommunen er i den forbindelse heller ikke enig i, at de pågældende sager taler for, at Gladsaxe Kommune er forpligtet til at betale godtgørelse, selv hvis det måtte lægges til grund, at kommunen er uden nævneværdig skyld. I begge sager viser det britiske datatilsyns egen omtale således, at afgørelserne beror på en konkret vurdering blandt andet af, i hvilket om-fang de pågældende virksomheder havde forsømt at foretage tilstrækkeli-ge tekniske og sikkerhedsmæssige foranstaltninger med henblik på gene-

relt at modvirke uberettigedes adgang til deres it-systemer. Udfaldet i de to sager har derfor været bestemt af sagernes konkrete omstændigheder.

I øvrigt bemærkes det, at de to sager fra ICO som nævnt ikke udgør endelige bødeafgørelser, idet sagerne alene er udtryk for ICO's hensigt om at pålægge de pågældende virksomheder bøder afhængig af resultatet af partshøringer mv. Gladsaxe Kommune er ikke bekendt med, om der efterfølgende er truffet endelige afgørelser i sagerne.

3.7. Særligt om erstatningsansvarslovens § 26, stk. 1

Erstatningsansvarslovens § 26, stk. 1, fastsætter, at den, der er ansvarlig for en retsstridig krænkelse af en andens frihed, fred, ære eller person, skal betale den forurettede godtgørelse for tort (…).

Det er vores opfattelse, at sagsøgerne heller ikke efter denne bestemmelse har grundlag for et krav mod kommunen.

En af betingelserne for at opnå tortgodtgørelse efter § 26, stk. 1, er således, at det skal kunne lægges til grund, at der er sket en krænkelse af den en-kelte sagsøgers frihed, ære eller person i den forstand, som dette udtryk i § 26, stk. 1, må forstås.

Herom bemærkes, at de pågældende computeres bortkomst ganske vist – i hvert fald i princippet – kan indebære en risiko for, at oplysningerne om sagsøgerne er kommet eller vil kunne komme uvedkommende i hænde. Imidlertid foreligger der ingen oplysninger, der giver grundlag for at formode, at udefrakommende personer, som er ansvarlige for computernes bortkomst, overhovedet har haft viden om eller været interesseret i de eventuelle oplysninger om blandt andet sagsøgerne, der kunne ligge på den omhandlede fil. I mangel af sådanne oplysninger må det anses for sandsynligt, at de pågældende personer har stjålet computerne og dernæst f.eks. i forbindelse med videresalg eller anden anvendelse har tømt dem og bortskaffet indholdet på en sådan måde, at der ikke er nogen, som efterfølgende vil opnå kendskab til endsige interessere sig for indholdet. Uanset at det i sagens natur ikke er muligt at fastslå med sikkerhed, om det forholder sig på denne måde, må det således lægges til grund, at sandsynligheden for, at uvedkommende overhovedet opnår kendskab til de bortkomne oplysninger om sagsøgerne, er lav.

Endvidere må det indgå i vurderingen, at sandsynligheden for uvedkommendes uretmæssige anvendelse af oplysningerne om sagsøgerne må an-ses for at være meget lav. Ud over at der som anført alene vil være en lav

sandsynlighed for, at uvedkommende overhovedet har opnået eller vil op-nå kendskab til endsige interessere sig for oplysningerne om sagsøgerne, er det således heller ikke sandsynliggjort, at der vil ske misbrug af oplys-ningerne i form af f.eks. identitetstyveri. Tværtimod må en sådan sand-synlighed generelt anses for at være endog meget lav, jf. også det svar, som kommunen har givet Datatilsynet i sagen, og som henviser til en vur-dering indhentet fra PwC, hvori det er anført, at der i de seneste år har væ-ret en lang række sager, hvor navne og cpr-numre er blevet eksponeret over for uvedkommende, uden at det har medført direkte sager om identi-tetstyveri (…).

I den forbindelse bemærkes endvidere, at der var opsat en adgangskode på den pågældende computer. Det forhold, at der dermed ikke var nogen umiddelbar tilgængelighed til computerens indhold, må således også ta-ges i betragtning ved en vurdering af, om sagsøgerne overhovedet kan tænkes at kunne være blevet udsat for en krænkelse i denne sag.

