

SIKKER@MAIL 

DATABEHANDLERAFKTALE

Version 1.2.1

INDHOLDSFORTEGNELSE

1	GENERELT	3
2	FORMÅL	3
3	DATAANSVARLIGES RETTIGHEDER OG FORPLIGTELSE	4
4	LEVERANDØRENS FORPLIGTELSE	4
5	UNDERLEVERANDØR (UNDERDATABEHANDLER)	5
6	INSTRUKSER	6
7	TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER.....	6
8	OVERFØRSLER TIL ANDRE LANDE	7
9	TAVSHEDSPLIGT OG FORTROLIGHED	8
10	KONTROLLER OG ERKLÆRINGER	8
11	ÆNDRINGER I AFTALEN	8
12	SLETNING AF DATA	9
13	MISLIGHOLDELSE OG TVISTIGHEDER	9
14	ERSTATNING OG FORSIKRING	9
15	IKRAFTTRÆDEN OG VARIGHED	9
16	FORMKRAV.....	10
17	LEVERANDØRENS INTERNE PROCEDURER	10
18	BILAG 1 – SIKKERHED	10
19	BILAG 2 – OPLYSNINGER OM LOKATIONER FOR BEHANDLING OG UNDERLEVERANDØRER (UNDERDATABEHANDLERE)	13
20	BILAG 3 – INSTRUKS.....	14
21	AFTALEINDGÅELSE	16

DATABEHANDLERAFTALE**MELLEM**

Logiva A/S

CVR-nr. 21742473

Brendstrupgårdsvej, 7, 2. TV

8200 Århus N

(i det følgende også benævnt "Leverandøren")

OG

SIKKER@MAIL Forhandler:

MENTOR IT A/S

CVR-nr. 25576861

Lindevej 8

6710 Esbjerg V

(i det følgende benævnt "Samarbejdspartner", som er virksomheden der har indgået SIKKER@MAIL forhandleraftale)

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

Aftalen er et tillæg til "SIKKER@MAIL FORHANDLERAFTALE af den 10.10.19" (i det følgende benævnt "Hovedaftalen")

Aftalen er udarbejdet ud fra "Skabelon for databehandleraftaler mellem kommuner og IT-leverandører – version 2.0 af 30. maj 2018", udgivet af kommunernes IT-fællesskab KOMBIT.

1 GENERELT

- 1.1 Aftalen vedrører Leverandørens forpligtelse til at efterleve de sikkerhedskrav, som fremgår af Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 (herefter Databeskyttelsesforordningen).
- 1.2 Leverandøren og Samarbejdspartneren har indgået Hovedaftalen om levering af en sikkermail-løsning til brug for Samarbejdspartneren og Samarbejdspartnerens slutkunder. Når Samarbejdspartneren leverer sikkermail-løsningen til sine slutkunder, vil disse i overensstemmelse med Databeskyttelseslovgivningen være dataansvarlig. Når Samarbejdspartneren anvender sikkermail-løsningen til egne forhold, vil Samarbejdspartneren derimod være den dataansvarlige. Denne Aftale gælder for behandling af personoplysninger af Leverandøren på vegne af Samarbejdspartneren som dataansvarlig. Aftalen gælder også, hvis Leverandøren i forhold til Samarbejdspartnerens slutkunder behandler personoplysninger i forbindelse med sikkermail-løsningen. I det følgende henvises der til Samarbejdspartneren og dennes slutkunder i forening som "Dataansvarlig".
- 1.3 I Aftalen er indarbejdet de krav, som Databeskyttelsesforordningen stiller til databehandleraftaler.
- 1.4 Til at understøtte god databehandling og datatilgængelighed, der lever op til lovgivningskravene, har Leverandøren implementeret et internt instruksystem (pkt. 17).
- 1.5 Leverandøren skal behandle personoplysninger i overensstemmelse med god databehandlingskik, jf. de til enhver tid gældende regler og forskrifter for behandling af personoplysninger.
- 1.6 Leverandøren er alene forpligtet til at foretage databehandling, som beskrevet i Aftalen. Leverandøren er således **ikke** forpligtet til at gøre sig bekendt med Dataansvarliges interne it-sikkerhedsregulativ, it-sikkerhedspolitik og følge de eventuelle, dertilhørende uddybende it-sikkerhedsregler.

