



Databehandleraftale

Standardkontraktbestemmelser i henhold til artikel 28, stk. 3

DataHop ApS

Version 1.0 · 16. september 2026



Standardkontraktsbestemmelser

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

Parterne

Denne databehandlersaftale ("Bestemmelserne") er indgået mellem

Kunden – den virksomhed eller myndighed, som har indgået aftale med DataHop om brug af et eller flere af DataHops softwareløsninger (DH-produkterne) ("Aftalen"), og som er identificeret med navn, CVR-nummer og adresse i Aftalen, herefter "*den dataansvarlige*"

og

DataHop ApS

CVR-nummer 46353307

Andkær Bygade 35

7080 Børkop

Danmark

herefter "*databehandleren*"

der hver især er en "part" og sammen udgør "parterne".

Tiltrædelse

Bestemmelserne udgør en integreret del af Aftalen og tiltrædes af den dataansvarlige ved accept af Aftalen, herunder ved elektronisk accept af DataHops abonnementsvilkår eller ved oprettelse af kundens konto i et DH-produkt. Bestemmelserne er dermed indgået skriftligt, herunder elektronisk, jf. databeskyttelsesforordningens artikel 28, stk. 9. Særskilt underskrift er ikke nødvendig, men parterne kan efter ønske underskrive Bestemmelserne fysisk eller digitalt.

Den til enhver tid gældende version af Bestemmelserne er tilgængelig på datahop.dk/databehandlersaftale. DataHop opbevarer alle tidligere versioner med angivelse af gyldighedsperiode, så det til enhver tid kan dokumenteres, hvilken version der var gældende på et givet tidspunkt. Væsentlige ændringer varsles skriftligt til den dataansvarlige med samme varsel som angivet i Bestemmelse 7.3.

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.

Versionshistorik

Version	Gældende fra	Ændringer
1.0	16. september 2026	Første version.

1. Indhold

2. Præambel	4
3. Den dataansvarliges rettigheder og forpligtelser	4
4. Databehandleren handler efter instruks	5
5. Fortrolighed	5
6. Behandlingssikkerhed	5
7. Anvendelse af underdatabehandlere	6
8. Overførsel til tredjelande eller internationale organisationer	7
9. Bistand til den dataansvarlige	7
10. Underretning om brud på persondatasikkerheden	8
11. Sletning og returnering af oplysninger	9
12. Revision, herunder inspektion	9
13. Parternes aftale om andre forhold	9
14. Ikrafttræden og ophør	10
15. Kontaktpersoner hos den dataansvarlige og databehandleren	10
Bilag A Oplysninger om behandlingen	11
Bilag B Underdatabehandlere	16
Bilag C Instruks vedrørende behandling af personoplysninger	18

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 leveringen af DataHops softwareløsninger (DH-produkterne), som nærmere angivet i bilag A, 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 tre 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. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
10. 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 medlemsstaternes¹ 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.

¹Henvisning til "medlemsstat" i disse Bestemmelser skal forstås som en henvisning til "EØS-medlemsstater".

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.

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 generel skriftlig godkendelse fra den dataansvarlige.
3. 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 30 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.
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. Underdatabehandlersaftale(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 underdatabehandlersaftalen, skal ikke sendes til den dataansvarlige.

6. Databehandleren skal i sin aftale med underdatabehandleren indføre 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 bilag 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 insigelse
- 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 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 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.7. og C.8.
3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivning 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 den dataansvarliges tiltrædelse af Aftalen, jf. afsnittet "Tiltrædelse" ovenfor, og senest når databehandleren påbegynder behandling af personoplysninger på vegne af den dataansvarlige.
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.

15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpunkter.
2. Den dataansvarliges kontaktperson er den kontaktperson, som den dataansvarlige har angivet i Aftalen eller som administrator i det pågældende DH-produkt.
3. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner. Den dataansvarlige opdaterer sine kontaktoplysninger direkte i DH-produktet eller ved skriftlig meddelelse til databehandleren.