Herudover gøres det gældende, at de omhandlede oplysninger om sagsø-gerne omtalt ovenfor i pkt. 2.2. har et indhold og er gengivet i en form, der også er med til at indebære, at der under de anførte omstændigheder ikke foreligger en krænkelse omfattet af § 26, stk. 1. Ganske vist er der tale om til dels fortrolige personoplysninger, og visse af oplysningerne i forhold til enkelte af sagsøgerne er følsomme personoplysninger omfattet af databe-skyttelsesforordningens artikel 9. Imidlertid er det ikke oplysninger, der giver nogen nærmere viden om f.eks. Sagsøger 1's helbreds-forhold. Regnearket er desuden opstillet på en måde, som er meget indfor-stået og teknisk, og som derfor må anses for umiddelbart svært tilgænge-lig for uvedkommende. Også disse forhold må efter vores opfattelse til-lægges betydning ved en vurdering af, om der kan være tale om en kræn-kelse i forhold til sagsøgerne.

Det skal endvidere fremhæves, at vurderingen af, om der kan foreligge en krænkelse omfattet af § 26, stk. 1, må bero på en tilgang, hvor der bliver lagt vægt på, hvad der reelt er karakteren og omfanget af en påstået kræn-kelse. Ved vurderingen af, om § 26, stk. 1, finder anvendelse, kan der der-for ikke lægges vægt på, i hvilket omfang sagsøgerne måtte have en sub-jektiv bekymring i forbindelse med det formodede tyveri af filen. Heri lig-ger ikke, at kommunen afviser, at subjektive forhold af denne karakter ef-ter omstændighederne kan foreligge, men ved en juridisk vurdering af § 26, stk. 1, og dens rækkevidde må der nødvendigvis være en objektiveret tilgang, hvor der bliver lagt vægt på de reelle forhold.

På den anførte baggrund er det vores opfattelse, at sagsøgerne ikke har godtgjort, at de har været udsat for en krænkelse, således som dette ud-tryk i § 26, stk. 1, må forstås.

Selv hvis man måtte mene, at der som følge af oplysningernes bortkomst kan være sket en krænkelse i forhold til sagsøgerne, gøres det gældende, at Gladsaxe Kommune ikke er "ansvarlig" efter § 26, stk. 1, for de handlin-ger, der har forvoldt en sådan krænkelse. Når oplysningerne er bortkom-met, beror det således som anført på, at personer, hvis handlinger kom-munen ikke er ansvarlig for, ved en uretmæssig og formodentlig kriminel handling har sat sig i besiddelse af de pågældende computere. Der forelig-ger derfor ikke noget ansvarsgrundlag efter § 26, stk. 1, i forhold til kom-munen.

Vi bemærker herved også, at der under ingen omstændigheder er tale om, at kommunen har udvist f.eks. skødesløshed eller manglende opmærk-somhed på områder, hvor der ville foreligge en væsentlig risiko for umid-delbare og alvorlige skadevirkninger. Kommunen har derimod fastsat en række retningslinjer, der har til formål at sikre, at oplysninger om borger-ne ikke kommer til uvedkommendes kendskab. Hertil kommer, at der i sa-gen indgår andre mulige og helt konkrete omstændigheder, idet der her-ved blandt andet kan henvises til det anførte om en defekt dørlås i rådhus-bygningen.

Når der skete et sikkerhedsbrud i den foreliggende sag, må det således an-tages at skyldes et sammenfald af uheldige omstændigheder, der bestod i, at en medarbejder – som var bekendt med kommunens retningslinjer, og som selv straks gjorde opmærksom på det, da det formodede tyveri blev opdaget – ved en fejl havde gemt filen på computerens lokale skrivebord henover den pågældende weekend, hvor der var udvidet adgang til råd-huset og efterfølgende viste sig at være en defekt dørlås, og hvor der anta-geligt indfandt sig én eller flere personer, som begik tyveri.

