

DATABASEHANDLERAFTALE

Standardkontraktbestemmelser

i henhold til artikel 28, stk. 3, i forordning 2016/679 (databeskyttelsesforordningen) med henblik på databehandlerens behandling af personoplysninger

mellem

Navn Comby Denmark A/S
Adresse Japanvej 3 4200 Slagelse
CVR/VAT DK40881751

Navn Annette Wegeland
Titel It-sikkerhedsansvarlig
Telefon [+45 88326020](tel:+4588326020)
Mail AVW@comby.dk

og

Comby koncernen dækkende

Comby Denmark A/S
CVR 40 88 17 51
Japanvej 3
4200 Slagelse

Og

Comby Greenland A/S
CVR 12 35 63 58
Issortarfimmut 2
Postboks 1576
3905 Nuussuaq

herefter "databehandleren"

der hver især er en "part" og sammen udgør "parterne"

Har aftalt følgende standardkontraktbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder

1. Indhold

2. Præambel	3
3. Den dataansvarliges rettigheder og forpligtelser	3
4. Databehandleren handler efter instruks	4
5. Fortrolighed	4
6. Behandlingssikkerhed	4
7. Anvendelse af underdatabehandlere.....	5
8. Overførsel til tredjelande eller internationale organisationer	6
9. Bistand til den dataansvarlige.....	7
10. Underretning om brud på persondatasikkerheden	8
11. Sletning og returnering af oplysninger.....	8
12. Revision, herunder inspektion	9
13. Parternes aftale om andre forhold	9
14. Ikrafttræden og ophør.....	10
Kontaktpersoner hos den dataansvarlige og databehandleren	11
Bilag A.1 Oplysninger om behandlingen - Microsoft 365	12
Bilag A.2 Oplysninger om behandlingen – Adobe Cloud	13
Bilag A.3 Oplysninger om behandlingen – Microsoft Azure	15
Bilag A.4 Oplysninger om behandlingen – Webhotel	17
Bilag A.5 Oplysninger om behandlingen – Event.....	18
Bilag A.6 Oplysninger om behandlingen – Cloud Backup.....	19
Bilag A.7 Oplysninger om behandlingen – BCDR.....	21
Bilag A.8 Oplysninger om behandlingen – Microsoft 365 backup	23
Bilag A.9 Oplysninger om behandlingen – Antispam	25
Bilag A.10 Oplysninger om behandlingen – Sikker Mail.....	26
Bilag A.11 Oplysninger om behandlingen – Email signatur	27
Bilag A.12 Oplysninger om behandlingen – MFA.....	28
Bilag A.13 Oplysninger om behandlingen – Datto Workplace.....	30
Bilag A.14 Oplysninger om behandlingen – Flexfone telefoni	32
Bilag A.15 Oplysninger om behandlingen – SOC	33
Bilag A.16 Oplysninger om behandlingen – Managed Videoovervågning	34
Bilag A.17 Oplysninger om behandlingen – MDM.....	35
Bilag A.18 Oplysninger om behandlingen – Security Awareness Training	36
Bilag A.19 Oplysninger om behandlingen – Uniconta	37
Bilag B Underdatabehandlere	39
Bilag C Instruks vedrørende behandling af personoplysninger.....	46
Bilag D Parternes regulering af andre forhold.....	52

1. Disse Bestemmelser fastsætter databehandlerens rettigheder og forpligtelser, når denne foretager behandling af personoplysninger på vegne af den dataansvarlige.
2. 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 (databeskyttelsesforordningen).
3. I forbindelse med leveringen af de i bilag D aftale tjenesteydelser behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.
4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.
5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.
6. 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.
7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.
8. 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.
9. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke er omfattet af Bestemmelserne.
10. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
11. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

3. Den dataansvarliges rettigheder og forpligtelser

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes¹ nationale ret og disse Bestemmelser.

¹ Henvisninger til "medlemsstat" i disse bestemmelser skal forstås som en henvisning til "EØS medlemsstater".

2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.
3. 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

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller 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.
2. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

5. Fortrolighed

1. Databehandleren må kun give adgang til personoplysninger, som behandles på den dataansvarliges vegne, til personer, som er underlagt databehandlerens instruktionsbeføjelser, 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.
2. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

6. Behandlingssikkerhed

1. Databeskyttelsesforordningens 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:

- a. Pseudonymisering og kryptering af personoplysninger
- b. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester

- c. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
 - d. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.
2. Efter forordningens 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.
3. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens 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 forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens 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

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).
2. 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 45 dages forudgående 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.

3. 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 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 databeskyttelsesforordningen.

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

4. 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.
5. Databehandleren skal i sin aftale med underdatabehandleren indføre den dataansvarlige som begunstiget tredjemand, således at den dataansvarlige i tilfælde af at databehandleren faktisk eller retligt set er ophørt med at eksistere eller i tilfælde af databehandlerens konkurs, har ret til at opsigte underdatabehandleraftalen og instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.
6. 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 databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

8. Overførsel til tredjelande eller internationale organisationer

1. 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 databeskyttelsesforordningens kapitel V.
2. 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 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.
3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:
 - a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
 - b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
 - c. behandle personoplysningerne i et tredjeland
4. 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.

5. Disse Bestemmelser skal ikke forveksles med standardkontraktbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

9. Bistand til den dataansvarlige

1. 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 databeskyttelsesforordningens kapitel III.

