Datatilsynets standardkontrakt til indgåelse af databehandleraftale.

Changelog

| Version | ændringer |
| --- | --- |
| 1.1 | Ændringer i Bestemmelserne 7.7., 9.2., 10.4. og Bilag C.8. *(Tastefejl og opdaterede krydshenvisninger).* |
| 1.1b | Tilpasning af layout til Viborg Kommune, rettelse af stavefejl samt tilføjelse af vejledning til udfyldelse på side 0. Ingen ændringer i bestemmelserne. |
|  |  |

**Vejledning til databehandler**

Databehandleren skal læse databehandleraftalen grundigt igennem og derefter udfylde de GRØNNE felter. (Dataansvarlige udfylder de GULE felter.)

* I afsnit 14 og 15 indsættes oplysninger om underskriver samt kontaktperson.
* I Bilag B indsætter databehandleren oplysninger om underdatabehandlere.
* I Bilag C skal databehandleren udfylde flere afsnit:
  + I afsnit C.2. skal databehandleren ud fra dataansvarliges valgte sikkerhedsniveau, beskrive forhold vedr. deres sikkerhedsforanstaltninger. Når dataansvarlige modtager besvarelsen, vil de blive vurderet.
  + I afsnit C.5 skal databehandleren angive **alle** lokationer, hvor data vil blive behandlet. Dette gælder også lokationer ved underdatabehandlere.

|  |
| --- |
| Dokumentnummer: [Dokumentnummer]  Sagsnummer: [Sagsnummer]  Sagsbehandler: [Sagsbehandler]  Ref. til hovedaftalen: [Sagsnummer][Dokumentnummer] |
| DatabEhandleraftale |

Standardkontraktsbestemmelser

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

mellem

Viborg Kommune

CVR 29189846

Prinsens Alle 5

8800 Viborg

herefter ”den dataansvarlige”

og

[Databehandlerens navn]

CVR [Databehandlerens CVR-nummer]

[Databehandlerens adresse]

[Databehandlerens postnummer og by]

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 og frihedsrettigheder

# Indhold

[1 Indhold 2](#_Toc31787799)

[2 Præambel 3](#_Toc31787800)

[3 Den dataansvarliges rettigheder og forpligtelser 3](#_Toc31787801)

[4 Databehandleren handler efter instruks 4](#_Toc31787802)

[5 Fortrolighed 4](#_Toc31787803)

[6 Behandlingssikkerhed 4](#_Toc31787804)

[7 Anvendelse af underdatabehandlere 5](#_Toc31787805)

[8 Overførsel til tredjelande eller internationale organisationer 6](#_Toc31787806)

[9 Bistand til den dataansvarlige 6](#_Toc31787807)

[10 Underretning om brud på persondatasikkerheden 7](#_Toc31787808)

[11 Sletning og returnering af oplysninger 8](#_Toc31787809)

[12 Revision, herunder inspektion 8](#_Toc31787810)

[13 Parternes aftale om andre forhold 9](#_Toc31787811)

[14 Ikrafttræden og ophør 9](#_Toc31787812)

[15 Kontaktpersoner hos den dataansvarlige og databehandleren 10](#_Toc31787813)

[Bilag A Oplysninger om behandlingen 11](#_Toc31787814)

[Bilag B Underdatabehandlere 12](#_Toc31787815)

[Bilag C Instruks vedrørende behandling af personoplysninger 13](#_Toc31787816)

[Bilag D Parternes regulering af andre forhold 18](#_Toc31787817)

# 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 leveringen af levering af praktisk hjælp og/eller personlige pleje 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.

# 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]](#footnote-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.

# 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 Bilag 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.

# 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.

# 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.

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:

* 1. Pseudonymisering og kryptering af personoplysninger
  2. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
  3. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
  4. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.
  5. 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.
  6. 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.

# 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).

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

* 1. Databehandleren må kun gøre brug af underdatabehandlere med den dataansvarliges forudgående specifikke skriftlige godkendelse. Databehandleren skal indgive anmodningen om en specifik godkendelse mindst 6 måneder inden anvendelsen af den pågældende underdatabehandler. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af Bilag B.
  2. 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.

