Standardkontraktsbestemmelser

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

mellem

Kunden

herefter "den dataansvarlige"

og

Resights
CVR-NR: 41527080
Borgergade 24b
1300 København K
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 10
13. Parternes aftale om andre forhold 10
14. Ikrafttræden og ophør 10
15. Kontaktpersoner hos den dataansvarlige og databehandleren 11
Bilag A Oplysninger om behandlingen 12
Bilag B Underdatabehandlere 13
Bilag C Instruks vedrørende behandling af personoplysninger 16
Bilag D Parternes regulering af andre forhold 21

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 platform der skaber overblik over ejendoms- og virksomhedsrelationer 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 af 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 persondataforordningen 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 persondataforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes[1] nationale ret og disse Bestemmelser.

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

2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.

3. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

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. Persondataforordningens 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 persondataforordningens 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 det i Bilag B angivne 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 persondataforordningen.

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

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. 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 persondataforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

8. Overførsel til tredjelande eller internationale organisationer

1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra den dataansvarlige og skal altid ske i overensstemmelse med persondataforordningens kapitel V.

2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af den dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:

   a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
   b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
   c. behandle personoplysningerne i et tredjeland

4. Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i persondataforordningens kapitel V, som overførslen er baseret på, skal angives i bilag C.6.

5. Disse Bestemmelser skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i persondataforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i persondataforordningens 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 persondataforordningens kapitel III.

   Dette indebærer, at databehandleren så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:

   a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
   b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
   c. indsigtsretten
   d. retten til berigtigelse
   e. retten til sletning ("retten til at blive glemt")
   f. retten til begrænsning af behandling
   g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
   h. retten til dataportabilitet
   i. retten til indsigelse
   j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

2. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3., bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:

   a. den dataansvarliges forpligtelse til uden 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, 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 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, 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 unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.

2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 48 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. persondataforordningens 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 i det omfang personoplysningerne er lagret i databehandlerens IT-miljø, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne. For de oplysninger, der er lagret i Kundens IT-miljø, er det Kundens ansvar at slette oplysningerne i overensstemmelse med gældende regler. Databehandleren sletter kun disse oplysninger efter udtrykkelig instruks fra den dataansvarlige.

2. Følgende regler i EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne efter ophør af tjenesterne vedrørende behandling af personoplysninger:

   a) Ingen relevante regler identificeret hos Databehandleren.

   Databehandleren forpligter sig til alene at behandle personoplysningerne til de(t) formål, i den periode og under de betingelser, som disse regler foreskriver.

12. Revision, herunder inspektion

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af persondataforordningens 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. Procedurerne 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 persondataforordningen.

14. Ikrafttræden og ophør

1. Bestemmelserne træder i kraft på datoen for begge parters underskrift af aftalen eller ved opgavens start alt afhængig af, hvad der måtte komme først.

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

3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.

4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftligt varsel af begge parter.

15. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via de i forretningsbetingelserne specificerede kontaktpersoner.

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

Formålet med behandling af personoplysninger på vegne af den dataansvarlige er at levere en platform med oplysninger om aktuel og historisk ejerskab af virskomheder og ejendomme samt byggeprojekter, samt tillægsydelser udsprunget heraf, som yderligere beskrevet i forretningsbetingelserne mellem partnerne (”forretningsbetingelserne”).

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

Oplysninger indhentes fra offentlige registre og udstilles samlet, i et format så det er let tilgængeligt for den dataansvarlige.

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

Behandlingen af personoplysninger kan omfatte:

Almindelige personoplysninger (persondataforordningens artikel 6)	• Navn • Adresse • Telefonnummer, • Ejerforhold og relationer til ejendomme, aktuelt og historisk • Ejerforhold og relationer til virksomheder, aktuelt og historisk • Portefølje • Oplysninger om handler • Oplysninger fra personbogen
Straffedomme og lovovertrædelser efter databeskyttelseslovens § 10	• Databehandleren behandler ingen oplysninger om straffedomme og lovovertrædelser
CPR-nummer efter databeskyttelseslovens §§ 11 og 12	• Databehandleren behandler ingen oplysninger om CPR-nummer
Følsomme personoplysninger efter databeskyttelsesforordningens artikel 9	• Databehandleren behandler ingen følsomme personoplysninger