Det bestrides, at det forhold, at der er andre eksempler på sikkerhedsbrud inden for kommunen, har betydning ved en vurdering af, om kommunen har handlet ansvarspådragende i forhold til sagsøgerne. Det pågældende sikkerhedsbrud er heller ikke udtryk for, at Gladsaxe Kommune mere ge-nerelt har forsømt sine forpligtelser som dataansvarlig myndighed. I den forbindelse kan der blandt andet henvises til, at kommunen over for Data-tilsynet har nærmere redegjort for behandlingssikkerhed i henhold til da-tabeskyttelsesforordningens artikel 32 (…).Det fremgår heraf blandt andet, at Gladsaxe Kommunes informationssikkerhedspolitik og informations-sikkerhedshåndbog er baseret på standarderne ISO27001 og 27002. Desu-

den fremgår det, at kommunens fastlæggelse af politikker på området sker på grundlag af en nøje overvejet og risikobaseret tilgang til behandlingssikkerhed. Alt i alt må det derfor lægges til grund, at Gladsaxe Kommune har et højt sikkerhedsniveau.

Som ligeledes anført i pkt. 3.5. om databeskyttelsesforordningens artikel 82 kan det efter vores opfattelse heller ikke føre til et ansvar, at kommunen ikke havde krypteret harddisken i kommunens computere, herunder i den omhandlede computer, sådan at det ikke ville være teknisk muligt for en medarbejder at lagre personoplysninger ukrypteret på en computers loka-le drev. Kommunen havde i stedet gennem sine retningslinjer kommuni-keret på en klar og tydelig måde over for sine medarbejdere, at der ikke måtte ske ukrypteret lagring af personoplysninger.

Det bestrides også, at det forhold, at Gladsaxe Kommune er en offentlig myndighed, kan føre til en skærpet ansvarsvurdering. I stedet er det ved vurderingen relevant blandt andet at lægge vægt på, at kommuner og an-dre offentlige myndigheder som led i udførelsen af deres pligter og opga-ver nødvendigvis må behandle meget omfattende mængder af personoplysninger om borgere. Det ville derfor få vidtrækkende konsekvenser, hvis offentlige myndigheder kunne pådrage sig et ansvar i en situation som den foreliggende. Hvis sagsøgerne og de ca. 20.000 andre berørte borgere ville have ret til blot et relativt lille godtgørelsesbeløb på f.eks. 5.000 kr. af kommunen, ville det således indebære, at kommunen kunne blive forplig-tet til at betale samlet ca. 100 mio. kr. i godtgørelse i forbindelse med et sikkerhedsbrud, hvor de pågældende personoplysninger efterfølgende er bortkommet som følge af, at kommunen må antages at have været udsat for en kriminel handling.

Desuden skal vi pege på, at højesteretspraksis viser, at det forhold, at der måtte være sket en overtrædelse af databeskyttelsesretlige regler, ikke er er ensbetydende med, at der er ret til tortgodtgørelse. I dommen i U 2017.98 H (…), hvor en offentlig myndighed som arbejdsgiver i strid med den daværende persondatalov havde gjort sig bekendt med to ansattes helbredsoplysninger i forbindelse med behandlingen af sager om afskedigelse, fandtes der således ikke hermed at foreligge en sådan retsstridig krænkelse, at der var grundlag for tortgodtgørelse efter erstatningsansvarslovens § 26, stk. 1.

I den forbindelse gøres det endvidere gældende, at det skete sikkerheds-brud i den foreliggende sag ikke på nogen måde kan sammenlignes med de tilfælde, hvor der i retspraksis er tilkendt tortgodtgørelse, og hvor der i modsætning til nærværende sag har været tale om forsætlig og ulovlig vi-

deregivelse eller anden retsstridig disposition. Den foreliggende sag adskiller sig således på afgørende måde fra f.eks. dommen i U 2007.1967 V (…), hvor en arbejdsgiver blev dømt til at betale en tortgodtgørelse på 10.000 kr. ved som reaktion på en daværende medarbejders offentlige udtalelser, der kunne stille arbejdsgiveren i et uheldigt lys, at have offentliggjort blandt andet helbredsoplysninger om medarbejderen på sin hjemmeside. På samme måde adskiller sagen sig fra dommen i U 2011.2343 H (…), hvor en kommune havde videregivet oplysning om en tidligere an-sats mulige alkoholmisbrug til en anden kommune, hvor vedkommende skulle til jobsamtale. Højesteret fandt, at den videregivende kommune måtte vide, at oplysningen kunne være stærkt skadelig for vedkommende, som gentagne gange havde bestridt oplysningen og direkte anmodet den pågældende kommune om at hindre spredning af rygter herom. Videregi-velsen var derfor i strid med de persondataretlige regler og formentlig og-så med straffelovens regler om æreskrænkelser, og kommunen blev dømt til at betale en tortgodtgørelse på 25.000 kr.