Databehandlerens kontaktpunkt	DataHop
Funktion	CEO
Navn	Ole Ivang Hoffmann
Telefonnummer	31 39 70 15
E-mail	gdpr@datahop.dk

Bilag A Oplysninger om behandlingen

A.1 Omfattede produkter

Dette bilag beskriver databehandlerens behandling af personoplysninger i hvert af DataHops softwareløsninger (DH-produkterne). Bilaget gælder kun for de produkter, som den dataansvarlige har tilkøbt i henhold til Aftalen. Tilkøber den dataansvarlige senere yderligere produkter, omfattes disse automatisk af Bestemmelserne og de relevante afsnit i dette bilag fra tidspunktet for tilkøbet.

Følgende produkter er omfattet af denne version af bilaget: DHTid, DHForms, DHFlow og DHLead. Øvrige produkter tilføjes ved ny version af Bestemmelserne.

A.2 Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Formålet med behandlingen er udelukkende at levere, drifte, vedligeholde, supportere og videreudvikle de DH-produkter, som den dataansvarlige har tilkøbt i henhold til Aftalen, herunder at gøre det muligt for den dataansvarlige at anvende produkterne til de formål, der er beskrevet for hvert produkt i afsnit A.4. Databehandleren behandler ikke personoplysningerne til egne formål.

A.3 Behandlingens karakter

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige omfatter primært følgende behandlingsaktiviteter, som er fælles for alle DH-produkter:

- Indsamling og registrering af personoplysninger, som den dataansvarlige og dennes brugere indtaster i produktet, eller som overføres til produktet fra den dataansvarliges øvrige systemer via integrationer.
- Opbevaring og strukturering af personoplysningerne i produktets database og tilhørende lagring (herunder filer, billeder og vedhæftninger) hos databehandlerens underdatabehandlere, jf. bilag B.
- Visning, søgning, beregning og rapportering af personoplysninger for den dataansvarliges autoriserede brugere i produktets brugerflade og via eksport.
- Videregivelse af personoplysninger til de systemer, som den dataansvarlige har instrueret databehandleren i at integrere til (fx løn-, økonomi- eller ERP-systemer), i det omfang integrationen er sat op af eller efter aftale med den dataansvarlige.
- Drift, overvågning, logning, backup og genetablering af produktet, herunder fejlsøgning og teknisk support, hvor databehandlerens medarbejdere kan få adgang til personoplysninger i det omfang, det er nødvendigt for at løse opgaven.
- Vedligeholdelse og videreudvikling af produktet, herunder test. Databehandleren anvender som udgangspunkt ikke personoplysninger i forbindelse med test. Personoplysninger kan dog indgå i test eller fejlretning, hvis det er vanskeligt eller umuligt at genskabe en fejl uden, og i så fald under mindst samme sikkerhedskrav som produktionsmiljøet.
- Sletning og tilbagelevering af personoplysninger i overensstemmelse med Bestemmelse 11 og bilag C.4.

Behandlingen sker ved hjælp af automatiseret databehandling i databehandlerens cloud-baserede systemer. Behandlingen omfatter ikke automatiske afgørelser eller profilering af de registrerede i databeskyttelsesforordningens artikel 22's forstand.

A.4 Produktspecifik beskrivelse af behandlingen

For hvert produkt er angivet produktets formål set fra den dataansvarliges side, de kategorier af registrerede, som behandlingen vedrører, og de typer af personoplysninger, der behandles.

Oplysningerne angives i det omfang, den dataansvarlige vælger at indtaste eller overføre dem – ikke alle oplysningstyper behandles for alle kunder.