A.4. Behandlingen omfatter følgende kategorier af registrerede

Behandling af personoplysninger vil i hovedsagen ske for identificerede fysiske personer, der har relation til den Dataansvarlige som:

i. Ejere og medejere af virksomheder og ejendomme

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

Den dataansvarliges behandling på vegne af databehandleren ophører som udgangspunkt når aftaleforholdet ophører og pkt. 11 i denne databehandleraftale er opfyldt.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	VIRKSOMHEDSNUMMER	ADRESSE	BESKRIVELSE AF BEHANDLING	SERVERLAND OG EVENTUELT OVERFØRSELSGRUNDLAG	AFTALE
Amazon Web Services	LEI: 2549000I2PRQGGIGCA75	38 Avenue John F. Kennedy L-1855 Luxembourg	Opbevaring af data	Tyskland	På anmodning
Whereby	EUID: NOFOR.997742346	Gate 1 107 6700 MÅLØY, Norge	Afholdelse og optagelse af møder	Luxemborg	På anmodning
Demio	CIK: 0001826011 (fundet på Banzai International, Inc.)	435 ERICKSEN AVE NE, SUITE 250, BAINBRIDGE ISLAND, WA, 98110, USA	Tilmelding og afholdelse af webinar	USA, Frankrig	På anmodning
Intercom	EUID: IECRO.907190	LOWER CAMDEN STREET, DUBLIN 2, D02RP27 DUBLIN, Irland	Chat på hjemmeside	Irland, Luxemborg	På anmodning
Notion	CIK: 0001781814	2300 HARRISON STREET, SAN FRANCISCO, CA, 94110	Notesbog	USA	På anmodning
Slack	CIK: 0001764925 (LEI er lapsed)	500 HOWARD STREET, SAN FRANCISCO, CA, 94105	Intern kommunikation	Tyskland Frankrig	På anmodning
Jiminny	Company number (fra Companies House I UK): 10999438	100 Fenchurch Street, Second Floor, London, England, EC3M 5JD	Optagelse af møder	Dublin, Irland	På anmodning

NAVN	VIRKSOMHEDSNUMMER	ADRESSE	BESKRIVELSE AF BEHANDLING	SERVERLAND OG EVENTUELT OVERFØRSELSGRUNDLAG	AFTALE
Mailgun	VAT: US 1296	112 E Pecan St, #1135, San Antonio, TX, 78205	Automatisk afsendelse af mails	Tyskland, Holland	På anmodning
Zapier	LEI: 254900XIXKZQ7A7N1M29	C/O COGENCY GLOBAL INC. 850 NEW BURTON ROAD, SUITE 201, 19904, DOVER, US-DE, USA	Automatisering af workflows	USA	På anmodning
Microsoft	EUID: DKCVR.13612870	Kanalvej 7, 2800 Kgs. Lyngby, Denmark	MS 365	Danmark	På anmodning
Dovetail	EUID: IECRO.361512	The GEC, Taylors Lane, D08 C9TX DUBLIN, Ireland	Analyse og statistik	USA	På anmodning
Distributionplus A/S	EUID: DKCVR.30913078	Charles Lindberghs Vej 9, 9430 Vadum, Danmark	Brevdistribution	Denmark	På anmodning
Linear	CIK: 0000059641	2055 CORTE DEL NOGAL CARLSBAD, CALIFORNIA 92009, USA	Prioritering af udviklingsopgaver fra kunder	USA	På anmodning
NewRelic	LEI: 549300AB8FY2HQILL804	88 Spear St, San Francisco, CA 94105, USA	Monitorering af infrastuktur	USA, Tyskland og Irland	På anmodning
Snowflake	LEI: 254900CJNSY1K7T53Z16	106 East Babcock Street, Suite 3a, Bozeman, Montana, 59715, USA	Datalagring	USA	På anmodning
Datapeeps	EUID: DKCVR.40540776	Oliefabriksvej 61, 1 sal, 2770 Kastrup, Danmark	Indsamling af telefonnumre	Irland, Holland	På anmodning

NAVN	VIRKSOMHEDSNUMMER	ADRESSE	BESKRIVELSE AF BEHANDLING	SERVERLAND OG EVENTUELT OVERFØRSELSGRUNDLAG	AFTALE
BonaMea	EUID: NOFOR.812415972	Ytrebygdsvegen 215, 5258 Blomsterdalen, Norge	Datarum	Norge	På anmodning
Danmarks Statistik	CVR: 17150413	Sankt Kjelds Pl. 11, 2100 København, Danmark	Indsamling af data	Danmark	På anmodning

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.

B.2. Varsel for godkendelse af underdatabehandlere

Databehandleren varsler den dataansvarlige 30 dage forud for anvendelse af en ny underdatabehandler.

Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører de i forretningsbetingelserne nærmere fastsatte ydelser.

