

Standard Databehandlervilkår for brug af Alment Datavarehus

Version 2 af d. 9. januar 2025 – tilpasset fra Datatilsynets standardskabelon

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

mellem

Brugeren af Alment Datavarehus

herefter "den dataansvarlige"

og

Landsbyggefonden
CVR 6247 5412
Stuadiestræde 50
1554 København V
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 og frihedsrettigheder. Bestemmelserne supplerer de almindelige brugervilkår, som gælder ved brug af Alment Datavarehus, i de tilfælde hvor brugeren vælger at indlæse persondata i den tilhørende portal-løsning.

1. Indhold

Side 2 af 14

2. Præambel	3
3. Den dataansvarliges rettigheder og forpligtelser	4
4. Databehandleren handler efter instruks	4
5. Fortrolighed	4
6. Behandlingssikkerhed	4
7. Anvendelse af underdatabehandlere.....	5
8. Overførsel til tredjelande eller internationale organisationer	6
9. Bistand til den dataansvarlige.....	7
10. Underretning om brud på persondatasikkerheden	8
11. Sletning og returnering af oplysninger	8
12. Revision, herunder inspektion	8
13. Ikrafttræden og ophør	9
14. Kontaktpersoner hos den dataansvarlige og databehandleren	9
Bilag A Oplysninger om behandlingen	10
Bilag B Underdatabehandlere	11
Bilag C Instruks vedrørende behandling af personoplysninger	12

1. Disse Bestemmelser udgør en standard databehandleraftale udfærdiget af Landbyggefonden, som brugerne selvstændigt kan behandle deres egne persondata indenfor rammerne af. Hvis en bruger ikke kan acceptere standardvilkårene, skal brugeren undlade at indlæse persondata i portal-løsningen.
2. Disse Bestemmelser fastsætter databehandlerens (Landsbyggefonden) rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige (Brugeren).
3. 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).
4. I forbindelse med leveringen af Alment Datavarehus behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.
5. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.
6. Der hører tre bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.
7. 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.
8. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.
9. 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.
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.

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 medlemsstaternes¹ nationale ret og disse Bestemmelser.
2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål, 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.

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.

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

- 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 har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 21 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.
3. 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.

Side 6 af 14

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

4. 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.
5. 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 bilag C.6.
5. Disse Bestemmelser skal ikke forveksles med standardkontraktbestemmelser 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.

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 unødigt 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 unødigt 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 unødigt 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 48 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 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.

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. Procedurene for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.6.

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. Ikrafttræden og ophør

1. Nærværende databehandleraftale anses for indgået og accepteret af parterne, når den dataansvarlige indlæser persondata i portal-løsningen.
2. 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.
3. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bilag C.4, ophører Bestemmelserne automatisk med at finde anvendelse.
4. Såfremt en bruger af Alment Datavarehus ikke ønsker at acceptere vilkårene i nærværende databehandleraftale, så skal brugeren afstå fra at indlæse persondata i portalløsningen.

14. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.
2. Den dataansvarlige forpligter sig til at kunne kontaktes via den bruger, som er oprettet i portalløsningen.
3. Databehandleren kan kontaktes gennem følgende:

Telefonnummer	+45 33762000
E-mail	lbf@lbf.dk

4. Databehandlerens databeskyttelsesrådgiver kan kontaktes gennem følgende:

Telefonnummer	+45 33762000
E-mail	DPO@lbf.dk

Bilag A Oplysninger om behandlingen

Side 10 af 14

Formålet med Alment Datavarehus er som udgangspunkt ikke at behandle persondata og den behandling, som Landsbyggefonden er ansvarlig for, indebærer ikke behandling af persondata.

Brugerne får imidlertid i forbindelse med deres brug af Alment Datavarehus, stillet en portal-løsning til rådighed, hvor de kan indlæse deres data, inden de lægges op i Alment Datavarehus. Og desuden foretage egne datamodelleringer, hvor de både benytter de udstillede data fra Alment Datavarehus samt deres egne indlæste data. I denne forbindelse kan der i mindre omfang forekomme ikke-følsomme persondata i brugernes data-

Eftersom Landsbyggefonden driver Alment Datavarehus, inklusive portalløsningen, er Landsbyggefonden derfor databehandler for de persondata, som brugerne måtte lægge op.

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

Formålet med databehandlerens behandling er at stille Alment Datavarehus til rådighed sådan at den dataansvarlige ved hjælp heraf kan forberede data til indlæsning og foretage brugerspecifik datamodellering.