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

- a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
 - b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
 - c. indsigtretten
 - d. retten til berigtigelse
 - e. retten til sletning ("retten til at blive glemt")
 - f. retten til begrænsning af behandling
 - g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
 - h. retten til dataportabilitet
 - i. retten til indsigelse
 - j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering
2. 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:
 - a. den dataansvarliges forpligtelse til uden unødigt forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder
 - b. den dataansvarliges forpligtelse til uden unødigt forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder
 - c. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)

- d. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet, 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.
3. 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

1. Databehandleren underretter uden unødigt forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.
2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 24 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.
3. I overensstemmelse med Bestemmelse 9.2.a 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:
 - a. 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
 - b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden
 - c. 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.
4. Parterne skal i bilag C 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

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlige, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

Databehandleren forpligter sig til alene at behandle personoplysningerne til de(t) formål, i den periode og under de betingelser, som disse regler foreskriver.

12. Revision, herunder inspektion

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens 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.
2. Procedurene for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.
3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen 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

1. 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 databeskyttelsesforordningen.

1. Bestemmelserne træder i kraft på datoen for begge parter underskrift heraf.
2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.
3. 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.
4. 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 skriftlig varsel af begge parter.
5. Underskrift

På vegne af den dataansvarlige

Navn [NAVN]
Stilling [STILLING]
Telefonnummer [TELEFONNUMMER]
E-mail [E-MAIL]
Underskrift

På vegne af databehandleren

Navn [NAVN]
Stilling [STILLING]
Telefonnummer [TELEFONNUMMER]
E-mail [E-MAIL]
Underskrift

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

Navn	[NAVN]
Stilling	[STILLING]
Telefonnummer	[TELEFONNUMMER]
E-mail	[E-MAIL]

Navn	[NAVN]
Stilling	[STILLING]
Telefonnummer	[TELEFONNUMMER]
E-mail	[E-MAIL]

A.1.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Formålet med databehandlerens behandling af personoplysninger er at levere, drifte, vedligeholde og supportere Microsoft 365-tjenester til den dataansvarlige.

Behandlingen sker med henblik på at sikre funktionalitet, sikkerhed, tilgængelighed og løbende optimering af de aftalte Microsoft 365-tjenester, herunder brugerstyring, datalagring, kommunikation og samarbejdsværktøjer.

A.1.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)

Behandlingen omfatter indsamling, registrering, organisering, strukturering, opbevaring, tilpasning, ændring, søgning, brug, transmission, sammenstilling, begrænsning og sletning af personoplysninger.

Databehandleren udfører desuden teknisk support og fejlsøgning.

A.1.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Afhængigt af den dataansvarliges anvendelse af tjenesten, kan den dataansvarlige vælge at inkludere personoplysninger fra en eller flere af følgende kategorier i de behandlede data:

Almindelige personoplysninger:

- Identitetsoplysninger (navn, brugernavn, e-mailadresse, stilling)
- Kontaktoplysninger (telefonnummer, adresse)
- Oplysninger om IT-brug (logfiler, adgangsdata, brugeraktiviteter)
- Indhold af kommunikation (e-mails, dokumenter, kalenderaftaler, chatbeskeder)
- Eventuelle andre personoplysninger, som den dataansvarlige vælger at lagre eller behandle via Microsoft 365-plattformen

Særlige kategorier af personoplysninger:

- Særlige kategorier af personoplysninger (f.eks. race eller etnisk oprindelse, politiske holdninger, religiøse eller filosofiske overbevisninger, fagforeningsmedlemskab, genetiske data, biometriske data med henblik på entydig identifikation af en fysisk person, helbredsoplysninger, oplysninger om en fysisk persons seksuelle forhold eller orientering, eller oplysninger om straffedomme og lovovertrædelser).

A.1.4. Behandlingen omfatter følgende kategorier af registrerede

- **Kunder** Personer, som er eller har været kunder/medlemmer/klienter/patienter hos den dataansvarlige, eller er potentielle kunder/medlemmer/klienter/patienter
- **Ansatte** Personer, som er eller har været ansatte/bestyrelsesmedlemmer hos den dataansvarlige, eller er nye jobansøgere.
- **Leverandører** Personer som er eller har været forretningsforbindelser, herunder leverandører og samarbejdspartnere hos den dataansvarlige, eller er potentielle forretningsforbindelser

A.1.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser ikrafttræden. Behandlingen har følgende varighed

Behandlingen er ikke tidsbegrænset og varer, indtil Bestemmelserne opsiges eller ophæves af en af partner. Bestemmelserne skal dog forblive i kraft frem til det tidspunkt, hvor databehandleren ikke længere behandler personoplysninger på vegne af den dataansvarlige.

Bilag A.2 Oplysninger om behandlingen – Adobe Cloud

A.2.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Formålet med databehandlerens behandling af personoplysninger er at levere og understøtte adgang til Adobe Cloud-tjenester, herunder software til dokumenthåndtering, grafisk design, digital signatur og samarbejde.

Behandlingen sker med henblik på at muliggøre den dataansvarliges anvendelse af Adobe Cloud i forbindelse med interne forretningsprocesser og kundevedtatte aktiviteter.

A.2.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)

Behandlingen omfatter primært lagring, overførsel, visning, redigering og sletning af personoplysninger via Adobe Cloud-plattformen. Derudover kan der forekomme behandling i form af teknisk support, systemvedligeholdelse og sikkerhedsovervågning, som er nødvendige for at sikre drift og dataintegritet.

