

Databehandleraftale

Mellem

(den "Dataansvarlige")

og

Brunata A/S
CVR-nr. 22166514
Vesterlundvej 14
2730 Herlev
Danmark
("Brunata" eller "Databehandleren")

(hver for sig kaldet en "Part" og samlet "Parterne")

er indgået nærværende, lovpligtige databehandleraftale ("Aftalen") om Databehandlerens behandling af Personoplysninger på vegne af den Dataansvarlige. Dette dokument s bilag 1-3 skal betragtes som en integreret del af Aftalen. I tilfælde af uoverensstemmelse mellem dette dokument og bilagene, vil bilagene have forrang.

Aftalen gælder for kontrakt(er)/ordrebekræftelse(r) indgået mellem Parterne vedrørende levering af målere, forbrugsregnskaber og/eller målerdata ("Hovedaftalen").

1. Aftalens omfang

- 1.1 Denne Aftale er indgået med henblik på opfyldelse af Parternes Hovedaftale, herunder i forbindelse med Databehandlerens indsamling af målerdata med henblik på at kunne udarbejde forbrugsregnskaber for den Dataansvarlige.
- 1.2 Denne Aftale har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem Parterne.
- 1.3 Ved "Personoplysning" forstås enhver form for information om en identificeret eller identificerbar, fysisk person, jf. artikel 4(1) i Forordning (EU) 2016/679 af 27. april 2016 ("Persondataforordningen"). Hvis der som led i opfyldelsen af Aftalen behandles andre fortrolige oplysninger end Personoplysninger, f.eks. oplysninger som i medfør af lov om finansiel virksomhed anses for fortrolige, så omfatter enhver henvisning til "Personoplysninger" også de øvrige fortrolige oplysninger.
- 1.4 Aftalen er udformet med henblik på overholdelse af artikel 28 i Persondataforordningen.

2. Formål og instruks

- 2.1 Databehandleren er databehandler i Persondataforordningens forstand, idet Databehandleren varetager de i Bilag 1 beskrevne databehandlingsopgaver for den Dataansvarlige. Databehandleren er instrueret i alene at behandle Personoplysninger med det formål at varetage de i Bilag 1 fastsatte behandlingsopgaver. Databehandleren må ikke behandle eller anvende Personoplysninger til andre formål.
- 2.2 Den Dataansvarlige er berettiget til at slette og/eller tilføje yderligere typer af Personoplysninger og/eller registrerede per soner ved fremsendelse af en ny oversigt over Personoplysninger og/eller registrerede personer til Databehandleren.
- 2.3 Databehandleren må herudover benytte anonymiserede Personoplysninger og behandle sådanne anonymiserede data til statistiske formål og produktudvikling (dvs. at identificerbare data er slettet).
- 2.4 Databehandleren skal straks underrette den Dataansvarlige, hvis Databehandleren finder, at en given instruks er eller senere måtte blive i strid med persondatalovgivningen.
- 2.5 Databehandleren skal under hensyntagen til behandlingens karakter snarest muligt assistere den Dataansvarlige med håndtering af enhver anmodning fra en registeret i henhold til kapitel III i Persondataforordningen, herunder anmodning om indsigt, berigtigelse, blokering eller sletning. Under hensyntagen til behandlingens karakter kan Databehandleren vælge at behandle henvendelser direkte fra den registrerede om berigtigelse af oplysninger, jf. art. 28, stk. 3, litra e.

- 2.6 Databehandleren skal ligeledes implementere passende tekniske og organisatoriske foranstaltninger til at bistå den Dataansvarlige med opfyldelse af dennes forpligtigelse til at besvare sådanne anmodninger.

3. Den Dataansvarliges forpligtelser

- 3.1 Den Dataansvarlige indestår for, at formålet med behandlingen af Personoplysningerne er lovligt og sagligt, og at der ikke overlades flere Personoplysninger til Databehandleren end nødvendigt til opnåelse af formålet.
- 3.2 Den Dataansvarlige er ansvarlig for, at der på tidspunktet for Personoplysningernes overlevering til Databehandleren eksisterer et gyldigt behandlingsgrundlag, herunder samtykke, lovgrundlag eller kontraktgrundlag. Den Dataansvarlige er forpligtet til på Databehandlerens anmodning skriftligt at redegøre for og/eller dokumentere behandlingsgrundlaget i tilfælde af, at Databehandler har en mistanke om, at Dataansvarlig ikke har et gyldigt behandlingsgrundlag.
- 3.3 Den Dataansvarlige indestår endvidere for, at de registrerede personer, som Personoplysningerne vedrører, har fået tilstrækkelig information vedrørende behandlingen af Personoplysningerne.

