Databehandleraftale

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

mellem

Min Dag Min Energi ApS
CVR 45629627
Kærvejen 32
7171 Uldum
Danmark

herefter "den dataansvarlige"

og

A/S ScanNet
Højvangen 4
8660 Skanderborg
Danmark
CVR.nr.: 29412006

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.

1. Indhold

2. Præambel

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

2.2. 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).

2.3. I forbindelse med leveringen af services behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.

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

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

2.6. 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.

2.7. Bilag B indeholder en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.

2.8. 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.

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

2.10. Bilag E indeholder en beskrivelse af databehandlerkæden

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

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

3. Den dataansvarliges rettigheder og forpligtelser

3.1. 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.

3.2. 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.

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

3.3. 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

4.1. 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.

4.2. 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

5.1. 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.

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

6. Behandlingssikkerhed

6.1. 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.

6.2. 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.

6.3. 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.

6.4. 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.

6.5. 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.

6.6. Såfremt den dataansvarlige kræver skærpede sikkerhedsforanstaltninger i forhold til det allerede aftalte mellem parterne i medfør af Bestemmelserne og Bilag C, implementerer databehandleren, så vidt det er muligt, sådanne foranstaltninger, forudsat at databehandleren modtager betaling herfor.

7. Anvendelse af underdatabehandlere

7.1. 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).

7.2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den dataansvarlige. Den dataansvarlige kan altid gøre sig bekendt med databehandlerens underdatabehandlere på databehandlerens hjemmeside på www.scannet.dk/compliance.

7.3. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal via e-mail underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 70 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

7.4. Såfremt den dataansvarlige ikke ønsker, at databehandleren anvender en ny underdatabehandler som varslet, jf. pkt. 7.3, skal den dataansvarlige skriftlig gøre indsigelse til databehandleren mod anvendelsen af sådan ny underdatabehandler senest 60 dage efter varslet blev afgivet. I tilfælde af, at databehandleren ikke ser sig i stand til at imødekomme en eventuel indsigelse fra den dataansvarlige mod en ny underdatabehandler, meddeles dette til den dataansvarlige snarest mulig, og den dataansvarlige kan i så

fald herefter opsige de leverede services med en måneds varsel fra d. 1. i en måned. For at indsigelsen skal resultere i dette opsigelsesvarsel, skal indsigelsen være sagligt begrundet.

7.5. Ved den dataansvarliges indsigelse accepterer den dataansvarlige samtidig, at databehandleren kan være forhindret i at levere hele eller dele af de aftalte tjenester. Sådan manglende opfyldelse kan ikke tilskrives databehandlerens misligholdelse.

7.6. 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 databeskyttelsesforordningen.

7.7. 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.

7.8. Såfremt den Dataansvarlige måtte ønske at instruere underdatabehandlere direkte, bør dette alene ske efter drøftelse med og via databehandleren. Hvis den dataansvarlige afgiver instruks direkte overfor underdatabehandlere, skal den dataansvarlige senest samtidig underrette databehandleren om instruksen og baggrunden for denne. Hvor den dataansvarlige instruerer underdatabehandlere direkte, a) er databehandleren fritaget for ethvert ansvar, og enhver følge af sådan instruks er alene den dataansvarliges ansvar, b) hæfter den dataansvarlige for enhver omkostning, som instruksen måtte medføre for databehandleren, herunder er databehandleren berettiget til at fakturere den dataansvarlige med sin sædvanlige timetakst for al arbejdstid, som en sådan direkte instruks måtte medføre for databehandleren og c) den dataansvarlige er selv ansvarlig over for underdatabehandlere for enhver omkostning, vederlag eller anden betaling til underdatabehandleren, som den direkte instruks måtte medføre.

8. Overførsel til tredjelande eller internationale organisationer

8.1. 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.

8.2. 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.

8.3. 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

8.4. 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.

8.5. 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

9.1. 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.

9.2. 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

9.3. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.4, bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:

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

b. den dataansvarliges forpligtelse til uden unødig forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder

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

d. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, 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.

