Databehandleraftale

Databehandleraftale
Version 9, 18.11.2026 13:31

Advania Danmark A/S ("Organisationen")
Kay Fiskers Plads 10, 3
2300 København S
DK
CVR: 32643485

Indholdsfortegnelse

1. Parterne
2. Præambel
3. Den Dataansvarliges rettigheder og forpligtelser
4. Databehandleren handler efter instruks
5. Fortrolighed
6. Behandlingssikkerhed
7. Anvendelse af underdatabehandlere
8. Overførsel til tredjelande eller internationale organisationer
9. Bistand til den Dataansvarlige
10. Underretning om brud på persondatasikkerheden
11. Sletning og returnering af oplysninger
12. Revision, herunder inspektion
13. Parternes aftale om andre forhold
14. Ikrafttræden og ophør
15. Kontaktpersoner hos den Dataansvarlige og Databehandleren
16. Bilag A - Oplysninger om behandlingen
17. Bilag B - Underdatabehandlere
18. Bilag C - Instruks vedrørende behandling af personoplysninger
19. Bilag D - Parternes regulering af andre forhold

1. Parterne

Databehandleraftale udarbejdet efter Datatilsynets standardkontraktbestemmelser accepteret af Det Europæiske Databeskyttelsesråd i henhold til artikel 28, stk. 3, i forordning 2016/679 (GDPR) med henblik på databehandlerens behandling af personoplysninger

mellem

kunden, herefter den "Dataansvarlige"

og

Advania Danmark A/S
Kay Fiskers Plads 10, 3
2300 København S
DK
CVR: 32643485

herefter "Databehandleren"

der hver især er en "Part" og sammen udgør "Parterne"

HAR AFTALT følgende standardkontraktbestemmelser ("Bestemmelserne") med henblik på at overholde GDPR og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder.

2. Præambel

Disse bestemmelser fastsætter Databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysningerne på vegne af den Dataansvarlige.

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 ("GDPR").

I forbindelse med leveringen af Tjenesterne behandler Databehandleren personoplysninger på vegne af den Dataansvarlige i overensstemmelse med disse Bestemmelser.

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

Der hører 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 betingelser for Databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den Dataansvarlige har godkendt brugen af.

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.

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

Hvis standardkontraktbestemmelser som omhandlet i GDPR, artikel 46, stk. 1, litra c og d, udgør grundlag for overførsel af personoplysninger mellem den Dataansvarlige og Databehandleren til tredjelande som omhandlet i GDPR, kapitel V, er disse vedlagt i engelsk version som Bilag E og E1.

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

Disse Bestemmelser frigør ikke Databehandleren fra forpligtelser, som Databehandleren er pålagt efter GDPR eller enhver anden lovgivning.

3. Den Dataansvarliges rettigheder og forpligtelser

Den Dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med GDPR (se GDPR, artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller EU/EØS-medlemsstaternes nationale ret og disse Bestemmelser.

3.1 Den Dataansvarliges beslutningskompetence

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

3.2 Behandlingsgrundlag for personoplysninger

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

Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den Dataansvarlige, medmindre det kræves i henhold til EU-ret eller EU-/EØS-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.

4.1 Underretning om ulovlige instrukser

Databehandleren underretter omgående den Dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med GDPR eller databeskyttelsesbestemmelser i anden EU-ret eller EU-/EØS-medlemsstaternes nationale ret.

5. Fortrolighed

5.1 Adgang til personoplysninger og fortrolighed

Databehandleren må kun give adgang til personoplysninger, som behandles på den Dataansvarliges vegne, til personer, som er underlagt Databehandlerens instruktionsbeføjelser, og 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 Dokumentation for tavshedspligt

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 Tekniske og organisatoriske sikkerhedsforanstaltninger

GDPR, 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:

1. Pseudonymisering og kryptering af personoplysninger
2. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
3. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
4. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

6.2 Databehandlerens risikovurdering

Efter GDPR, 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 Bistand til overholdelse af behandlingssikkerhed

Derudover skal Databehandleren bistå den Dataansvarlige med vedkommendes overholdelse af den Dataansvarliges

forpligtelse efter GDPR, 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 GDPR, artikel 32, og al anden information, der er nødvendig for den Dataansvarliges overholdelse af sin forpligtelse efter GDPR, 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

Databehandleren skal opfylde de betingelser, der er omhandlet i GDPR, artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).