2 FORMÅL

- 2.1 Leverandøren behandler i medfør af Hovedaftalen personoplysninger for Dataansvarlig, hvor Leverandørens behandling og formålet med behandlingerne er håndtering af krypterede og signerede e-mails, samt personoplysninger kommunikeret sikkert via Internetblanketter.

3 DATAANSVARLIGES RETTIGHEDER OG FORPLIGTELSE

- 3.1 Dataansvarlig er dataansvarlig for de personoplysninger, som Dataansvarlig instruerer Leverandøren om at behandle. Dataansvarlig har ansvaret for, at de personoplysninger, som Dataansvarlig instruerer Leverandøren om at behandle, må behandles af Leverandøren, herunder at behandlingen er nødvendig og legitim i forhold til Dataansvarliges opgavevaretagelse.
- 3.2 Dataansvarlig har de rettigheder og forpligtelser, som er givet en dataansvarlig i medfør af lovgivningen, jf. Aftalens pkt. 1.1 samt Lov nr. 502 af 23/05/2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (Databeskyttelsesloven).
- 3.3 Dataansvarlig er **ikke** forpligtet til at orientere Leverandøren i tilfælde af Dataansvarliges eventuelle skærpede it-sikkerhedsregler og ved ændringer i Dataansvarliges it-sikkerhedspolitik og it-sikkerhedsregulativ.

4 LEVERANDØRENS FORPLIGTELSE

- 4.1 Leverandøren er databehandler for de personoplysninger, som Leverandøren behandler på vegne af Dataansvarlig, jf. pkt. 6 og bilag 3 (Instruks - pkt. 20). Leverandøren har som databehandler de forpligtelser, som er pålagt en databehandler i medfør af lovgivningen, jf. Aftalens pkt. 1.1.
- 4.2 Leverandøren behandler alene de overladte personoplysninger efter instruks fra Dataansvarlig, jf. pkt. 6 og bilag 3 (Instruks - pkt. 20), og alene med henblik på opfyldelse af Hovedaftalen.
- 4.3 Leverandøren skal føre fortegnelser over behandlingen af personoplysninger, samt fortegnelser over alle brud på persondatasikkerheden.
- 4.4 Leverandøren skal sikre personoplysningerne via tekniske og organisatoriske sikkerhedsforanstaltninger, jf. bilag 1 (Sikkerhed - pkt. 18).
- 4.5 Leverandøren skal på opfordring fra Dataansvarlig hjælpe med at opfylde Dataansvarliges 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 Dataan-

svarliges forpligtelser i forhold til underretning af den registrerede ved brud på persondatasikkerheden, i medfør af Databeskyttelsesforordningens kap. III samt artikel 34.

- 4.6 Leverandøren skal hjælpe Dataansvarlig med at efterleve dennes forpligtelser efter Databeskyttelsesforordningens artikel 32-36, jf. Databeskyttelsesforordningens artikel 28, stk. 3, litra f.
- 4.7 Al kommunikation til Samarbejdspartnerens slutkunder foretages af Samarbejdspartneren, medmindre andet aftales.
- 4.8 Leverandøren garanterer at levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at implementere passende tekniske og organisatoriske foranstaltninger sådan, at Leverandørens behandling af Dataansvarliges personoplysninger opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.
- 4.9 Leverandøren er forpligtet til at oplyse med præcise adresseangivelser, hvor Dataansvarliges personoplysninger opbevares, jf. bilag 2 (Oplysninger om lokationer for behandling og underleverandører - pkt. 19). Leverandøren skal ajourføre oplysningerne over for Dataansvarlig ved enhver ændring.