Der kan desuden henvises til U 2020.1615 H (…), hvor Højesteret med henvisning til en række lovforarbejder mere generelt udtalte, at tort forudsætter en culpøs krænkelse af en vis grovhed, og at krænkelsen skal angå den pågældendes selv- og æresfølelse, dvs. vedkommendes opfattelse af eget værd og omdømme. I den konkrete sag bestod krænkelsen i, at der var anvendt tv-overvågning til i betydeligt omfang – uden saglig grund – løbende at kontrollere vedkommende under udførelsen af sit arbejde, og Højesteret fandt, at vedkommende som følge heraf med føje have følt sig konstant overvåget på sin arbejdsplads, og at dette havde medført en stor psykisk belastning. Den uberettigede anvendelse af tv-overvågningen havde på den baggrund haft den fornødne grovhed og havde været egnet til at krænke vedkommendes selv- og æresfølelse, og der blev herefter til-kendt en tortgodtgørelse på 20.000 kr. Som det fremgår, adskiller dommen sig fra den foreliggende sag blandt andet ved, at der var tale om en ar-bejdsgivers konstante videoovervågning af og løbende kontrol med, at en underordnet ansat udførte sit arbejde korrekt.

I modsætning til den netop omtalte dom blev der i U 2020.1879 H (…) ikke tilkendt nogen tortgodtgørelse i en sag, hvor vedkommende havde stået på en liste, som en tredjeperson sendte til et ugeblad med navne på en række offentligt kendte personer, og hvor tredjepersonen i et antal tilfælde have skaffet sig adgang til oplysninger om vedkommendes kreditkort-transaktioner og videregivet oplysningerne til ugebladet, der havde an-vendt en af disse oplysninger, der ikke afslørede følsomme forhold, i en artikel. Uanset at vedkommende herved havde været udsat for grove rets-stridige krænkelser, fandt Højesteret, at disse krænkelser efter deres ka-

rakter og omfang ikke var egnet til at påvirke vedkommendes selv- og æresfølelse. Dommen er således et eksempel på, at selv når der er tale om bevidste og grove krænkelser, vil der ikke nødvendigvis være ret til tort-godtgørelse efter erstatningsansvarslovens § 26, stk. 1.

3.8. Forrentning

Det bestrides, at et eventuelt erstatnings- eller godtgørelseskrav vil kunne forrentes fra et tidspunkt, der ligger forud for sagens anlæg…"

Rettens begrundelse og resultat

Hændelsen

I weekenden den 30. november til den 2. december 2018 blev der stjålet 4 bærbare PC´ere fra Gladsaxe Kommunes rådhus. På den ene PC var der på et lokaldrev lagret et regneark med oplysninger om 20.620 borgere, herunder de 7 sagsøgere, Sagsøger 1, Sagsøger 2, Sagsøger 3, Sagsøger 4, Sagsøger 5, Sagsøger 6 og Sagsøger 7.

Oplysningerne om sagsøgerne i regnearket

Der er enighed om, at der i regnearket var personoplysninger om alle sagsøger-ne som omhandlet i databeskyttelsesforordningens artikel 4, nr. 1 samt CPR-numre.

Der er videre enighed om, at der for så vidt angår Sagsøger 1, Sagsøger 3, Sagsøger 6 og Sagsøger 7 tillige var hel-bredsoplysninger, som omhandlet i databeskyttelsesforordningens artikel 4, nr. 15.

Vedrørende Sagsøger 4 er der tvist om, hvorvidt de yderligere oplys-ninger om ham kan anses for helbredsoplysninger. Det fremgik af regnearket, at han var registreret med ophold på institutionen Egebo, hvilket beroede på en fejlregistrering. Det fremgår, at Egebo er en institution, der henvender sig til personer med psykisk funktionsnedsættelse, ofte med skizofreni diagnoser.