DHTid

Produkt	DHTid
Formål	Tidsregistrering skræddersyet til den dataansvarlige: registrering af arbejdstid fordelt på arbejdstyper, fravær og kørsel som grundlag for den dataansvarliges lønbehandling, fakturering og overholdelse af arbejdstidsregler.
Kategorier af registrerede	Den dataansvarliges medarbejdere (ansatte, vikarer, timelønnede) Den dataansvarliges administratorer og kontaktpersoner Kontaktpersoner hos den dataansvarliges kunder, i det omfang tid registreres på kundesager eller projekter
Typer af personoplysninger	Identifikations- og kontaktoplysninger: navn, medarbejdernummer, e-mail, telefonnummer, brugernavn Ansættelsesoplysninger: stilling, afdeling, arbejdssted, ansættelsesforhold, normtid, overenskomst Tidsregistreringer: arbejdstid, pauser, overtid, flex samt de arbejdstyper, opgaver og sager, tiden er registreret på Fraværsoplysninger: fraværstype og periode (ferie, feriefridage, afspadsering, barsel, sygefravær m.v.). Sygefravær registreres alene som fraværstype uden angivelse af årsag eller diagnose Registreringer, der indgår i den dataansvarliges løngrundlag: arbejdstyper, tillægsgivende timer, udlæg og diæter. Lønsatser, timesats og løn behandles ikke Kørsel og lokation: kørselsregistrering med start- og slutadresse, rute og kilometer samt søgning på adresser og lokationer. Der sker ingen løbende GPS-sporing eller lagring af medarbejderens position Tekniske oplysninger: login-tidspunkter, enhedsoplysninger og systemlog
Bemærkning	CPR-nummer behandles ikke, medmindre det er særskilt aftalt med den dataansvarlige, fx til brug for overførsel til lønssystem. Kørselsregistrering viser, hvor en medarbejder har kørt fra og til, og den dataansvarlige er ansvarlig for at have opfyldt sin oplysningspligt over for medarbejderne om denne registrering.

DHForms

Produkt	DHForms
Formål	Digitale formularer: den dataansvarlige opretter egne standardformularer (fx kvalitetssikring, egenkontrol, skades- og hændelsesrapporter, tjeklister), som medarbejderne udfylder, og som opbevares og kan analyseres i produktet.

Kategorier af registrerede	Den dataansvarliges medarbejdere (udfylder og godkender formularer) Den dataansvarliges administratorer og kontaktpersoner Tredjeparter, der omtales i eller fremgår af formularindholdet, fx den dataansvarliges kunder, leverandører, besøgende eller personer involveret i en hændelse
Typer af personoplysninger	Identifikations- og kontaktoplysninger: navn, e-mail, telefonnummer, brugernavn, stilling Formularindhold: de svar, fritekst, tal, valg, billeder, vedhæftede filer, underskrifter, tidspunkter og eventuelle lokationer, som indtastes i formularerne Metadata: hvem der har oprettet, udfyldt, ændret og godkendt en formular, og hvornår Tekniske oplysninger: login-tidspunkter, enhedsoplysninger og systemlog
Bemærkning	Den dataansvarlige bestemmer selv formularernes indhold og dermed hvilke personoplysninger, der behandles. Formularer kan efter den dataansvarliges valg komme til at indeholde følsomme oplysninger, fx om personskade i en hændelsesrapport. Den dataansvarlige er ansvarlig for kun at designe formularer, der indsamler oplysninger, som den dataansvarlige har lovligt grundlag for at behandle, og skal skriftligt underrette databehandleren, hvis en formular tilsigtet skal indeholde følsomme oplysninger (jf. A.6), så parterne kan vurdere behovet for yderligere foranstaltninger.

DHFlow

Produkt	DHFlow
Formål	Integrationer og procesautomatisering: automatisk udveksling af data mellem den dataansvarliges systemer (fx DH-produkter, økonomi-, løn-, ERP- og CRM-systemer) og automatisering af arbejdsgange på tværs af disse.
Kategorier af registrerede	Den dataansvarliges medarbejdere Den dataansvarliges administratorer og kontaktpersoner Kontaktpersoner hos den dataansvarliges kunder, leverandører og samarbejdspartnere Øvrige registrerede, hvis oplysninger indgår i de systemer, den dataansvarlige vælger at integrere
Typer af personoplysninger	Stamdata om medarbejdere, kunder og kontaktpersoner: navn, adresse, e-mail, telefonnummer, kundennummer, medarbejdernummer, stilling Transaktions- og procesdata, der udveksles mellem de integrerede systemer, fx ordrer, fakturaer, timeregistreringer, sager og statusser, i det omfang de indeholder personoplysninger Integrationslog: tidspunkter, status og fejlbeskeder for de enkelte dataoverførsler, som kan indeholde uddrag af de overførte oplysninger Tekniske oplysninger: login-tidspunkter og systemlog

