

Databehandleraftale

MED ORIGO SYSTEMS APS

Baseret på Kombits skabelon version 1.0 af 3. april 2017

DATABEHANDLERAFTALE

Mellem

CVR. nr.:
(herefter "Kunden")

og

Origo Systems ApS
Sjællandsgade 72

8000 Aarhus C
CVR. nr.: 26098688
(herefter "Leverandøren")

er der indgået nedenstående databehandleraftale (herefter "Aftalen") om
Leverandørens behandling af personoplysninger på vegne af Kunden:

1. Generelt

- 1.1. Aftalen beskriver Leverandørens forpligtelse til at efterleve de sikkerhedskrav, som fremgår af Lov nr. 429 af 31/05/2000 med senere ændringer om behandling af personoplysninger (Persondataloven) § 42, jf. § 41, stk. 3-5. Kravene er beskrevet i:
 - (i) Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (Sikkerhedsbekendtgørelsen).
 - (ii) Vejledning nr. 37 af 02/04/2001 til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (Sikkerhedsvejledningen).
- 1.2. Den 25. maj 2018 erstattes Persondataloven af Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 (herefter Databeskyttelsesforordningen) således, at Aftalens pkt. 1.1 (i) – (ii) herefter erstattes med Databeskyttelsesforordningen.
- 1.3. I Aftalen er indarbejdet de krav, som såvel Persondataloven som de kommende regler i Databeskyttelsesforordningen stiller til databehandleraftaler.
- 1.4. Leverandøren skal behandle personoplysninger i overensstemmelse med god databehandlingsskik, jf. de til enhver tid gældende regler og forskrifter for behandling af personoplysninger.

2. Formål

- 2.1. Aftalen vedrører sikkerhed og databehandling i forbindelse med Kundens brug af Leverandørens infrastrukturtilbud, Infrastructure as a Service bestående af storage, netværk og CPU-ressourcer, fremover kaldet Tjenesten.
- 2.2. Tjenesten kan stilles til rådighed for Kunden såvel i form af direkte adgang til Leverandørens infrastruktur-cloud, som i form af adgang til en managed cloud som typisk ejes af Kunden selv, eller en organisation Kunden har et separat forhold til, men som administreres af Leverandøren.
- 2.3. Aftalen indgås fordi Kunden vurderer, at der vil indgå personoplysninger i de data og processer Kunden eller dennes underleverandører behandler og opbevarer i Tjenesten. I det omfang Leverandøren eller dennes underleverandører fungerer som databehandlere, f.eks. i forbindelse med fysisk sikkerhed og sikkerhed i forhold til adgang via Internettet til den til rådighed stillede infrastruktur, regulerer denne aftale Leverandørens sikkerhedsforpligtelser samt Kundens forpligtelser i forhold til Leverandøren.

3. Omfang

- 3.1. Aftalen omfatter udelukkende data hørende til tjenester som Kunden har en aktiv serviceaftale med Leverandøren omkring.

4. Kundens rettigheder og forpligtelser

- 4.1. Kunden er dataansvarlig for de personoplysninger, som Kunden instruerer Leverandøren om at behandle.
- 4.2. Kunden har de rettigheder og forpligtelser, som er givet en dataansvarlig i medfør af lovgivningen, jf. Aftalens pkt. 1.1 og 1.2.
- 4.3. I det omfang Kunden vurderer at det er relevant for Leverandøren at kende til den specifikke behandling og opbevaring af persondata i Leverandørens infrastruktur, oplyser Kunden Leverandøren om disse detaljer skriftligt og separat.
- 4.4. Kunden er forpligtet til at orientere Leverandøren i tilfælde af Kundens eventuelle skærpede it-sikkerhedsregler og ved ændringer i Kundens it-sikkerhedspolitik og it-sikkerhedsregulativ.