Retten finder herefter, at de anførte oplysninger om Sagsøger 4 var eg-nede til at give fejlagtige informationer om hans mentale helbred eller levering af sundhedsydelser i form af institutionsophold, hvilket er information om hans helbredstilstand. Der var således også for så vidt angår Sagsøger 4 tale

helbredsoplysninger, som omhandlet i databeskyttelsesforordningens artikel 4, nr. 15.

Lovlighed, dataminimering og nødvendighed

Sagsøgernes personoplysninger skal herefter afhængigt af deres karakter blandt andet behandles i overensstemmelse med reglerne i databeskyttelsesforordningens artikel 5, 6 og 9 samt databeskyttelseslovens § 5-7.

Sagsøgerne har gjort gældende, at personoplysningerne i regnearket ikke blev behandlet lovligt og rimeligt og dermed i strid med databeskyttelsesforordnin-gens artikel 5, stk. 1, litra a og b, og databeskyttelseslovens § 5, stk. 1.

Det fremgår, at regnearket var udarbejdet til brug for kommunens sagsbehand-ling om mellemkommunal refusion. Efter de oplysninger, der er fremkommet fra kommunen til Datatilsynet og under denne sag om baggrunden for udarbej-delsen af regnearket, er der ikke grundlag for at tilsidesætte kommunens vurde-ring af, at der alene var medtaget rimelige og relevante oplysninger i forhold til formålet med regnearket. Det må herefter lægges til grund, at borgernes perso-noplysninger blev behandlet lovligt, rimeligt og på en gennemsigtig måde til brug for relevante og legitime formål, jf. databeskyttelsesforordningens artikel 5, stk. 1, litra a og b, og databeskyttelseslovens § 5, stk. 1.

Sagsøgerne har videre gjort gældende, at Gladsaxe Kommune ved udarbejdel-sen af regnearket ikke har iagttaget databeskyttelsesforordningens krav i artikel 5, stk. 1, litra c, om dataminimering. Det er blandt andet anført, at der i regnear-ket var medtaget oplysninger om for mange borgere og sagskategorier samt, at der for nogles vedkommende var oplysninger om medlemskab af Folkekirken og fødselsregistreringssted, hvilket var uden betydning for det arbejde, regnear-ket skulle bruges til.

Der er ikke for nogen af de 7 sagsøgere oplysninger om medlemskab af Fol-kekirken eller deres fødselsregistreringssted. I forhold til vurderingen af de 7 sagsøgeres sager er der allerede derfor ikke grundlag for at fastslå, at der for så vidt angår de nævnte oplysninger er medtaget irrelevante oplysninger i strid med databeskyttelsesforordningens artikel 5, stk. 1, litra c og databeskyttelses-lovens § 5, stk. 1.

Som anført ovenfor må det antages, at kommunens behandling af oplysninger-ne var rimelig og relevant. Retten finder endvidere, at behandlingen af oplys-ningerne må antages at have været nødvendig til det af kommunen oplyste for-mål. Behandlingen af oplysningerne var således i overensstemmelse med data-beskyttelsesforordningens artikel 6, stk. 1, litra e og artikel 9, stk. 2, litra f, som anført af kommunen.

Der er herefter ikke grundlag for at fastslå, at Gladsaxe Kommune har handlet i strid med principperne for behandling af personoplysninger i databeskyttelses-forordningens artikel 5, stk. 1, litra a, b eller c, ligesom der er behandlet i over-ensstemmelse med forordningens artikel 6, stk. 1, litra e og artikel 9, stk. 2, litra f og databeskyttelseslovens § 5, stk. 1.

Behandlingssikkerhed

Det fremgår af borgmesterens redegørelse om sagen på byrådsmødet den 19. december 2018, at det ikke var muligt at arbejde i regnearket og gennemføre kontrollen af den mellemkommunale refusion, mens regnearket var lagret i kommunens dokumenthåndteringssystem. Det var derfor nødvendigt for den medarbejder, der udførte arbejdet, at lagre regnearket midlertidigt et andet sted. Det fremgår, at medarbejderen gemte regnearket på sin PC´s skrivebord onsdag den 28. november 2018, og at det fortsat var lagret sådan op til weeken-den den 30. november 2018. Den omhandlede PC og 3 andre bærbare PC´ere blev stjålet en af de næstfølgende dage, hvilket blev opdaget mandag den 3. de-cember 2018.