5 UNDERLEVERANDØR (UNDERDATABEHANDLER)

- 5.1 Ved underdatabehandler forstås en underleverandør, til hvem Leverandøren har overladt hele eller dele af den behandling, som Leverandøren foretager på vegne af Dataansvarlig.
- 5.2 Leverandøren må ikke uden udtrykkelig forudgående skriftlig godkendelse fra Dataansvarlig anvende andre underdatabehandlere end dem, der er angivet i bilag 2 (Oplysninger om lokationer for behandling og underleverandører - pkt. 19), herunder foretage udskiftning af disse, til at behandle de personoplysninger, som Dataansvarlig har overladt til Leverandøren i medfør af Hovedaftalen.
- 5.3 Hvis Leverandøren overlader behandlingen af personoplysninger, som Dataansvarlig er dataansvarlig for, til underdatabehandlere, skal Leverandøren indgå en skriftlig (under)databehandleraftale med underdatabehandleren.
- 5.4 Underdatabehandleraftalen, jf. pkt. 5.3, skal pålægge underdatabehandleren de samme databeskyttelsesforpligtelser, som Leverandøren er pålagt efter Aftalen, herunder, at underdatabehandleren garanterer at kunne levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at kunne implementere de passende tekniske og organisatoriske foranstaltninger så-

ledes, at underdatabehandlerens behandling opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.

- 5.5 Når Leverandøren overlader behandlingen af personoplysninger, som Dataansvarlig er dataansvarlig for, til underdatabehandlere, har Leverandøren over for Dataansvarlig ansvaret for underdatabehandlernes overholdelse af disses forpligtelser, jf. pkt. 5.3.
- 5.6 Dataansvarlig kan til enhver tid forlange dokumentation fra Leverandøren for eksistensen og indholdet af underdatabehandlertaaler for de underdatabehandlere, som Leverandøren anvender i forbindelse med opfyldelsen af sine forpligtelser over for Dataansvarlig.
- 5.7 Al kommunikation mellem Dataansvarlig og underdatabehandleren sker via Leverandøren.

6 INSTRUKSER

- 6.1 Leverandørens behandling af personoplysninger på vegne af Dataansvarlig sker udelukkende efter dokumenteret instruks, jf. bilag 3 (Instruks - pkt. 20), medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Leverandøren er underlagt; i så fald underretter Leverandøren Dataansvarlig om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.
- 6.2 Leverandøren giver omgående besked til Dataansvarlig, hvis en instruks efter Leverandørens vurdering er i strid med lovgivningen, jf. pkt. 1.1.

7 TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER

- 7.1 Leverandøren skal, jf. bilag 1 (Sikkerhed - pkt. 18), iværksætte alle sikkerhedsforanstaltninger, der kræves for at sikre et passende sikkerhedsniveau.
- 7.2 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, jf. pkt. 7.1, samt bilag 1 (Sikkerhed - pkt. 18).
- 7.3 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.

- 7.4 Leverandøren har pligt til at instruere de ansatte, der har adgang til eller på anden måde varetager behandling af Dataansvarliges personoplysninger, om Leverandørens forpligtelser, herunder bestemmelserne om tavshedspligt og fortrolighed, jf. pkt. 9.
- 7.5 Leverandøren er forpligtet til straks, og senest 24 timer efter leverandøren er blevet bekendt med bruddet, at underrette Dataansvarlig om ethvert brud på persondatasikkerheden samt
- (i) ved enhver anmodning om videregivelse af personoplysninger omfattet af Aftalen fra en myndighed, medmindre orienteringen af Dataansvarlig 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 forpligtelser
- uanset, om dette sker hos Leverandøren eller hos en underdatabehandler.
- 7.6 Leverandøren må ikke hverken offentligt eller til tredjeparter kommunikere om brud på persondatasikkerheden, jf. pkt 7.5, uden forudgående skriftlig aftale med Dataansvarlig 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 Dataansvarliges instruks herfor, jf. bilag 3 (Instruks - pkt. 20), medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Leverandøren er underlagt; i så fald underretter Leverandøren Dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning.
- 8.2 Ved overførsel til tredjelande er Leverandøren og Dataansvarlig i fællesskab ansvarlige for, at der foreligger et gyldigt overførselsgrundlag.
- 8.3 Leverandøren må kun overføre eller tillade overførsel af personoplysninger til udlandet jf. pkt. 8.1 og pkt. 8.2.