5. Leverandørens forpligtelser

- 5.1. Leverandøren er databehandler for de personoplysninger, som Leverandøren behandler på vegne af Kunden, jf. pkt. 7 og bilag 3.
- 5.2. Leverandøren behandler alene de overladte personoplysninger efter instruks fra Kunden, jf. pkt. 7 og bilag 3.
- 5.3. Leverandøren skal fra 25. maj 2018 løbende føre en fortegnelse over behandlingen af personoplysninger samt en fortegnelse over alle sikkerhedsbrud.
- 5.4. Leverandøren skal sikre personoplysningerne via tekniske og organisatoriske sikkerhedsforanstaltninger, som beskrevet i Sikkerhedsbekendtgørelsen og Sikkerhedsvejledningen (frem til 25. maj 2018) og Databeskyttelsesforordningen (fra 25. maj 2018), jf. bilag 1 – Sikkerhed.
- 5.5. Leverandøren skal på opfordring fra Kunden og imod betaling til gældende timepriser hjælpe med at opfylde Kundens forpligtelser i forhold til den registreredes rettigheder, herunder besvarelse af anmodninger fra borgere om indsigt i egne oplysninger, udlevering af borgerens oplysninger, rettelse og sletning af oplysninger, begrænsning af behandling af borgerens oplysninger, samt Kundens forpligtelser i forhold til underretning af den registrerede ved sikkerhedsbrud, fra 25. maj 2018 i medfør af Databeskyttelsesforordningens kap. III samt artikel 34.
- 5.6. Leverandøren skal fra 25. maj 2018 hjælpe Kunden med at efterleve dennes forpligtelser efter Databeskyttelsesforordningens artikel 32-36. Såfremt dette afstedkommer ekstraarbejde hos Leverandøren, afregnes dette til gældende timepriser.
- 5.7. Leverandøren garanterer fra 25. maj 2018 at levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at implementere passende tekniske og organisatoriske foranstaltninger sådan, at Leverandørens behandling af Kundens personoplysninger opfylder kravene i Databeskyttelsesforordningen

og sikrer beskyttelse af den registreredes rettigheder.

- 5.8. Leverandøren er forpligtet til at oplyse med præcise adresseangivelser, hvor Kundens personoplysninger opbevares, jf. bilag 2. Leverandøren skal ajourføre oplysningerne over for Kunden ved enhver ændring.
- 5.9. Hvis Leverandøren er etableret i en anden EU-medlemsstat, skal Leverandøren frem til 25. maj 2018 ligeledes overholde de bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den pågældende medlemsstat.

6. Underleverandør (underdatabehandler)

- 6.1. Ved underdatabehandler forstås en underleverandør, til hvem Leverandøren har overladt hele eller dele af den behandling, som Leverandøren foretager på vegne af Kunden.
- 6.2. Hvis Leverandøren overlader behandlingen af personoplysninger, som Kunden er dataansvarlig for, til underdatabehandlere, skal Leverandøren indgå en skriftlig (under)databehandleraftale med underdatabehandleren.
- 6.3. Underdatabehandleraftalen skal pålægge underdatabehandleren de samme databeskyttelsesforpligtelser, som Leverandøren er pålagt efter Aftalen, herunder, at underdatabehandleren fra 25. maj 2018 garanterer at kunne levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at kunne implementere de passende tekniske og organisatoriske foranstaltninger således, at underdatabehandlerens behandling opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.
- 6.4. Når Leverandøren overlader behandlingen af personoplysninger, som Kunden er dataansvarlig for, til underdatabehandlere, har Leverandøren over for Kunden ansvaret for underdatabehandlerens overholdelse af disses forpligtelser.
- 6.5. Kunden kan til enhver tid forlange dokumentation fra Leverandøren for eksistensen og indholdet af underdatabehandleraftaler for de underdatabehandlere, som Leverandøren anvender i forbindelse med opfyldelsen af sine forpligtelser over for Kunden
- 6.6. Al kommunikation mellem Kunden og underdatabehandleren sker via Leverandøren.

7. Instrukser

- 7.1. Leverandørens behandling af personoplysninger på vegne af Kunden sker udelukkende efter dokumenteret instruks, jf. bilag 3.
- 7.2. Leverandøren giver fra 25. maj 2018 omgående besked til Kunden, hvis en instruks efter Leverandørens vurdering er i strid med lovgivningen, jf. pkt. 1.2.