9.4. 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, 9.2 og 9.3.

10. Underretning om brud på persondatasikkerheden

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

10.2. Databehandlerens underretning til den dataansvarlige skal om muligt ske uden unødig forsinkelse 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.

10.3. I overensstemmelse med Bestemmelse 9.3.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.

11. Sletning og returnering af oplysninger

11.1. 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 dataansvarlig, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

12. Revision, herunder inspektion

12.1. 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.

12.2. Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.

12.3. 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

13.1. 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

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

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

14.3. 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.

14.4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne slettes i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges af begge parter.

14.5. Underskrift

På vegne af den dataansvarlige	**På vegne af databehandleren**
Underskrift:	Underskrift:
Signed by: 635219FE30A84F7...	DocuSigned by: Lotte Bendstrup 4D66656C96C641D...
Navn: Berit Therkelsen	Navn: Lotte Bendstrup
Dato: 24-09-2025	Dato: 24-09-2025

15. Kontaktpersoner hos den dataansvarlige og databehandleren

15.1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

Dataansvarlige:	**Databehandleren:**
Navn/afdeling: Berit Therkelsen	Navn/afdeling: Compliance team
E-mail: info@mindagminenergi.dk	E-mail: compliance@scannet.dk

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

Bilag A Oplysninger om behandlingen

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

Databehandleren vil i aftalens løbetid og som en del af de leverede services, værende en Cloud Server, behandle personoplysninger på vegne af den dataansvarlige med henblik på at opbevare de pågældende personoplysninger.

Databehandleren forpligter sig til ikke at behandle personoplysninger til andre formål og kun i overensstemmelse med denne aftale.

A.2. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Databehandleraftalen og tilhørende instruks omfatter alle typer af personoplysninger, som overlades af den dataansvarlige til databehandleren i henhold til den mellem parterne indgåede aftale om levering af services. Der kan være tale om følgende oplysningstyper:

ALMINDELIGE PERSONOPLYSNINGER	PERSONOPLYSNINGER SÆRLIGT REGULERET I DATABESKYTTELSESLOVEN	SÆRLIGE KATEGORIER AF PERSONOPLYSNINGER
• Navn • E-mail • Telefonnummer • Fødselsdag • Brugertype		• Helbredsoplysninger

A.3. Behandlingen omfatter følgende kategorier af registrerede

Kategorierne af de registrerede personer, som personoplysningerne vedrører, udgøre patienter.

A.4. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen har følgende varighed

Databehandleren behandler personoplysninger på vegne af den dataansvarlige i aftalens løbetid, medmindre databehandleren modtager andre instrukser fra den dataansvarlige.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING

Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks
Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende:

- Databehandleren vil i aftalens løbetid og som en del af de leverede services behandle personoplysninger på vegne af den dataansvarlige med henblik på at opbevare de pågældende personoplysninger.

C.2. Behandlingssikkerhed
Sikkerhedsniveauet skal afspejle:

Introduktion
Som hostingleverandør er vores vigtigste sikkerhedsopgave at passe godt på dine data og sørge for, at du til enhver tid lever op til sikkerhedskravene fra dine kunder.
Sikkerhed er derfor et område, som vi tager meget seriøst - på alle niveauer.

Organisering af sikkerhed
Vi har etableret et brancheledende informationssikkerhedsprogram (ISMS), der giver vores kunder den bedste beskyttelse og højeste grad af tillid.
Programmet følger ISO 27001-sikkerhedsstandarden, som vi har været certificeret efter siden 2015.

Politikker, procedurer og standarder
Vi har defineret et sæt af politikker, procedurer og standarder for, hvordan vi opererer i virksomheden og bedst passer på dine data. Dokumenterne opdateres løbende i takt med eventuelle ændringer i vores risikovurderinger. På den måde sikrer vi, at vi hele tiden prioriterer vores indsats dér, hvor der er mest brug for den.

