

Databehandleraftale
mellem
NRGi Systems A/S og XXX

Standardkontraktsbestemmelser

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

mellem

XXX

CVR: XX XX XX XX

XXX

XXX

herefter "den dataansvarlige"

og

NRGi Systems A/S

CVR 30 92 58 15

Dusager 22

8200 Aarhus N

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

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	8
10. Underretning om brud på persondatasikkerheden	9
11. Sletning og returnering af oplysninger	9
12. Revision, herunder inspektion	9
13. Parternes aftale om andre forhold	10
14. Ikrafttræden og ophør	10
16. Kontaktpersoner hos den dataansvarlige og databehandleren	11
Bilag A Oplysninger om behandlingen	12
Bilag B Underdatabehandlere	13
Bilag C Instruks vedrørende behandling af personoplysninger	14

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 en online softwareløsning til brug for energiberegning af bygninger behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.
4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.
5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.
6. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.
7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.
8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.
9. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke er omfattet af Bestemmelserne.
10. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
11. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

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.

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

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. Den dataansvarlige er endvidere ansvarlig for, at der foreligger samtykke fra dennes medarbejdere, der anvender softwareløsningen, i forbindelse med databehandlerens indsamling af relevante personoplysninger for de enkelte medarbejdere.

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 14 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. 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.
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

- 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.
- 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.
- 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
- 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.

- 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. indsigtretten
 - 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 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 tilbagelevere alle personoplysningerne og slette eksisterende kopier, 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 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. 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 begge parters underskrift heraf.
2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.
3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.
4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftligt varsel af begge parter.

15. Underskrift

På vegne af den dataansvarlige

Navn	XXX
Stilling	XXX
Telefonnummer	XXX
E-mail	XXX

Underskrift

På vegne af databehandleren

Navn	Jacob Nørgaard Hansen
Stilling	Salgs- & Kundecheff
Telefonnummer	3153 7311
E-mail	jnha@nrgisystems.dk

Underskrift

16. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.
2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

Navn	XXX
Stilling	XXX
Telefonnummer	XXX
E-mail	XXX

Navn	Jacob Nørgaard Hansen
Stilling	Salgs- & Kundecheff
Telefonnummer	3153 7311
E-mail	jnha@nrgisystems.dk

Bilag A Oplysninger om behandlingen

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

Formålene med databehandlerens behandling af personoplysninger er:

- At databehandleren leverer en online softwareløsning, hvori den dataansvarlige kan lave energiberegninger, herunder udarbejde dynamiske energimærkninger.
- Personoplysningerne indsamles alene med det legitime formål at kunne registrere brugeren i softwareløsningen, således at brugeren kan anvende systemet selvstændigt, herunder modtage målrettet kundesupport via bl.a. telefon, e-mail og nyhedsbreve.

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

- NRGi Systems foretager behandling af personoplysninger i forbindelse med kundens anvendelse af softwareløsningen ved at opbevare personoplysninger, som kunden indtaster i løsningen.

For så vidt angår Energy10/Energy Projects:

- Når den dataansvarlige anvender Energy10/Energy Projects og eventuelt registreret forbrugsoplysninger om deres kunder, behandler NRGi Systems personoplysninger om disse kunder på vegne af den dataansvarlige.

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

Vedrørende den dataansvarliges kunder i softwareløsningen Energy10 bliver der registreret følgende løsninger personoplysninger i Energy10:

- Navn på kontaktperson
- E-mailadresse
- Telefonnummer

A.4. Behandlingen omfatter følgende kategorier af registrerede

- Medarbejdere hos den dataansvarlige.

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

Opbevaring og behandling af personoplysningerne ophører først ved ophør af licensaftalen eller ved den dataansvarliges tilbagetrækning af godkendelsen af de anførte brugsbetingelser.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Global Connect A/S	26759722	Havneholmen 6, 2450 København SV	Hosting

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.

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:

- Leverer en online softwareløsning til energiberegninger med tilhørende vejledning, dokumentation og support.

Databehandleren må alene behandle personoplysningerne med det formål at varetage de fastsatte databehandlingsopgaver i dette bilag. Databehandleren må ikke behandle eller anvende personoplysningerne til andre formål end dem, der er angivet i denne aftale.

Databehandleren er ansvarlig for at dataansvarliges instruks sendes til eventuelle underdatabehandlere.

C.2. Behandlingssikkerhed

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

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

Generelle sikkerhedsforanstaltninger

Databehandleren skal sikre, at:

- Samtlige medarbejdere, der har adgang til personoplysninger, har forpligtet sig til tavshed i forhold til personoplysninger og behandlingsaktiviteter, og at en sådan tavshedspligt også gælder efter ophør af parternes samarbejde, samt efter medarbejderens ansættelse hos databehandleren er ophørt.
- Samtlige medarbejdere hos databehandleren, der har adgang til personoplysninger, underlægges interne politikker for IT-sikkerhed og databeskyttelse.
- Samtlige medarbejdere hos databehandleren, der har adgang til personoplysninger, undervises løbende i IT-sikkerhed og databeskyttelse.
- Systemer, databehandleren anvender til behandlingen af personoplysninger, udvikles med udgangspunkt i datasikkerhed og best practice inden for databeskyttelse.

