

Databehandlraftale

1. Databehandleraftalen omfatter

DATAANSVARLIG

ORGANISATION	[Kundens virksomhedsnavn, adresse & CVR-nr]	
CVR-NR.		
ADRESSE		
KONTAKTPERSON	AFTALEANSVARLIG	DATAANSVARLIG KONTAKTPERSON
	[Kundens navn]	
DIREKTE TELEFONNR.		
E-MAIL	[email]	

herefter "den dataansvarlige" og:

DATABASEHANDLER

ORGANISATION	Geomatic A/S
CVR-NR.	28 86 22 45
ADRESSE	Regnbuepladsen 7, 2 1550 København V
KONTAKTPERSON	Tina Forsberg
DIREKTE TELEFONNR.	+45 29 38 70 47
E-MAIL	Tina.forsberg@geomatic.dk

herefter "databehandler",
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

BILAG TIL DATABASEHANDLERAFTALEN

BILAG A)	Oplysninger om behandlingen
BILAG B)	Instruks vedrørende behandling af personoplysninger
BILAG C)	Underdatabehandlere
BILAG D)	Parternes regulering af andre forhold

Indholdsfortegnelse

1. Databehandleraftalen omfatter	2
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 af personoplysninger	9
12. Revision, herunder inspektion	9
13. Parternes aftale om andre forhold	9
14. Ikrafttræden og ophør	9
15. Kontaktpersoner hos den dataansvarlige og databehandleren	9
Bilag A) Oplysninger om Behandlingen	10
Bilag B) Instruks vedrørende behandling af personoplysninger	12
Bilag C) Underdatabehandlere	16
Bilag D) Parternes regulering af andre forhold	17

2. Præambel

2.1. 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 tjenesten 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 fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.

- 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.
- Bilag B 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.
- Bilag C indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.
- Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke er omfattet af Bestemmelserne.

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

2.7. 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 medlemsstaternes 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.

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 B. 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.

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. 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.

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.

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.

6.2. 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.

6.3. 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 B.

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.

7.3. 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 2 måneders 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 C. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag C.

7.4. 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.

7.5. 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 og anden fortrolig information, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.

7.6. 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.

7.7. Hvis databehandleren 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

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 B.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) indsichtsretten
- 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 9.1., 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.

9.4. Parterne skal i bilag B 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 dette afsnit 9.1. og 9.2.

10. Underretning om brud på persondatasikkerheden

10.1. Databehandleren underretter uden unødigt 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 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.

10.3. 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.

10.4. Parterne skal i bilag B 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 af personoplysninger

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 dataansvarlige, 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. Procedurene for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i bilag B.7 og B.8.

12.3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivning har adgang til den dataansvarliges og databehandlerens faciliteter, eller repræsentanter, der optræder på myndighedens 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 u hensigtsmæssigheder 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 er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag B.4, kan Bestemmelserne opsiges med skriftligt varsel af begge parter.

15. Kontaktpersoner hos den dataansvarlige og databehandleren

15.1. Parterne kan kontakte hinanden via anførte kontaktoplysninger på side 2.

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

Bilag A) Oplysninger om Behandlingen

Den dataansvarlige er ansvarlig for at oplysningerne om behandlingen er retvisende for den databehandling, databehandleren skal foretage. Dette gælder også, hvor den dataansvarlige anmoder om databehandlerens bistand til udfyldelsen. I så fald skal den dataansvarlige kontrollere oplysningerne om behandlingen inden databehandleraftalen underskrives af begge Parter.

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

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er primært datavask, analyse og segmentering hvor der indgår offentligt tilgængelige personoplysninger og andre typer af data end persondata, samt Geomatics egne statistiske datamodeller. Behandlingen er nærmere specificeret i bilag B.

Den dataansvarlige skal anvende de behandlede personoplysninger til følgende formål: Formålet med behandlingen er at udarbejde en rapport, der giver virksomheden indsigt i sociodemografiske karakteristika inden for kundebasen, med henblik på at styrke virksomhedens evne til at udnytte disse indsigter strategisk.

Den dataansvarlige agerer i følgende rolle (som defineret i gældende databeskyttelseslovgivning):

Dataansvarlig ☒

Databehandler ☐

(NB: I denne databehandlerrolle handler den dataansvarlige baseret på en autorisation/instruks fra tredjepartsdataansvarlige, f.eks. den dataansvarlige's virksomhedskunde)

Databehandlerne agerer i følgende rolle (som defineret i gældende databeskyttelseslovgivning):

Databehandler ☒

Underdatabehandler ☐

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

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige vedrører de(n) behandlingstype(r) der er afkrydset i bilag B.

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

Der behandles følgende indgående og udgående personoplysninger om de registrerede:

Almindelige personoplysninger (GDPR art. 6)

Kontaktoplysninger (navn, adresse, e-mail, tlf.)

