DATABEHANDLERAFTALE vedr. Indkøbsordning til visiterede borgere i eget hjem

Mellem

Hvidovre Kommune
Hvidovrevej 278
2650 Hvidovre

Glostrup Kommune
Rådhusparken 2
2600 Glostrup
(CVR nr. 65120119)

Rødovre Kommune
Rødovre Parkvej 150
2610 Rødovre
CVR: 65307316

Herefter benævnt Dataansvarlig

Og

<Navn på databehandler>
<Adresse på databehandler>
<Postnr. og by på databehandler>
(CVR nr. <databehandler>)

Herefter benævnt Databehandler

Generelt
Databehandleren indestår for at Databehandleren overholder de til enhver tid gældende regler og forskrifter for behandling af personoplysninger som Databehandleren behandler på vegne af den Dataansvarlige, herunder:

- Lov nr. 429 af 31/05/2000 med senere ændringer om behandling af personoplysninger (Persondataloven).

- Bekendtgørelse nr. 528 af 15/06/2000 med senere ændringer (Sikkerhedsbekendtgørelsen)

- Vejledning nr. 37 af 02/04/2001 til bekendtgørelse nr. 528 af 15/06 2000 (Sikkerhedsvejledningen)

Når Databehandleren foretager behandling af personoplysninger på vegne af den dataansvarlige handler Databehandleren som databehandler og den Dataansvarlige som dataansvarlig i henhold til lov om behandling af personoplysninger § 42 (Persondataloven).

Databehandleren handler alene efter instruks fra den Dataansvarlige. Den Dataansvarlige afgør, til hvilke formål og hvordan, herunder med hvilke hjælpemidler, der må foretages behandling af personoplysninger. Databehandleren indestår for, at nærværende Databehandleraftale og databehandlerinstruks, udleveres og efterleves af Databehandlerens ansatte, eller ansatte hos en evt. underleverandør, der varetager behandling af personoplysninger for Databehandleren.

Reglerne i lov om behandling af personoplysninger § 41, stk. 3-5, gælder ligeledes for data-behandlerens behandling af personoplysninger på vegne af den Dataansvarlige.

Denne databehandleraftale og databehandlerinstruks kan til enhver tid ændres uden varsel, såfremt ændringen er nødvendig for at overholde de til enhver tid gældende regler og forskrifter for behandling af personoplysninger, herunder overholde ændringer i lov nr. 429 af 31/05/2000 med senere ændringer, bekendtgørelse nr. 528 af 15/06/2000 med senere ændringer samt vejledning nr. 37 af 02/04/2001.

Såfremt data behandles uden for Databehandlerens datacenter i Danmark (fx ved et "cloud center beliggende i et andet EU land") skal Databehandleren sikre, at nærværende databehandleraftale og det pågældende EU lands sikkerhedskrav overholdes jf. § § 42 stk. 2, 3.punktum i lov nr. 429 af 31/05/2000 med senere ændringer om behandling af personoplysninger.

Hvis Databehandleren som led i sin forretning overfører persondata til behandling uden for Databehandlerens datacenter i Danmark (fx ved et "cloud center beliggende i et andet EU land") skal Databehandleren

sikre, at nærværende databehandleraftale og det pågældende EU lands sikkerhedskrav overholdes jf. § 42 stk. 2, 3.punktum i lov nr. 429 af 31/05/2000 med senere ændringer om behandling af personoplysninger.

Databehandleren kan alene overføre data til behandling fra Databehandlerens datacenter beliggende i Danmark eller et andet EU land til et tredjeland (fx ved et "cloud center beliggende uden for EU") efter forudgående samtykke fra den Dataansvarlige og datatilsynets tilladelse jf. reglerne i § 27 i lov nr. 429 af 31/05/2000 med senere ændringer om behandling af personoplysninger.

Sikkerhedsforanstaltninger
Databehandleren træffer de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at data eller informationer kommer til uvedkommendes kendskab, misbrug eller i øvrigt behandles i strid med de til enhver tid gældende regler og forskrifter for behandling af personoplysninger. Databehandleren skal på den Dataansvarliges anmodning give den Dataansvarlige tilstrækkelige oplysninger til at den Dataansvarlige kan påse, at de nævnte tekniske og organisatoriske sikkerhedsforanstaltninger er truffet.

Databehandleren skal én gang årligt, afgive en vederlagsfri og skriftlig erklæring (f.eks. ISAE 3000) fra en ekstern uafhængig autoriseret revisor til den Dataansvarlige, der dokumenterer, at Databehandleren opfylder persondataloven, herunder sikkerhedsbekendtgørelsens krav.

Databehandleren har pligt til at fastsætte og gennemføre de i sikkerhedsbekendtgørelsen krævede interne bestemmelser om sikkerhedsforanstaltninger.

Databehandleren skal i sine retningslinjer fastsætte regler, der sikrer, at dennes ansatte kun har adgang til personoplysninger, som er nødvendige for den ansattes udførelse af sine arbejdsopgaver.