* 1. 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.
  2. 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.
  3. 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.

# 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:
  4. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
  5. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
  6. behandle personoplysningerne i et tredjeland
  7. 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 Bilag C.6.
  8. 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.

# 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:

* 1. oplysningspligten ved indsamling af personoplysninger hos den registrerede
  2. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
  3. indsigtsretten
  4. retten til berigtigelse
  5. retten til sletning (”retten til at blive glemt”)
  6. retten til begrænsning af behandling
  7. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
  8. retten til dataportabilitet
  9. retten til indsigelse
  10. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering
  11. 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:

1. 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
2. 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
3. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)
4. 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.
   1. 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.

# 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 12 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:
  4. 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
  5. de sandsynlige konsekvenser af bruddet på persondatasikkerheden
  6. 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.
  7. 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.

# Sletning og returnering af oplysninger

* 1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlige, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

# 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 Bilag C.7 og C.8.
  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.

# 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.

# 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 Bilag C.4, kan Bestemmelserne opsiges med skriftligt varsel af begge parter.
  5. Underskrift

På vegne af den dataansvarlige

Navn Maila Tandrup

Stilling Omsorgschef

Telefonnummer 51156840

E-mail mbta@viborg.dk

Underskrift

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

På vegne af databehandleren

Navn [NAVN]

Stilling [STILLINGl]

Telefonnummer [TELEFONNUMMER]

E-mail [E-MAIL]

Underskrift

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# 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 Databeskyttelsesrådgiveren

Stilling DPO

Telefonnummer 87 87 41 55

E-mail [dpo\_dbr@viborg.dk](mailto:dpo_dbr@viborg.dk)

***Særligt ved sikkerhedsbrud, jf. afsnit 10:***

E-mail [sikkerhedsbrud@viborg.dk](mailto:sikkerhedsbrud@viborg.dk)

**Databehandler**

Navn [NAVN]

Stilling [STILLING]

Telefonnummer [TELEFONNUMMER]

E-mail [E-MAIL]

1. Oplysninger om behandlingen
   1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Databehandleren må behandle oplysninger i dataansvarliges omsorgssystem (KMD Nexus) med henblik på at levere praktisk hjælp/personlig pleje ved borgere, som har valgt dem som leverandør, jf. servicelovens § 91.

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

Leverandøren må behandle oplysninger om de borgere i Viborg Kommune, som de skal levere ydelser til. Disse oplysninger kan leverandøren tilgå via kommunens omsorgssystem (KMD Nexus), hvor adgangen er afgrænset til disse borgere.

Derudover skal leverandøren dokumentere i KMD Nexus. Anvendelsen af KMD Nexus og krav til dokumentation er reguleret i Hovedaftalen.

* 1. Behandlingen omfatter følgende typer af personoplysninger om de registrerede
     1. Overordnede typer af personoplysninger

Behandlingen af personoplysninger omfatter nedenstående afkrydsede typer:

Almindelige personoplysninger (Databeskyttelsesforordningens artikel 6):

Almindelige personoplysninger

Følsomme personoplysninger (Databeskyttelsesforordningens artikel 9):

Racemæssig eller etnisk baggrund

Politisk overbevisning

Religiøs overbevisning

Filosofisk overbevisning

Fagforeningsmæssige tilhørsforhold

Helbredsforhold, herunder misbrug af medicin, narkotika, alkohol m.v.