Databehandleren må anonymisere oplysningerne med henblik på at anvende dem til statistikker o.lign., såfremt databehandleren stiller fornødne garantier for overholdelse af persondataforordningen og databeskyttelsesloven.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet på databehandlernes IT-miljø skal afspejle:

Behandlingen af personoplysninger omfatter primært personoplysninger omfattet af persondataforordningens artikel 6 (almindelige personoplysninger).

Databehandleren behandler oplysninger om strafbare handlinger eller undladelser efter persondataforordningens artikel 10 samt oplysninger om CPR-nummer efter databeskyttelseslovens § 10.

Databehandleren skal ikke behandle personoplysninger omfattet af persondataforordningens artikel 9 (særlige kategorier af oplysninger).

Databehandleren er herefter 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:

Teknisk sikkerhed	Beskrivelse
Antivirus	Al data tilgås udelukkende via cloud-platform, som indeholder sikkerhed på server-, storage- og netværksniveau med integreret virus- og malwarebeskyttelse.
Firewall	Databehandleren anvender cloud-baseret infrastruktur med indbygget firewall-beskyttelse. Alle arbejdsstationer har aktiveret firewall, som administreres centralt gennem vores device management system. Sikkerhedspolitikker håndhæves konsistent uanset enhedens placering.
Netværkssegmentering	Netværkssegmentering på fysiske lokationer er implementeret med separate netværk for medarbejdere og gæster. For cloud-ressourcer styres adgang gennem sikkerhedspolitikker baseret på brugeridentitet, bruger risikoprofil og enhedsstatus. Databehandlerens cloud-leverandør sikrer netværksadskillelse på platformniveau.

Brugeradgang	Databehandleren styrer brugeradgang gennem centraliseret identitets- og adgangsstyring. Rettigheder tildeles ud fra medarbejderens jobfunktion og arbejdsbetingede behov. Adgange gennemgås regelmæssigt, og der foretages automatisk deaktivering ved fratrædelse. Al brugeraktivitet logges.
Systemovervågning	Alle systemer overvåges kontinuerligt via Databehandlerens cloud security platform. Der er implementeret automatisk alerting ved sikkerhedshændelser. Sikkerhedsstatus monitoreres løbende, og der tages daglig backup af overvågningsdata til dansk backupleverandør.
Kryptering ved transmission via web og mail	Al datakommunikation er krypteret med minimum TLS 1.2, hvilket overholder Datatilsynets minimumskrav. Dette gælder både for web-trafik og e-mailkommunikation. Databehandlerens cloud-platform sikrer krypteret kommunikation, og særligt følsomme data kan beskyttes gennem ekstra kryptering.
Logning	Logning er implementeret på alle systemer. Cloud-leverandøren gennemgår løbende logs for driften af den samlede cloud-platform, mens logs med kundedata, specifikt for Databehandleren, overvåges internt i virksomheden.
Logbeskyttelse	Logs beskyttes gennem cloud-sikkerhedsmekanismer og replikeres mellem datacentre. Der anvendes backup-leverandør som uafhængig sikkerhedskopi. Adgang til logs er begrænset til autoriserede administratorer, og al adgang dokumenteres.
Testmiljø	Databehandleren har separate miljøer for udvikling, test og produktion. Produktionsdata anvendes ikke i test- eller udviklingsmiljøer. Udviklere har adgang til isolerede udviklingsmiljøer.
Sårbarhedstest	Der udføres regelmæssig sårbarheds-scanning og sikkerhedsvurdering af systemer og infrastruktur. Cloud-leverandører udfører sikkerhedstest på platformniveau. Identificerede sårbarheder udbedres efter fastlagt proces, og resultater dokumenteres.
Opdateringer, patches, mv.	Sikkerhedsopdateringer administreres centralt gennem device management platform. Alle enheder tildeles automatisk krav om opdateringer. Kritiske sikkerhedsopdateringer implementeres inden for 24 timer efter frigivelse. Opdateringsstatus dokumenteres og backuppes regelmæssigt.
Forretningsgang for brugeradgang	Brugeradgange tildeles gennem standardiserede processer ud fra et arbejdsbetinget behov. Der er fastlagt en procedure ved on- og offboarding af medarbejdere og underleverandører og opdelt i henhold til den opgave, som den enkelte bruger skal varetage. Ændringer i brugeradgange følger fastlagte procedurer og dokumenteres systematisk.

To-faktor-adgang	To-faktor autentificering er påkrævet for Databehandlerens brugere ved systemadgang. Sikkerhedspolitikker evaluerer login-forsøg baseret på lokation og enhedstype. Ved login fra ikke-godkendte enheder eller ikke-forud godkendte lokationer kræves yderligere verifikation. Alle autentificeringsforsøg logges.

