



UDVIKLING

HOSTING

SUPPORT

Der er dags dato indgået følgende

Databehandleraftale

mellem

Firmanavn:

Adresse:

Postnummer og by:

CVR.nr.:

Kontakt e-mail:

(Kunden, herefter benævnt Dataansvarlige)

og

Bellcom Hosting
Bredgade 20, 1 sal
6000 Kolding
Cvr.nr.: 31779626

(Leverandøren, herefter benævnt Databehandler)

1. Generelt

- 1.1 Aftalen vedrører Databehandlerens forpligtelse til at efterleve de sikkerhedskrav, som fremgår af Rådets forordning (EU) 2016/679 af 27. april 2016 (herefter Databeskyttelsesforordningen)
- 1.2 I Aftalen er indarbejdet de krav og regler som Databeskyttelsesforordningen stiller til databehandleraftaler.
- 1.3 Principperne og anbefalingerne i ISAE3000 med senere ændringer vil på alle relevante områder finde anvendelse i det omfang andet ikke fremgår af Aftalen.
- 1.4 Databehandleren skal behandle personoplysninger i overensstemmelse med god databehandlingsetik, jf. de til enhver tid gældende regler og forskrifter for behandling af personoplysninger.

2. Formål

- 2.1 Denne aftale er indgået i forbindelse med den Dataansvarliges brug af Databehandlerens tjenester som led i aftalen om Udvikling, Hosting og Support på Dataansvarliges løsning(er), som beskrevet i Hovedaftalen: "Bellcoms forretningsbetingelser".
- 2.2 Aftalen og hovedaftalen er indbyrdes afhængige og kan ikke opsiges særskilt. Aftalen kan dog erstattes af en anden databehandleraftale uden at opsige hovedaftalen.

3. **Dataansvarliges rettigheder og forpligtelser**

- 3.1 Den Dataansvarlige er ansvarlig for de personoplysninger, som den Dataansvarlige instruerer Databehandleren om at behandle. Den Dataansvarlige garanterer, at personoplysningerne behandles til legitime og objektive formål og at databehandleren ikke behandler flere personoplysninger end nødvendigt for at opfylde formålet.
- 3.2 Den Dataansvarlige har de rettigheder og forpligtelser, som er givet en Dataansvarlig i medfør af lovgivningen, jf. Aftalens pkt. 1.1. Den dataansvarlige skal ligeledes sikre at der er et gyldigt retsgrundlag for behandlingen ved overførsel af personoplysninger til Databehandleren. Desuden skal den Dataansvarlige sikre, at de registrerede som personoplysningerne vedrører, har fået tilstrækkelige oplysninger om behandling af deres personoplysninger.
- 3.3 Den Dataansvarlige er forpligtet til at orientere Databehandleren i tilfælde af eventuelle skærpede it-sikkerhedsregler og it-sikkerhedsinstruks og ved ændringer i den Dataansvarliges it-sikkerhedspolitik.

4. **Databehandlerens forpligtelser**

- 4.1 Databehandleren behandler personoplysninger på vegne af den Dataansvarlige, jf. pkt. 6. Databehandleren har de forpligtelser, som er pålagt en databehandler i medfør af lovgivningen, jf. Aftalens pkt. 1.1 og 1.2.
- 4.2 Databehandleren behandler alene de overladte personoplysninger efter instruks fra den Dataansvarlige, jf. pkt. 6 og alene med henblik på opfyldelse af Hovedaftalen.
- 4.3 Databehandleren skal fra 25. maj 2018 løbende føre en fortegnelse over behandlingen af personoplysninger samt en fortegnelse over alle sikkerhedsbrud.
- 4.4 Databehandleren skal sikre personoplysningerne via tekniske og organisatoriske sikkerhedsforanstaltninger, som beskrevet i Databeskyttelsesforordningen, jf. bilag 1 – Sikkerhed.
- 4.5 Under hensyntagen til behandlingens art skal Databehandleren, så vidt muligt, bistå den Dataansvarlige med passende tekniske og organisatoriske foranstaltninger, for opfyldelse af den Dataansvarliges forpligtelse til at besvare anmodninger fra registrerede om indsigt i egne oplysninger, udlevering af registreredes oplysninger, rettelser og sletning af oplysninger, begrænsning af behandling af registreredes oplysninger, samt den Dataansvarliges forpligtelser i forhold til underretning af den registrerede ved sikkerhedsbrud, fra 25. maj 2018 i medfør af Databeskyttelsesforordningens kap. III samt artikel 34. Ydelsen leveres på timebasis.