9 TAVSHEDSPLIGT OG FORTROLIGHED

- 9.1 Leverandøren er - under og efter Hovedaftalens 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 Leverandøren skal sikre, at alle, der behandler oplysninger 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 Dataansvarlig nødvendige oplysninger til, at Dataansvarlig til enhver tid kan sikre sig, at Leverandøren overholder de krav, der følger af denne Aftale.
- 10.2 Dataansvarlig, en repræsentant for Dataansvarlig 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 indhenter én gang årligt en ISAE-3000 erklæring om overholdelse af denne Aftale. Efter anmodning fra dataansvarlig fremsendes erklæringen vederlagsfrit. Anmodning skal efterkommes inden for 14 dage.
- 10.4 I tilfælde af, at Dataansvarlige 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 uden yderligere omkostninger for Dataansvarlige at stille tid og ressourcer til rådighed herfor.
- 10.5 Dataansvarliges tilsyn med eventuelle underleverandører sker som udgangspunkt gennem Leverandøren.

11 ÆNDRINGER I AFTALEN

- 11.1 Ændring af Aftalen kan ske, når Dataansvarlig og Leverandør er enige herom. I det omfang ændringer i lovgivningen, eller tilhørende praksis, giver anledning til ændringer, skal ændringer i aftalen foretages snarest muligt, efter nærmere aftale mellem parterne.

12 SLETNING AF DATA

- 12.1 Dataansvarlig træffer beslutning om, hvorvidt der skal ske sletning eller tilbagelevering af personoplysningerne efter, at behandlingen af personoplysningerne er ophørt i medfør af Hovedaftalen.
- 12.2 Dataansvarlig kan senest 30 dage inden Hovedaftalens ophør skriftligt meddele Leverandøren, hvorvidt alle personoplysningerne skal slettes eller tilbageleveres til Dataansvarlig. I begge tilfælde skal Leverandøren ligeledes slette eventuelle kopier, medmindre EU-retten eller national ret foreskriver opbevaring af personoplysningerne. Leverandøren skal sikre, at eventuelle underdata-behandlere ligeledes efterlever Dataansvarliges meddelelse.
- 12.3 Persondata slettes løbende efter 30 dage i aftalens løbetid. Ved aftalens ophør slettes persondata således senest efter 30 dage. Løsning, samt dennes opsætningsdata, slettes senest 3 måneder efter aftaleophør. Leverandøren skal skriftligt overfor Dataansvarlig bekræfte, at den påkrævede sletning, jf. pkt. 12.2, er foretaget. Leverandøren indeholder selv eventuelle omkostninger ved en sådan bekræftelse.
- 12.4 Dataansvarlig stiller ikke krav til, at Leverandørens sletning af data, jf. pkt. 12.2, skal overholde eksplicit navngiven standard for sletning, som eksempelvis NIST 800-88.
- 12.5 Ved tilbagelevering af data til Dataansvarlig, sikrer Leverandøren
- at data er sammenstillet på struktureret vis, således at informationsværdien er bevaret.
 - at data er leveret i et elektronisk format, som giver et basis-grundlag for viderebearbejdning mht. import i andet system.
 - at Leverandøren i øvrigt vil være behjælpelig med at fortolke data.

13 MISLIGHOLDELSE OG TVISTIGHEDER

- 13.1 Misligholdelse og tvistigheder er reguleret i Hovedaftalen.

14 ERSTATNING OG FORSIKRING

- 14.1 Erstatnings- og forsikrings spørgsmål er reguleret i Hovedaftalen.

15 IKRAFTTRÆDEN OG VARIGHED

- 15.1 Aftalen indgås ved begge parter underskrift og løber indtil ophør af Hovedaftalen.

- 15.2 Aftalen kan af begge parter kræves genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Aftalen giver anledning hertil.
- 15.3 Opsigelse af Aftalen kan ske i henhold til de opsigelsesvilkår, inkl. opsigelsesvarsel, som fremgår af Hovedaftalen.
- 15.4 Aftalen er gældende, så længe behandlingen består. Uanset Hovedaftalens og/eller Aftalens opsigelse, vil Aftalen forblive i kraft frem til behandlingens ophør og oplysningernes sletning og/eller tilbagelevering hos Leverandøren og eventuelle underleverandører.