Fysiske sikkerhedsforanstaltninger

Databehandleren skal sikre, at:

- Fysiske lokationer, fra hvilke der sker behandling af personoplysninger, er beskyttet med indbrudssikring og elektronisk overvågning.
- Adgang til fysiske lokationer, fra hvilke der sker behandling af personoplysninger, kun kan ske via personligt nøglekort eller anden adgangskontrolforanstaltning.
- Besøgende ikke uden opsyn tillades adgang til fysiske lokationer, fra hvilke der sker behandling af personoplysninger.

Kryptering af personoplysninger

Databehandleren skal sikre, at:

- Al transmission af følsomme og fortrolige personoplysninger sker via en tilstrækkeligt krypteret forbindelse.
- Krypteringsnøgler er stærke og opbevares på en sikker lokation med identitetsbaseret adgangskontrol og kontrolpolitikker.
- Udstyr, der anvendes til behandling af personoplysninger, er krypteret.

Sikring af vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester

Databehandleren skal sikre, at:

- Kun databehandlerens autoriserede medarbejdere har adgang til personoplysninger.
- Databehandlerens medarbejdere alene har adgang til personoplysninger i det omfang, det er nødvendigt for udførelsen af deres arbejde.
- Alle medarbejdere har unikke brugernavne og passwords.
- Der er implementeret passwordpolitikker, der sikrer, at passwords er tilstrækkeligt stærke.
- Der anvendes flerfaktor-autentifikation ved fjernadgang til personoplysninger, herunder i forbindelse med hjemmearbejde.
- Udstyr, som databehandlerens medarbejdere får udleveret til brug i udførelsen af deres arbejde, skal sikres med adgangskontrol.
- Medarbejdere pålægges at opretholde adgangskontrollen og sikre, at adgangskoder forbliver personlige og fortrolige.
- Der skal implementeres procedurer, der sikrer, at medarbejdere låser deres skærm, når den forlades, ligesom der skal implementeres automatisk skærmlås, der aktiveres efter kort tids inaktivitet.
- Der er etableret velfungerende backup, og at der foretages løbende stikprøvekontrol af, at backup foretages.
- Adgang til systemer, der anvendes til behandling af personoplysninger, er sikrede med individuelle fortrolige adgangskoder og VPN-forbindelser.
- Der implementeres procedurer, der skal sikre imod skadelige hændelser i driftsudstyr.
- Der implementeres procedurer, der skal sikre imod at personoplysninger, der opbevares på elektronisk udstyr og fysisk materiel, tilintetgøres, tabes, ændres eller uautoriseret videregives.
- Driftservere alene har nødvendige services og porte åbne og sikkerhedsopdateres løbende.
- Der anvendes firewalls og antivirusprogrammer på alt udstyr, der anvendes til behandling af personoplysninger, og at sådanne firewalls og antivirusprogrammer til enhver tid er opdaterede.
- Alle systemer der anvendes til behandling af personoplysninger, skal til enhver tid være opdaterede med seneste sikkerhedsopdatering.

Logning

Databehandleren skal sikre, at der sker logning af al adgang til og behandling af personoplysninger og at der gennemføres stikprøvekontrol med det formål at sikre, at adgang til og behandling af personoplysninger logges korrekt.

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:

Assistance i overensstemmelse med pkt. 9.1:

Bistand til varetagelse af de registreredes rettigheder

Databehandleren yder bistand til varetagelse af de registreredes rettigheder ved at sikre, at databehandlerens systemer og interne processer er indrettet på sådan en måde, der gør det muligt for databehandleren at bistå den dataansvarlige med at varetage de registreredes rettigheder i tilfælde, hvor den dataansvarlige ikke er i stand til at gøre dette, uden den dataansvarliges medvirken samt i tilfælde, hvor databehandleren på forhånd er blevet instrueret i at varetage en eller flere af de registreredes rettigheder på vegne af den dataansvarlige.

Databehandleren vil i de tilfælde, hvor det er muligt og relevant i forhold til den pågældendes behandling, sørge for at databehandlerens systemer er indrettet på en måde, der gør det muligt for den dataansvarlige selv at varetage de registreredes rettigheder direkte i databehandlerens systemer således, at databehandlerens bistand ikke vil være påkrævet.

Modtager databehandleren en henvendelse fra en registreret, hvis personoplysninger databehandleren behandler på vegne af den dataansvarlige, tager databehandleren kontakt til den dataansvarlige for at blive instrueret i, hvordan en sådan henvendelse skal håndteres, medmindre databehandleren på forhånd er blevet instrueret i at varetage en sådan henvendelse. En sådan instruks skal fremgå af dette afsnit.