Sæt kryds:

☒

Behandlingen foretages ved hjælp af følgende datakilder

Nummeroplysningsdata

Geomatics datamodeller

Statistiske data

Sæt kryds:

☒

☒

☒

A.4 Behandlingen omfatter følgende kategorier af registrerede

Behandlingen omfatter følgende kategorier af registrerede:

Kunder/medlemmer



Tidligere kunder/medlemmer



A.5 Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter databehandleraftalens ikrafttræden.

Behandlingen er ikke tidsbegrænset og varer indtil aftalen opsiges eller ophæves af en af Parterne.

Bilag B) Instruks vedrørende behandling af personoplysninger

Den dataansvarlige er ansvarlig for, at instruksen er retvisende for den databehandling, databehandleren skal foretage. Dette gælder også, hvor den dataansvarlige anmoder om databehandlerens bistand til udfyldelsen. I så fald skal den dataansvarlige kontrollere instruksen inden databehandleraftalen underskrives af begge Parter.

B.1 Behandlingens genstand/instruks

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

Behandlingstype

Analyse og segmentering

Sæt kryds



B.2 Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

Behandlingen omfatter personoplysninger, som skal beskyttes via nedenstående sikkerhedsforanstaltninger. Yderligere sikkerhedsforanstaltninger skal aftales mellem parterne.

Databehandleren er 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 der er i overensstemmelse med sikkerhedskrav efter ISAE 3402, og som er aftalt med den dataansvarlige:

a. Generelt

Databehandleren skal etablere interne politikker, procedurer og guidelines, som skal sikre det nødvendige sikkerhedsniveau for håndtering af personoplysninger, og skal svare til kravene i ISAE 3402 og 3000 eller tilsvarende for at reducere risikoen for brud på persondatasikkerheden samt informationssikkerheden.

b. Organisering af informationssikkerheden

Databehandleren skal træffe de fornødne tekniske og organisatoriske foranstaltninger mod, at personoplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med lovgivningen.

Databehandleren skal på baggrund af en risikovurdering træffe de tekniske og organisatoriske foranstaltninger, der tager højde for at sikre fortroligheden, tilgængeligheden og integriteten af personoplysninger, som fremgår af dette bilag B.2.

c. Interne sikkerhedsretningslinjer

Databehandleren skal fastsætte og gennemføre interne risikobaserede retningslinjer for sikker behandling af personoplysninger i overensstemmelse med den til enhver tid gældende lovgivning om behandling af personoplysninger.

Databehandleren skal endvidere implementere relevante databeskyttelsespolitikker.

Databehandlerens relevante retningslinjer skal gennemgås i samarbejde med den dataansvarlige, hvis der med rimelighed, er grund til at tro, at de interne retningslinjer ikke er fyldestgørende.

d. Fysisk sikkerhed og IT-sikkerhed

Der skal træffes sikkerhedsforanstaltninger til hindring af uvedkommendes adgang til personoplysninger, som Databehandleren behandler i medfør af Bestemmelserne.

Databehandleren skal have procedure for fjernadgang fx via hjemmearbejdspladser og skal beskytte adgangen til personoplysninger via 2-faktor godkendelse via VPN-adgang.

e. Transmission af oplysninger og opbevaring

Personoplysninger transmitteres kun via SFTP eller FTPS eller HTTPS. Anden metode for transmission af personoplysninger skal aftales eksplicit mellem parterne inklusiv nødvendige sikkerhedsforanstaltninger.

Personoplysninger opbevares kun på sikre drev, som autoriserede medarbejdere har adgang til ud fra et nødvendighedsprincip. Fysiske lokaliteter, hvori drev med personoplysninger opbevares, sikres efter anerkendte standarder.

f. Adgangsstyring

Kun de personer hos databehandleren, som er autoriseret hertil, må have adgang til personoplysningerne. Der må ikke gives adgangsrettigheder til personoplysningerne i videre omfang, end de pågældende har behov for i forhold til deres jobfunktion.

Medarbejderens adgangskoder skal følge anerkendte best practices.

Databehandleren må ikke anvende software, programmel og hardwarekonfigurationer med kendte svagheder og sårbarheder, som kan udnyttes til at få adgang til personoplysningerne.

g. Logning

Databehandleren skal udarbejde logfiler over brugeraktiviteter. Logfiler skal gennemgås regelmæssigt med henblik på at opdage uautoriserede aktiviteter i relation til den IT-tjeneste, der er anvendt.

h. Back-up

Databehandleren skal sikre, at IT-systemer er dækket af en backup-løsning, og at sikkerhedskopier opbevares særskilt og beskyttes mod uautoriseret adgang

i. Antivirus/malware og patching

Alle IT-tjenester skal, hvor det er relevant, beskyttes mod skadelig software med en opdateret antivirus eller lignende løsning.

Databehandleren skal have en patch management-procedure, der sikrer at alle nødvendige programrettelser og sikkerhedsopdateringer er installeret på IT-tjenesten.

j. Sikker konfiguration

Databehandleren skal følge softwareleverandørers/producenters best practices eller retningslinjer for hærkning, hvor det er relevant.

B.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:

Databehandleren vil stille relevante medarbejdere til rådighed for at opfylde bistandsforpligtelsen.