7.1 Generel skriftlig godkendelse

Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse fra den Dataansvarlige.

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 30 kalenderdages 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.

7.2 Forpligtelser for underdatabehandlere

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 EU-/EØS-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 GDPR.

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

7.3 Dokumentation for underdatabehandleraftaler

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.

7.4 Ansvar for underdatabehandlere

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 GDPR, herunder særligt GDPR, artikel 79 og 82, over for den Dataansvarlige og Databehandleren, herunder underdatabehandleren.

8. Overførsel til tredjelande eller internationale organisationer

8.1 Instruks ved overførsel til tredjelande

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 GDPR, kapitel V.

Uden dokumenteret instruks fra den Dataansvarlige kan Databehandleren således ikke inden for rammerne af disse Bestemmelser:

1. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
2. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
3. 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 GDPR, artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i GDPR, kapitel V, medmindre sådanne standardkontraktbestemmelser er vedhæftet i Bilag E.

8.2 Underretning ved retligt krav om overførsel

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 EU-/EØS-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.

9. Bistand til den Dataansvarlige

9.1 Bistand ved registreredes rettigheder

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 GDPR, kapitel III.

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

1. oplysningspligten ved indsamling af personoplysninger hos den registrerede
2. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
3. indsigtsretten
4. retten til berigtigelse
5. retten til sletning (”retten til at blive glemt”)
6. retten til begrænsning af behandling
7. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
8. retten til dataportabilitet
9. retten til indsigelse
10. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

9.2 Bistand ved sikkerhedsbrud og konsekvensanalyser

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:

1. 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 Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder
2. 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
3. den Dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)
4. den Dataansvarliges forpligtelse til at høre Datatilsynet, som måtte have kompetence 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.

9.3 Fastlæggelse af bistand i bilag C

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

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

10.1 Frist for underretning om brud

Databehandlerens underretning til den Dataansvarlige skal om muligt ske straks og senest 36 timer efter det tidspunkt, hvor databehandleren er blevet bekendt med bruddet på persondatasikkerheden, sådan at den Dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. GDPR, artikel 33.

10.2 Bistand ved anmeldelse af brud

I overensstemmelse med bestemmelse 9.2.1 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:

1. 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
2. de sandsynlige konsekvenser af bruddet på persondatasikkerheden
3. 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.

Parterne skal i Bilag D 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

11.1 Tilbagelevering og sletning af personoplysninger ved ophør

Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er Databehandleren forpligtet til at tilbagelevere alle personoplysningerne og slette eksisterende kopier, medmindre EU-retten eller EU-/EØS-medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

12. Revision, herunder inspektion

12.1 Bistand til revision og inspektion

Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af GDPR, 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 Procedurer for revision og inspektion

Procedurerne for den Dataansvarliges revisioner, herunder inspektioner, med Databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7 og C.8 .

12.3 Adgang for tilsynsmyndigheder

Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivning har adgang til den

Dataansvarliges eller Databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til Databehandlerens fysiske faciliteter mod behørig legitimation.

13. Parternes aftale om andre forhold

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 GDPR.

14. Ikrafttræden og ophør

14.1 Ikrafttræden

Bestemmelserne er bindende mellem Parterne.

14.2 Genforhandling

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

14.3 Varighed

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 Opsigelse

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.

14.5 Bindende virkning

Databehandleren er bundet af Bestemmelserne uden Parternes underskrift. Bestemmelserne indgås således uden fysiske/ digitale underskrifter, idet Bestemmelserne er bindende i overensstemmelse med kravet i GDPR, artikel 28, stk. 3, 1. pkt.

15. Kontaktpersoner hos den Dataansvarlige og Databehandleren

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

Kontaktoplysninger for den Dataansvarlige:

Se Rammeaftalen

Kontaktoplysninger for Databehandleren:

Advania Danmark A/S, gdpr@advania.dk

16. Bilag A - Oplysninger om behandlingen

16.1 Formålet med Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige

Følgende formål ligger til grund for Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige:

Disse bilag forudsætter, at den dataansvarlige køber en eller flere tjenester fra databehandleren inden for definitionen nedenfor.
Primær opbevaring af personlige data, levering af infrastrukturtjenester til primær arbejdsbelastninger såsom databaser, backup af Persondata og support, konsulenttjenester, der indebærer behandling af personoplysninger som anmodet af den dataansvarlige, levering af solgt IT-udstyr.