Seksuelle forhold

Biometriske data

Oplysninger om enkeltpersoners rent private forhold (Databeskyttelsesforordningens artikel 6 og 9):

Strafbare forhold

Andre rent private forhold

Oplysninger om cpr-nummer (Databeskyttelsesforordningens artikel 87):

CPR-numre

* + 1. Specifikke typer af personoplysninger

Databehandleren må behandle følgende oplysninger om borger

* Navn
* Adresse
* Telefonnummer
* CPR-nummer
* Visiterede ydelser
* Oplysninger om borgerens helbred

Derudover må databehandleren også behandlere oplysninger om medarbejdere og samarbejdspartnere, herunder

* Navn
* Stilling
* Arbejdssted
* Telefonnummer
* E-mail
  1. Behandlingen omfatter følgende kategorier af registrerede

|  |  |
| --- | --- |
|  | Borgere, som databehandleren skal levere ydelser ved |
|  | Medarbejdere i Viborg Kommune |

* 1. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen har følgende varighed:

Behandlingen foregår indtil hovedaftalens ophør.

1. Underdatabehandlere
   1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

|  |  |  |  |
| --- | --- | --- | --- |
| **NAVN** | **CVR** | **ADRESSE** | **BESKRIVELSE AF BEHANDLING** |
| [Navn] | [CVR] | [Adresse] | [Overordnet beskrivelse af databehandlingen] |
| [Navn] | [CVR] | [Adresse] | [Overordnet beskrivelse af databehandlingen] |

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.

1. Instruks vedrørende behandling af personoplysninger
   1. Behandlingens genstand/instruks

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

Leverandøren må behandle oplysninger om de borgere i Viborg Kommune, som de skal levere ydelser til. Disse oplysninger kan leverandøren tilgå via kommunens omsorgssystem (KMD Nexus), hvor adgangen er afgrænset til disse borgere.

Derudover skal leverandøren dokumentere i KMD Nexus. Anvendelsen af KMD Nexus og krav til dokumentation er reguleret i Hovedaftalen.

Leverandøren må ikke tilgå oplysninger om borgeren, som ikke er relevante for deres arbejde, jf. FVL § 32. Dette gælder for eksempel, men er ikke afgrænset til, adviser i korrespondancemodulet i KMD Nexus. Leverandøren er kun berettiget til at læse adviser, som er adresseret direkte til dem.

Leverandøren må overføre stamoplysninger om borgerne til eget system med henblik på udarbejdelse af kørelister eller lignende. Leverandøren må printe disse oplysninger og arbejde med uddata i det omfang, det er nødvendigt. Disse under forudsætning af at Leverandøren etablerer passende sikkerhedsforanstaltninger udarbejdet efter en risikobaseret tilgang. Disse skal være beskrevet i Bilag C, afsnit C.2.7.

Såfremt Leverandørens eget system er hosted ved 3. part (underdatabehandler) skal dette naturligvis oplyses ved databehandleraftalens indgåelse og noteres i Bilag B.

* 1. Behandlingssikkerhed

Dataansvarlige arbejder med 3 sikkerhedsklassificeringer, når der foretages behandling af personoplysninger:

* ***Niveau 01: Almindelige personoplysninger / interne informationer***

Databehandlingen kan kun inkludere almindelige personoplysninger (DBF, art. 6).

* ***Niveau 02: Følsomme, fortrolige og strafferetslige personoplysninger***

Databehandlingen kan inkludere almindelige personoplysninger (DBF, art. 6), fortrolige personoplysninger (DBF, art. 6; STRFL § 152; FVL § 27), følsomme personoplysninger (DBF, art. 9) og oplysninger om straffedomme mv. (DBF, art. 10).

* ***Niveau 03: Fortrolige informationer af særlig karakter***

Databehandlingen kan inkludere almindelige personoplysninger (DBF, art. 6), fortrolige personoplysninger (DBF, art. 6; STRFL § 152; FVL § 27), følsomme personoplysninger (DBF, art. 9) og oplysninger om straffedomme mv. (DBF, art. 10). Derudover er det af dataansvarlige vurderet til at være personoplysninger, der har en særlig sensitiv karakter. Tab af fortrolighed (læk af data) vil være særligt kompromitterende for både dataansvarlige og den registrerede.

Databehandleren skal etablere et sikkerhedsniveau, der skal afspejle Niveau 02: Følsomme, fortrolige og strafferetslige personoplysninger.