4. Databehandlerens forpligtelser

- 4.1 Databehandleren må alene behandle de Personoplysninger, der er overført og indsamlet i overensstemmelse med den Dataansvarliges instrukser og er i øvrigt forpligtet til at overholde den til enhver tid gældende persondatalovgivning.
- 4.2 Databehandleren skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger, som krævet i henhold til Persondataforordningens art. 32, herunder sådanne yderligere foranstaltninger, som måtte være nødvendige mod, at de behandlede Personoplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt Behandles i strid med persondatalovgivningen. Databehandlerens generelle sikkerhedspolitik vedlægges denne Aftale som Bilag 2.
- 4.3 Databehandleren bistår den dataansvarlige med at sikre overholdelse af den dataansvarliges forpligtelser i medfør af Persondataforordningens art. 32-36 under hensynstagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, jf. Persondataforordningens art. 28, stk. 3, litra f.
- 4.4 Databehandleren skal sikre, at de medarbejdere, der er involveret i at behandle Personoplysningerne, har forpligtet sig til fortrolighed eller er underlagt lovbestemt tavshedspligt.
- 4.5 Databehandleren skal på den Dataansvarliges anmodning redegøre for og/eller dokumentere, at Databehandleren opfylder kravene i persondatalovgivningen og

forpligtelserne i medfør af denne Aftale, herunder at de nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger er truffet.

- 4.6 Hvis Databehandleren måtte blive bekendt med et persondatasikkerhedsbrud, hvorved forstås et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitterede, opbevarede eller på anden måde behandlere, er Databehandleren forpligtet til uden unødigt forsinkelse at give den Dataansvarlige meddelelse herom, samt søge at lokalisere sådant brud og søge at begrænse opstået skade i videst muligt omfang, samt, i det omfang det er muligt, at reetablere eventuelt mistede data.
- 4.7 Databehandleren skal på den Dataansvarliges anmodning give den Dataansvarlige tilstrækkelige oplysninger til, at denne kan påse, at Databehandleren har truffet de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger.
- 4.8 Såfremt den Dataansvarlige ønsker at foretage tilsyn, skal den Dataansvarlige give Databehandleren et varsel på mindst 30 dage.
- 4.9 Databehandler skal på Dataansvarliges anmodning og bekostning gennemgå revision vedr. behandling af Personoplysninger af en uafhængig tredjepart. I tilfælde af at Dataansvarlig kan sandsynliggøre at der foreligger væsentlig brud på Persondataforordningens bestemmelser, afholdes omkostningerne til revisionen af Databehandleren.
- 4.10 Databehandleren skal, efter den dataansvarliges valg slette eller tilbagelevere alle personoplysninger til den dataansvarlige efter at tjenesterne vedrørende behandling er ophørt, og sletter eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

5. Overførsel af oplysninger til andre databehandlere eller tredjeparter

- 5.1 Ved underskrivelsen af Aftalen godkender den Dataansvarlige, at Databehandleren kan gøre brug af underleverandører ("Underdatabehandlere") i forbindelse med Databehandlerens opfyldelse af sine forpligtelser efter denne Aftale. Ved Aftalens indgåelse anvender Databehandleren de i Bilag 3 oplistede Underdatabehandlere.
- 5.2 Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af underdatabehandlere og give den Dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer.
- 5.3 Udover det i pkt. 5.1 anførte, er Databehandleren ikke berettiget til at videregive personoplysninger til tredjeparter eller databehandlere uden den Dataansvarliges forudgående skriftlige instruks eller samtykke, medmindre sådan videregivelse følger af lovgivningen.
- 5.4 Underdatabehandlere er under Databehandlerens instruks. Databehandleren har indgået skriftlig databehandleraftale med Underdatabehandlere, hvori det er sikret, at

Underdatabehandlere opfylder krav tilsvarende dem, som stilles til Databehandleren af den Dataansvarlige i medfør af Aftalen.

- 5.5 Den behandling af Personoplysninger, som Databehandleren foretager efter aftale med den Dataansvarlige, må alene foretages af Databehandleren eller Underdatabehandlere inden for det Europæiske Økonomiske Samarbejde (EØS). Databehandleren er ingenlunde berettiget til at lade databehandling foregå uden for EØS uden den Dataansvarliges skriftlige samtykke.
- 5.6 Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser.