- 4.6 Databehandleren skal bistå den Dataansvarlige med at sikre opfyldelse af den Dataansvarliges forpligtelser i henhold til Databeskyttelsesforordningens artikel 32-36. Denne bistand tager hensyn til behandlingens art og de oplysninger, der er til rådighed for Databehandleren.
- 4.7 Databehandleren garanterer fra 25. maj 2018 at levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at implementere passende tekniske og organisatoriske foranstaltninger sådan, at Databehandlerens behandling af den Dataansvarliges personoplysninger opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.
- 4.8 Personoplysninger, der opbevares/hostes i Databehandlerens systemer, hostes i eget datacenter i Danmark. Som supplement hertil ligger der en backup-løsning i EU (Underdatabehandler).

5. Underdatabehandler

- 5.1 Ved Underdatabehandler forstås en underleverandør, til hvem Databehandleren har overladt hele eller dele af den behandling, som Databehandleren foretager på vegne af den Dataansvarlige.
- 5.2 Databehandleren skal opfylde betingelserne i Databeskyttelsesforordningen artikel 28, stk. 2 og 4 om brug af Underdatabehandler.
- 5.3 Databehandleren må ikke uden udtrykkelig skriftlig godkendelse fra kunden anvende andre Underdatabehandlere, herunder foretage udskiftning af disse, til at behandle de personoplysninger, som den Dataansvarlige har overladt til Databehandleren i medfør af Hovedaftalen.
- 5.4 Den Dataansvarlige giver hermed Databehandleren en generel skriftlig tilladelse til at indgå aftaler med Underdatabehandlere. Databehandleren skal underrette den Dataansvarlige om alle ændringer vedrørende tilføjelse eller udskiftning af Underdatabehandlere. Den Dataansvarlige kan gøre rimelige og relevante indsigelser mod sådanne ændringer. Hvis Databehandleren fortsat ønsker at bruge en Underdatabehandler som den Dataansvarlige har gjort indsigelser imod, har parterne ret til at opsige aftalen og evt. hovedaftalen med den anførte varsel i Bellcoms forretningsbetingelser (Hovedaftalen). I løbet af denne periode må den Dataansvarlige ikke kræve, at Databehandleren ikke bruger den pågældende Underdatabehandler.
- 5.5 Hvis Databehandleren overlader behandlingen af personoplysninger, som den Dataansvarlige er dataansvarlig for, til Underdatabehandlere, skal Databehandleren indgå en skriftlig (Under)databehandleraftale med Underdatabehandleren.

- 5.6 Underdatabehandleraftalen, jf. pkt. 5.5, skal pålægge Underdatabehandleren de samme databeskyttelsesforpligtelser, som Databehandleren 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.
- 5.7 Når Databehandleren overlader behandlingen af personoplysninger, som den dataansvarlige er dataansvarlig for, til Underdatabehandlere, har Databehandleren over for den Dataansvarlige ansvaret for Underdatabehandlerens overholdelse af disses forpligtelser, jf. pkt. 5.6.
- 5.8 Databehandleren skal indgå databehandleraftaler med Underdatabehandlere indenfor EU/EØS. Hvis der indgås aftale med Underdatabehandlere udenfor EU/EØS skal databehandleren indgå standardaftaler i henhold til Kommissionens beslutning 2010/87/EU af 5. februar 2010 om overførsel af personoplysninger til Underdatabehandlere, der er etableret i tredjelande eller i henhold til EU/US Privacy Shield.
- 5.9 Den Dataansvarlige giver herved Databehandleren en generel fuldmagt til at indgå standardkontrakter med Underdatabehandlere udenfor EU/EØS.
- 5.10 Den Dataansvarlige kan til enhver tid forlange dokumentation fra Databehandleren for eksistensen og indholdet af underdatabehandleraftaler for de Underdatabehandlere, som Databehandleren anvender i forbindelse med opfyldelsen af sine forpligtelser over for den Dataansvarlige.
- 5.11 Al kommunikation mellem den Dataansvarlige og Underdatabehandleren sker via Databehandleren.