Korrespondancer skal primært foregå skriftligt.

Bistandens omfang og udtrækning vil være som angivet i Bestemmelse 9.1 og 9.2 og 9.3

Databehandleren har krav på betaling efter dokumenteret medgået tid og forbrugte materialer for bistand i medfør af databehandlerens bistand efter Bestemmelse 9.1, 9.2 og 9.3, dog således at der ikke er krav på betaling, hvis bistanden sker som led i misligholdelse.

B.4 Opbevaringsperiode/sletterutine

Personoplysningerne opbevares som udgangspunkt i 12 måneder efter ophør af tjenesterne vedrørende behandling af personoplysninger, hvorefter de slettes hos databehandleren, medmindre den dataansvarlige har angivet en anden opbevaringsperiode.

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 på opfordring, bekræfte over for den dataansvarlige, at oplysningerne er slettet.

B.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:

Inden for Danmarks grænser hos databehandleren og på underdatabehandlernes adresse angivet i bilag C.

B.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.

Såfremt den dataansvarlige giver samtykke til, at databehandleren foretager behandling af personoplysninger uden for EU/EØS, skal dette fremgå særskilt af bilag C. Databehandleren skal sikre et korrekt juridisk grundlag for overførsel af personoplysninger uden for EU/EØS på vegne af den dataansvarlige i overensstemmelse med databeskyttelsesforordningens kapitel V.

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

Der er enighed mellem Parterne om, at databehandleren skal indhente en ISAE 3402- samt ISAE 3000 revisionserklæring for egen regning fra en uafhængig tredjepart vedrørende databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og Bestemmelserne. Revision foretages årligt, og de nyeste rapporter kan tilgås her: <https://geomatic.dk/isae>.

Baseret på resultaterne af revisionsrapporterne er den dataansvarlige berettiget til skriftligt at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af den til enhver tid gældende databeskyttelsesforordning og Bestemmelserne.

Den dataansvarlige skal specificere eventuelle yderligere foranstaltninger, der skal foretages, samt oplysninger, den dataansvarlige anmoder databehandleren om at stille til rådighed.

Den dataansvarlige, eller en repræsentant for den dataansvarlige, har herudover adgang, mod behørig legitimation, til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne, hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når den dataansvarlige finder det nødvendigt.

Den dataansvarlige skal skriftligt underrette databehandleren minimum 14 dage forud for foretagelsen af fysiske inspektioner, så databehandleren kan allokere de nødvendige ressourcer.

Den dataansvarliges eventuelle udgifter i forbindelse med en fysisk inspektion afholdes af den dataansvarlige selv. Databehandleren er forpligtet til at afsætte de ressourcer, der er nødvendige, for at den dataansvarlige kan gennemføre sin inspektion. Databehandleren har krav på betaling for afsatte ressourcer for den dataansvarlige inspektion og yderligere revision efter den til enhver tid gældende timepris, dog

således at der ikke er krav på betaling, hvis inspektionen sker som led i databehandlerens eller underdatabehandlerens misligholdelse.

Den dataansvarliges tilsyn med eventuelle underdatabehandlere sker som udgangspunkt gennem databehandleren.

Databehandleren skal dokumentere overholdelse af databeskyttelsesforordningen og Bestemmelserne inden for rimelig tid.

Bilag C) Underdatabehandlere

C.1 Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

- IT Relation A/S, CVR 27001092, i medfør af IT system- og brugersupport samt hosting af drift og servere.
Adresse: Nygårdsvej 5A, 2. sal, 2100 København Ø

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 D) Parternes regulering af andre forhold

D.1 Erstatningsansvar

Parterne er ikke ansvarlige for hændelser, der ikke direkte kan tilskrives den enkelte aftalepart.

Databehandleren hæfter kun for den skade, der er forvoldt af behandling, hvis databehandleren ikke har opfyldt forpligtelser i forordningen, der er rettet specifikt mod databehandlere, eller hvis databehandleren har undladt at følge eller handlet i strid med den dataansvarliges lovlige instrukser, jf. databeskyttelsesforordningens art. 82, stk. 2.

I forhold til betaling af erstatning til fysiske personer som følge af en ulovlig behandlingsaktivitet eller enhver anden behandling i strid med Databeskyttelseslovgivningen, finder databeskyttelseslovens § 40 og databeskyttelsesforordningens art. 82 anvendelse.

De involverede skadevoldere hæfter solidarisk, jf. databeskyttelsesforordningens art. 82, stk. 4. Uanset databeskyttelsesforordningens art. 82, stk. 5 kan en Part, der har udredt erstatningsbeløb til en skadelidt, der ikke svarer til fuld erstatning, gøre regres i overensstemmelse med betingelserne i art. 82, stk. 2, jf. princippet i art. 82, stk. 5.

Parterne kan ikke gøre regres eller erstatningskrav gældende over for den anden Part for bøder eller anden straf, der er pålagt i medfør af databeskyttelseslovens § 41, samt for bødeforlæg accepteret efter Databeskyttelseslovens § 42.