16 FORMKRAV

- 16.1 Aftalen skal foreligge skriftligt, herunder elektronisk, hos Dataansvarlig og Leverandøren.

17 LEVERANDØRENS INTERNE PROCEDURER

- 17.1 Til at understøtte god databehandling og datatilgængelighed, der lever op til lovgivningskravene, har Leverandøren implementeret et internt instrukssystem. Instrukssystemet beskriver relevante interne arbejdsgange, og virksomhedens medarbejdere er individuelt akkrediteret til at kunne udføre de enkelte instrukser. Instrukssystemet indeholder logbog over opdatering af instrukser, ændring af akkrediteringer samt andre relevante hændelser. Minimum en gang årligt udføres en samlet intern revision af instruktionssystemet.

Instrukssystemet indgår i revisors ISAE-3000 vurdering.

18 BILAG 1 – SIKKERHED

Leverandøren gennemfører følgende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der passer til de aftalte behandlinger, jf. bilag 3 (Instruks - pkt. 20), og som dermed opfylder Databeskyttelsesforordningens artikel 32.

- 18.1 Generelle sikkerhedsforanstaltninger
- 18.1.1 Krypteret kommunikation
- I forbindelse med databehandling jf. Hovedaftalen foregår al kommunikation over Internettet krypteret:
- mellem Send Sikker Knappen og Leverandørens server over HTTPS
 - mellem browser og Leverandørens server over HTTPS
 - mellem Internetblanketter og Leverandørens server over HTTPS

- mellem Dataansvarliges Mailserver og Leverandørens server med IMAP og SMTP over SSL/TLS
- mellem Leverandørens server og eksterne services som eksempelvis Digital Post, CPR, Serviceplatformen og Danid over HTTPS
- mellem Leverandørens server og Dataansvarliges interne systemer, som eksempelvis AD, med systemspecifikke protokoller over SSL

18.1.2 Backup

Der foretages Point In Time recovery backup, så data kan genetableres pr. et givent tidspunkt.

18.2 Autorisation og adgangskontrol

Dataansvarlig administrerer selv adgange for egne brugere.

Leverandøren har instrukspecifikke individuelle medarbejderakkrediteringer til support adgang, jf. pkt. 17.

Der gives fysisk adgang til Hostingcenter for de af Leverandørens medarbejdere der er akkrediteret hertil jf. Leverandørens interne instruksystem, og som samtidig er akkrediteret hos det aktuelle Hostingcenter.

18.3 Inddatamateriale som indeholder personoplysninger

E-mails er ustrukturerede data, og kan derfor potentielt indeholde personoplysninger.

Internetblanketter kan sagsafhængigt potentielt indeholde personoplysninger.

18.4 Uddatamateriale som indeholder personoplysninger

E-mails er ustrukturerede data, og kan derfor potentielt indeholde personoplysninger.

Internetblanketter kan sagsafhængigt potentielt indeholde personoplysninger.

18.5 Eksterne kommunikationsforbindelser

SIKKER@MAIL kommunikerer med følgende eksterne systemer:

- Dataansvarliges mailsystem
- Digital Post
- CPR opslag
- Serviceplatformen
- Nemid

Internetblanketter kan kommunikere med:

- Dataansvarliges mailsystem
- CPR opslag
- Nemid
- NemLog-in
- Nets via Quickpay
- Sagsspecifikke fagsystemer aftalt med Dataansvarlig

18.6 Kontrol med afviste adgangsforsøg

Afviste adgangsforsøg til Leverandørens systemer logges. På udvalgte funktioner etableres lås eller forsinker ved gentagne afviste adgangsforsøg.

18.7 Logning

18.7.1 Logning - SIKKER@MAIL

SIKKER@MAIL logger alle metadata for ind- og udgående mails – herunder eksempelvis:

- Tidspunkt
- Emne
- Modtager
- Afsender
- Signaturbevis
- Osv.

Der logges **ikke** indhold af mails.