8. Tekniske og organisatoriske sikkerhedsforanstaltninger

- 8.1. Leverandøren skal frem til 25. maj 2018, jf. bilag 1, træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at personoplysninger:
- (i) tilintetgøres, mistes, ændres eller forringes,
 - (ii) kommer til uvedkommendes kendskab eller misbruges, eller
 - (iii) i øvrigt behandles i strid med lovgivningen, jf. pkt. 1.1 eller i strid med Kundens uddybende it-sikkerhedsregler, jf. bilag 6.
- 8.2. Leverandøren skal fra 25. maj 2018, jf. bilag 1, iværksætte alle sikkerhedsforanstaltninger, der kræves for at sikre et passende sikkerhedsniveau.
- 8.3. Leverandøren skal mindst en gang årligt gennemgå sine interne sikkerhedsforskrifter og retningslinjer for behandlingen af personoplysninger med henblik på at sikre, at de fornødne sikkerhedsforanstaltninger til stadighed er iagttaget.
- 8.4. Leverandøren samt dennes ansatte er underlagt forbud mod at skaffe sig oplysninger af enhver art, som ikke har betydning for udførelsen af den pågældendes opgaver.
- 8.5. Leverandøren har pligt til at instruere de ansatte, der har adgang til eller på anden måde varetager behandling af Kundens personoplysninger, om Leverandørens forpligtelser, herunder bestemmelserne om tavshedspligt og fortrolighed, jf. pkt 9.
- 8.6. Leverandøren er forpligtet til straks at underrette Kunden om ethvert sikkerhedsbrud samt ved
- (i) enhver anmodning om videregivelse af personoplysninger omfattet af Aftalen fra en myndighed, medmindre orienteringen af Kunden er eksplicit forbudt ved lov, f.eks. i medfør af regler, der har til formål at sikre fortroligheden af en retshåndhævende myndigheds efterforskning,
 - (ii) anden manglende overholdelse af Leverandørens, samt eventuelle underdatabehandlers forpligtelse
- uanset, om dette sker hos Leverandøren eller hos en underdatabehandler.
- 8.7. Leverandøren må ikke hverken offentligt eller til tredjeparter kommunikere om sikkerhedsbrud, jf. pkt 7.6, uden forudgående skriftlig orientering af Kunden om indholdet af en sådan kommunikation, medmindre Leverandøren har en retlig forpligtelse til sådan kommunikation.

8. Overførsler til andre lande

- 8.1. Leverandørens overførsel af personoplysninger til lande, der ikke er medlem af EU (tredjelande), f.eks. via en cloudløsning eller en underdatabehandler, skal ske i overensstemmelse med Kundens instruks herfor, jf. bilag 3.
- 8.2. Ved overførsel til tredjelande er Leverandøren og Kunden i fællesskab ansvarlige for, at der foreligger et gyldigt overførselsgrundlag.
- 8.3. Hvis Kundens personoplysninger overføres til en EU-medlemsstat, er det frem til 25. maj 2018 Leverandørens ansvar, at de til enhver tid gældende bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den pågældende medlemsstat, overholdes.
- 8.4. Leverandøren må ikke overføre eller tillade overførsel af personoplysninger til udlandet.

9. Tavshedspligt og fortrolighed

- 9.1. Leverandøren er pålagt fuld tavshedspligt omkring alle personoplysninger, denne bliver bekendt med gennem samarbejdet. Aftalen indebærer, at tavshedspligtsbestemmelserne i straffelovens §§ 152-152f, jf. straffelovens § 152a, finder anvendelse.
- 9.2. Leverandøren skal fra 25. maj 2018 sikre, at alle, der behandler personoplysninger omfattet af Aftalen, herunder ansatte, tredjeparter (f.eks. en reparatør) og underdatabehandlere, forpligter sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

10. Kontroller og erklæringer

- 10.1. Leverandøren er forpligtet til uden ugrundet ophold at give Kunden nødvendige oplysninger til, at Kunden til enhver tid kan sikre sig, at Leverandøren overholder de krav, der følger af denne Aftale.
- 10.2. Kunden, en repræsentant for Kunden eller dennes revision (såvel intern som ekstern) har adgang til at foretage inspektioner og revision hos Leverandøren, få udleveret dokumentation, herunder logs, stille spørgsmål m.v. med henblik på at konstatere, at Leverandøren overholder de krav, der følger af denne Aftale.
- 10.3. Leverandøren skal på Kundens anmodning fremsende en erklæring til Kunden om overholdelse af denne Aftale. Kunden og Leverandøren skal aftale Leverandørens pris herfor. Erklæringen skal udarbejdes i overensstemmelse medgældende anerkendte branchestandarder på området, og skal omfatte både Leverandørens og eventuelle underdatabehandlers databehandling.
- 10.4. I tilfælde af, at Kunden og/eller relevante offentlige myndigheder, særligt Datatilsynet, ønsker at foretage en inspektion af de ovennævnte foranstaltninger i henhold til denne aftale, forpligter Leverandøren og

Leverandørens underleverandører sig til at stille tid og ressourcer til rådighed herfor, som afregnes til gældende timepriser.

11. Ændringer i Aftalen

- 11.1. I det omfang ændringer i lovgivningen, jf. pkt 1.1 og 1.2, eller tilhørende praksis, giver anledning til dette, er både Kunden og Leverandøren med et varsel på 30 dage, berettiget til at foretage ændringer i Aftalen. Ændringer foretaget af Kunden som medfører ekstra arbejde hos Leverandøren afregnes til gældende timepriser.