16.2 Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige drejer sig primært om (karakteren af behandlingen)

- Indsamling: Modtagelse af personoplysninger som leveret eller anvist af den dataansvarlige.
- Opbevaring: Sikker opbevaring af personoplysninger inden for databehandlerens infrastruktur.
- Hosting: Levering af infrastruktur til hosting af primære arbejdsbelastninger, f.eks. databaser, der indeholder personlige data.
- Sikkerhedskopiering og gendannelse: Oprettelse og vedligeholdelse af sikkerhedskopier af personlige data for at sikre datatilgængelighed og modstandsdygtighed.
- Adgang/læsning: Adgang til og læsning af personoplysninger efter behov for at levere support- og konsulenttjenester.
- Sletning: Sletning af personoplysninger efter instruks fra den dataansvarlige eller som krævet for at overholde gældende opbevaringspolitikker.
- Design, implementering, service og/eller drift af serviceløsninger.
- Systemadministration eller andre tjenester til servere eller netværksudstyr.
- Tjenester til arbejdsstationer og andet slutbrugerudstyr.
- Vedligeholdelse og reparation af hardware, der kan indeholde data.
- Implementering, service og/eller drift af informationssystemer i generel forretningsdrift, såsom: cloud-tjenester (f.eks. Microsoft O365), integrationsløsninger, databaser, datavarehuse eller andre lignende informationssystemer, der sælges og serviceres af Advania.
- Rådgivning om system- og databaseintegration.
- Generel rådgivning og/eller revision inden for informationsteknologi.

Servicen kan udføres hos den dataansvarlige, hos databehandleren eller eksternt fra Advania-medarbejderens arbejdsstation.

Ved videresalg af cloud-tjenester, f.eks. fra Microsoft, er Advania ikke processor af tjenesten, men den respektive producent. Advania betragtes kun som databehandler for de opgaver, Advania udfører i forbindelse med cloud-tjenesten, såsom implementering eller systemadministration.

Nedenfor finder du generelle kategorier af personoplysninger, som Advania medarbejdere kan komme i kontakt med under udførelsen af de førnævnte opgaver. En opgave falder kun ind under dette bilag, hvis de personoplysninger, som en Advania-medarbejder er betroet at behandle, passer inden for de kategorier, der er defineret nedenfor

16.3 Typer af personoplysninger

Behandlingen omfatter følgende typer af personoplysninger om de registrerede:

På grund af karakteren af Databehandlerens leverede tjenester kan følgende personoplysninger blive behandlet:
(i) Identifikations- og kontaktoplysninger om medarbejdere og kunder, herunder navn, adresse, privat- og erhvervstelefonnummer, civilstand, private og forretningsmæssige e-mailadresser, pasnummer
(ii) Sundhedsoplysninger om ansatte, herunder oplysninger om medarbejdernes sygdom, barselsorlov mv.
(iii) Straffeattester for kunder/modparter
(iv) Personoplysninger: Navn, e-mailadresse, telefonnummer, adresse, stilling/titel, uddannelse, økonomiske detaljer såsom kreditkortoplysninger, løn osv., fotos, personlighedstest, familieforhold, andre relationer, social status, lignende sociale og personlige oplysninger, der er relevante for sagen.
(v) Nationalt identifikationsnummer (CPR-nummer)
(vi) Følsomme personoplysninger, herunder racemæssig/etnisk baggrund, politisk overbevisning, religiøs overbevisning, filosofisk overbevisning, fagforeningsmedlemskab, seksuelle forhold, helbredstilstand, patientdata.
(vii) Oplysninger om strafbare handlinger: Straffeattest, relevante sociale problemer og andre lignende private forhold.
(viii) Oplysninger om finansielle transaktioner og finansiel status
(ix) Anmodninger fra den registrerede (anmodninger, meddelelser eller klager)
(x) Brugeroplysninger (brugeridentifikatorer og logposter i systemer)
--
I sidste ende vil databehandleren behandle de personoplysninger, som den dataansvarlige beslutter at behandle under de leverede tjenester, derfor er det overnævnte kun relevant for de tjenester den dataansvarlig har købt. Advania indsamler og behandler kun personoplysninger, hvis det er strengt nødvendigt for formålet med behandlingen. Når det er sagt, er Advania nogle gange nødt til at indsamle og behandle personoplysninger til legitime forretningsformål. Advanias medarbejderes tavshedspligt og de tekniske og organisatoriske foranstaltninger, der er beskrevet i denne behandlingsaftale, har til formål at mindske risikoen for behandling af følsomme personoplysninger.