Assistance i overensstemmelse med pkt. 9.2:

Bistand til anmeldelse af brud til tilsynsmyndigheden og underretning af de registrerede

Databehandlerens systemer og interne processer er indrettet på en sådan måde, at databehandleren, uden unødigt forsinkelse, og senest 48 timer efter, at denne er blevet bekendt med bruddet, kan underrette den dataansvarlige om brud på persondatasikkerheden.

Databehandleren bistår, under hensyn til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med de nødvendige oplysninger om bruddet således, at den dataansvarlige kan opfylde sin forpligtelse til uden unødigt forsinkelse, og om muligt senest 72 timer efter, at denne er blevet bekendt med bruddet at anmelde brud på persondatasikkerheden. Oplysninger om bruddet fremsendes til dataansvarlige på e-mail til kontaktpersonen angivet i afsnit 15.

Databehandlerens systemer og interne processer er ligeledes indrettet på en sådan måde, at databehandleren kan stille de nødvendige oplysninger til rådighed for den dataansvarlige således, at den dataansvarlige kan vurdere, hvorvidt de registrerede skal underrettes om brud på persondatasikkerheden. Vurderer den dataansvarlige herefter, at der skal foretages underretning af de registrerede, bistår databehandleren, efter anmodning fra den dataansvarlige, med at foretage underretningen i tilfælde, hvor underretning ikke kan ske uden databehandlerens medvirken.

Bistand til foretagelse af konsekvensanalyse:

Databehandlerens systemer og interne processer er indrettet på en sådan måde, at databehandleren, under hensyn til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, kan bistå dataansvarlige med dennes forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse) samt at bistå den dataansvarlige med dennes forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet, inden behandling, såfremt konsekvensanalysen viser, at behandlingen vil føre til en høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.

C.4 Opbevaringsperiode/sletterutine

Personoplysningerne opbevares hos databehandleren, indtil den datasansvarlige anmoder om at få oplysningerne slettet eller tilbageleveret.

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

Dokumentationen skal tydeligt angive datoen for ændringen og beskrive eventuelle særlige dokumentationskrav og procedurer, som skal iagttages i forbindelse med ændringen.

C.5 Lokalitet for behandling

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

NRGi Systems

Dusager 22,
8200 Aarhus N

Global Connect

Industriparken 20A, 2750 Ballerup
Hørskættens 3, 2630 Taastrup

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

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

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

På den dataansvarliges skriftlige anmodning skal databehandleren inden for rimelig tid stille de oplysninger til rådighed, der er nødvendige for at kunne påvise, at databehandlerens overholdelse af Databeskyttelsesforordningens artikel 28 samt disse Bestemmelser.

I tillæg til ovenstående skal databehandleren på den dataansvarliges skriftlige anmodning og med et rimeligt varsel give adgang til at den dataansvarlige, herunder revisorer, der er bemyndiget af den dataansvarlige og underlagt tilstrækkelig tavshedspligt, kan foretage revisioner og inspektioner, der er nødvendige for at påvise databehandlerens overholdelse af Databeskyttelsesforordningens artikel 28 samt kravene i disse Bestemmelser. Databehandleren er for sin bistand, herunder sit tidsforbrug forbundet med bistanden, berettiget til at modtage vederlag i henhold til de kommercielle rammer og vilkår som fastsat i Hovedaftalen. Den dataansvarlige afholder egne omkostninger, herunder omkostninger til eksterne revisorer i forbindelse med revisioner og inspektioner.

Databehandleren kan én gang hvert år for den dataansvarliges regning indhente en revisionserklæring fra en uafhængig tredjepart angående databehandlerens overholdelse af denne databehandleraftale med tilhørende bilag. Revisionserklæringen sendes snarest muligt efter indhentelsen til den dataansvarlige til orientering. Den

dataansvarlige kan – hvis det findes nødvendigt – vælge at initiere og deltage på en fysisk inspektion hos underdatabehandleren. Dette kan blive aktuelt, såfremt den dataansvarlige vurderer, at databehandlerens tilsyn med underdatabehandleren ikke har givet den dataansvarlige tilstrækkelig sikkerhed for, at behandlingen hos underdatabehandleren sker i overensstemmelse med denne databehandlersaftale. Den dataansvarliges eventuelle deltagelse i et tilsyn hos underdatabehandleren ændrer ikke ved, at databehandleren også herefter har det fulde ansvar for underdatabehandlerens overholdelse af databeskyttelseslovgivningen og denne databehandlersaftale. Databehandlerens og underdatabehandlerens eventuelle udgifter i forbindelse med afholdelse af et fysisk tilsyn/en inspektion hos underdatabehandleren afholdes af den dataansvarlige.

Commented [F1]: Det markerede afsnit kan slettes.