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

At stille portal-tjenesten til rådighed for brugerne. Databehandleren stiller de tekniske faciliteter til rådighed for brugeren, således at brugeren kan lave analyser med både egne data og data fra Alment Datavarehus.

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

Ikke-følsomme persondata, som brugeren vælger at indlæse i portalen. Typisk, men ikke begrænset til, navne, roller og kontaktoplysninger.

A.4. Behandlingen omfatter følgende kategorier af registrerede

Forretningskontaktpersoner, lejere og repræsentanter for boligselskaberne.

A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen har følgende varighed

Behandlingen varer indtil brugeren selv sletter data, eller når brugeren nedlægges som bruger af løsningen, hvorefter data slettes af Landsbyggefonden.

Landsbyggefonden driver selv Alment Datavarehus. Selve datacenteret, som serverne står i, tilhører en ekstern leverandør, som ikke har adgang til data. Udvikling og vedligehold varetages af KMD.

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere.

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
KMD A/S	26911745	Lautrupparken 40 2450 Ballerup	Udvikling og vedligehold

KMD anvender selv følgende underdatabehandlere.

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING	OVERFØR-SELSGRUNDLAG
CalmCo (TARGET)	N/A	Gasværksvej 2, 9000 Aalborg, Danmark	Analyse	N/A
Microsoft	N/A	1 Microsoft Way, Redmond, WA 98052, USA	Databaser, Azure komponenter	EU-US Data Privacy Framework
Emagine Consulting ApS	26249627	Sydhavnsgade 16, 2450 København SV, Danmark	Test og udvikling	N/A

B.2. Varsel for ændring af underdatabehandlere

I tilfælde af ændringer i sammensætningen af underdatabehandlere vil databehandleren udsende en orienteringsmail til dataansvarlige, senest 21 dage inden ændringen træder i kraft. Såfremt en bruger ikke kan acceptere en ny underdatabehandler, kan brugeren vælge at opføre sig med at indlæse perondata og slette de eksisterende data i portalen.

B.3 Godkendte underdatabehandlers vilkår

Databehandleren indestår for at underdatabehandlerne, som minimum, lever op til de samme krav som databehandleren selv har forpligtet sig til med disse bestemmelser.

C.1. Behandlingens genstand/instruks

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

Hosting af data, udvikling af Alment Datavarehus, udvikling af rapporter og rapportløsning i portal-løsningen. Der henvises i øvrigt til Bilag A. Personoplysninger der anvendes til statistiske modelleringer, videreføres ikke i det statistiske output.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle at behandlingen omfatter ikke-følsomme persondata, som brugeren selv vælger at indlæse. Alment Datavarehus er ikke designet eller risikovurderet til behandling af følsomme persondata.

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.

Risikovurderingen viste at den største risiko f.s.v.a. fysiske personers rettigheder var udfald i tjenesten, vurderet til en lav-middel risiko, som derfor er blevet accepteret af dataansvarlige.

Fortrolighed sikres gennem princippet om minimum bundprivilegier. Og kun de personer, som er godkendt, kan få adgang til data og systemer.

C.2.a. Brugerkonti og adgange

Alle databehandlerens brugerkonti er underlagt princippet om opdeling af ansvar (segregation of duties). Brugeradgange hos databehandleren trækkes tilbage, hvis brugeren ikke længere opfylder adgangskriterierne.

Databehandleren anvender passende logiske autentifikationsmekanismer, to-faktor autentificering eller lignende mekanismer. De anvendte autentifikationsmekanismer efterlever, hvad der anses som god praksis indenfor feltet, såsom længde på adgangskode og kompleksitet.

Databehandleren har passende tekniske foranstaltninger til at begrænse risikoen for uautoriseret adgang og/eller installation af ondsindet software.

C.2.b. Fortrolighed og tavshedpligt

Databehandleren kræver aftale om fortrolighed forud for al deling af intern og fortrolig information med eksterne parter inklusive leverandører, konsulenter og andre samarbejdspartnere. Databehandlerens medarbejdere er underlagt fortrolighed i deres ansættelseskontrakter. Kun behørigt autoriserede medarbejdere gives adgang til persondata behandlet under denne Databehandleraftale.

C.2.c. Sikkerhed ved datatransmission

Databehandleren bruger kryptografiske metoder til at overholde lovbestemmelser (fx. beskyttelse af personoplysninger under transmission).

C.2.d. Sikkerhedskopiering

Databehandleren sørger for sikkerhedskopiering og backup af systemer og data, og sikrer at sådanne sikkerhedskopier opbevares sikkert.