Medarbejdersikkerhed
Alle medarbejdere og konsulenter med adgang til systemer og faciliteter er underlagt vores sikkerhedspolitikker. Alle gennemgår obligatorisk undervisning, hvor de bliver præsenteret for alle relevante og aktuelle privacy- og sikkerhedsemner. Dette sker både ved start og løbende gennem deres ansættelse. Formålet er at ruste medarbejderne til at modstå aktuelle trusler mod virksomhedens og kundernes data.
For at højne det generelle niveau i branchen og for at vedligeholde egne kompetencer deltager vores medarbejdere aktivt i communitites og ERFA-grupper. Vi opfordrer vores medarbejdere til hele tiden at være på forkant med den nyeste udvikling og til at erhverve de højeste certificeringer inden for sikkerhed, netværk, osv.

Dedikerede sikkerheds-og persondatakompetencer
Vores sikkerchef er ansvarlig for at implementere og vedligeholde vores informationssikkerhedsprogram. Vores interne auditører gennemgår regelmæssigt vores sikkerhedssetup og rapporterer direkte til ledelsen. Endelig har vi interne, juridiske kompetencer inden for persondata, som sikrer, at persondata behandles efter de gældende regler både internt i virksomheden og på vegne af vores kunder.

Operationel sikkerhed - Beskyttelse af kundedata
Den vigtigste opgave i vores sikkerhedsprogram er at passe godt på dine data. For at gøre det er vores sikringsmiljø inddelt i flere lag:

- Fysisk sikkerhed

Vores datacentre er state-of-the-art og vores datacenterleverandør er ansvarlig for de fysiske rammer som fx strøm, køl, brandslukning og adgangskontrol, og vi fører skarp kontrol med, at vores underleverandører efterlever de gældende sikkerhedsregler på området.

- Netværk
  Vores netværk er segmentet, så kunder er beskyttet mod hinanden og mod trusler, der bevæger sig på tværs i netværket. Next Generation firewalls begrænser angreb mod kundernes miljøer, og DDoS-beskyttelse begrænser den påvirkning, som evt. angreb måtte have på serverne. Avanceret netværksinspektion opfanger mønstre og angrebsforsøg fra kendte, ondsindede ip-adresser og alarmerer vores driftsafdeling ved behov.

- Logiske adgange
  Vi tildeler kun rettigheder til de medarbejdere, der har brug for dem, og vurderer dem løbende. Kun særligt privilegerede medarbejdere har adgang til at administrere interne systemer.

- Overvågning
  Vi overvåger vores infrastruktur og relevante services døgnet rundt. Alle afvigelser registreres i vores incident management system. Som supplement til overvågningen har vi tilknyttet en 24/7-vagt-ordning.

- Logning
  Vi logger alle adgange til management- og kundemiljøer. På den måde sikrer vi integritet og sporbarhed og kan sammenkøre hændelser. Vores centrale logplatform sikrer, at vi kan korrelere logs fra mange kilder.

- Backup
  Vi udfører backup ud fra den individuelle aftale med kunden eller den indgåede SLA. Backupdata opbevares altid på en anden lokation end produktionsdata, så der altid er en tilgængelig kopi i tilfælde af et kritisk nedbrud.

Beredskab og disaster recovery
Beredskab handler om at være forberedt på hændelser, som kan have kritisk eller katastrofal påvirkning på driften. Vi har derfor beredskabsplaner som fastlægger vores procedurer, rutiner og roller i tilfælde af en katastrofe. Medarbejdere trænes i beredskabet flere gange årligt.
For at sikre vores tekniske infrastruktur og sprede risikoen ved kritiske nedbrud bruger vi flere uafhængige datacenterleverandører. Vi opbevarer altid mindst én kopi af backupdata i et datacenter, hvor vi ikke har produktionsdata.