A.2.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Behandlingen kan omfatte følgende typer af personoplysninger:

Almindelige personoplysninger:

- Identifikationsoplysninger (f.eks. navn, e-mailadresse, brugernavn)
- Kontaktoplysninger (f.eks. telefonnummer, adresse)
- Digitale spor (f.eks. IP-adresse, loginhistorik, brugeraktivitet)
- Dokumentindhold, som kan indeholde personoplysninger afhængigt af den dataansvarliges anvendelse af Adobe Cloud

A.2.4. Behandlingen omfatter følgende kategorier af registrerede

- **Kunder** Personer, som er eller har været kunder/medlemmer/klienter/patienter hos den dataansvarlige, eller er potentielle kunder/medlemmer/klienter/patienter
- **Ansatte** Personer, som er eller har været ansatte/bestyrelsesmedlemmer hos den dataansvarlige, eller er nye jobansøgere.
- **Leverandører** Personer som er eller har været forretningsforbindelser, herunder leverandører og samarbejdspartnere hos den dataansvarlige, eller er potentielle forretningsforbindelser

A.2.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen har følgende varighed

Side 14 af 52

Behandlingen er ikke tidsbegrænset og varer, indtil Bestemmelserne opsiges eller ophæves af en af partner. Bestemmelserne skal dog forblive i kraft frem til det tidspunkt, hvor databehandleren ikke længere behandler personoplysninger på vegne af den dataansvarlige.

A.3.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Formålet med databehandlerens behandling af personoplysninger er at levere og understøtte adgang til Microsoft Azure-tjenester, herunder cloudbaseret infrastruktur, platforme og software, som den dataansvarlige anvender til drift af egne IT-systemer og forretningsapplikationer.

Behandlingen sker med henblik på at sikre skalerbar, sikker og effektiv databehandling i overensstemmelse med den dataansvarliges instrukser.

A.3.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)

Behandlingen omfatter primært lagring, overførsel, visning, analyse og sletning af personoplysninger via Microsoft Azure-plattformen. Derudover kan der forekomme behandling i form af teknisk support, systemvedligeholdelse, overvågning og sikkerhedsforanstaltninger, som er nødvendige for at sikre drift og dataintegritet. Behandlingen kan desuden inkludere sikkerhedskopiering af personoplysninger via Microsoft Azure Backup, som en del af virksomhedens databeskyttelses- og beredskabsforanstaltninger.

A.3.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Afhængigt af den dataansvarliges anvendelse af tjenesten, kan den dataansvarlige vælge at inkludere personoplysninger fra en eller flere af følgende kategorier i de behandlede data:

Almindelige personoplysninger:

- Identifikationsoplysninger (f.eks. navn, e-mailadresse, brugernavn)
- Kontaktoplysninger (f.eks. telefonnummer, adresse)
- Digitale spor (f.eks. IP-adresse, loginhistorik, brugeraktivitet)
- Indhold i dokumenter, databaser og applikationer, som kan indeholde personoplysninger afhængigt af den dataansvarliges anvendelse af Microsoft Azure

Særlige kategorier af personoplysninger:

- Særlige kategorier af personoplysninger (f.eks. race eller etnisk oprindelse, politiske holdninger, religiøse eller filosofiske overbevisninger, fagforeningsmedlemskab, genetiske data, biometriske data med henblik på entydig identifikation af en fysisk person, helbredsoplysninger, oplysninger om en fysisk persons seksuelle forhold eller orientering, eller oplysninger om straffedomme og lovovertrædelser).

A.3.4. Behandlingen omfatter følgende kategorier af registrerede

- **Kunder** Personer, som er eller har været kunder/medlemmer/klienter/patienter hos den dataansvarlige, eller er potentielle kunder/medlemmer/klienter/patienter
- **Ansatte** Personer, som er eller har været ansatte/bestyrelsesmedlemmer hos den dataansvarlige, eller er nye jobansøgere.
- **Leverandører** Personer som er eller har været forretningsforbindelser, herunder leverandører og samarbejdspartnere hos den data-

A.3.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen har følgende varighed

Behandlingen er ikke tidsbegrænset og varer, indtil Bestemmelserne opsiges eller ophæves af en af partner. Bestemmelserne skal dog forblive i kraft frem til det tidspunkt, hvor databehandleren ikke længere behandler personoplysninger på vegne af den dataansvarlige.

A.4.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Formålet med databehandlerens behandling af personoplysninger er at levere og drifte webhotel-tjenester, herunder hosting af hjemmesider, e-mailkonti, databaser og tilknyttede domæner.

Behandlingen sker med henblik på at sikre stabil og sikker drift af den dataansvarliges digitale tilstedeværelse.

A.4.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)

Behandlingen omfatter primært lagring, overførsel, backup, visning og sletning af personoplysninger via webhotellets infrastruktur. Derudover indgår teknisk support, overvågning, fejlfinding og vedligeholdelse som en del af behandlingen, herunder brug af SSL, SMTP og FTP-tjenester.

