DATABEHANDLERAFTALE

MELLEM

GREVE KOMMUNE OG LEVERANDØRER

REVIDERET VERSION - JANUAR 2020

Standardkontraktsbestemmelser

i henhold til artikel 28, stk. 3, i forordning 2016/679 (databeskyttelsesforordningen) med henblik på databehandlerens behandling af personoplysninger.

Mellem

Greve Kommune
CVR: 44 02 39 11
Rådhusholmen 10
2670 Greve
Danmark

herefter ”den dataansvarlige”

og

Navn
CVR:
Adresse
Postnummer og by
Danmark

herefter ”databehandleren”

der hver især er en ”part” og sammen udgør ”parterne”

HAR AFTALT følgende standardkontraktsbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder.

1. Indhold

2. Præambel

1. Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.

2. Disse bestemmelser er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (databeskyttelsesforordningen).

3. I forbindelse med levering af opgaver under aftalen NAVN af den xx. måned 202x behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.

5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.

6. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.

7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.

8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.

9. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke af omfattet af Bestemmelserne.

10. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.

11. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

3. Den dataansvarliges rettigheder og forpligtelser

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel

24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes[1] nationale ret og disse Bestemmelser.

2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.

3. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

4. Databehandleren handler efter instruks

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt. Denne instruks skal være specificeret i bilag A og C. Efterfølgende instruks kan også gives af den dataansvarlige, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Bestemmelser.

2. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

5. Fortrolighed

1. Databehandleren må kun give adgang til personoplysninger, som behandles på den dataansvarliges vegne, til personer, som er underlagt databehandlerens instruktionsbeføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og kun i det nødvendige omfang. Listen af personer, som har fået tildelt adgang, skal løbende gennemgås. På baggrund af denne gennemgang kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.

2. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

6. Behandlingssikkerhed

1. Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

1 Henvisninger til "medlemsstat" i disse bestemmelser skal forstås som en henvisning til "EØS-medlemsstater".

Den dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

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. Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den dataansvarlige stille den nødvendige information til rådighed for databehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.

3. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

   Hvis imødegåelse af de identificerede risici – efter den dataansvarliges vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som databehandleren allerede har gennemført, skal den dataansvarlige angive de yderligere foranstaltninger, der skal gennemføres, i bilag C.

7. Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).

2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående specifik skriftlig godkendelse fra den dataansvarlige.

3. Databehandleren må kun gøre brug af underdatabehandlere med den dataansvarliges forudgående specifikke skriftlige godkendelse. Databehandleren skal indgive anmodningen om en specifik godkendelse mindst 14 arbejdsdage inden anvendelsen af den pågældende underdatabehandler. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

   Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.

5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.

6. Databehandleren skal i sin aftale med underdatabehandleren indføje den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandlere, som f.eks. gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.

7. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

8. Overførsel til tredjelande eller internationale organisationer

1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra den dataansvarlige og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.

2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af den dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:

   a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation,

b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland,
c. behandle personoplysningerne i et tredjeland.

4. Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, skal angives i afsnit C.6.

5. Disse Bestemmelser skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

9. Bistand til den dataansvarlige

1. Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel III.

   Dette indebærer, at databehandleren så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

   a. oplysningspligten ved indsamling af personoplysninger hos den registrerede,
   b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede,
   c. indsigtsretten,
   d. retten til berigtigelse,
   e. retten til sletning (”retten til at blive glemt”),
   f. retten til begrænsning af behandling,
   g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling,
   h. retten til dataportabilitet,
   i. retten til indsigelse,
   j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering.

2. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3, bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:

   a. den dataansvarliges forpligtelse til uden unødig forsinkelse og om muligt senest 72 timer efter, at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.

   b. den dataansvarliges forpligtelse til uden unødig forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis

vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder.

c. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse).

d. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet, inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.

3. Parterne skal i bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå den dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 9.1. og 9.2.

10. Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 24 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.

3. I overensstemmelse med Bestemmelse 9.2.a skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:

   a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger.

   b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden.

   c. de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

4. Parterne skal i bilag C angive den information, som databehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

11. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at tilbagelevere alle personoplysningerne og slette

eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

12. Revision, herunder inspektion

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.

2. Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i afsnit C.7.

3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

13. Parternes aftale om andre forhold

1. Parterne kan aftale andre bestemmelser vedrørende tjenesten vedrørende behandling af personoplysninger om f.eks. erstatningsansvar, så længe disse andre bestemmelser ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

14. Ikrafttræden og ophør

1. Bestemmelserne træder i kraft på datoen for begge parters underskrift heraf.

2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.