6. Instrukser

- 6.1 Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker udelukkende efter den Dataansvarliges instruks.
- 6.2 Databehandleren giver fra 25. maj 2018 omgående besked til den Dataansvarlige hvis en instruks efter Databehandlerens vurdering er i strid med lovgivningen, jf. pkt. 1.1 og 1.2.

7. Tekniske og organisatoriske sikkerhedsforanstaltninger

- 7.1 Databehandleren skal fra 25. maj 2018, jf. bilag 1, iværksætte alle sikkerhedsforanstaltninger, der kræves for at sikre et passende sikkerhedsniveau.

- 7.2 Databehandleren skal mindst én 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, jf. pkt. 7.1 samt bilag 1.
- 7.3 Databehandleren samt dennes ansatte er underlagt forbud mod at skaffe sig oplysninger af enhver art, som ikke har betydning for udførelsen af den pågældendes opgaver.
- 7.4 Databehandleren har pligt til at instruere de ansatte, der har adgang til eller på anden måde varetager behandling af den dataansvarliges personoplysninger, om Databehandlerens forpligtelser, herunder bestemmelserne om tavshedspligt og fortrolighed, jf. pkt 9.
- 7.5 Leverandøren er forpligtet til straks indenfor normal arbejdstid at underrette den Dataansvarlige om ethvert sikkerhedsbrud.
- 7.6 Databehandleren må ikke hverken offentligt eller til tredjeparter kommunikere om sikkerhedsbrud, jf. pkt 7.5, uden forudgående skriftlig aftale med kunden om indholdet af en sådan kommunikation, medmindre Databehandleren har en retlig forpligtelse til sådan kommunikation.

8. **Overførsler til andre lande**

- 8.1 Databehandlerens 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 Dataansvarliges instruks./accept, jf. pkt 5.
- 8.2 Ved overførsel til tredjelande er Databehandleren og den Dataansvarlige i fællesskab ansvarlige for, at der foreligger et gyldigt overførselsgrundlag.

9. **Tavshedspligt og fortrolighed**

- 9.1 Databehandleren er - under og efter ophør - pålagt fuld tavshedspligt omkring alle oplysninger, denne bliver bekendt med gennem samarbejdet. Aftalen indebærer, at tavshedspligtsbestemmelserne i straffelovens §§ 152-152f, jf. straffelovens § 152a, finder anvendelse.
- 9.2 Databehandleren skal sikre, at alle, der behandler oplysninger omfattet af Bellcoms forretningsbetingelser (Hovedaftalen), 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 Databehandleren er forpligtet til uden ugrundet ophold at give den Dataansvarlige nødvendige oplysninger til, at den Dataansvarlige til enhver tid kan sikre sig, at Databehandleren overholder de krav, der følger af denne Aftale.

11. **Ændringer i Aftalen**

- 11.1 Den dataansvarlige kan til enhver tid, med et forudgående varsel på mindst 90 dage, foretage ændringer i Aftalen og instruksen. Ændringsprocessen og omkostningerne aftales skriftligt mellem den dataansvarlige og databehandleren. Databehandleren skal ved sådanne ændringer uden ugrundet ophold sikre, at underdatabehandlerne tillige forpligtes af ændringerne.
- 11.2 I det omfang ændringer i lovgivningen, jf. pkt 1.1 og 1.2, eller tilhørende praksis, giver anledning til dette, er databehandleren med et varsel på 90 dage og uden at dette medfører krav om betaling fra den dataansvarlige, berettiget til at foretage ændringer i Aftalen.

12. **Sletning af data**

- 12.1 Den dataansvarlige træffer beslutning om, hvorvidt der skal ske sletning eller tilbagelevering af personoplysningerne efter, at behandlingen af personoplysningerne er ophørt.
- 12.2 Ved ophør af abonnement er Databehandleren forpligtet til, på den dataansvarliges skriftlige anmodning, at slette eller returnere alle personoplysninger til den dataansvarlige samt til at slette alle eksisterende kopier, medmindre opbevaring af personoplysninger er fastsat ved EU-ret eller national ret.

13. **Tvistigheder**

- 13.1 Tvistigheder fremgår i Hovedaftalen: Bellcoms Forretningsbetingelser.