A.4.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Behandlingen kan omfatte følgende typer af personoplysninger:

Almindelige personoplysninger:

- Identifikationsoplysninger (f.eks. navn, e-mailadresse, brugernavn)
- Kontaktoplysninger (f.eks. telefonnummer, adresse)
- Tekst- og billedindhold i hostede hjemmesider og databaser
- Logdata og digitale spor (f.eks. IP-adresser, browserdata, besøgsstatistik)

A.4.4. Behandlingen omfatter følgende kategorier af registrerede

- **Kunder** Personer, som er eller har været kunder/medlemmer/klienter/patienter hos den dataansvarlige, eller er potentielle kunder/medlemmer/klienter/patienter
- **Ansatte** Personer, som er eller har været ansatte/bestyrelsesmedlemmer hos den dataansvarlige, eller er nye jobansøgere.
- **Leverandører** Personer som er eller har været forretningsforbindelser, herunder leverandører og samarbejdspartnere hos den dataansvarlige, eller er potentielle forretningsforbindelser

A.4.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen har følgende varighed

Behandlingen er ikke tidsbegrænset og varer, indtil Bestemmelserne opsiges eller ophæves af en af partner. Bestemmelserne skal dog forblive i kraft frem til det tidspunkt, hvor databehandleren ikke længere behandler personoplysninger på vegne af den dataansvarlige.

A.5.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Formålet med databehandlerens behandling af personoplysninger er at levere og drifte Event Management-tjenester, herunder overvågning af IT-infrastruktur, servere, arbejdsstationer, netværksudstyr og kritiske systemer.

Behandlingen sker med henblik på at sikre stabil drift, identificere fejl og hændelser, og understøtte den dataansvarliges IT-sikkerhed og forretningskontinuitet.

A.5.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)

Behandlingen omfatter primært overvågning, logning, rapportering, fejlhåndtering og teknisk support på kritiske services.

A.5.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Behandlingen kan omfatte følgende typer af personoplysninger:

Almindelige personoplysninger:

- Identifikationsoplysninger (f.eks. navn, e-mailadresse, brugernavn)
- Kontaktoplysninger (f.eks. telefonnummer, arbejdsplads)
- Systemdata og logfiler (f.eks. IP-adresser, loginhistorik, hændelsesdata)

A.5.4. Behandlingen omfatter følgende kategorier af registrerede

- **Kunder** Personer, som er eller har været kunder/medlemmer/klienter/patienter hos den dataansvarlige, eller er potentielle kunder/medlemmer/klienter/patienter
- **Ansatte** Personer, som er eller har været ansatte/bestyrelsesmedlemmer hos den dataansvarlige, eller er nye jobansøgere.
- **Leverandører** Personer som er eller har været forretningsforbindelser, herunder leverandører og samarbejdspartnere hos den dataansvarlige, eller er potentielle forretningsforbindelser

A.5.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen har følgende varighed

Behandlingen er ikke tidsbegrænset og varer, indtil Bestemmelserne opsiges eller ophæves af en af partner. Bestemmelserne skal dog forblive i kraft frem til det tidspunkt, hvor databehandleren ikke længere behandler personoplysninger på vegne af den dataansvarlige.

A.6.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Formålet med databehandlerens behandling af personoplysninger er at levere og drifte cloud backup-løsninger, som sikrer kontinuerlig beskyttelse, gendannelse og tilgængelighed af data.

Backup-tjenesterne understøtter den dataansvarliges behov for forretningskontinuitet og dataintegritet.

A.6.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)

Behandlingen omfatter primært automatisk backup, lagring, kryptering, gendannelse og sletning af personoplysninger. Derudover indgår overvågning, versionering, retention management og adgangskontrol som en del af backup-løsningens funktionalitet. Backupdata behandles både i transit og i hvile med kryptering.

A.6.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Afhængigt af den dataansvarliges anvendelse af tjenesten, kan den dataansvarlige vælge at inkludere personoplysninger fra en eller flere af følgende kategorier i de behandlede data:

Almindelige personoplysninger:

- Fornavn, efternavn, initialer, køn, telefonnummer)
- Autentifikationsoplysninger (f.eks. brugernavn, adgangskode eller PIN-kode, sikkerhedsspørgsmål, revisionsspor).
- Kontaktoplysninger (f.eks. adresser, e-mail, telefonnumre).
- Unikke identifikationsnumre og signaturer (f.eks. CPR-nummer, bankkontonummer, pas- og ID-kortnummer, IP-adresser, medarbejdernummer, studienummer, patientnummer, signatur,
- Pseudonyme identifikatorer.
- Finansielle og forsikringsrelaterede oplysninger (f.eks. policenummer, bankkontonavn og -nummer, kreditkortoplysninger, fakturanummer, indkomst, forsikringstype, betalingsadfærd, kreditværdighed).
- Kommercielle oplysninger (f.eks. købshistorik, særlige tilbud, abonnementsoplysninger, betalingshistorik).
- Biometriske oplysninger (f.eks. DNA, fingeraftryk og ansigtsscanninger).
- Lokaliseringsdata (f.eks. geolokaliseringsdata fra netværk, placering ved opkaldsstart/-slut, placering baseret på brug af Wi-Fi-adgangspunkter).
- Foto-, video- og lydoptagelser.
- Internetaktivitet (f.eks. browserhistorik, søgehistorik, læsevaner, tv- og radiobrug).
- Enhedsidentifikation (f.eks. IMEI-nummer, SIM-kortnummer, MAC-adresse).
- HR- og rekrutteringsdata (f.eks. ansættelsesstatus, rekrutteringsoplysninger såsom CV, ansættelseshistorik, uddannelsesoplysninger, job- og stillingsdata, arbejdstimer, vurderinger og løn, arbejdstilladelse, tilgængelighed, ansættelsesvilkår, skatteoplysninger, betalingsoplysninger, forsikringsoplysninger, arbejdssted og organisatorisk tilknytning).
- Uddannelsesdata (f.eks. uddannelseshistorik, igangværende uddannelse, karakterer og resultater, højeste opnåede grad, læringsvanskeligheder).