16.4 Kategorier af registrerede

Behandlingen omfatter følgende kategorier af registrerede:

(i) Medarbejdere (tidligere, nuværende og fremtidige)
(ii) Jobkandidater
(iii) Studerende
(iv) Kunder
(v) Samarbejdspartnere og leverandører

16.5 Varighed

Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden.

Personoplysningerne behandles indtil ophør af tjenesterne vedrørende behandling af personoplysninger, hvorefter personoplysningerne slettes eller returneres i overensstemmelse med afsnit 11. Behandlingen foretages således så længe den eller de bagvedliggende kommercielle aftaler består.

17. Bilag B - Underdatabehandlere

17.1 Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den Dataansvarlige godkendt brugen af følgende underdatabehandlere:

Monitoring as a Service (hvis relevant):
LogicMonitor, Inc.:

- Adresse: 820 State Street, 5th Floor, Santa Barbara, CA 93101, USA
- EIN: 451344638
- Behandlingsaktiviteter: Opbevarer adgangsoplysninger (login), e-mailadresser, mobilnumre og IP-adresser på arbejdsstationer for platformens brugere i aftalens løbetid.
- Lokation for data: Amazon Web Services, eu-west-1, Dublin, Irland

Hjemmeside (hvis relevant):
Data Design AS:

- Adresse: Bryggegata 14, 0250 Oslo, Norge
- Org.nr.: 911197146
- Behandlingsaktiviteter: Adgang til de kundeoplysninger, der udfyldes ved afgivelse af en ordre
- Lokation for data: Norge

AI-assisteret inferens (hvis relevant):
OpenAI Ireland Ltd. (aftalepart i EØS; amerikansk moderselskab OpenAI OpCo, LLC):

- Adresse: OpenAI OpCo, LLC, 1455 3rd Street, San Francisco, CA 94158, USA
- Registreringsnummer (Irland, CRO): 737350
- Behandlingsaktiviteter: Leverer inferens med store sprogmodeller, som databehandleren anvender til at generere svar og til at bistå med håndtering og besvarelse af kundehenvendelser. Personoplysninger, der indgår i prompts indsendt af databehandleren, behandles udelukkende for at returnere det ønskede modeloutput og opbevares kun i den periode, der er fastsat i den gældende aftale. I henhold til OpenAI's API-/kommercielle databehandlertillæg (Data Processing Addendum) anvendes input- og outputdata IKKE til at træne eller forbedre OpenAI's modeller. [Zero data retention aktiveret: ja/nej.]
- Lokation for data: USA. Overførsler sker på grundlag af EU's standardkontraktbestemmelser (modul 2 og/eller 3), som er indarbejdet i OpenAI's databehandleraftale.

Anthropic, PBC (amerikansk aftalepart; enhed i EØS: Anthropic Ireland, Limited):

- Adresse: 548 Market Street, PMB 90375, San Francisco, CA 94104, USA
- Registreringsnummer (Irland, CRO): 760497
- Behandlingsaktiviteter: Leverer inferens med store sprogmodeller (Claude), som databehandleren anvender til at generere svar og til at bistå med håndtering og besvarelse af kundehenvendelser. Personoplysninger, der indgår i prompts, behandles udelukkende for at returnere det ønskede modeloutput og opbevares kun i den periode, der er fastsat i den gældende aftale. I henhold til Anthropic's kommercielle vilkår (Commercial Terms) og databehandleraftale anvendes kundeindhold IKKE til at træne Anthropic's modeller.
- Lokation for data: USA. Overførsler sker på grundlag af EU's standardkontraktbestemmelser (modul 2 og/eller 3), som er indarbejdet i Anthropic's databehandleraftale.

18. Bilag C - Instruks vedrørende behandling af personoplysninger

18.1 Behandlingens genstand/instruks

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige involverer primært sikker opbevaring og håndtering af personlige data, levering af infrastrukturtjenester til at understøtte primære arbejdsbelastninger (f.eks. databaser), backup og gendannelse af personoplysninger og levering af support- og konsulentydelser som anmodet af den dataansvarlige.

18.2 Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

Databehandleren skal etablere et passende sikkerhedsniveau under hensyntagen til behandlingens karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.