Bemærkning	Hvilke personoplysninger, der konkret behandles, bestemmes af de systemer og datafelter, den dataansvarlige vælger at integrere. Integrationerne opsættes efter den dataansvarliges instruks, og opsætningen udgør en del af instruksen efter Bestemmelse 4. DHFlow opbevarer som udgangspunkt kun personoplysninger midlertidigt under overførslen samt i integrationsloggen, jf. bilag C.4.
-------------------	---

DHLead

Produkt	DHLead
Formål	Kundekartotek og CRM: registrering og opfølgning på den dataansvarliges kunder, leads, kontaktpersoner, møder, tilbud og aftaler samt pipeline-styring.
Kategorier af registrerede	Kontaktpersoner hos den dataansvarliges kunder, kundeemner (leads), leverandører og samarbejdspartnere Privatkunder og private kundeemner, hvis den dataansvarlige sælger til privatpersoner Den dataansvarliges medarbejdere (brugere af systemet)
Typer af personoplysninger	Identifikations- og kontaktoplysninger: navn, virksomhed, stilling, adresse, e-mail, telefonnummer Kunde- og salgsoplysninger: kundennummer, kundestatus, pipeline-fase, tilbud, aftaler, produkter og historik Kommunikation og noter: mødereferater, opgaver, e-mailkorrespondance og fritekstnoter, som den dataansvarliges brugere registrerer om kontaktpersonerne Brugeroplysninger om den dataansvarliges medarbejdere: navn, e-mail, rolle, aktivitetslog Tekniske oplysninger: login-tidspunkter og systemlog
Bemærkning	Fritekstfelter og noter må efter den dataansvarliges instruks kun anvendes til saglige, forretningsmæssige oplysninger. Den dataansvarlige er ansvarlig for, at der ikke registreres følsomme oplysninger om kontaktpersoner i fritekstfelter.

A.5 Varighed af behandlingen

Behandlingen kan påbegyndes, når den dataansvarlige har tiltrådt Bestemmelserne, og varer, så længe Aftalen om det pågældende produkt løber. Ved Aftalens ophør – helt eller for et enkelt produkt – slettes eller tilbageleveres personoplysningerne i overensstemmelse med Bestemmelse 11 og de frister, der er angivet i bilag C.4.

A.6 Særlige kategorier af personoplysninger

Nedenstående oversigt angiver, om databehandleren som led i den aftalte behandling behandler følsomme personoplysninger (databeskyttelsesforordningens artikel 9), oplysninger om straffedomme og lovovertrædelser (artikel 10) samt CPR-numre (databeskyttelseslovens § 11). Den dataansvarlige er forpligtet til skriftligt at underrette databehandleren, inden produkterne anvendes til andre typer oplysninger end angivet nedenfor.

Oplysningstype	DHTid	DHForms	DHFlow	DHLead
Race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold	Nej	Efter instruks	Efter instruks	Nej
Helbredsoplysninger	Nej*	Efter instruks	Efter instruks	Nej
Seksuelle forhold eller seksuel orientering	Nej	Efter instruks	Efter instruks	Nej
Genetiske eller biometriske data	Nej	Nej	Nej	Nej
Straffedomme og lovovertrædelser (art. 10)	Nej	Efter instruks	Efter instruks	Nej
CPR-nummer	Kun efter særskilt aftale	Nej	Efter instruks	Nej

* Sygefravær registreres i DHTid alene som fraværstype uden angivelse af årsag eller diagnose og udgør dermed ikke en helbredsoplysning.

Forklaring: "Nej" betyder, at produktet ikke er designet til oplysningstypen, og at den dataansvarlige er instrueret i ikke at registrere den. "Efter instruks" betyder, at oplysningstypen kan forekomme, fordi den dataansvarlige selv bestemmer indholdet (formularer, fritekst, integrerede systemer), og at behandlingen i så fald sker efter den dataansvarliges dokumenterede instruks og på den dataansvarliges ansvar for behandlingsgrundlaget.