Den PC, regnearket var lagret på, var sikret med sædvanlige Windows foran-staltninger om brugernavn og adgangskode. Harddisken var ikke krypteret.

Det kan efter oplysningerne fra Datatilsynet lægges til grund, at det forholdsvis enkelt er muligt at tilgå harddisken, hvis den kobles på en anden PC. Der er imidlertid ikke for nogen af sagsøgerne grundlag for at fastslå, om andre er kommet i besiddelse af regnearket med oplysningerne om dem.

Lagringen af regnearket med oplysninger om 20.620 borgere på den bærbare PC´s lokaldrev var en overtrædelse af kommunens informationssikkerhedspoli-tik, hvoraf det fremgår, at der ikke måtte lagres personoplysninger på ikke-krypterede flytbare medier. Det var endvidere en overtrædelse af kommunes 15 sikkerhedsbud, hvor det blandt andet fremgår, at der ikke måtte lagres perso-noplysninger på lokale drev.

Under hensyn til omfanget af personoplysninger i regnearket sammenholdt med, at det var kommunen bekendt, at arbejdet med oplysningerne i regnearket ikke kunne foregå i dokumenthåndteringssystemet, var der særlig anledning for kommunen til at overveje tekniske og organisatoriske sikkerhedsforanstalt-ninger for at sikre et passende sikkerhedsniveau til imødegåelse af den ikke us-andsynlige risiko for, at der skete lagring af dokumenter på ikke sikrede drev og tyveri. Kommunen traf ikke sådanne foranstaltninger.

Retten finder herefter, at kommunen som dataansvarlig ikke har overholdt databeskyttelsesforordningens krav til behandlingssikkerhed som omhandlet i databeskyttelsesforordningens artikel 32, stk. 1, og stk. 2, jf. artikel 5, stk. 1, litra f.

Ret til erstatning og erstatningsansvar

Det følger af forordningens artikel 82, stk. 1, og databeskyttelseslovens § 40, at enhver, der har lidt materiel eller immateriel skade som følge af en ulovlig behandlingsaktivitet eller enhver anden behandling i strid med loven eller forordningen, har ret til erstatning efter forordningens artikel 82.

Fritagelse for erstatningsansvar

Efter forordningens artikel 82, stk. 3, fritages den dataansvarlige for erstatningsansvar, hvis det bevises, at den pågældende er uden skyld i den begivenhed, der medførte skaden.

Retten bemærker, at tyveri af bærbare elektroniske enheder ikke er ualminde-ligt, hvorfor det forhold, at PC´en blev stjålet, ikke i sig selv kan begrunde ansvarsfrihed.

Som fastslået ovenfor kan det bebrejdes kommunen, at der ikke var truffet passende tekniske eller organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der tog højde for omfanget af de personoplysninger, der indgik i regnear-ket, sammenholdt med den ikke usandsynlige risiko for, at medarbejderen gem-te regnearket på et ikke sikret lokale drev og for tyveri.

Retten finder herefter, at der ikke er grundlag for at statuere ansvarsfrihed efter forordningens artikel 82, stk. 3.

Sagsøgernes krav

Sagsøgernes krav vedrører ikke-økonomisk skade, der i dansk ret betegnes som godtgørelse.

Det er ikke i databeskyttelsesforordningens artikel 82 og databeskyttelseslovens § 40 defineret, hvad der skal forstås ved immateriel skade. Bemærkningerne til databeskyttelseslovens § 40 kan forstås således, at der ikke i forordningens arti-kel 82 er hjemmel til godtgørelse for ikke-økonomisk skade. Vurderingen heraf må bero på en nærmere fortolkning af forordningens skadesbegreb.

Skadesbegrebet i databeskyttelsesforordningens artikel 82

Det følger af ordlyden af databeskyttelsesforordningens artikel 82, stk. 1, at enhver, som har lidt materiel eller immateriel skade som følge af en overtrædelse af forordningen, har ret til erstatning for den forvoldte skade fra den dataansvarlige eller databehandleren.

Det kan af bestemmelsens ordlyd ikke udledes, om bestemmelsen udover økonomisk skade også omfatter ikke-økonomisk skade.