Databehandleren er herefter 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, som er aftalt med den Dataansvarlige:

Fysisk sikkerhed
Databehandleren gennemfører følgende fysiske sikkerhedsforanstaltninger:

- Databehandleren anvender nøglestyring, dvs. udlevere nøgler til de relevante og nødvendige medarbejdere mv.
- Databehandleren har alarmsystem til at opdage og forhindre indbrud.
- Databehandleren har brandalarm og røgdetektorer.
- Databehandleren har testet beredskabs- og evakueringsplan til nødsituationer.
- Databehandleren og besøgende m.fl. identificeres ved brug af identifikationskort.
- Databehandlerens bygning(er) er opdelt i adgangszoner, hvorefter adgangskort er påkrævet for adgang til zonerne.
- Databehandlerens kontorlokaler kan aflåses.
- Databehandlerens medarbejdere har pligt til at bære identitetskort.
- Databehandlerens udstyr (herunder PC'er, eventuelle servere mv.) er sikret bag låste døre.
- Der anvendes kontrolproces eller -system til kontrol med besøgendes identitet.
- Der er overvågning af databehandlerens bygninger, lokaler og faciliteter eller adgangsveje (billede eller videoovervågning).
- Der føres protokol over Databehandlerens besøgende.
- Reception bemandes 24/7 eller der er vagtselskab udenfor kontortid.

Organisatorisk sikkerhed
Databehandleren gennemfører følgende organisatoriske sikkerhedsforanstaltninger:

- Alle medarbejdere er underlagt fortrolighedsforpligtelse, der gælder for alle behandlede personoplysninger.
- Databehandleren har en dokumenteret procesbeskrivelse for brud på persondatasikkerheden, der minimum tages op til revidering årligt.
- Databehandleren har en fast proces, der sikrer, at der ved reparation, service og kassation af hardware sørges for sletning eller fortsat fortrolighed vedrørende personoplysninger på det berørte hardware.
- Databehandleren har en it-sikkerhedspolitik.

- Databehandleren har mulighed for at reagere ansættelsesretligt på medarbejderes brud på databehandlerens datasikkerhed eller brud på instruks om behandling af personoplysninger.
- Databehandlerens medarbejdere dokumenterer og rapporterer regelmæssigt brud på persondatasikkerheden eller risici herfor.
- Medarbejdere med adgang til følsomme personoplysninger eller kritiske it-systemer er sikkerhedsgodkendt inden ansættelse.
- Medarbejdere med adgang til personoplysninger eller kritiske it-systemer er sikkerhedsgodkendt forinden ansættelse.
- Medarbejderes behandling af personoplysninger logges helt eller delvis og kan kontrolleres efter behov.
- Medarbejdernes adgang til personoplysninger i systemer og på eventuelle fysiske medier eller faciliteter er begrænset, sådan at det kun er de relevante medarbejdere, der har adgang til de relevante personoplysninger.

Teknisk sikkerhed: Adgang til og beskyttelse af systemer
Databehandleren gennemfører følgende tekniske sikkerhedsforanstaltninger vedrørende adgang til og beskyttelse af systemer:

- Databehandleren benytter antivirus-programmer, som opdateres jævnligt.
- Databehandleren kræver, at medarbejdere anvender individuelle adgangskoder (passwords).
- Databehandlerens PC'er har automatisk adgangsbeskyttelse ved inaktivitet, dvs. låst pauseskærm.
- Databehandlerens systemer har logisk adgangskontrol ved brugernavn og adgangskode eller anden autorisation.
- Der anvendes politik for sammensætningen af adgangskoder, herunder minimumskrav.
- Der er procedure(r) for tilbagekaldelse af tilladelser, når en medarbejder stopper hos databehandleren eller skifter afdeling.
- Der er procedure(r) for tildeling af autorisationer til it-systemer ved en medarbejders ansættelse.
- Der foretages logning og kontrol af uautoriserede eller gentagne mislykkede forsøg på log-in på databehandlerens systemer.