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

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

* + 1. Pseudonymisering og kryptering af personoplysninger

Dataansvarlige indestår for krypteringen af personoplysninger i KMD Nexus. Såfremt databehandleren anvender et system fra 3. part, beskrives kryptering herunder.

[DATABEHANDLEREN BESKRIVER FORHOLD VEDRØRENDE PSEUDONYMISERING OG KRYPTERING AF PERSONOPLYSNINGER]

* + 1. Sikre vedvarende fortrolighed, integritet, tilgængelighed

Dataansvarlige indestår for, at sikre vedvarende fortrolighed, integritet og tilgængelighed ift. KMD Nexus. Såfremt databehandleren anvender systemer fra 3. part, beskrives det herunder.

[DATABEHANDLEREN BESKRIVER FORHOLD VEDRØRENDE EVNEN TIL AT SIKRE VEDVARENDE FORTROLIGHED, INTEGRITET, TILGÆNGELIGHED OG ROBUSTHED AF BEHANDLINGSSYSTEMER OG –TJENESTER]

* + 1. Evnen til rettidigt at genoprette tilgængeligheden

Dataansvarlige indestår for evnen til rettidigt at genoprette tilgængeligheden ved anvendelse af KMD Nexus.

* + 1. Regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger

Dataansvarlige indestår for den regelmæssige afprøvning, vurdering og evaluering af effektiviteten af de tekniske foranstaltninger ift. KMD Nexus.

[DATABEHANDLEREN BESKRIVER FORHOLD VEDRØRENDE PROCEDURER FOR REGELMÆSSIG AFPRØVNING, VURDERING OG EVALUERING AF EFFEKTIVITETEN AF DE TEKNISKE OG ORGANISATORISKE FORANSTALTNINGER TIL SIKRING AF BEHANDLINGSSIKKERHEDEN]

* + 1. Adgang til oplysningerne via internettet

Databehandlerens IP-adresse skal godkendes i forhold til at tilgå KMD Nexus. Dette indebærer, at databehandleren skal sikre sig, at der er etableret en fast IP-adresse. Al kommunikation med KMD Nexus foregår via denne ene faste IP-adresse. Ønsker databehandleren at tilkoble sig til KMD Nexus fra andre lokationer, skal dette ske via en VPN-forbindelse, således Leverandørens faste, godkendte IP-adresse benyttes.

Såfremt databehandleren anvender et system fra 3. part, som tilgås via internettet, skal dette beskrives herunder:

[DATABEHANDLEREN BESKRIVER FORHOLD VEDRØRENDE ADGANG TIL OPLYSNINGERNE VIA INTERNETTET]

* + 1. Beskyttelse af oplysninger under transmission

Dataansvarlige indestår for sikkerheden ved transmission af personoplysninger ved anvendelse af KMD Nexus. Såfremt databehandleren anvender egne systemer, skal transmissionssikkerheden ved disse beskrives herunder.

[DATABEHANDLEREN BESKRIVER FORHOLD VEDRØRENDE BESKYTTELSE AF OPLYSNINGER UNDER TRANSMISSION]

* + 1. Beskyttelse af oplysninger under opbevaring

Dataansvarlige indestår for beskyttelsen af personoplysninger under opbevaring i KMD Nexus.

Databehandleren bedes beskrive hvordan de sikrer beskyttelse af uddata (papir) samt evt.

* + 1. Vedrørende fysisk sikring af lokaliteter

[DATABEHANDLEREN BESKRIVER FORHOLD VEDRØRENDE FYSISK SIKRING AF LOKALITETER, HVOR DER BEHANDLES OP-LYSNINGER]

* + 1. Hjemme-/fjernarbejdspladser

KMD Nexus kan kun tilgås fra godkendte IP-adresser, jf. afsnit C.2.5.

* + 1. Logning

Dataansvarlige foretager logning af alle transaktioner i KMD Nexus. Såfremt databehandleren anvender system fra 3. part, skal forhold vedr. logning beskrives herunder.