Det fremgår af præamblen til databeskyttelsesforordningen, at beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger er en grundlæggende rettighed, og at formålet med forordningen er at beskytte fysiske personer i forbindelse med behandling af deres personoplysninger.

Af præambelbetragtning nr. 85 i forordningen henvises blandt andet til, at brud på persondatasikkerheden kan påføre fysiske personer fysisk, materiel eller immateriel skade, såsom tab af kontrol over deres personoplysninger eller begrænsning af deres rettigheder, forskelsbehandling, identitetstyveri eller -svig, finansielle tab, uautoriseret ophævelse af pseudonymisering, skade på omdøm-me, tab af fortrolighed for oplysninger, der er omfattet af tavshedspligt, eller andre betydelige økonomiske eller sociale konsekvenser for den berørte fysiske person.

Det fremgår videre af præambelbetragtning nr. 146 blandt andet, at den dataansvarlige eller databehandleren bør yde erstatning for enhver skade, som en person måtte lide som følge af behandling, der overtræder denne forord-ning, og at begrebet »skade« bør fortolkes bredt i lyset af retspraksis ved Dom-stolen, således at det fuldt ud afspejler formålene for denne forordning.

EU-Domstolen har ikke fortolket skadesbegrebet i databeskyttelsesforordnin-gens artikel 82, stk. 1, men har fortolket skadesbegrebet i andre EU-retsakter, og af afgørelser fra EU-Domstolen fremgår, at EU-Domstolen i flere tilfælde har tilkendegivet, at skadesbegrebet må fortolkes i lyset af blandt andet formålet med den pågældende retsakt. Det fremgår videre, at EU-Domstolen - ved fortolk-ning af bestemmelser i andre retsakter om skadesbegrebet, hvor det i den på-gældende bestemmelse ikke er præciseret, om ikke-økonomisk skade er omfat-tet - har anlagt en bred fortolkning af skadesbegrebet, og at EU-Domstolen blandt andet under hensyn til beskyttelseshensyn har konkluderet, at erstatning for ikke økonomisk skade er omfattet.

Der henvises herved blandt andet til EU-Domstolens dom af 12. marts 2002, sag nr. C-168/00, som omhandler en præjudiciel forelæggelse om fortolkningen af artikel 5 i Rådets direktiv 90/314/EØF af 13. juni 1990 om pakkerejser, herunder pakkeferier og pakketure, og til EU-Domstolens dom af 24. oktober 2013, C-277/12, som angik en præjudiciel forelæggelse om fortolkning af skadesbegrebet

i artikel 3, stk. 1, i Rådets direktiv 72/166/EØF af 24. april 1972 om indbyrdes tilnærmelse af medlemsstaternes lovgivning om ansvarsforsikring for motorkøretøjer og kontrollen med forsikringspligtens overholdelse.

Det følger af retspraksis fra EU-Domstolen, at begrebet "immateriel skade" ikke er entydig og i nogle tilfælde bruges om ikke-økonomisk skade, hvilket blandt andet fremgår af den ovenfor nævnte dom fra EU-Domstolen af 24. oktober 2013, C-277/12.

Skader som følge af overtrædelse af databeskyttelsesforordningen må ofte antages at være af ikke-økonomisk karakter, og der henvises herved blandt andet til de eksempler på immateriel skade af ikke-økonomisk karakter, som er anført i præambelbetragtning 85.

Der er i databeskyttelsesforordningen ikke præambelbetragtninger eller bestemmelser, som giver holdepunkter for at lægge til grund, at EU-lovgiver med bestemmelsen i artikel 82, stk. 1, har villet begrænse retten til erstatning således, at der kun kan kræves erstatning for økonomisk tab. Derimod fastslås det udtrykkeligt i præambelbetragtning nr. 146, at begrebet »skade« bør fortolkes bredt i lyset af retspraksis ved Domstolen, således at det fuldt ud afspejler for-målene for forordningen.

Herefter og når henses til beskyttelseshensynene i databeskyttelsesforordnin-gen, må forordningens artikel 82, stk. 1, fortolkes således, at bestemmelsen også omfatter erstatning/godtgørelse for ikke-økonomisk skade.