3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.

4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og afsnit C.4, kan Bestemmelserne opsiges med skriftligt varsel af begge parter.

5. Underskrift

   På vegne af den dataansvarlige

Navn	Martin Nordentoft Rasmussen
Stilling	Centerchef, Center for Sundhed & Pleje
Telefonnummer	43 97 94 66
E-mail	mnr@greve.dk
Dato	
Underskrift	

På vegne af databehandleren

Navn
Stilling
Telefonnummer
E-mail
Dato
Underskrift

15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

Dataansvarlig:

Navn	Susanne Hass
Stilling	Fagkoordinator, Center for Sundhed & Pleje
Telefonnummer	43 97 95 48
E-mail	has@greve.dk

Databehandler:
Navn
Stilling
Telefonnummer
E-mail

Bilag A Oplysninger om behandlingen

A.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Databehandler varetager hjemmepleje i form af praktisk hjælp på vegne af Greve Kommune. Hjemmepleje omfatter levering af ydelser jf. Aftalen til borgere, der bor i eget hjem i kommunen. De leverede ydelser skal dokumenteres på den enkelte borger i Greve Kommunes omsorgssystem. Ligeledes skal databehandleren have adgang til at læse oplysninger om den enkelte borgere i omsorgssystemet.

A.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)

Dokumentation i Greve Kommunes omsorgssystem af leverede ydelser samt af relevante og nødvendige oplysninger om den enkelte borger. Dokumentation skal foregå jf. gældende procedurer.

A.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Almindelige personoplysninger som navn, adresse og telefonnummer.
Oplysninger om helbredsforhold
CPR. nr.

A.4. Behandlingen omfatter følgende kategorier af registrerede

Borgere i Greve Kommune.

A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen har følgende varighed

Behandlingen af personoplysninger følger varigheden af aftalen NAVN af den xx. måned 202x.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden den dataansvarliges skriftlige godkendelse – gøre brug af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden underdatabehandler til denne behandlingsaktivitet.

B.2. Varsel for godkendelse af underdatabehandlere

Der henvises til afsnit 7.3 i Bestemmelserne.

Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende:

Der henvises til godkendelsesmaterialet (bilag 2-7.1), der indgå som del af aftalen.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

Behandlingen omfatter en større mængde personoplysninger omfattet af databeskyttelsesforordningens artikel 9 om "særlige kategorier af personoplysninger", hvorfor der skal etableres et "højt" sikkerhedsniveau.

Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etableret det nødvendige (og aftalte) sikkerhedsniveau.

Databehandleren skal dog – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige:

Kontakt punkt

Databehandleren skal udpege et fast kontakt punkt, som over for den dataansvarlige skal varetage ethvert forhold i relation til behandlingen af personoplysninger på vegne af den dataansvarlige.

Risici for sikkerhed

Databehandleren skal tage de nødvendige skridt til at identificere, vurdere og begrænse enhver, med rimelighed forudsigelig, intern og ekstern risiko for tilgængeligheden, fortroligheden, og/eller integriteten af alle personoplysninger omfattet af databehandleraftalen.

Databehandleren skal have passende tekniske foranstaltninger til at begrænse risikoen for enhver uautoriseret adgang. Databehandleren skal desuden, hvor det er nødvendigt, evaluere og forbedre effektiviteten af sådanne forholdsregler.

Databehandleren skal dokumentere de identificerede risici og – for enhver af disse risici – hvordan risikoen er nedbragt til et acceptabelt niveau.

Databehandleren skal have formelle processer for håndtering af sikkerhedshændelser. Databehandleren skal ved hændelser, hvor personoplysningers fortrolighed, integritet eller tilgængelighed kan være eller have været negativt påvirket, underrette den dataansvarlige uden ugrundet ophold.

Autorisation og adgangskontrol

Databehandleren skal især iagttage følgende vedrørende autorisation og adgangskontrol:
Autorisationer skal angive, i hvilket omfang brugeren må forespørge eller inddatere personoplysninger.

Databehandleren skal sikre, at der foretages et efter omstændighederne passende baggrundstjek for alt personale, der i forbindelse med deres ansættelse vil have adgang til personoplysninger omfattet af databehandleraftalen, uanset i hvilket format personoplysninger måtte være tilgængelige.

Kun de personer, som autoriseres dertil, må have adgang til personoplysninger, der behandles.