Bilag B Underdatabehandlere

B.1 Godkendte underdatabehandlere

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

Navn og adresse	CVR/VAT-nr.	Land og datalokation	Bistår databehandleren med	Anvendes i
nordicway ApS Ny Banegårdsgade 48 8000 Aarhus C Danmark	40745769	Virksomhed: Danmark Datalokation: Tyskland (Hetzner Online GmbH, datacenter i Tyskland)	Hosting og drift af de servere, databaser og lagring, hvorpå DH- produkterne afvikles, herunder backup	Alle produkter
Microsoft Ireland Operations Ltd. One Microsoft Place South County Business Park Leopardstown, Dublin 18, Irland	IE8256796U	Virksomhed: Irland (EU) Databehandling: EU (Microsofts EU Data Boundary)	Azure Maps: opslag af adresser og beregning af ruter og afstande i forbindelse med kørselsregistrering. Kun adresser og koordinater sendes; ingen medarbejderidentitet	DHTid

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, medmindre proceduren i B.2 er fulgt.

Databehandleren har indgået databehandlersaftale med hver underdatabehandler, jf. Bestemmelse 7.4, og fører tilsyn med underdatabehandlerne som beskrevet i bilag C.8. Underdatabehandlernes egne underleverandører (fx nordicway ApS' brug af Hetzner Online GmbH til datacenterdrift) er omfattet af underdatabehandlerens databehandlersaftale med databehandleren.

Databehandlerens egne medarbejdere er ikke underdatabehandlere. Databehandleren anvender ikke eksterne udviklere, konsulenter eller supportpartnere med adgang til den dataansvarliges personoplysninger.

B.2 Varsel og godkendelse af underdatabehandlere

Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle påtænkte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer. Underretningen skal være i den dataansvarliges besiddelse mindst 30 dage før, ændringen træder i kraft, jf. Bestemmelse 7.3.

Underretning sker ved e-mail til den kontaktperson, som den dataansvarlige har angivet i Aftalen eller som administrator i det pågældende DH-produkt, samt ved offentliggørelse af en opdateret liste over underdatabehandlere på datahop.dk/databehandlersaftale. Underretningen skal indeholde underdatabehandlerens navn, land, datalokation og den behandlingsaktivitet, underdatabehandleren skal bistå med.

Hvis den dataansvarlige har indsigelser mod ændringen, skal den dataansvarlige skriftligt underrette databehandleren herom inden fristens udløb. Den dataansvarlige kan kun gøre indsigelse, hvis den dataansvarlige har en rimelig og konkret grund hertil. Parterne skal herefter i god tro søge at finde en løsning, fx ved at databehandleren tilbyder en alternativ løsning uden brug af den pågældende underdatabehandler.

Kan parterne ikke nå til enighed, er den dataansvarlige berettiget til at opsige Aftalen for det eller de berørte produkter med virkning fra det tidspunkt, hvor den nye underdatabehandler tages i brug, uden at dette anses for misligholdelse fra nogen af parternes side. Personoplysningerne slettes eller tilbageleveres herefter i overensstemmelse med Bestemmelse 11 og bilag C.4.

Udskiftning af en underdatabehandlers underleverandør (fx datacenter) eller ændring af en underdatabehandlers adresse eller selskabsform, som ikke ændrer datalokationen eller behandlingsaktiviteten, kræver ikke særskilt varsel, men afspejles i den offentliggjorte liste.

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 de behandlingsaktiviteter, der er beskrevet i bilag A, med henblik på at levere de DH-produkter, den dataansvarlige har tilkøbt i henhold til Aftalen.

Den dataansvarliges instruks består af Aftalen, dette bilag samt de valg og opsætninger, som den dataansvarliges administratorer foretager i produkterne (fx oprettelse af brugere, opsætning af integrationer, design af formularer og aktivering af funktioner). Yderligere instruks kan gives skriftligt til databehandlerens kontaktpunkt, jf. Bestemmelse 15. Databehandleren er berettiget til at afvise instrukser, som ligger uden for produkternes funktionalitet, eller som efter databehandlerens vurdering er i strid med databeskyttelsesforordningen, jf. Bestemmelse 4.2.