C.2.e. Sikkerhedsopdatering

Sikkerhedsopdateringer til standardsoftwarekomponenter testes og installeres uden ugrundet ophold. Egenudviklede softwarekomponenter overvåges løbende for sårbarheder og der udvikles sikkerhedsopdateringer, når det er nødvendigt for at overholde de øvrige krav i nærværende Bilag C.

C.2.f. Fysiske adgangskontrol

Databehandleren har etableret fysiske adgangsbegrænsninger. Områder, hvor personoplysninger behandles, er adskilt med adgangskontrolmekanismer fra områder med generel adgang. Sådanne mekanismer inkluderer eksempelvis systemer til fysisk adgangskontrol, låse, adgangskontrol-porte, sikkerhedsvagter og overvågningsudstyr.

C.2.g. Databehandlerens brug af hjemme-/ fjernarbejdspladser

Databehandlerens medarbejdere har mulighed for udføre arbejde ved brug af fjernarbejdspladser (herunder hjemmearbejdspladser) med fjernadgang til databehandlerens it-systemer, forudsat at det udføres på en sikker måde.

C.2.i. Databehandlerens logning

Aktiviteter, der udføres af databehandlerens systemadministratorer og operatører og andre med udvidede privilegier, logges som minimum med: Tidspunkt, bruger og handling/aktivitet.

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:

C.3.a. Begæring vedrørende registreredes rettigheder

Såfremt databehandleren modtager en begæring vedrørende den registreredes rettigheder, skal databehandleren hurtigst muligt videregive denne begæring til den dataansvarlige. Se også punkt 9 i Databehandleraftalen.

C.3.b. Underretning om brud på persondatasikkerheden

Det påhviler databehandleren at underrette den dataansvarlige hurtigst muligt og uden unødigt forsinkelse efter at være blevet bekendt med et brud på persondatasikkerheden. Underretningen vil om muligt indeholde følgende oplysninger:

1. En beskrivelse af hændelsen, herunder hvor den fysisk fandt sted.
2. Et hændelsesforløb, indeholdende information om hændelsens start, konstatering og (forventet) afslutning.
3. Karakteren af bruddet på persondatasikkerheden, herunder eventuelt involveret teknologi, kategorierne af oplysninger og registrerede samt det omtrentlige antal berørte registrerede og om muligt det omtrentlige antal registreringer.
4. En generel vurdering af den sandsynlige konsekvens for de registrerede.
5. En beskrivelse af de foranstaltninger, som databehandleren har truffet eller/og foreslår truffet af den dataansvarlige for at håndtere hændelsen og begrænse bruddets skadevirkninger.

6. Oplysning om, at underretningen er endelig, eller om og hvordan der vil følge yderligere information.
7. Oplysning om, hvor den dataansvarlige kan få yderligere information.

C.3.c. Bistand i øvrigt efter punkt 9.1 og 9.2 i Databehandleraftalen

På den dataansvarliges anmodning bistår databehandleren - under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren – i rimeligt omfang med input/bidrag til den dataansvarliges udførelse af sine opgaver og overholdelse af sine forpligtelser anført i punkt 9.1 og 9.2 i Databehandleraftalen.

C.4 Opbevaringsperiode/sletterutine

Hvor ikke andet er aftalt, opbevares personoplysninger, som databehandleren behandler på den dataansvarliges vegne, hos databehandleren, indtil den dataansvarlige anmoder om at få oplysningerne slettet. Senest ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren tilbagelevere alle personoplysninger, som databehandleren behandler på den dataansvarliges vegne, og slette eksisterende kopier i overensstemmelse med Hovedaftalen samt punkt 11 i Databehandleraftalen. På anmodning fra den dataansvarlige skal databehandleren skriftligt bekræfte, at sletning er foretaget.

C.5 Lokaltet for behandling

Oplysningerne om behandlingssted kan udleveres, i det omfang udlevering kan ske uden sikkerhedsmæssig risiko, efter databehandlerens vurdering. I sådanne tilfælde udleveres da i udgangspunktet kun oplysninger om land og by for databehandlingsstedet.

Databehandlerens datacenter befinder sig i Danmark i Storkøbenhavn.

C.6 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren

Den dataansvarlige eller en repræsentant for den dataansvarlige kan foretage tilsyn hos 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.

Den dataansvarliges eventuelle udgifter i forbindelse med en fysisk 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.

Databehandleren fører selv løbende tilsyn med underdatabehandler, som igen fører tilsyn med sine underdatabehandlere. Dette sker gennem løbende indhentning af ISAE 3402 type 2 erklæringer.