12. Sletning af data

- 12.1. Kunden træffer beslutning om, hvorvidt der skal ske sletning eller tilbagelevering af personoplysningerne efter, at behandlingen af personoplysningerne er ophørt i medfør af Kundens ophør med at benytte Leverandørens IaaS-tilbud.
- 12.2. Kunden skal senest 30 dage inden ophør af brug af Tjenesten skriftligt meddele Leverandøren, hvorvidt alle personoplysningerne skal slettes eller tilbageleveres til Kunden. I det tilfælde, hvor personoplysningerne tilbageleveres til Kunden, skal Leverandøren ligeledes slette eventuelle kopier. Leverandøren skal sikre, at eventuelle underdatabehandlere ligeledes efterlever Kundens meddelelse.
- 12.3. Leverandøren skal fremsende dokumentation for, at den påkrævede sletning, jf. pkt. 12.2, er foretaget.

13. Ikrafttræden og varighed

- 13.1. Aftalen indgås ved begge parter underskrift og løber indtil Kunden ophører med at benytte Tjenesten ved at nedlægge sin adgang til Tjenesten / slette sin konto, eller instruerer Leverandøren i at gøre dette.

14. Formkrav

- 14.1. Aftalen skal foreligge skriftligt, herunder elektronisk, hos Kunden og Leverandøren.

For Kunden

Dato

For Leverandøren

Dato

Bilag:

Bilag 1 – Sikkerhed

Bilag 2 – Oplysninger om lokationer for behandling og underleverandører
(underdatabehandlere)

Bilag 3 – Instruks

Bilag 1 – Sikkerhed

1. Indledning

Dette bilag indeholder en beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger, som Leverandøren i medfør af Aftalen har ansvar for at gennemføre, overholde og sikre overholdelse af hos dennes underdatabehandlere, som er angivet i bilag 2.

2. Sikkerhedskrav indtil 25. maj 2018

Leverandøren gennemfører følgende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der opfylder kravene i Sikkerhedsbekendtgørelsen og tilhørende praksis.

Foranstaltningerne gennemføres for at undgå, at personoplysninger:

- tilintetgøres, mistes, ændres eller forringes,
- kommer til uvedkommendes kendskab eller misbruges,
- eller i øvrigt behandles i strid med lovgivningen, jf. Aftalens pkt. 1.1

Generelle sikkerhedsforanstaltninger

Leverandørens interne sikkerhedsbestemmelser tager udgangspunkt i gældende anerkendte branchestandarder.

Fysisk sikkerhed er som minimum i Skafor klasse rød.

Al netværksbaseret adgang er sikret i hht. anerkendte standarder i branchen, herunder anvendelse af kryptering og lokationsbegrænset adgangskontrol.

Alle administrative loginforsøg til infrastruktur logges.

Udtjente harddiske, SSD'er og anden storage kasseres ved anvendelse af certificerede kassationsvirksomheder.

I det omfang reparation og service kræver fysisk tilstedeværelse af underleverandører i driftsfaciliterne eller etablering af netværksbaseret adgang, sker reparation og service altid under overvågning af driftspersonale fra Leverandøren.

Autorisation og adgangskontrol

Al fysisk adgang til serverrum er forsynet med personlig og logget adgangskontrol.

Al administrativ adgang til infrastruktur via netværk logges og kan kun ske fra autoriserede IP-adresser.

Kun autoriseret driftspersonale har fysisk og netværksbaseret adgang til administration af infrastruktur.

Eksterne kommunikationsforbindelser

Tjenesten er et Internetbaseret tilbud, der primært tilgås og administreres af Kunden via webadgang og primært benyttes af Kunden til at tilbyde

Internetbaserede tjenester. Der er således i sagens natur etableret eksterne kommunikationsforbindelser til og fra Tjenesten.

Den administrative adgang til Tjenesten via Internettet er sikret via SSL/TLS. Tjenester som Kunden vælger at etablere vha. Tjenesten er det Kundens eget ansvar at sikre på passende vis.

Kontrol med afviste adgangsforsøg

Alle afviste såvel som vellykkede adgangsforsøg til administration af Tjenesten logges. Brugerkonti spærres automatisk efter et aftalt antal fejlslagne adgangsforsøg.

Logning

Alle væsentlige driftshændelser i Tjenesten, såsom start af servere, sletning af disk-images, osv., initieret af såvel Kunden som Leverandøren, logges såvel lokale som via centraliseret syslog. I det omfang Kunden etablerer tjenester vha. den infrastruktur der stilles til rådighed i Tjenesten, er det Kundens eget ansvar at foretage relevant logning.