14. **Ansvar og erstatning**

- 14.1 Ansvar og erstatningsspørgsmål fremgår i hovedaftalen: Bellcoms Forretningsbetingelser.

15. Ikrafttræden og varighed

- 15.1 Databehandleraftalen indgås ved begge parter underskrift og løber indtil ophør.
- 15.2 Ved opsigelse af hovedaftalen, ophører denne Databehandleraftale også. Databehandleren forbliver undergivet de forpligtelser, der fremgår af denne Databehandleraftale, så længe Databehandleren behandler personoplysninger på vegne af den Dataansvarlige.

16. Formkrav

- 16.1 Aftalen skal foreligge skriftligt, herunder elektronisk, hos Databehandleren og den Dataansvarlige.

For Dataansvarlig

For Databehandler

Dato / -

Dato / -

Kunden

Bellcom Hosting ApS

Bilag:

Bilag 1 – Sikkerhed

Databehandleraftale: version 1.1

Bilag 1 – Sikkerhed

1. Indledning

Dette bilag indeholder en beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger, som Databehandleren i medfør af Aftalen har ansvar for at gennemføre, overholde og sikre overholdelse af hos dennes Underdatabehandlere.

2. Sikkerhedskrav

Leverandøren gennemfører tekniske og organisatoriske sikkerhedsforanstaltninger der opfylder kravene i Databeskyttelsesforordningens artikel 32.

Generelle sikkerhedsforanstaltninger

De af den Dataansvarliges løsning(er) hostet af Bellcom ligger på centrale, sikrede servere, hvor data og datalinjer er sikre og krypterede. Data kan kun tilgås af kunden, og det sker via sikre og krypterede datalinjer.

Ansatte i Bellcom har således ikke adgang til Persondata på kundens løsning. Eneste undtagelse er serveradministrator og hoved-applikationsadministrator (User 1). Disses særlige adgang og beskyttelse heraf er beskrevet nedenfor under autorisationer og adgangskontrol.

Alle ansatte i Bellcom er via (tillæg til) ansættelseskontrakt gjort bekendt med de skærpede krav til behandling af personoplysninger, der følger af arbejdet med data og løsninger for Bellcoms kunder.

Bellcoms servere er beliggende på særskilt lokation. Selve serverrummet er en klima- og brandbeskyttet "bygning i bygningen". Adgang hertil sker med brik og kode. Autoriseret adgang hertil udløser SMS til driftsleder og driftsteam, og der sker fotodokumentation af, hvem der er i rummet (konstant fotoovervågning af døren til rummet indefra). Forsøg på uautoriseret adgang udløser alarm til Dansikring/Verisure samt driftvagten hos Bellcom.

Serverrummet er forsynet med CTS kontrolsystem, eltavle, tre serverskabe med fysiske diske (konfigureret som virtuelle servere med redundans), kommunikationscontrollere, to firewalls (1 redundant), tre UPS, tre klimaanlæg, vandalarmer (gulv, kølekondens og tag) samt brandalarm og -sikring med Inergen brandslukningsanlæg. Desuden er der egen nødstrømsgenerator på adressen. Alle systemer og sensorer overvåges af CTS, og overvågningsdata logges direkte samt på server (med backup).

Autorisation og adgangskontrol

Bellcom, Databehandleren har ansvaret for administration af adgang til applikation og server i løsninger, som hostes af Bellcom. Ansvar for brugeradministration og adgang til data i applikationen ligger hos den Dataansvarlige.

Det er kun driftsleder/driftsteam hos Bellcom, der har serveradgang og adgang som hoved-applikationsadministrator. Ved nedbrud eller kritisk support kan udviklings- eller supportmedarbejder hos Bellcom tildeles éngangsadgang som hovedapplikations-administrator.

Det er ikke muligt at logge ind i applikationen uden brug af password. Der sker logning af alle login og loginforsøg. Ved gentagne, systematiske forsøg på uautoriseret adgang fra en IP-adresse kan den blokeres.

Inddatamateriale som indeholder personoplysninger

Bellcom har ikke adgang til inddatamateriale.

Uddatamateriale som indeholder personoplysninger

Bellcom har ikke adgang til uddatamateriale.

Eksterne kommunikationsforbindelser

Der benyttes sikre linjer (SSH2) til kommunikation til og fra servere.