Databehandleren må ikke behandle personoplysningerne til egne formål, herunder til markedsføring, salg af data eller træning af modeller. Databehandleren må anvende anonymiserede og aggregerede oplysninger, som ikke kan henføres til den dataansvarlige eller fysiske personer, til statistik og forbedring af produkterne.

C.2 Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle, at behandlingen primært omfatter almindelige personoplysninger om den dataansvarliges medarbejdere og forretningsforbindelser, og at produkterne efter den dataansvarliges eget valg kan indeholde fortrolige og – i begrænset omfang – følsomme oplysninger, jf. bilag A.6. Der skal derfor etableres et sikkerhedsniveau, der er passende for denne risiko.

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:

Organisatoriske foranstaltninger

- Adgang til personoplysninger gives kun til databehandlerens egne medarbejdere, som har et arbejdsbetinget behov, og som er underlagt fortrolighedsforpligtelse i deres ansættelsesaftale, jf. Bestemmelse 5.
- Databehandleren fører en oversigt over, hvilke medarbejdere der har adgang til produktionsmiljøet, og gennemgår oversigten mindst én gang årligt samt ved fratrædelse, hvor adgange lukkes straks.
- Databehandlerens medarbejdere instrueres i sikker håndtering af personoplysninger, herunder at kundedata ikke må kopieres til lokale enheder, private konti eller uautoriserede tjenester.
- Databehandleren har en procedure for håndtering af sikkerhedshændelser, jf. C.3, som sikrer, at brud identificeres, begrænses, dokumenteres og rapporteres til den dataansvarlige inden for fristen i Bestemmelse 10.2.
- Ændringer i produkterne gennemføres via versionsstyring og testes inden idriftsættelse. Test sker som udgangspunkt uden brug af produktionsdata, jf. bilag A.3.

Tekniske foranstaltninger

- Al kommunikation mellem brugernes enheder og produkterne samt mellem produkterne og integrerede systemer er krypteret i transit (HTTPS/TLS).
- Adgang til produkterne kræver personligt login med brugernavn og adgangskode. Adgangskoder opbevares kun i hashet form. Den dataansvarlige administrerer selv sine brugere og deres rettigheder i produktet.
- Adgang til servere, databaser og hostingleverandørens administrationspanel er begrænset til databehandlerens egne medarbejdere og er beskyttet med personlige konti og tofaktor-godkendelse.
- Logisk adskillelse mellem kunder: hver kundes oplysninger er adskilt fra andre kunders oplysninger, så en kundes brugere ikke kan tilgå andre kunders data.
- Login til hostingleverandørens administrationspanel og servere logges af hostingleverandøren. Produkterne logger væsentlige brugerhandlinger (oprettelse, ændring, sletning) med tidspunkt og bruger.
- Der tages daglig backup af databaser og filer. Backups opbevares i 30 dage hos hostingleverandøren under samme sikkerhedsniveau som produktionsmiljøet, jf. bilag B, og genetablering fra backup testes mindst én gang årligt.
- Servere og programmel holdes opdateret med sikkerhedsrettelser. Kendte sårbarheder i anvendte komponenter afhjælpes uden unødigt forsinkelse.
- Fysisk sikkerhed, netværkssikkerhed og driftsovervågning af den underliggende infrastruktur varetages af hostingleverandøren, jf. bilag B, og er reguleret i databehandlerens databehandlersaftale med denne.

Hvis den dataansvarlige – ud fra sin egen risikovurdering – har behov for yderligere foranstaltninger, fx kryptering af data i hvile på databaseniveau, tofaktor-godkendelse for den dataansvarliges egne brugere eller udvidet logning, skal den dataansvarlige angive dette skriftligt til databehandleren. Parterne aftaler herefter, om og på hvilke vilkår foranstaltningerne kan gennemføres.