Retningslinjerne skal være udformet efter Datatilsynets vejledning til sikkerhedsbekendtgørelsen (se www.datatilsynet.dk).
Opmærksomheden henledes på, at der i henhold hertil gælder særligt skærpede krav for behandling af følsomme oplysninger.

De interne retningslinjer skal gennemgås mindst én gang om året med henblik på at sikre, at de er fyldestgørende og afspejler de faktiske forhold, og Databehandleren er pligtig at uddanne alle sine ansatte, der beskæftiger sig med personoplysninger på vegne af den Dataansvarlige.

Den Dataansvarlige kan til enhver tid kræve at få udleveret kopi af Databehandlerens interne sikkerhedsforskrifter.

Den Dataansvarlige eller en af den Dataansvarliges udpeget tredjemand - samt Datatilsynet - er berettiget til, når som helst, at komme på uanmeldt kontrolbesøg hos Databehandleren for at konstatere, om Databehandleren overholder nærværende data-behandleraftale og gældende lovgivning.

Ved ophør af nærværende databehandleraftale skal databehandleren på skriftlig anmodning fra den Dataansvarlige udlevere eller destruere data efter Dataansvarliges valg indenfor den af den Dataansvarlige fastsatte frist.

Beskyttelse af personoplysninger i åbne net.
I overensstemmelse med Datatilsynets udtalelse af 23. marts 2004 skal der ved tilslutning til internet eller andre åbne net træffes foranstaltninger, som sikrer mod uvedkommende trafik og forhindrer adgang fra det åbne net til den Dataansvarliges interne net. Databehandleren skal i denne forbindelse overholde de retningslinjer, som til enhver tid er fastsat af Datatilsynet.

På tidspunktet for underskrivelsen af nærværende databehandleraftale skal Databehandler som minimum træffe følgende foranstaltninger:

- Etablering og vedligeholdelse af en firewall, som sikrer gennemførelse af den Dataansvarliges sikkerhedspolitik, herunder f.eks. spærring for adgang til visse hjemmesider.
- Ajourføring af servere og devices anvendt af medarbejdere (fx pc'er, tablets, iPads, smartphones ect.) med sikkerhedsopdateringer, som sikrer mod ondsindet udnyttelse af sårbarheder i de anvendte programmer.
- Etablering af virusværn, som løbende holdes ajourført.
- Opsætning af sikkerhedsindstillingerne fx i browseren og e-post klienten, der sikrer gennemførelsen af den Dataansvarliges sikkerhedspolitik omkring websteder, cookies og modtagelse af eksekverbar kode (plug-ins m.v.)

Efter en vurdering af den konkrete sikkerhedsrisiko og under hensyntagen til øvrige sikkerhedsforanstaltninger kan yderligere sikkerhedsforanstaltninger være hensigtsmæssige, herunder f.eks. installation af anti-spyware programmer på de enkelte pc-arbejdspladser.

Lagring og udskrivning af oplysninger uden for den Dataansvarliges lokaliteter
Ved anvendelse af hjemmearbejdspladser eller mobile arbejdsstationer, skal Databehandleren særligt sikre følgende:

- Såfremt det er nødvendigt, at hjemme-pc'en ikke bare anvendes som terminal mod det centrale system, men også til lagring af oplysninger fra det centrale system, skal oplysningerne krypteres.
- Såfremt det er nødvendigt, at der skal udskrives oplysninger fra hjemme-pc'en, skal der fastsættes regler og gives instruktion vedrørende opbevaring og tilintetgørelse af udskrifter, så oplysningerne ikke kommer uvedkommende til kendskab.
- Såfremt Databehandleren tillader anden anvendelse af hjemme-pc'en, f.eks. til privat brug og/eller af andre end den ansatte, skal der fastsættes retningslinjer for denne anvendelse og etableres de nødvendige sikkerhedsforanstaltninger i forbindelse dermed, herunder passwordbeskyttelse.
- Såfremt etablering af forbindelse fra hjemmearbejdspladsen til det centrale system sker ved anvendelse af opkaldsforbindelse (analog telefonforbindelse, ISDN, mobiltelefon etc.), skal der i denne forbindelse træffes foranstaltninger mod, at uvedkommende kan foretage opkald til det centrale system og i det hele taget gribe ind i kommunikationen.

Som eksempler på sådanne foranstaltninger kan nævnes tilbagekald, passwordbeskyttelse og lukkede brugergrupper. Endvidere kan anvendes særlige tidsrum, hvor hjemmearbejdspladsen ikke kan anvendes, og etablering af en særlig logning af dens anvendelse.

Databehandleren skal endvidere være opmærksom på den fysiske sikring i hjemmemiljøet, herunder mod tyveri, hærværk og uvedkommendes adgang.

Der skal løbende ske en ajourføring af de særlige retningslinjer vedrørende hjemmearbejdspladser for at sikre, at bestemmelserne om sikkerhedsforanstaltninger iagttages.

Ved underskrivelse accepterer, databehandler ovenstående.

Dato: _____

Navn: _____

Underskrift: _____