Revision, compliance og uafhængige tredjepartsvurderinger
Vi har et omfattende compliance-program, som sikrer, at vi efterlever vedtagne standarder, interne politikker og relevant lovgivning på området, med det formål at understøtte og sikre din forretning:

- ISO 27001
  ISO 27001 er en international standard for håndtering af informationssikkerhed. Flere af vores konkurrenter påstår, at de følger standarden, men er ikke certificerede. Vi har været certificeret siden marts 2015. Certificeringen skal fornyes én gang om året og revideres af både interne og eksterne auditører.

- ISAE 3402 Type 2
  ISAE 3402 Type 2 beskriver, hvordan vi sikrer de ydelser, som vi leverer til vores kunder, og indeholder en uafhængig revisors konklusion på, om beskrivelsen af vores kontroller er retvisende, hensigtsmæssigt udformet, og om kontrollerne har fungeret effektivt i hele erklæringsperioden.

Ændringer til sikkerhedsforanstaltninger
Databehandleren er altid berettiget til at gennemføre alternative sikkerhedsforanstaltninger, forudsat at sådanne sikkerhedsforanstaltninger som minimum svarer til eller giver større sikkerhed end de sikkerhedsforanstaltninger, der er beskrevet i bilag C. Databehandleren kan ikke reducere sikkerhedsniveauet uden forudgående skriftlig tilladelse fra den dataansvarlige.

Ovennævnte rapporter og certificeringer er de rapporter og certificeringer, der i øjeblikket indhentes med henblik på at kontrollere vores sikkerhedsforanstaltninger. Databehandleren er til enhver tid berettiget til at indhente andre typer rapporter eller certificeringer for at gennemgå og kontrollere relevante sikkerhedsforanstaltninger, f.eks. ISAE 3000, SOC2.

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, 9.2 og 9.3 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

For alle services gør det sig gældende, at den dataansvarlige selv kan besvare og opfylde anmodninger fra data subjekter for at kunne overholde den registreredes rettigheder.

Databehandleren skal så vidt muligt bistå den dataansvarlige med at opfylde den dataansvarliges forpligtelser til at besvare anmodninger fra data subjekter, der ønsker at udøve deres rettigheder, hvis det er databehandleren, der behandler sådanne personoplysninger. Databehandleren skal straks informere den dataansvarlige, når databehandleren modtager sådanne henvendelser fra registrerede.

Den dataansvarlige har ansvaret for at dække alle omkostninger, som databehandleren afholder i forbindelse med bistand udført i henhold til Bestemmelse 9.1, 9.2 og 9.3. Prisen for databehandlerens bistand beregnes i henhold til den aktuelt gældende timesats for udførelse af sådant arbejde.

C.4 Opbevaringsperiode/sletterutine

Databehandleren er forpligtet af denne Databehandleraftale, så længe databehandleren behandler personoplysninger på vegne af den dataansvarlige, idet den dataansvarlige snarest muligt og senest 14 dage efter ophør af aftalen om levering af services skal oplyse databehandleren skriftligt, hvorvidt databehandleren skal slette de behandlede personoplysninger. 30 dage efter ophøret af aftalen om levering af services er databehandleren berettiget til at slette alle personoplysninger, som er blevet behandlet under den ophørte aftale på vegne af den dataansvarlige. Databehandleren må dog altid opbevare de behandlede data, såfremt dette følger af EU-retten eller medlemsstaternes nationale ret.

C.5 Lokalitet for behandling
Personoplysninger behandles på de nedenfor anførte steder og på underdatabehandlerens driftsadresser.

Databehandlerens lokationer:

Hovedkvarter: Højvangen 4, 8660, Skanderborg
Datacenter #1: 8660 Skanderborg, Denmark

Datacenter #2: 8660 Skanderborg, Denmark
Datacenter #3: 8270 Højbjerg, Denmark
Datacenter #4: 8362 Hørning, Denmark
Datacenter #5: 8920 Randers, Denmark
Datacenter #6: 8260 Viby J, Denmark
Datacenter #7: 8382 Hinnerup, Denmark

De nøjagtige adresser på vores datacentre holdes fortrolige af sikkerhedshensyn. Den dataansvarlige kan altid finde adresserne (postnummer og by) på datacentrene i det ISO 27001-certifikat, der er udstedt til databehandleren.