- Oplysninger om statsborgerskab og ophold (f.eks. statsborgerskab, naturaliseringsstatus, civilstand, nationalitet, immigrationsstatus, pasoplysninger, detaljer om opholds- eller arbejdstilladelse).

Særlige kategorier af personoplysninger:

- Særlige kategorier af personoplysninger (f.eks. race eller etnisk oprindelse, politiske holdninger, religiøse eller filosofiske overbevisninger, fagforeningsmedlemskab, genetiske data, biometriske data med henblik på entydig identifikation af en fysisk person, helbredsoplysninger, oplysninger om en fysisk persons seksuelle forhold eller orientering, eller oplysninger om straffedomme og lovovertrædelser).

A.6.4. Behandlingen omfatter følgende kategorier af registrerede

- **Kunder** Personer, som er eller har været kunder/medlemmer/klienter/patienter hos den dataansvarlige, eller er potentielle kunder/medlemmer/klienter/patienter
- **Ansatte** Personer, som er eller har været ansatte/bestyrelsesmedlemmer hos den dataansvarlige, eller er nye jobansøgere.
- **Leverandører** Personer som er eller har været forretningsforbindelser, herunder leverandører og samarbejdspartnere hos den dataansvarlige, eller er potentielle forretningsforbindelser

A.6.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen har følgende varighed

Behandlingen er ikke tidsbegrænset og varer, indtil Bestemmelserne opsiges eller ophæves af en af partner. Bestemmelserne skal dog forblive i kraft frem til det tidspunkt, hvor databehandleren ikke længere behandler personoplysninger på vegne af den dataansvarlige.

A.7.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Formålet med databehandlerens behandling af personoplysninger er at levere og drifte BCDR-tjenester, herunder backup, gendannelse og sikring af data i tilfælde af systemnedbrud, cyberangreb eller anden form for datatab.

Tjenesten understøtter den dataansvarliges behov for forretningskontinuitet og dataintegritet ved at sikre, at personoplysninger kan genskabes hurtigt og sikkert.

A.7.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)

Behandlingen omfatter automatisk, backup af systemer og data, lagring i Datto Cloud, kryptering, gendannelse af data, overvågning af backupstatus og rapportering. Behandlingen sker via softwarebaserede løsninger uden behov for lokal hardware.

A.7.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Afhængigt af den dataansvarliges anvendelse af tjenesten, kan den dataansvarlige vælge at inkludere personoplysninger fra en eller flere af følgende kategorier i de behandlede data:

Almindelige personoplysninger:

- Fornavn, efternavn, initialer, køn, telefonnummer)
- Autentifikationsoplysninger (f.eks. brugernavn, adgangskode eller PIN-kode, sikkerhedsspørgsmål, revisionsspor).
- Kontaktoplysninger (f.eks. adresser, e-mail, telefonnumre).
- Unikke identifikationsnumre og signaturer (f.eks. CPR-nummer, bankkontonummer, pas- og ID-kortnummer, IP-adresser, medarbejdernummer, studienummer, patientnummer, signatur,
- Pseudonyme identifikatorer.
- Finansielle og forsikringsrelaterede oplysninger (f.eks. policenummer, bankkontonavn og -nummer, kreditkortoplysninger, fakturanummer, indkomst, forsikringstype, betalingsadfærd, kreditværdighed).
- Kommercielle oplysninger (f.eks. købshistorik, særlige tilbud, abonnementsoplysninger, betalingshistorik).
- Biometriske oplysninger (f.eks. DNA, fingeraftryk og ansigtsscanninger).
- Lokaliseringsdata (f.eks. geolokaliseringsdata fra netværk, placering ved opkaldsstart/-slut, placering baseret på brug af Wi-Fi-adgangspunkter).
- Foto-, video- og lydoptagelser.
- Internetaktivitet (f.eks. browserhistorik, søgehistorik, læsevaner, tv- og radiobrug).
- Enhedsidentifikation (f.eks. IMEI-nummer, SIM-kortnummer, MAC-adresse).
- HR- og rekrutteringsdata (f.eks. ansættelsesstatus, rekrutteringsoplysninger såsom CV, ansættelsehistorik, uddannelsesoplysninger, job- og stillingsdata, arbejdstimer, vurderinger og løn, arbejdstilladelse, tilgængelighed, ansættelsesvilkår, skatteoplysninger, betalingsoplysninger, forsikringsoplysninger, arbejdssted og organisatorisk tilknytning).
- Uddannelsesdata (f.eks. uddannelseshistorik, igangværende uddannelse, karakterer og resultater, højeste opnåede grad, læringsvanskeligheder).

- Oplysninger om statsborgerskab og ophold (f.eks. statsborgerskab, naturaliseringsstatus, civilstand, nationalitet, immigrationsstatus, pasoplysninger, detaljer om opholds- eller arbejdstilladelse).

Særlige kategorier af personoplysninger:

- Særlige kategorier af personoplysninger (f.eks. race eller etnisk oprindelse, politiske holdninger, religiøse eller filosofiske overbevisninger, fagforeningsmedlemskab, genetiske data, biometriske data med henblik på entydig identifikation af en fysisk person, helbredsoplysninger, oplysninger om en fysisk persons seksuelle forhold eller orientering, eller oplysninger om straffedomme og lovovertrædelser).