6. Ansvar

- 6.1 Både den Dataansvarlige og Databehandleren er i overensstemmelse med den kontrakt/ordrebekræftelse indgået mellem parterne – herunder de ansvarsbegrænsninger og -fraskrivelser, der fremgår deraf – ansvarlige over for den anden part for ethvert direkte tab, der måtte opstå som følge af eller i forbindelse med manglende opfyldelse af forpligtelserne i henhold til denne Aftale.
- 6.2 Bøder pålagt den dataansvarlige som følge af Databehandlerens misligholdelse af sine forpligtelser i henhold til databehandlersaftalen er dog ikke omfattet af ansvarsbegrænsninger og fraskrivelser aftalt mellem Parterne i Hovedaftalen.

7. Ikrafttrædelse og ophør

- 7.1 Nærværende Aftale og de(n) kontrakt(er)/ordrebekræftelse(r) indgået mellem _____ og Brunata a/s ("Hovedaftalen") er indbyrdes afhængige og kan ikke opsiges særskilt. Nærværende Aftale kan alene opsiges eller ophæves i overensstemmelse med bestemmelserne om opsigelse og ophævelse i Hovedaftalen.

8. Lovvalg og værneting

- 8.1 Denne Aftale reguleres af dansk ret.
- 8.2 Ethvert krav og enhver tvist, der udspringer af eller på anden måde er forbundet med denne Aftale, skal afgøres ved Retten i København.

9. Databeskyttelsesrådgiver (DPO)

- 9.1 Brunata har udpeget en Databeskyttelsesrådgiver jf. Persondataforordningens Afdeling 4.

Databeskyttelsesrådgiveren kan kontaktes i forbindelse med spørgsmål til Brunatas håndtering af persondata og har følgende kontaktoplysninger:

Tony Franke
E-mail: tofr@Brunata.com

10. Underskrifter

- 10.1 Denne Aftale er underskrevet i to enslydende, originale eksemplarer, hvoraf hver Part modtager et eksemplar.

Dato:

Dato: 1. april 2019

For:

For: Brunata A/S


Keld Forchhammer

Bilag 1

Instruks vedr. behandlingsopgaver

Dette bilag udgør den Dataansvarliges instruks til Brunata i forbindelse med Brunatas databehandling på vegne af den Dataansvarlige og udgør en integreret del af Aftalen.

Behandlingen af personoplysninger

a) Formål og beskrivelse af databehandlingen:

Brunata indsamler målerdata med henblik på at kunne udarbejde forbrugsregnskaber eller på anden vis stille målerdata til rådighed for Dataansvarlig og den registrerede, eksempelvis ved oversigter eller visualiseringer. Brunata indsamler samtidig billeder af evt. nedtagne eller utilgængelige målere med henblik på at sikre tilstrækkelig dokumentation overfor Kunden.

b) Kategorier af registrerede personer:

- I. Potentielle kunder
- II. Kunder
- III. Beboere

c) Kategorier af personoplysninger

Re b) I: Navn, emailadresse, adresse, telefonnummer, målerdata, billeder af målere

Re b) II: Navn, emailadresse, adresse, telefonnummer, målerdata, billeder af målere

Re b) III: Navn, emailadresse, adresse, telefonnummer, målerdata, billeder af målere

e) Lokation(er), inklusive angivelse af land for behandlingen

- I. Brunata A/S, Vesterlundvej 14, 2730 Herlev
- II. Microsoft, Datacenter Nord Europa, Irland
- III. ATEA A/S, Lautrupvang 6, 2750 Ballerup,
- IIII. Oracle Danmark ApS, Metalbuen 66, 2750 Ballerup

f) Særlige krav til sikkerhedsforanstaltninger fastsat af kunden:

Ingen

Bilag 2

Sikkerhedspolitik

Indledning

Denne sikkerhedspolitik er grundlag for alle sikkerhedstiltag i Brunata og understøtter vores værdigrundlag og vision samt de strategiske mål for anvendelse af it-systemer.

Sikkerhedspolitikken skal endvidere tilkendegive over for alle, som har en arbejdsmæssig relation til Brunata, at anvendelsen af data og systemer er underlagt vores standarder og retningslinjer for it-sikkerhed.

Formål

Det er vitalt for Brunata at have et højt niveau af kvalitet og driftssikkerhed i virksomhedens it-systemer for at kunne yde den ønskede service til interne og eksterne kunder.

Formålet med informationssikkerhedspolitikken er at definere rammen for styring af sikkerheden i Brunata, med særlig fokus på sikring af de kritiske og følsomme informationssystemer ift. fortrolighed, integritet og tilgængelighed.

Det valgte sikkerhedsniveau besluttet af ledelsen i Brunata og er tilpasset det aktuelle risiko- og trusselsniveau samt overholdelse af nationale lovkrav og aftaler, herunder EU's databeskyttelsesforordning.