Der må kun autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for.

Der må endvidere autoriseres personer, for hvem adgang til personoplysningerne er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver.

Den autoriserede bruger udstyres med en personlig brugeridentifikation og et password, der skal anvendes hver gang, der logges på systemet. Som udgangspunkt anvendes 2-faktor-autentificering ved adgang til systemer med følsomme personoplysninger via internettet eller andet usikkert netværk. Autentifikationsmetoden kan f.eks. være NemID, SMS-token, Rfid eller lignende.

Databehandleren skal sikre, at databehandlerens medarbejdere modtager tilstrækkelig uddannelse og instruktioner, inklusiv – men ikke begrænset til – uddannelse der tilsigter mod at øge medarbejdernes generelle sikkerhedsbevidsthed, introduktion af relevante sikkerhedspolitikker og procedurer, samt adgang til og uddannelse i dokumenterede processer og arbejdsbeskrivelser særligt vedrørende behandling af personoplysninger. Uddannelse og instruktioner skal omfatte de emner, der er relevante for at sikre, at personoplysninger behandles i overensstemmelse med såvel lovgivningen som databehandlerens og den dataansvarliges relevante politikker og procedurer.

Autorisation gives til den dataansvarliges systemer af den dataansvarlige efter den dataansvarliges indstilling.

Der skal træffes foranstaltninger til at sikre, at kun autoriserede brugere kan få adgang til personoplysninger, og at brugeren kun kan få adgang til de personoplysninger og anvendelser (behandlinger), som den pågældende er autoriseret til.

Alle ansatte hos databehandleren, der har med elektronisk databehandling at gøre, udstyres med en brugeridentifikation og et password med henblik på adgang til databehandlerens netværk. Brugeridentifikation og password skal anvendes hver gang, brugeren skaber sig intern adgang til databehandling. Eksternt skal adgange til databehandling etableres med 2-faktor-autentifikation.

Databehandleren skal have rimelige restriktioner for fysisk adgang. Områder, hvor der sker behandling af personoplysninger, skal ved etablering af ovennævnte adgangskontrol mekanismer være effektivt adskilt fra områder, hvortil der er generel adgang.

Databehandleren skal have formelle procedurer for håndtering af nulstilling af adgangskoder og andre situationer, hvor den normale logiske adgangskontrol sættes ud af kraft.

Databehandleren skal have formelle procedurer, som håndterer periodisk skift af password til systemerne.
For Greve Kommune gælder følgende sikkerhedsniveau i forhold til password:

- Password skal som minimum være 8 karakterer (tegn) langt.
- Password skal skiftes minimum hver 3 måned.
- Password skal være dannet af tegn, bogstaver og tal.

Der skal mindst en gang hvert halve år foretages kontrol af, at brugerne kun er tildelt de adgange, som de har behov for. Denne kontrol kan f.eks. indebære, at der i systemerne dannes en statistik over den enkelte brugers anvendelse af systemet, således at det kan konstateres, om der er udstedte autorisationer, som ikke er anvendt, og som derfor eventuelt bør inddrages. Ved anvendelse af en sådan statistisk opfølgning vil der fortsat være behov for en konkret vurdering af, om medarbejderen har et fortsat arbejdsmæssigt behov for adgang.

Databehandleren skal uden ugrundet ophold inddrage autorisationer (og herunder adgange) for brugere, der ikke længere har behov for autorisationen i forbindelse med brugerens arbejde.

Kontrol med afviste adgangsforsøg og logning

Databehandleren skal iagttage følgende vedrørende kontrol med afviste adgangsforsøg og logning:

1. Der skal foretages registrering af alle afviste adgangsforsøg. Afviste adgangsforsøg sagsbehandles enkeltvist, og der blokeres for yderligere forsøg, når dette vurderes nødvendigt. Adgangen åbnes først, når årsagen til afviste adgangsforsøg er klarlagt.

2. Der skal foretages maskinel registrering (logning) af alle anvendelser af personoplysninger omfattet af lov om behandling af personoplysninger. Loggen skal mindst indeholde oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte eller det anvendte søgekriterium. Loggen skal opbevares i seks måneder, hvorefter den skal slettes, medmindre der i overensstemmelse med loggens formål fastsættes en længere opbevaringsperiode, dog højest 5 år, af hensyn til at kunne anvende den som værktøj til brug ved efterforskning.