A.7.4. Behandlingen omfatter følgende kategorier af registrerede

- **Kunder** Personer, som er eller har været kunder/medlemmer/klienter/patienter hos den dataansvarlige, eller er potentielle kunder/medlemmer/klienter/patienter
- **Ansatte** Personer, som er eller har været ansatte/bestyrelsesmedlemmer hos den dataansvarlige, eller er nye jobansøgere.
- **Leverandører** Personer som er eller har været forretningsforbindelser, herunder leverandører og samarbejdspartnere hos den dataansvarlige, eller er potentielle forretningsforbindelser

A.7.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen har følgende varighed

Behandlingen er ikke tidsbegrænset og varer, indtil Bestemmelserne opsiges eller ophæves af en af partner. Bestemmelserne skal dog forblive i kraft frem til det tidspunkt, hvor databehandleren ikke længere behandler personoplysninger på vegne af den dataansvarlige.

A.8.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Formålet med databehandlerens behandling af personoplysninger er at levere og drifte backup-tjenester for Microsoft 365, herunder Exchange Online, SharePoint, OneDrive og Teams.

Tjenesten har til formål at sikre forretningskontinuitet og dataintegritet ved at muliggøre gendannelse af data i tilfælde af utilsigtet sletning, systemfejl, ransomware eller anden hændelse, som medfører datatab.

A.8.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)

Behandlingen omfatter automatisk backup, lagring, kryptering, gendannelse og sletning af personoplysninger.

A.8.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Afhængigt af den dataansvarliges anvendelse af tjenesten, kan den dataansvarlige vælge at inkludere personoplysninger fra en eller flere af følgende kategorier i de behandlede data:

Almindelige personoplysninger:

- Fornavn, efternavn, initialer, køn, telefonnummer)
- Autentifikationsoplysninger (f.eks. brugernavn, adgangskode eller PIN-kode, sikkerhedsspørgsmål, revisionsspor).
- Kontaktoplysninger (f.eks. adresser, e-mail, telefonnumre).
- Unikke identifikationsnumre og signaturer (f.eks. CPR-nummer, bankkontonummer, pas- og ID-kortnummer, IP-adresser, medarbejdernummer, studienummer, patientnummer, signatur,
- Pseudonyme identifikatorer.
- Finansielle og forsikringsrelaterede oplysninger (f.eks. policenummer, bankkontonavn og -nummer, kreditkortoplysninger, fakturanummer, indkomst, forsikringstype, betalingsadfærd, kreditværdighed).
- Kommercielle oplysninger (f.eks. købshistorik, særlige tilbud, abonnementsoplysninger, betalingshistorik).
- Biometriske oplysninger (f.eks. DNA, fingeraftryk og ansigtsscanninger).
- Lokaliseringsdata (f.eks. geolokaliseringsdata fra netværk, placering ved opkaldsstart/-slut, placering baseret på brug af Wi-Fi-adgangspunkter).
- Foto-, video- og lydoptagelser.
- Internetaktivitet (f.eks. browserhistorik, søgehistorik, læsevaner, tv- og radiobrug).
- Enhedsidentifikation (f.eks. IMEI-nummer, SIM-kortnummer, MAC-adresse).
- HR- og rekrutteringsdata (f.eks. ansættelsesstatus, rekrutteringsoplysninger såsom CV, ansættelsehistorik, uddannelsesoplysninger, job- og stillingsdata, arbejdstimer, vurderinger og løn, arbejdstilladelse, tilgængelighed, ansættelsesvilkår, skatteoplysninger, betalingsoplysninger, forsikringsoplysninger, arbejdssted og organisatorisk tilknytning).
- Uddannelsesdata (f.eks. uddannelseshistorik, igangværende uddannelse, karakterer og resultater, højeste opnåede grad, læringsvanskeligheder).

- Oplysninger om statsborgerskab og ophold (f.eks. statsborgerskab, naturaliseringsstatus, civilstand, nationalitet, immigrationsstatus, pasoplysninger, detaljer om opholds- eller arbejdstilladelse).

Særlige kategorier af personoplysninger:

Særlige kategorier af personoplysninger (f.eks. race eller etnisk oprindelse, politiske holdninger, religiøse eller filosofiske overbevisninger, fagforeningsmedlemskab, genetiske data, biometriske data med henblik på entydig identifikation af en fysisk person, helbredsoplysninger, oplysninger om en fysisk persons seksuelle forhold eller orientering, eller oplysninger om strafdomme og lovovertrædelser).

A.8.4. Behandlingen omfatter følgende kategorier af registrerede

- **Kunder** Personer, som er eller har været kunder/medlemmer/klienter/patienter hos den dataansvarlige, eller er potentielle kunder/medlemmer/klienter/patienter
- **Ansatte** Personer, som er eller har været ansatte/bestyrelsesmedlemmer hos den dataansvarlige, eller er nye jobansøgere.
- **Leverandører** Personer som er eller har været forretningsforbindelser, herunder leverandører og samarbejdspartnere hos den dataansvarlige, eller er potentielle forretningsforbindelser

A.8.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen har følgende varighed

Behandlingen er ikke tidsbegrænset og varer, indtil Bestemmelserne opsiges eller ophæves af en af partner. Bestemmelserne skal dog forblive i kraft frem til det tidspunkt, hvor databehandleren ikke længere behandler personoplysninger på vegne af den dataansvarlige.