Teknisk sikkerhed: Adgang til personoplysninger (data)
Databehandleren gennemfører følgende tekniske sikkerhedsforanstaltninger vedrørende adgang til personoplysninger:

- Databehandleren foretager logning og kontrol af uautoriserede eller gentagne mislykkede forsøg på adgang til data.
- Databehandleren foretager logning og kontrol af uautoriserede eller gentagne mislykkede forsøg på sletning af data.
- Databehandleren foretager regelmæssig gennemgang og kontrol af brugerautorisationer til specifikke systemer.
- Databehandleren foretager regelmæssigt gennemgang af systemkontrol.
- Databehandleren har procedure(r) for at genskabe/reetablere data fra backup.
- Databehandleren har sporbarhed af adgang til, ændring af og sletning af data foretaget af individuelle brugere.
- Databehandleren tildeler enkelte eller grupper af brugere autorisationer til at tilgå, ændre og slette behandlede personoplysninger.

Teknisk sikkerhed: Kryptering
Databehandleren gennemfører følgende tekniske sikkerhedsforanstaltninger vedrørende kryptering:

- Adgangskoder opbevaret på databehandlerens computere mv. er krypterede.
- Databehandlerens computere har krypterede harddiske.
- Databehandlerens hjemmesider anvender HTTPS (Hyper Text Transfer Protocol Secure).
- Der anvendes kryptering af netværk.

- Følsomme personoplysninger krypteres i systemer og/eller på opbevaringsmedier.
- Indhold på eksterne harddiske og USB-nøgler mv. er krypteret, når disse medier indeholder personoplysninger eller følsomme personoplysninger.
- Personoplysninger krypteres i relevante systemer og/eller på opbevaringsmedier.

Teknisk sikkerhed: Pseudonymisering
Databehandleren gennemfører følgende tekniske sikkerhedsforanstaltninger vedrørende pseudonymisering:

Databehandleren anvender pseudonymisering af personoplysninger. Ved pseudonymisering sikres det, at oplysninger, som kan medvirke til at identificere den registrerede person, er adskilt og opbevaret i et separat, beskyttet it-system.
Teknisk sikkerhed: Tilgængelighed og robusthed
Databehandleren gennemfører følgende tekniske sikkerhedsforanstaltninger vedrørende tilgængelighed og robusthed:

- Aktiv alarmering ved forsøg på uautoriseret adgang til serverrum og/eller behandlingssystemer og data.
- Databehandlerens har procedurebeskrivelse(r) for brud på persondatasikkerheden, der minimum tages op til revidering årligt.
- Der anvendes uafbrudt strømforsyning (UPS).
- Der er regler og retningslinjer for backup af data.
- Der er regler og retningslinjer for genskabelse af data fra backup.
- Der foretages regelmæssig backup (enten egen eller hos leverandør).
- Kun autoriserede medarbejdere har adgang til databehandlerens eventuelle egne servere.
- Serverrum har airconditionsystem.
- Serverrum har røgalarm og brandslukkere.
- Temperatur og luftfugtighed overvåges i serverrum.
- Tilgængelighed og robusthed i databehandlerens systemer og servere er sikret af tredjemand, som databehandleren har en aftale med.

18.3 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:

- Hvis den Dataansvarlige modtager en anmodning om udøvelsen af personers rettigheder efter gældende databeskyttelseslovgivning, og korrekt besvarelse af anmodningen kræver bistand fra Databehandleren, skal Databehandleren bistå den Dataansvarlige med nødvendige og relevante oplysninger og dokumentation samt passende tekniske og organisatoriske sikkerhedsforanstaltninger.
- Hvis den Dataansvarlige vil have hjælp til at besvare en anmodning fra en registreret person, skal den Dataansvarlige sende skriftlig anmodning herom til Databehandleren, og Databehandleren skal som svar herpå levere den nødvendige hjælp eller dokumentation hurtigst muligt og senest 7 kalenderdage efter modtagelse af anmodning herom.
- Hvis Databehandleren modtager en anmodning om udøvelsen af personers rettigheder efter gældende databeskyttelseslovgivning fra andre end den Dataansvarlige, og anmodningen vedrører personoplysninger behandlet på vegne af den Dataansvarlige, skal Databehandleren uden unødvendig forsinkelse videresende anmodningen til den Dataansvarlige.

18.4 Opbevaringsperiode/sletterutine

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal Databehandleren tilbagelevere og slette personoplysningerne i overensstemmelse med Bestemmelse 11.1 medmindre den Dataansvarlige – efter underskriften af

disse bestemmelser – har ændret sit oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til Bestemmelserne.

18.5 Lokalitet for behandling

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

Hos databehandleren selv og hos godkendte underdatabehandlere, som specificeret i Bilag B, dvs. på egne hovedkontorer, samt ved datacentrelokationerne som specificeret nedenfor.