18.7.2 Logning - Internetblanketter

For Internetblanketter logges registrering af blanketten, samt hændelser på den sag, der bærer Internetblankettens data, herunder brugeraktioner på sagen. Log data er tilgængelig indtil sagen slettes.

18.8 Hjemmearbejdspladser

En delmængde af Leverandørens medarbejdere er akkrediteret til hjemmearbejdsplads. Dette sker som VPN-adgang med 2 factor autentifikation.

19 BILAG 2 – OPLYSNINGER OM LOKATIONER FOR BEHANDLING OG UNDERLEVERANDØRER (UNDERDATABEHANDLERE)

19.1 Underdatabehandlere

Der benyttes ikke underdatabehandlere.

19.2 Underleverandører

Leverandøren benytter dels eksterne Hostingcentre hvor Leverandøren selv har serverkapacitet, og dels eksterne Hostingcentre hvor serverkapacitet er en del af hostingleverancen.

Hostingcentrenes leverance er alene fysiske rammer samt evt. serverkapacitet, og underleverandørerne er således ikke underdatabehandlere i den aktuelle sammenhæng.

Leverandøren forpligter sig til at lokation for hosting faciliteter altid vil være indenfor EU, også i forbindelse med et eventuelt senere skifte af hosting leverandør.

19.2.1 Lokationer for Hostingcentre hvor Leverandøren selv har serverkapacitet

Hostingcentrenes leverance består af rackskabe placeret i datacenter med redundant Internetforbindelse, samt redundant strømforsyning med forsvarlig strømbakup. Leverandøren er selv ansvarlig for serverudstyr.

For at sikre det korrekte høje niveau for de fysiske rammer, indhenter Leverandøren årligt ISAE-3402 erklæring fra alle anvendte Hostingcentre. ISAE-3402 erklæring udleveres til Dataansvarlig på forlangende.

Leverandøren forpligter sig til at lokation for hosting faciliteter altid vil være indenfor EU, også i forbindelse med et eventuelt senere skifte af hosting leverandør.

Leverandøren har hosting aftaler med følgende hostingcentre:

- Itadel A/S (CVR. 37 03 20 34)
Sletvej 30
8310 Tranbjerg J
De fysiske servere der varetager databehandling er placeret på Itadels serverlokation i Århus N
- Global Connect A/S (CVR. 26 75 97 22)
Niels Bohrs Vej 19
DK-8660 Skanderborg
De fysiske servere der varetager databehandling er placeret på Global Connects serverlokation i Stilling

19.2.2 Lokationer for Hostingcentre hvor serverkapacitet er en del af hostingleverancen

Leverandøren har hosting aftaler med følgende hostingcentre:

- Google Cloud

Leverandøren anvender alene fysiske servere i Google Cloud der er placeret på serverlokationer indenfor EU. Google Cloud er certificeret på niveau med ISAE-3402.



SSAE16 / ISAE 3402 (SOC 2/3)

The American Institute of Certified Public Accountants (AICPA) SOC 2 (Service Organization Controls) and SOC 3 audit framework defines Trust Principles and criteria for security, availability, processing integrity, and confidentiality. Google has both SOC 2 and SOC 3 reports for Google Cloud Platform and G Suite.

For til stadighed at sikre det korrekte høje niveau for hosting hos Google Cloud, sikrer Leverandøren sig min. en gang årligt at certificering fortsat er foreliggende.

20 BILAG 3 – INSTRUKS

20.1 Behandlingens formål

Behandling af Dataansvarliges oplysninger sker i henhold til formålet i Hovedaftalen.

Leverandøren må ikke anvende oplysningerne til andre formål.

Oplysningerne må ikke behandles efter instruks fra andre end den Dataansvarlige.