A.9.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Formålet med databehandlerens behandling af personoplysninger er at levere og drifte anti-spam-tjenester, herunder filtrering af uønskede e-mails, beskyttelse mod phishing, malware og spam, samt sikring af e-mailkommunikationens integritet og tilgængelighed.

A.9.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)

Behandlingen omfatter automatisk scanning, analyse, klassificering og filtrering af e-mails og vedhæftede filer. Derudover indgår lagring af metadata, logning af hændelser, rapportering og teknisk support.

A.9.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Behandlingen kan omfatte følgende typer af personoplysninger om de registrerede:

Almindelige personoplysninger:

- Identifikationsoplysninger (f.eks. navn, e-mailadresse, IP-adresse)
- Kommunikationsindhold (f.eks. e-mailtekst, vedhæftede filer)
- Metadata (f.eks. afsendelsestidspunkt, modtager, emnefelt)
- Logdata og sikkerhedshændelser

A.9.4. Behandlingen omfatter følgende kategorier af registrerede

- **Kunder** Personer, som er eller har været kunder/medlemmer/klienter/patienter hos den dataansvarlige, eller er potentielle kunder/medlemmer/klienter/patienter
- **Ansatte** Personer, som er eller har været ansatte/bestyrelsesmedlemmer hos den dataansvarlige, eller er nye jobansøgere.
- **Leverandører** Personer som er eller har været forretningsforbindelser, herunder leverandører og samarbejdspartnere hos den dataansvarlige, eller er potentielle forretningsforbindelser

A.9.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen har følgende varighed

Behandlingen er ikke tidsbegrænset og varer, indtil Bestemmelserne opsiges eller ophæves af en af partner. Bestemmelserne skal dog forblive i kraft frem til det tidspunkt, hvor databehandleren ikke længere behandler personoplysninger på vegne af den dataansvarlige.

A.10.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Formålet med databehandlerens behandling af personoplysninger er at levere og drifte sikker mail-tjenester, herunder kryptering, signering og sikker overførsel af e-mails.

Tjenesten understøtter den dataansvarliges behov for at beskytte fortrolige og følsomme oplysninger under elektronisk kommunikation.

A.10.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)

Behandlingen omfatter automatisk kryptering og dekryptering af e-mails, digital signering, filtrering, lagring af metadata, logning af hændelser samt teknisk support.

Der anvendes avancerede krypteringsprotokoller (f.eks. S/MIME og tunnelmail) for at sikre, at kun autoriserede modtagere kan tilgå indholdet af de behandlede e-mails.

A.10.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Behandlingen kan omfatte følgende typer af personoplysninger om de registrerede:

Almindelige personoplysninger:

- Identifikationsoplysninger (f.eks. navn, e-mailadresse, IP-adresse)
- Kommunikationsindhold (f.eks. e-mailtekst, vedhæftede filer)
- Metadata (f.eks. afsendelsestidspunkt, modtager, emnefelt)
- Logdata og sikkerhedshændelser

A.10.4. Behandlingen omfatter følgende kategorier af registrerede

- **Kunder** Personer, som er eller har været kunder/medlemmer/klienter/patienter hos den dataansvarlige, eller er potentielle kunder/medlemmer/klienter/patienter
- **Ansatte** Personer, som er eller har været ansatte/bestyrelsesmedlemmer hos den dataansvarlige, eller er nye jobansøgere.
- **Leverandører** Personer som er eller har været forretningsforbindelser, herunder leverandører og samarbejdspartnere hos den dataansvarlige, eller er potentielle forretningsforbindelser

A.10.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen har følgende varighed

Behandlingen er ikke tidsbegrænset og varer, indtil Bestemmelserne opsiges eller ophæves af en af partner. Bestemmelserne skal dog forblive i kraft frem til det tidspunkt, hvor databehandleren ikke længere behandler personoplysninger på vegne af den dataansvarlige.

A.11.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Formålet med databehandlerens behandling af personoplysninger er at levere og drifte e-mail signaturtjenester, herunder central administration, tilføjelse og vedligeholdelse af e-mail signaturer, disclaimers i den dataansvarliges e-mailkommunikation.

Tjenesten understøtter den dataansvarliges behov for ensartet branding i e-mailkorrespondance.

A.11.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)

Behandlingen omfatter automatisk indsættelse af e-mail signaturer og disclaimers, behandling og synkronisering af brugeroplysninger fra virksomhedens katalogtjenester (f.eks. Azure AD) og lagring af signaturskabeloner. Derudover kan der behandles metadata om e-mailtrafik og brugerdefinerede attributter, som anvendes til personalisering af signaturer.

A.11.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Behandlingen kan omfatte følgende typer af personoplysninger om de registrerede:

Almindelige personoplysninger:

- Identifikationsoplysninger (f.eks. navn, stilling, afdeling, e-mailadresse, telefonnummer)
- Kontaktoplysninger (f.eks. adresse, mobilnummer)
- Brugerdefinerede attributter (f.eks. LinkedIn-profil, professionelle certifikater)
- Metadata om e-mailtrafik (f.eks. tidspunkt, afsender, modtager, emnefelt)
- Eventuelle billeder (f.eks. profilbillede i signatur)

A.11.4. Behandlingen omfatter følgende kategorier af registrerede

- **Ansatte** Personer, som er eller har været ansatte/bestyrelsesmedlemmer hos den dataansvarlige, eller er nye jobansøgere.