Hjemmearbejdspladser

Leverandørens behandling af personoplysninger kan i forbindelse med f.eks. genetablering af fra backup, ske ved anvendelse af hjemmearbejdspladser

Al administration af infrastruktur mv. i forbindelse med Tjenesten som foretages ved anvendelse af hjemmearbejdspladser sker udelukkende ved logget fjernadgang fra godkendte IP-adresser og krypteret VPN.

Sikkerhedskrav fra 25. maj 2018

Leverandøren gennemfører i forbindelse med instrukser tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der passer til de aftalte behandlinger, jf. Instruks (bilag 3), og som dermed opfylder Databeskyttelsesforordningens artikel 32.

Foranstaltningerne fastlægges ud fra overvejelser om:

1. Hvad der kan lade sig gøre rent teknisk
2. Implementeringsomkostningerne
3. Den pågældende behandlings karakter, omfang, sammenhæng og formål, jf. Instruks (bilag 3)
4. Konsekvenserne for borgerne ved et sikkerhedsbrud
5. Den risiko, der er forbundet med behandlingerne, herunder risikoen for:
 - a) tilintetgørelse af oplysningerne
 - b) tab af oplysningerne
 - c) ændring af oplysningerne

- d) uautoriseret videregivelse af oplysningerne
- e) uautoriseret adgang til oplysningerne

Bilag 2 – Oplysninger om lokationer for behandling og underleverandører (underdatabehandlere)

1. Lokation(er) for behandlingen

Klosterport 4H, 8000 Aarhus C

2. Underdatabehandlere

Bilag 3 – Instruks

Instruks

Kunden instruerer hermed Leverandøren om at foretage behandling af Kundens oplysninger hørende til Kundens tjenester afviklet i Tjenesten.

Leverandøren er ansvarlig for, at Kundens instruks fremsendes til eventuelle underdatabehandlere.

1. Behandlingens formål

Behandling af Kundens oplysninger sker udelukkende i henhold til denne instruks.

Leverandøren må ikke anvende oplysningerne til andre formål.

Oplysningerne må ikke behandles efter instruks fra andre end Kunden.

2. Generel beskrivelse af behandlingen

Her beskriver Kunden udførligt de typer af behandling, som Leverandøren skal udføre, herunder processer, varigheden og karakteren af behandlingen.

3. Typen af personoplysninger

Behandlingerne indeholder personoplysninger i de nedenfor afkrydsede kategorier. Leverandørens og eventuelle underdatabehandlers niveau for behandlingssikkerhed bør afspejle oplysningernes følsomhed, jf. bilag 1.

Almindelige personoplysninger (indtil 25. maj 2018, jf. Persondatalovens § 6, fra 25. maj 2018, jf. Databeskyttelsesforordningens artikel 6)

☐ Almindelige personoplysninger

Følsomme personoplysninger (indtil 25. maj 2018, jf. Persondatalovens § 7, fra 25. maj 2018, jf. Databeskyttelsesforordningens artikel 9):

- ☐ Racemæssig eller etnisk baggrund
- ☐ Politisk overbevisning
- ☐ Religiøs overbevisning
- ☐ Filosofisk overbevisning
- ☐ Fagforeningsmæssige tilhørsforhold
- ☐ Helbredsforhold, herunder misbrug af medicin, narkotika, alkohol m.v.
- ☐ Seksuelle forhold

Oplysninger om enkeltpersoners rent private forhold (indtil 25. maj 2018, jf. Persondatalovens § 8, fra 25. maj 2018, jf. Databeskyttelsesforordningens artikel 6 og 9):

- ☐ Strafbare forhold
 - ☐ Væsentlige sociale problemer
 - ☐ Andre rent private forhold, som ikke er nævnt ovenfor:
-
-

Oplysninger om cpr-nummer (indtil 25. maj 2018, jf. Persondatalovens § 11, fra 25. maj 2018, eventuelt national lovgivning, jf. Databeskyttelsesforordningens artikel 87)

- ☐ CPR-numre

4. Kategorier af registrerede

Der behandles oplysninger om følgende kategorier af registrerede (f.eks. borgere, elever, kontanthjælpsmodtagere m.m.):

- A) [Indsæt kategori af personer]
- B) [Indsæt kategori af personer]
- C) [Indsæt kategori af personer]

5. Tredjelande (ikke EU-medlemslande)

Leverandøren må overføre personoplysninger til følgende tredjelande:

[Kunden udfylder]

Gyldigt overførselsgrundlag for overførslerne er:

[Udfyldes i forhold til hvilke(t) tredjeland(e), Kunden har godkendt overførsel til]