3. Bestemmelsen i punkt 2 finder ikke anvendelse for personoplysninger, som indgår i tekstbehandlingsdokumenter og lignende, der ikke foreligger i endelig form. Det samme gælder sådanne dokumenter, som foreligger i endelig form, hvis der sker sletning inden for 30 dage. Logning kravet vil fortsat gælde ved rutinemæssig administration som har karakter af føring af et edb-register.

4. Bestemmelsen i punkt 2 finder ikke anvendelse, hvis behandlingen af personoplysninger sker ved afvikling af programmer, som foretager en foruddefineret masse behandling af personoplysninger, eller hvis behandlingen sker med henblik på statistiske eller videnskabelige undersøgelser, og identifikationsoplysningerne forinden enten er krypteret eller erstattet med kodenummer eller lignende. Der skal dog i begge tilfælde foretages maskinel logning af brugeren og tidspunktet for behandlingen, jf. punkt 2.

Inddatamateriale som indeholder personoplysninger

Databehandleren skal iagttage følgende vedrørende inddatamateriale, der indeholder personoplysninger:

1. Inddatamateriale, som ikke indgår i en manuel sag eller et manuelt register, må kun anvendes af personer, som er beskæftiget med inddateringen. Inddatamateriale, som indeholdende personoplysninger, skal opbevares på en sådan måde, at uvedkommende ikke kan få adgang til at gøre sig bekendt med de personoplysninger, der er indeholdt heri, når det ikke anvendes.

2. Inddatamateriale, som er nævnt i punkt 1, skal slettes eller tilintetgøres, når det ikke længere er nødvendigt at bevare det af hensyn til de formål, som behandlingen varetager eller til kontrol med de inddaterede personoplysninger.

3. Bestemmelsen i pkt. 2 gælder ikke, såfremt materialet er omfattet af bevarings-/kassationsbestemmelser fastsat i henhold til anden lovgivning. Inddatamateriale, der er journaliseret i henhold til gældende journaliseringsbestemmelser, behandles efter de almindelige arkivbestemmelser om bevaring, herunder aflevering af arkivalier til Statens Arkiver. Databehandler orienteres, hvis denne bestemmelse gør sig gældende.

4. Ved tilintetgørelse af inddatamateriale skal der træffes fornødne sikkerhedsforanstaltninger for at undgå, at materialet misbruges eller, at materialet kommer til uvedkommendes kendskab.

Uddatamateriale som indeholder personoplysninger

Databehandleren skal iagttage følgende vedrørende uddatamateriale som indeholder personoplysninger:

1. Uddata må kun anvendes af personer, der er beskæftiget med de formål, til hvilke behandlingen af personoplysningerne foretages.

2. Udover bestemmelsen i punkt 1 må uddatamateriale anvendes af personer, som er beskæftiget med sikkerheds- og/eller forvaltningsmæssig revision eller drifts- og systemtekniske opgaver vedrørende det pågældende system og systemets anvendelse.

3. Uddatamateriale skal både fysisk og teknisk opbevares på en sådan måde, at uvedkommende ikke kan få adgang til at gøre sig bekendt med de personoplysninger, som er indeholdt i materialet.

4. Uddatamateriale skal tilintetgøres, når det ikke længere er nødvendigt til de formål, som behandlingen varetager.

5. Bestemmelsen i punkt 4 gælder ikke, såfremt materialet er omfattet af bevarings-/kassationsbestemmelser i henhold til anden lovgivning.

6. Uddatamateriale, der er journaliseret i henhold til vedtagne journaliseringsbestemmelser, behandles efter de almindelige arkivbestemmelser om bevaring, herunder aflevering af arkivalier til Statens Arkiver. Databehandler orienteres, hvis denne bestemmelse gør sig gældende.

7. Ved tilintetgørelse af uddatamateriale skal der træffes de fornødne sikkerhedsforanstaltninger for at undgå, at materialet misbruges eller, at materialet kommer til uvedkommendes kendskab.

8. Bestemmelserne i punkterne 1-5 gælder ikke for uddatamateriale, som indgår i en manuel sag eller i et manuelt register.

Mobile lagringsmedier

Databehandleren skal iagttage følgende vedrørende mobile lagringsmedier:

1. Mobile lagringsmedier med personoplysninger skal være mærket og skal opbevares krypteret under opsyn eller under lås, når de ikke benyttes.

2. Mobile lagringsmedier med personoplysninger må kun udleveres til medarbejdere samt til autoriserede personer, der har adgang til personoplysningerne, med henblik på revision eller drifts- og systemtekniske opgaver.