Fysisk sikkerhed	Beskrivelse
Adgangsforhold	Selve tilgangen til Databehandlerens kontor sker i almindelig arbejdstid via en åben entre, som er aflåst mellem 17:00 til 8:00. Efter entreen skal medarbejdere anvende deres nøglebrik til at anvende elevatoren eller få adgang til kontoret. Der er bemanding i åbningstiden. Udenfor åbningstid er dørene låst, hvilket sker automatisk via en digital løsning. Medarbejderne har nøglebrikker til alle døre. Endvidere er kontoret udstyret med en alarm, sættes alarmen i gang sendes der direkte besked til alarmselskabet, og de kan tænde kameraet og se hvem der er på kontoret, de kontakter og den ansvarlige hos databehandleren. Udover medarbejdere hos databehandleren, har et rengøringsfirma adgang til kontoret uden for åbningstiden. Alle medarbejdere er instrueret i, at personoplysninger skal opbevares utilgængeligt for uvedkommende, som ikke skal have adgang til personoplysningerne.

Organisatorisk sikkerhed	Beskrivelse
Personalehåndbog om IT-sikkerhed	Databehandleren har udarbejdet personalehåndbog, der beskriver hvilke sikkerhedstiltag, som medarbejderen skal overholde. Denne accepteres af alle medarbejdere ved ansættelse.
Medarbejdertillid	Der er en generel procedure for at efterprøve medarbejderens omdømme i forbindelse med ansættelse. Dette inkluderer indhentning af straffeattester for de ansatte, der skal varetage opgaver, som kræver en høj grad af fortrolighed.
Fortrolighed	Alle databehandlerens medarbejdere er dækket af en tavshedspligts- og fortrolighedsklausul.
Fratrædelsesprocedurer	Fratræder en medarbejder, sikres det, at data overleveres til anden medarbejder, som har sammenlignelige kompetencer og adgangsrettigheder til at kunne overtage data i overgangsfasen. Medarbejderen adgang til enheder med kundedata lukkes straks efter medarbejderen fratræder. Dette sker i samarbejde med alle relevante aktører.

Awareness-træning	Alle medarbejdere hos databehandleren har fået udtrykkelig instruks angående opbevaring, behandling, sletning og sikkerhed vedrørende behandling af personoplysninger. Der afholdes også et årligt online seminar om relevante databeskyttelsesretlige aspekter.

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:

Sende hændelseslog over konstaterede sikkerhedsbrud hos databehandleren samt bistå efter nærmere aftale i tilfælde af sikkerhedsbrud.

C.4 Opbevaringsperiode/sletterutine
Oplysningerne om brugere opbevares så længe det er nødvendigt for at opfylde aftaleforholdet mellem Parterne.

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 dataansvarlige oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne. Ved ophør af samarbejdet afsluttes databehandlerens databehandling for den dataansvarlige.

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:

Alle steder, hvor databehandleren finder det nødvendigt for at levere ydelsen og som sker på Kundens eller databehandlerens sikrede hardware eller hos godkendte underdatabehandlere.

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 usikre 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

Med henvisning til Datatilsynets "Vejledning om tilsyn med databehandlere, Pointskala og seks tilsynskoncepter, oktober 2021" følger databehandleren minimum tilsynskoncept 2 og afholder udgifterne forbundet hertil:

Koncept 2:
Databehandleren bekræfter skriftligt, at alle krav i databehandleraftalen stadig efterleves.

Databehandleren udarbejder årligt i Q1 en opdateret skriftlig status på databehandlerens hjemmeside, her, som er tilgængelig for den dataansvarlige og er gældende indtil det

følgende års status. Databehandleren er således ikke forpligtet til at opdatere erklæringen på øvrige tidspunkter af året, medmindre det specifikt aftales med den dataansvarlige.

Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover adgang 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. Databehandleren stiller sig til rådighed for fysiske inspektioner, men den dataansvarlige afholder udgifterne forbundet hermed, inklusiv rimelige omkostninger hos databehandleren.

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

Databehandleren er ansvarlig for at indhente revisionserklæringer mv. fra underdatabehandlere efter samme principper som beskrevet i punkt C.7. Databehandleren risikovurderer hvilket koncept der vil være hensigtsmæssigt at anvende ved revisionen. Revisionsmaterialet fremsendes til den dataansvarlige på anmodning.

Bilag D Parternes regulering af andre forhold

Databehandlerens standardtakst for de ydelser, der følger af Bestemmelsernes punkt 9 og 10, afregnes i henhold til de gældende timesatser – 3600,- pr. time.

Den dataansvarlige skal dog ikke afholde omkostninger for fejl, forsømmelser eller mangler, der kan henføres til databehandlerens handlinger eller undladelser.