C.3 Bistand til den dataansvarlige

Databehandleren skal så vidt muligt – inden for det nedenfor angivne omfang – bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

De registreredes rettigheder (Bestemmelse 9.1)

- Den dataansvarlige kan i produkterne selv slå oplysninger op, rette dem, eksportere dem og slette brugere og registreringer, og kan dermed som udgangspunkt selv besvare anmodninger om indsigt, berigtigelse, sletning og dataportabilitet.
- Hvor det ikke er muligt gennem produktet, leverer databehandleren efter skriftlig anmodning et udtræk af de oplysninger, der behandles om en konkret registreret, eller sletter eller begrænser behandlingen af disse, senest 10 arbejdsdage efter anmodningen.
- Modtager databehandleren en henvendelse direkte fra en registreret, videresender databehandleren henvendelsen til den dataansvarlige uden unødigt forsinkelse og besvarer ikke selv henvendelsen ud over at henvise til den dataansvarlige.

Brud på persondatasikkerheden (Bestemmelse 9.2.a og 9.2.b, jf. Bestemmelse 10)

Ved brud på persondatasikkerheden underretter databehandleren den dataansvarliges kontaktperson pr. e-mail inden for fristen i Bestemmelse 10.2 og giver, i det omfang oplysningerne er tilgængelige for databehandleren, følgende oplysninger – om nødvendigt i flere omgange, efterhånden som de tilvejebringes:

- en beskrivelse af hændelsen, herunder hvornår den er sket, hvornår den er opdaget, og hvilke produkter den berører
- karakteren af bruddet (fx uautoriseret adgang, tab af tilgængelighed, fejlagtig videregivelse)
- kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer
- de sandsynlige konsekvenser af bruddet
- de foranstaltninger, databehandleren har truffet eller foreslår truffet for at håndtere bruddet og begrænse dets skadevirkninger
- kontaktpunkt hos databehandleren for yderligere oplysninger.

Konsekvensanalyse og forudgående høring (Bestemmelse 9.2.c og 9.2.d)

Databehandleren stiller den dokumentation om produkterne og sikkerhedsforanstaltningerne, som er beskrevet i dette bilag, til rådighed for den dataansvarlige og besvarer efter skriftlig anmodning konkrete spørgsmål, som er nødvendige for den dataansvarliges konsekvensanalyse eller forudgående høring af Datatilsynet.

Bistand efter dette afsnit, som går ud over det, der er beskrevet ovenfor, eller som skyldes forhold hos den dataansvarlige, kan databehandleren fakturere efter medgået tid til databehandlerens til enhver tid gældende timepris.

C.4 Opbevaringsperiode/sletterutine

Personoplysningerne opbevares hos databehandleren, så længe Aftalen om det pågældende produkt løber. Den dataansvarlige kan i aftaleperioden selv slette registreringer og brugere i produkterne inden for produkternes funktionalitet.

Ved ophør af Aftalen – helt eller for et enkelt produkt – gælder følgende:

- Den dataansvarlige kan inden for 90 dage efter ophør skriftligt anmode databehandleren om at få udleveret et udtræk af sine personoplysninger i et almindeligt anvendt, maskinlæsbart format (fx CSV eller Excel). Udtrækket leveres senest 30 dage efter anmodningen. Databehandleren kan fakturere udtrækket efter medgået tid, medmindre andet følger af Aftalen.
- Senest 90 dage efter ophør sletter databehandleren alle den dataansvarliges personoplysninger i produktionsmiljøet, medmindre den dataansvarlige forinden skriftligt har anmodet om en kortere frist, eller EU-retten eller dansk ret kræver fortsat opbevaring.
- Backups, der indeholder de slettede oplysninger, overskrives automatisk inden for backupperioden på 30 dage, jf. C.2, således at alle oplysninger er slettet senest 120 dage efter ophør. Oplysninger i backups genetableres ikke efter sletningen, medmindre det er nødvendigt for at genoprette driften efter en teknisk hændelse, og de slettes i så fald igen straks efter genetableringen.
- Databehandleren bekræfter skriftligt over for den dataansvarlige, at sletningen er gennemført, jf. Bestemmelse 11.1.

Databehandleren kan efter ophør opbevare oplysninger, som er nødvendige for at dokumentere aftaleforholdet og opfylde bogføringsloven (fx fakturaer og korrespondance med den dataansvarliges kontaktpersoner). Disse oplysninger behandler databehandleren som selvstændig dataansvarlig.