20.2 Generel beskrivelse af behandling

20.2.1 SIKKER@MAIL

SIKKER@MAIL er en kommunikationsservice der omfatter:

- **Afsendelse og modtagelse af Sikker Mail,**
som kan anvendes, når man ønsker sikker kommunikation med det offentlige, eller med andre virksomheder, der har et Sikker Mail system.
SIKKER@MAIL henter udgående post fra Dataansvarliges mailserv, virus-tjekker mailindhold, signerer og krypterer denne og sender denne via Dataansvarliges egen mailserv til endelig modtager.
SIKKER@MAIL henter indgående krypteret post fra Dataansvarliges mailserv, dekrypterer denne, tjekker signatur, genererer signaturbevis, virus-tjekker mailindhold og sender slutteligt mail og signaturbevis videre internt via Dataansvarliges egen mailserv.

- **Afsendelse og modtagelse via SikkerMailBox,**

som kan anvendes, når der ønskes sikker kommunikation med andre virksomheder, der ikke har et Sikker Mail system, med privatpersoner, og med personer/virksomheder i udlandet.

SIKKER@MAIL henter udgående post fra Dataansvarliges mailserver, og placerer denne på SIKKER@MAIL serveren. Der sendes en signeret e-mail til modtager, at en krypteret besked er tilgængelig. Endvidere sendes en SMS med engangskode til modtager. Modtager kan via en krypteret browseradgang og login med fremsendte engangskode få adgang til beskeden, placeret på SIKKER@MAIL serveren.

Modtagelse sker ved at afsender indtaster sin besked via en krypteret browseradgang (Internetblanket). Beskeden modtages på SIKKER@MAIL serveren og konverteres til en e-mail som sendes videre internt via Dataansvarliges egen mailserver.

- **Afsendelse og modtagelse af Virk.dk og Borger.dk post,**

som kan anvendes, hvis man kommunikerer via Digital Post.

SIKKER@MAIL henter udgående post fra Dataansvarliges mailserver og uploader denne til Digital Post via REST.

Ved modtagelse stiller SIKKER@MAIL en REST service til rådighed, som Digital Post indsender til. Post modtages af SIKKER@MAIL og konverteres til en e-mail som sendes videre internt via Dataansvarliges egen mailserver.

SIKKER@MAIL stilles til rådighed, som en ekstra knap i Outlook e-mail programmet.

SIKKER@MAIL opbevarer kommunikationer i en kort periode for at muliggøre afvikling, fejlfinding og evt. genfremsendelse. Leverandøren tilgår kun data i forbindelse med fejlfinding og evt. genfremsendelse.

20.2.2 Internetblanketter

Leverandørens system modtager data krypteret via Internetblanket, og sender disse videre til interne fagsystemer – herunder bl.a. som interne e-mails.

For enkelte Internetblanketløsninger foregår der en egentlig intern sagsbehandling.

For hver Internetblanket aftales der med Dataansvarlig, hvor længe data opbevares. Som udgangspunkt opbevares persondata 30 dage medmindre andet aftales.

20.3 Overvågning, support og fejlhåndtering

Logiva overvåger kontinuerligt driften af SIKKER@MAIL og Internetblanketter. I den forbindelse kan der detekteres fejl der kræver manuel håndtering. Eksempelvis sikre mails der ikke kan håndteres og afleveres korrekt, hvorfor modtager og/eller afsender skal underrettes.

I den forbindelse kan Logivas supportmedarbejdere undtagelsesvist få visuel adgang til persondata. Enhver adgang til persondata logges, også under support sessioner.

Logivas medarbejdere er underlagt fortrolighed.

20.4 Typen af personoplysninger

Da Leverandørens systemer databehandler ustrukturerede oplysninger, kan alle data potentielt indeholde såvel almindelige som følsomme personoplysninger af enhver art.

20.5 Kategorier af registrerede

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

20.6 Tredjelande (ikke EU-medlemslande)

Da Dataansvarlige selv bestemmer modtager af data, kan personoplysninger potentielt blive fremsendt til alle verdens lande. Det er Dataansvarliges eget ansvar, at dataoverførsel kun sker til lande, hvor dette er tilladt.

Leverandøren opbevarer kun data indeholdende personoplysninger midlertidigt – op til 30 dage. Disse data opbevares inden for EU jfr. pkt. 19.2.

21 AFTALEINDGÅELSE

For Samarbejdspartneren

For Leverandøren

Dato: 10/10-19

Dato 10/10 2019