Sagsøgernes krav på erstatning/godtgørelse for ikke-økonomisk skade

Vurderingen af, om sagsøgerne har været udsat for en ikke-økonomisk skade, der kan begrunde en godtgørelse efter databeskyttelsesforordningens artikel 82, må bero på arten og karakteren af den krænkelse, sagsøgerne har været udsat for, sammenholdt med databeskyttelsesforordningens beskyttelsesformål og hensynet til en effektiv håndhævelse af forordningen.

Som ovenfor anført er skaden for så vidt angår de 7 sagsøgere forvoldt ved, at Gladsaxe Kommune ikke har opfyldt sine forpligtelser i databeskyttelsesforordningen ved behandlingen af summariske personoplysninger i et regneark over de i alt 20.620 borgere, som de 7 sagsøgere er iblandt.

Oplysningerne vedrører personoplysninger for alle sagsøgere og - når bortses fra Sagsøger 5 og Sagsøger 2 – tillige helbredsoplys-ninger. For Sagsøger 5's vedkommende gør sig særskilt gældende, at hun har beskyttet adresse.

Oplysningerne i Sagsøger 3's og Sagsøger 5's sager giver ikke grundlag for at fastslå, at det, de har været udsat for vedrørende deres Ne-mid og netbank, har sammenhæng med oplysningerne om dem i regnearket.

Der er og vil imidlertid for alle sagsøgerne bestå en risiko for, at oplysningerne om sagsøgerne i regnearket uberettiget er kommet eller kommer i andres besid-delse.

En borger har en legitim og beskyttelsesværdig interesse i, at dennes personda-ta beskyttes, og efter Sagsøger 6, Sagsøger 3, Sagsøger 1 og til dels Sagsøger 4's forklaringer lægger ret-ten til grund, at de nævnte sagsøgere subjektivt set har følt sig krænkede over det brud på datasikkerheden, som er sket. Sådanne subjektive følelser kan imid-lertid ikke i sig selv anses for tilstrækkelige til, at sagsøgerne har ret til erstat-ning/godtgørelse for ikke-økonomisk skade i medfør af databeskyttelsesforord-ningens artikel 82, stk. 1.

Et krav på erstatning, herunder godtgørelse for ikke-økonomisk skade, efter da-tabeskyttelsesforordningen, må efter rettens opfattelse kræve, at det skete brud på datasikkerheden har medført skade eller nærliggende risiko for skade på fx omdømme, tab af fortrolighed, identitetstyveri eller andre økonomiske eller so-ciale konsekvenser for sagsøgerne af en vis kvalificeret karakter.

Efter en samlet vurdering af det skete brud på datasikkerheden og sammen-holdt med arten og karakteren af de summariske oplysninger om hver enkelt af sagsøgerne, bruddet har omfattet, er der ikke grundlag for at fastslå, at sagsø-gerne har været udsat for en sådan skade, der kan begrunde en erstatning.

Retten finder således, at der ikke er grundlag for at tilkende sagsøgerne en er-statning efter databeskyttelsesforordningens artikel 82 for ikke økonomisk ska-de.

Erstatningsansvarslovens § 26

Sagsøgerne har subsidiært gjort gældende, at de har krav på tortgodtgørelse ef-ter erstatningsansvarslovens § 26.

Henset til karakteren af de summariske oplysninger om hver enkelt af sagsøger-ne, som bruddet på datasikkerheden har omfattet, er der ikke grundlag for at fastslå, at sagsøgerne har været udsat for en sådan krænkelse, at der er grund-lag for tilkendelse af tortgodtgørelse.

Gladsaxe Kommunes frifindelsespåstande tages med disse bemærkninger til følge.

Sagsomkostninger

Ingen af sagsøgerne har fået medhold i de nedlagte påstande og har således tabt sagen.

Kommunen har imidlertid tabt hovedspørgsmålene om, hvorvidt der var den fornødne behandlingssikkerhed samt spørgsmålet om, hvorvidt der er hjemmel i databeskyttelsesforordningens artikel 82, stk. 1, til at yde godtgørelse for ikke økonomisk skade.

Retten finder på denne baggrund, at ingen af parterne skal betale sagsomkostninger til den anden part, og sagens omkostninger ophæves.

T H I K E N D E S F O R R E T :

Gladsaxe Kommune frifindes.

Ingen af parterne skal betale sagsomkostninger til den anden part eller til statskassen.


DANMARKS DOMSTOLE