3. Der skal føres en fortegnelse over, hvilke mobile lagringsmedier, der benyttes i forbindelse med databehandlingen.

4. Der skal udarbejdes skriftlige instrukser for anvendelse og opbevaring af udtagelige mobile lagringsmedier.

5. I forbindelse med reparation og service af dataudstyr, der indeholder personoplysninger, samt ved salg og kassation af anvendte datamedier skal der træffes fornødne foranstaltninger for at sikre, at personoplysningerne ikke hændeligt eller bevidst tilintetgøres, fortabes eller forringes eller, at personoplysningerne kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med persondataloven.

Beskyttelse mod ondsindet software
Databehandleren skal have formelle procedurer til sikring af udstyr er beskyttet mod ondsindet koder og programmer. Med dette menes at man har en antivirus løsning som er opdateret og periodisk scanner udstyr for virus samt at der udføres "patchning" af programmer og operativsystemer i henhold til "best practice".

Transmission af data
Databehandleren skal sikre at persondata ikke sendes ubeskyttet over det åbne net. Data skal således sendes i krypteret form når det sendes via internettet.

Driftsafbrydelser
Databehandleren skal have dokumenterede beredskabsprocedurer, der sikrer genetablering af services inden for rimelig tid i tilfælde af driftsafbrydelser.

Bortskaffelse af udstyr
Databehandleren skal have formelle processer med henblik på at sikre, at der sker effektiv sletning af personoplysninger inden bortskaffelse af elektronisk udstyr i overensstemmelse med den dataansvarliges krav.

Tilsyn
Databehandleren skal føre og dokumentere et tilsyn med databehandlerens organisations overholdelse af lovkrav, politikker og procedurer.

C.3 Bistand til den dataansvarlige
Databehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

Databehandleren skal på opfordring fra den dataansvarlige hjælpe med at opfylde den dataansvarliges forpligtelser i forhold til den registreredes rettigheder, herunder besvarelse af anmodninger fra borgere om indsigt i egne oplysninger, udlevering af borgerens oplysninger, rettelse og sletning af oplysninger, begrænsning af behandling af borgerens oplysninger, samt den dataansvarliges forpligtelser i forhold til underretning af den registrerede ved brud på sikkerheden, i medfør af Databeskyttelsesforordningens kap. III samt artikel 34.

Databehandleren skal hjælpe den dataansvarlige med at efterleve dennes forpligtelser efter Databeskyttelsesforordningens artikel 32-36.

Databehandleren garanterer at levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at implementere passende tekniske og organisatoriske foranstaltninger sådan, at

Databehandlerens behandling af den dataansvarliges personoplysninger opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.

Databehandleren er forpligtet til at oplyse med præcise adresseangivelser, hvor den dataansvarliges personoplysninger opbevares, jf. afsnit C.5. Databehandleren skal ajourføre oplysningerne over for den dataansvarlige ved enhver ændring.

C.4 Opbevaringsperiode/sletterutine
Al dokumentation og opbevaring af data foregår i den dataansvarliges omsorgssystem. Det er ikke tilladt at slette data i systemet.

Data i systemet arkiveres efter gældende regler.

C.5 Lokalitet for behandling
Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end følgende:

Navn leverandør og adresse

Databehandler er navn på leverandør.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande
Hvis den dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsel af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af disse Bestemmelser at foretage sådanne overførsler.

Der må ikke overføres personoplysninger til tredjeland.

C.7 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren
Databehandler er forpligtet til uden ugrundet ophold at give den dataansvarlige nødvendige oplysninger til, at den dataansvarlige til enhver tid kan sikre sig, at databehandleren overholder de krav, der følger af disse Bestemmelser.

Den dataansvarlige, en repræsentant for den dataansvarlige eller dennes revision (såvel intern som ekstern) har adgang til at foretage inspektioner og revision hos databehandleren, eksempelvis få udleveret dokumentation, stille spørgsmål m.v. med henblik på at konstatere, at databehandleren overholder de krav, der følger af disse Bestemmelser.

I tilfælde af, at den dataansvarlige og/eller relevante offentlige myndigheder, særligt Datatilsynet, ønsker at foretage en inspektion af de ovennævnte foranstaltninger i henhold til disse Bestemmelser, forpligter databehandleren og databehandlerens underleverandører sig til uden yderligere omkostninger for den dataansvarlige at stille tid og ressourcer til rådighed herfor.

Bilag D Parternes regulering af andre forhold

Ingen yderligere regulering.