[DATABEHANDLEREN BESKRIVER FORHOLD VEDRØRENDE LOGNING]

* 1. 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:

Sikkerhedsbrud skal indberettes til [sikkerhedsbrud@viborg.dk](mailto:sikkerhedsbrud@viborg.dk) jf. Bestemmelse 10. Endvidere står det databehandleren frit for at orientere systemejer og/eller andre kontaktpersoner i henhold til hovedaftalen.

* 1. Opbevaringsperiode/sletterutine

Senest 6 måneder efter ydelsens ophør ved den enkelte borger, skal personoplysninger vedr. borgere anonymiseres eller slettes, da alt journalpligtigt foretages i KMD Nexus.

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med bestemmelse 11.1, medmindre den dataansvarlige – efter underskriften af disse bestemmelser – har ændret den dataansvarlige oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne.

* 1. 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** | **CVR** | **ADRESSE** | **BESKRIVELSE AF BEHANDLING** |
| [Navn] | [CVR] | [Adresse] | [Overordnet beskrivelse af databehandlingen] |
| [Navn] | [CVR] | [Adresse] | [Overordnet beskrivelse af databehandlingen] |

Dette indbefatter **alle** lokationer for behandlingen, herunder lokaliteter ved underdatabehandlere.

* 1. Instruks vedrørende overførsel af personoplysninger til tredjelande

Ikke relevant.

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

* 1. Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren

Den dataansvarlige eller en repræsentant for den dataansvarlige foretager 1-2 gange hvert andet år en fysisk eller skriftlig inspektion af databehandleren, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen, med henblik på at fastslå databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Ud over det planlagte tilsyn, kan den dataansvarlige gennemføre en inspektion hos databehandleren, når den dataansvarlige finder det nødvendigt.

Den dataansvarliges eventuelle udgifter i forbindelse med en fysisk eller skriftlig inspektion afholdes af den dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendig(e) for, at den dataansvarlige kan gennemføre sin inspektion.

Baseret på resultaterne af inspektionen, er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Alternativt kan databehandleren for egen regning indhente en revisionserklæring fra en uafhængig tredjepart vedrørende databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Der er enighed mellem parterne om, at følgende typer af revisionserklæringer kan anvendes i overensstemmelse med disse Bestemmelser:

* Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med [Dataansvarlig]”

Revisionserklæringen fremsendes uden unødig forsinkelse til den dataansvarlige til orientering til e-mailadressen [dpo\_dbr@viborg.dk](mailto:dpo_dbr@viborg.dk). Den dataansvarlige kan anfægte rammerne for og/eller metoden erklæringen og kan i sådanne tilfælde anmode om en ny revisionserklæring under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af ERKLÆRINGEN, er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

* 1. Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere

Databehandleren skal årligt føre kontrol med sine underdatabehandlere, eksempelvis ved at indhente en revisionserklæring fra en uafhængig tredjepart vedrørende underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Ved dataansvarliges revision af databehandler, skal dokumentationen for databehandlerens kontrol af underdatabehandlere fremgå.

Baseret på resultaterne af tilsynet, er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Den dataansvarlige kan – hvis det findes nødvendigt – vælge at initiere og deltage på en fysisk inspektion hos underdatabehandleren. Dette kan blive aktuelt, hvis den dataansvarlige vurderer, at databehandlerens inspektion hos underdatabehandleren ikke har givet den dataansvarlige tilstrækkelig sikkerhed for, at behandlingen hos underdatabehandleren sker i overensstemmelse med databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Den dataansvarliges eventuelle deltagelse i en inspektion hos underdatabehandleren ændrer ikke ved, at databehandleren også herefter har det fulde ansvar for underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Databehandlerens og underdatabehandlerens eventuelle udgifter i forbindelse med en fysisk inspektion af underdatabehandlerens lokaliteter er den dataansvarlige uvedkommende – uanset om den dataansvarlige har initieret og deltaget i en sådan inspektion.

1. Parternes regulering af andre forhold

1. Henvisninger til ”medlemsstat” i disse bestemmelser skal forstås som en henvisning til ”EØS medlemsstater”. [↑](#footnote-ref-1)