Sikkerhedspolitikken skal endvidere tilkendegive over for alle, som har en arbejdsmæssig relation til Brunata, at anvendelse af data og systemer er underlagt virksomhedens regler og retningslinjer for it-sikkerhed, hvilket kan forhindre sikkerhedshændelser i at opstå samt begrænse skader og sikre genopretning af informationssystemerne.

Formålet er ligeledes at sikre, at interessenter, herunder kunder, leverandører og ejerkreds, kan føle sig sikre på, at fortroligheden, integriteten og tilgængeligheden af vores systemer og data bevares.

Anvendelsesområde

Denne politik:

- dækker alle virksomhedsoplysninger, uanset hvilken form de opbevares og distribueres i,
- gælder for alle ansatte uden undtagelse, både medarbejdere og personer, der midlertidigt arbejder for Brunata, eller får midlertidigt adgang til systemer og/eller data,
- dækker ved helt eller delvis outsourcing af it-operationer. Herved skal det sikres – i samarbejde med outsourcing-partneren – at Brunatas sikkerhedspolitik håndhæves.

Sikkerhedsniveau

Det er Brunatas politik at beskytte oplysninger og kun tillade adgang til og offentliggørelse af oplysninger i overensstemmelse med selskabets retningslinjer samt i overensstemmelse med gældende lovgivning.

Baseret på en løbende vurdering af de risici, der er relevante for branchen, it-systemer og data, opretholder Brunata et sikkerhedsniveau svarende hertil.

Mindst en gang om året vil der blive foretaget en formel it-risikovurdering, der gør det muligt for ledelsen at holde sig opdateret og ligeledes foretage eventuelle justeringer af sikkerhedsniveauet. Ved større ændringer i organisationen, it-systemer eller ved anvendelse af nye teknologier vil der blive foretaget en ny it-risikovurdering.

Informationssikkerhedspolitikken, samt underliggende politikker, retningslinjer og procedurer, tager udgangspunkt i ISO 27001. Det er dog ikke hensigten at efterleve standarden fuldt ud – kun hvor det giver værdi ift. formålet. De ISO-kontroller, der anses for relevante, implementeres i Brunatas organisation.

Det er vigtigt, at informationssikkerhed er integreret i alle forretningsprocesser, operationelle opgaver og projekter.

Ansvar

Direktionen er ansvarlig for informationssikkerhedspolitikens anvendelighed, tilstrækkelighed og effektivitet.

Ledelsen i Brunata informerer medarbejderne om deres ansvar som led i sikring af informationssystemers tilgængelighed, fortrolighed og integritet.

Brunatas it-chef er ansvarlig for at sikre, at informationssikkerhedspolitikken implementeres i de anvendte systemer og infrastruktur samt at overvåge det øvrige risiko- trusselsniveau med henblik på evt. justering af sikkerhedsniveauet.

Alle medarbejdere i Brunata er ansvarlige for overholdelsen af denne informationssikkerhedspolitik samt underliggende politikker, retningslinjer og procedurer. Til sikring heraf uddannes medarbejderne i deres ansvar herfor.

Den enkelte medarbejder har ansvar for:

- at overholde informationssikkerhedspolitikken og de regler, der er relevante for den enkeltes arbejdsopgaver og
- at rapportere om eventuelle sikkerhedsbrud eller mistanke herom til nærmeste chef eller it-chefen.

DPO er ansvarlig for rådgivning om overholdelse af databeskyttelsesloven og rapportering til ledelsen.

Det er ligeledes dennes ansvar at sikre rapportering til myndigheder og andre relevante personer i tilfælde af brud på sikkerheden.

Brud på sikkerheden

Medarbejdere, der overtræder informationssikkerhedspolitikken, retningslinjer eller procedurer, kan straffes disciplinært i overensstemmelse med Brunatas gældende regler og personalepolitik.

Beredskabsplanlægning

Effekten og tiden for et eventuelt nedbrud, datatab m.m. søges minimeret gennem en veltilrettelagt fysisk sikring og overvågning af bygninger, tekniske installationer og it-udstyr. Omfanget af disse foranstaltninger besluttet ud fra en afvejning af risici imod sikringsomkostninger og udmøntes i konkrete tiltag.

Brunatas it-beredskabsplan er afstemt ift. det aktuelle risiko- og trusselsniveau.

Bilag 3

Underdatabehandlere

Navne på eksisterende Underdatabehandlere:

NAVN	ADRESSE	LAND
ATEA A/S	Lautrupvang 6, 2750 Ballerup	Danmark
Oracle Danmark ApS	Metalbuen 66, 2750 Ballerup	Danmark
Microsoft Danmark ApS	Kanalvej 7, 2800 Kongens Lyngby	Danmark