Cibicom A/S
Reg nr: 25598008
Industriparken 35-37
2750
Ballerup
Denmark

GlobalConnect
Reg nr: 26759722
Ejbyindustrivej 1
2600
Glostrup
Denmark

GlobalConnect
Reg nr: 26759722
Hørskætten 5
2630
Taastrup
Denmark

GlobalConnect
Reg nr: 26759722
Hørskætten 6c
2630
Taastrup
Denmark

Digital Realty
Reg nr: 25147022
Industriparken 20A
2750
Ballerup
Denmark

Digital Realty
Reg nr: 25147022
Carl Jacobsens Vej 16-20
2500
Valby
Denmark

18.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Personoplysningerne behandles kun af Databehandleren på de lokationer, som er beskrevet i dette bilag.

Personoplysninger behandles på de lokationer, der er angivet i punkt 18.5. Når databehandleren anvender de underdatabehandlere til AI-inferens, der er oplistet i bilag B, kan begrænsede personoplysninger, der indgår i indsendte prompts, blive overført til USA. Sådanne overførsler sker på grundlag af EU's standardkontraktbestemmelser (afgørelse (EU) 2021/914), og underdatabehandlerne er kontraktligt forpligtet til ikke at anvende oplysningerne til træning af modeller.

Generelt
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.

Overførsel af personoplysninger må i alle tilfælde kun ske som foreskrevet i Bestemmelserne, på den Dataansvarliges instruks, og i det omfang det er tilladt i medfør af databeskyttelseslovgivningen.

Såfremt overførslen af personoplysningerne til tredjelande udenfor EU/EØS sker ved Databehandlerens overførsel til underdatabehandlere, giver den Dataansvarlige ved Bestemmelserne fuldmagt til, at Databehandleren på vegne af den Dataansvarlige kan indgå standardkontraktbestemmelserne vedtaget af Kommissionen med Databehandlerens underdatabehandlere, forudsat at alle regler i databeskyttelseslovgivningen for overførsel og behandling i øvrigt efterleves. Såfremt den Dataansvarlige selv er databehandler, og Databehandleren optræder som underdatabehandler for personoplysningerne i forhold til den Dataansvarliges ultimative kontraktpart(er), skal den Dataansvarlige indhente fuldmagt fra den ultimative kontraktpart til Databehandlerens indgåelse af standardkontraktbestemmelserne.

Når Databehandleren, i overensstemmelse med disse bestemmelser, overfører personoplysninger omfattet af aftalen videre til underdatabehandlere eller selvstændigt dataansvarlige i tredjelande, skal Databehandleren selv sørge for at sikre, at overførslen overholder kapitel 5 i Forordning 2016/679.

18.7 Procedurer for den Dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til Databehandleren

Databehandleren skal på skriftlig anmodning dokumentere overfor den Dataansvarlige, at Databehandleren

- overholder sine forpligtelser efter denne Databehandleraftale og Instruksen, og
- overholder bestemmelserne i GDPR, for så vidt angår personoplysningerne, som behandles på den Dataansvarliges vegne.

Databehandlerens dokumentation skal sendes til den Dataansvarlige inden for rimelig tid efter modtagelsen af anmodningen herom.

Databehandleren skal efter den dataansvarliges anmodning stille sin seneste ISAE 3000-erklæring, udstedt af en uafhængig revisor, til rådighed som en del af databehandlerens dokumentation for overholdelse af disse bestemmelser.

Uanset forudgående skal Databehandleren derudover give mulighed for og bidrage til revisioner og inspektioner hver 12. måned, der foretages af revisorer udpeget af den Dataansvarlige, de offentlige myndigheder i Danmark eller af anden kompetent jurisdiktion, i det omfang det er nødvendigt for at kontrollere, at Databehandleren overholder Bestemmelserne og gældende databeskyttelseslovgivning. Den pågældende revisor skal være underlagt fortrolighed i henhold til lov eller aftale. Den Dataansvarlige skal skriftligt varsle revisioner som beskrevet med 30 kalenderdage.

18.8 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere

Den dataansvarlige skal for egen regning være ansvarlig for at føre tilsyn med anvendte underdatebehandlere.

19. Bilag D - Parternes regulering af andre forhold

19.1 Øvrige forhold

Databehandleraftalen regulerer ikke øvrige forhold.