C.5 Lokaltet for behandling

Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end følgende:

- Databehandlerens forretningssted: DataHop ApS, Andkær Bygade 35, 7080 Børkop, Danmark, samt databehandlerens medarbejderes hjemmearbejdspladser i Danmark, hvor adgang alene sker via krypteret forbindelse til produktionsmiljøet, og hvor personoplysninger ikke lagres lokalt.
- Hostingleverandørens datacentre i Tyskland (nordicway ApS / Hetzner Online GmbH), jf. bilag B.
- Microsofts datacentre inden for EU for så vidt angår Azure Maps, jf. bilag B.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Den dataansvarlige har ikke instrueret databehandleren i at overføre personoplysninger til tredjelande eller internationale organisationer, og databehandleren overfører ikke som led i den aftalte behandling personoplysninger til tredjelande. Al behandling, herunder hos underdatabehandlere, sker inden for EU/EØS, jf. bilag B og C.5.

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.

Databehandlerens underdatabehandlere kan i deres aftaler med databehandleren have forbeholdt sig ret til at overføre oplysninger til et tredjeland, hvis det kræves for at yde support eller for at opfylde lovkrav. Bliver databehandleren bekendt med, at en sådan overførsel har fundet sted, underretter databehandleren den dataansvarlige uden unødigt ophold med oplysning om, hvilke oplysninger der er overført, til hvem og på hvilket overførselsgrundlag.

C.7 Procedurer for den dataansvarliges tilsyn med behandlingen hos databehandleren

Databehandleren dokumenterer sin overholdelse af Bestemmelserne over for den dataansvarlige på følgende måde:

- Databehandleren stiller på anmodning en skriftlig beskrivelse af de gennemførte tekniske og organisatoriske sikkerhedsforanstaltninger, jf. C.2, samt en opdateret liste over underdatabehandlere til rådighed for den dataansvarlige.
- Den dataansvarlige kan én gang årligt – og derudover ved begrundet mistanke om manglende overholdelse – sende et skriftligt spørgeskema eller anmode om dokumentation for konkrete forhold. Databehandleren besvarer anmodningen senest 30 dage efter modtagelsen.
- Ønsker den dataansvarlige at gennemføre en fysisk inspektion eller en revision ved en uafhængig tredjepart, skal dette varsles skriftligt med mindst 30 dage, ske inden for normal arbejdstid, under iagttagelse af databehandlerens sikkerhedsregler og uden at kompromittere andre kunders oplysninger. Den dataansvarlige afholder egne omkostninger og betaler databehandlerens medgåede tid efter gældende timepris. Tredjeparten skal være underlagt tavshedspligt.

- Viser tilsynet, at databehandleren ikke overholder Bestemmelserne, skal databehandleren uden unødigt forsinkelse afhjælpe forholdet og orientere den dataansvarlige herom.

Databehandleren er ikke forpligtet til at indhente en revisorerklæring (fx ISAE 3000). Vælger databehandleren senere at indhente en sådan erklæring, stilles den til rådighed for den dataansvarlige på anmodning og træder i stedet for det årlige spørgeskema.

C.8 Procedurer for tilsyn med behandlingen hos underdatabehandlere

Databehandleren fører tilsyn med sine underdatabehandlere på følgende måde:

- Databehandleren indhenter mindst én gang årligt dokumentation for underdatabehandlernes overholdelse af databeskyttelsesforordningen og databehandleraftalen med databehandleren, fx i form af underdatabehandlerens revisorerklæring, certificeringer, sikkerhedsdokumentation eller besvarelse af databehandlerens spørgsmål.
- Databehandleren gennemgår dokumentationen og vurderer, om underdatabehandleren fortsat lever op til kravene. Vurderingen og eventuelle opfølgningspunkter dokumenteres skriftligt af databehandleren.
- Databehandleren fremsender på den dataansvarliges skriftlige anmodning en kopi af den indhentede dokumentation eller et resumé af databehandlerens vurdering, i det omfang underdatabehandlerens vilkår tillader det.
- Konstaterer databehandleren væsentlige mangler hos en underdatabehandler, som ikke afhjælpes inden for rimelig tid, ophører databehandleren med at anvende underdatabehandleren og orienterer den dataansvarlige, jf. bilag B.2.