Hvis den dataansvarlige har fået tilladelse til at foretage et fysisk audit af faciliteterne, begynder det pågældende audit ved databehandlerens hovedkvarter, hvorefter eventuelle eksterne auditører eskorteres til det relevante datacenter.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

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

Databehandleren må ikke overføre personoplysninger til tredjelande uden instruks herom fra den dataansvarlige. Hvis sådanne overførsler til tredjelande bliver aktuelle for at levere en pågældende service, skal overførslerne som udgangspunkt reguleres af EU Standard Contractual Clauses.

C.7 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren

Såfremt den dataansvarlige ønsker at foretage tilsyn, i henhold til dette pkt. C.7, skal den dataansvarlige altid give databehandleren et varsel på mindst 30 dage i sådan forbindelse.

Databehandleren får én gang årligt udarbejdet en sikkerhedsrevisionserklæring, som beskriver sikkerhedsforholdene hos databehandleren. Den dataansvarlige er berettiget til at få udleveret en kopi heraf. Kopi af sådan sikkerhedsrevisionserklæring kan den dataansvarlige altid hente på databehandlerens hjemmeside.

Såfremt den dataansvarlige ønsker at få udarbejdet anden eller yderligere sikkerhedsrevisionserklæring udover de erklæringer som databehandleren allerede får udarbejdet på eget initiativ, eller at der i øvrigt ønskes foretaget tilsyn af databehandlerens eller underdatabehandlerens persondatabehandling, herunder såfremt den dataansvarlige ønsker sikkerhedsrevisionserklæring udarbejdet på et nærmere bestemt tidspunkt, aftales dette nærmere med databehandleren.

Når tilsyn sker på anmodning fra den dataansvarlige, fra tredjeparter på foranledning af den dataansvarlige, eller fra myndigheder grundet forhold hos den dataansvarlige afholder den dataansvarlige alle omkostninger i forbindelse med tilsyn af sikkerhedsforhold hos databehandleren samt i forhold til underdatabehandleren, herunder er databehandleren berettiget til at fakturere den dataansvarlige med sin sædvanlige timetakst for al databehandlerens arbejdstid, som sådant tilsyn måtte medføre for databehandleren.

C.8 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere

For at vi kan operere så effektivt som muligt, bruger vi underdatabehandlere til udvalgte services. Hvis underdatabehandlere kan have påvirkning på vores sikringsmiljø, sørger vi for, at de efterlever samme strenge krav som os selv. Det gør vi via kontrakter, databehandleraftaler, revisionserklæringer, egenkontrol og fortrolighedsaftaler. Vi kontrollerer løbende, at vores underdatabehandlere efterlever kravene.

Når tilsyn sker på anmodning fra den dataansvarlige, fra tredjeparter på foranledning af den dataansvarlige, eller fra myndigheder grundet forhold hos den dataansvarlige afholder den dataansvarlige alle omkostninger i forbindelse med tilsyn af sikkerhedsforhold hos underdatabehandleren, herunder er databehandleren berettiget til at fakturere den dataansvarlige med sin sædvanlige timetakst for al databehandlerens arbejdstid, som sådant tilsyn måtte medføre for databehandleren. Den dataansvarlige vil også være ansvarlig for at betale underdatabehandlerne for den tid, der er brugt på alt det arbejde, som en sådan inspektion ville medføre for underdatabehandleren.

Bilag D Parternes regulering af andre forhold

Databehandleren skal udarbejde en fuldstændig oversigt over databehandlere, som behandler den dataansvarliges personoplysninger. Oversigten udarbejdes og vedlægges i Bilag E.

Oversigten skal angive databehandlerens underdatabehandlere, og alle deres eventuelle underdatabehandlere, så hele kæden for behandling af personoplysninger er dokumenteret.

Databehandleren kan på forespørgsel fremvise et koncerndiagram over de koncernforbundne selskaber.

Bilag E Databehandlerkæden