A.11.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen har følgende varighed

Behandlingen er ikke tidsbegrænset og varer, indtil Bestemmelserne opsiges eller ophæves af en af partner. Bestemmelserne skal dog forblive i kraft frem til det tidspunkt, hvor databehandleren ikke længere behandler personoplysninger på vegne af den dataansvarlige.

A.12.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Formålet med databehandlerens behandling af personoplysninger er at levere og drifte MFA-tjenester (Multi-Faktor Autentificering) med henblik på at beskytte adgangen til den dataansvarliges systemer, applikationer og data.

MFA-tjenesten sikrer, at kun autoriserede brugere får adgang ved at kræve to eller flere uafhængige autentifikationsfaktorer.

A.12.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)

Behandlingen omfatter, lagring, validering og brug af autentifikationsoplysninger, herunder brugernavn, adgangskode, engangskoder (OTP), push-notifikationer, biometriske data (hvis aktiveret), samt logning af adgangsforsøg og sikkerhedshændelser. Derudover indgår integration med katalogtjenester (f.eks. Active Directory), administration af brugerprofiler og teknisk support.

A.12.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Behandlingen kan omfatte følgende typer af personoplysninger:

Almindelige personoplysninger:

- Identifikationsoplysninger (f.eks. navn, brugernavn, e-mailadresse)
- Autentifikationsoplysninger (f.eks. adgangskode, PIN-kode, engangskode, push-besked, biometriske data)
- Kontaktoplysninger (f.eks. telefonnummer til SMS eller app)
- Logdata og metadata (f.eks. IP-adresse, tidspunkt for login, anvendt enhed)
- Eventuelt oplysninger om brugerens rolle og adgangsrettigheder

Særlige kategorier af personoplysninger:

- Autentifikationsoplysninger (biometriske data, hvis aktiveret)

A.12.4. Behandlingen omfatter følgende kategorier af registrerede

- **Ansatte** Personer, som er eller har været ansatte/bestyrelsesmedlemmer hos den dataansvarlige, eller er nye jobansøgere.
- **Leverandører** Personer som er eller har været forretningsforbindelser, herunder leverandører og samarbejdspartnere hos den dataansvarlige, som har ekstern adgang til den dataansvarliges systemer

A.12.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen har følgende varighed

Behandlingen er ikke tidsbegrænset og varer, indtil Bestemmelserne opsiges eller ophæves af en af partner. Bestemmelserne skal dog forblive i kraft frem til det tidspunkt, hvor databehandleren ikke længere behandler personoplysninger på vegne af den dataansvarlige.

Side 29 af 52

Bilag A.13 Oplysninger om behandlingen – Datto Workplace

A.13.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Formålet med databehandlerens behandling af personoplysninger er at levere og drifte Datto Workplace-tjenester, herunder cloudbaseret filesynkronisering, deling og samarbejde.

Tjenesten understøtter den dataansvarliges behov for sikker og effektiv håndtering af dokumenter.

A.13.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)

Behandlingen omfatter lagring, synkronisering, deling, backup, gendannelse, adgangsstyring, logning af brugeraktiviteter og teknisk support. Derudover behandles metadata om filer og brugere, herunder versionshistorik og adgangsrettigheder.

A.13.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Afhængigt af den dataansvarliges anvendelse af tjenesten, kan den dataansvarlige vælge at inkludere personoplysninger fra en eller flere af følgende kategorier i de behandlede data:

Almindelige personoplysninger:

- Identifikationsoplysninger (f.eks. navn, e-mailadresse, brugernavn)
- Kontaktoplysninger (f.eks. telefonnummer, adresse)
- Kommunikations- og dokumentindhold (f.eks. filer, mapper, kommentarer)
- Metadata (f.eks. IP-adresse, loginhistorik, adgangsrettigheder, versionshistorik)
- Logdata og brugeraktiviteter
- Eventuelle andre personoplysninger, som den dataansvarlige vælger at lagre eller behandle via Datto Workplace

Særlige kategorier af personoplysninger:

- Særlige kategorier af personoplysninger (f.eks. race eller etnisk oprindelse, politiske holdninger, religiøse eller filosofiske overbevisninger, fagforeningsmedlemskab, genetiske data, biometriske data med henblik på entydig identifikation af en fysisk person, helbredsoplysninger, oplysninger om en fysisk persons seksuelle forhold eller orientering, eller oplysninger om straffedomme og lovovertrædelser).

A.13.4. Behandlingen omfatter følgende kategorier af registrerede

- **Kunder** Personer, som er eller har været kunder/medlemmer/klienter/patienter hos den dataansvarlige, eller er potentielle kunder/medlemmer/klienter/patienter
- **Ansatte** Personer, som er eller har været ansatte/bestyrelsesmedlemmer hos den dataansvarlige, eller er nye jobansøgere.
- **Leverandører** Personer som er eller har været forretningsforbindelser, herunder leverandører og samarbejdspartnere hos den data-

A.13.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen har følgende varighed

Behandlingen er ikke tidsbegrænset og varer, indtil Bestemmelserne opsiges eller ophæves af en af partner. Bestemmelserne skal dog forblive i kraft frem til det tidspunkt, hvor databehandleren ikke længere behandler personoplysninger på vegne af den dataansvarlige.

A.14.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Formålet med databehandlerens behandling af personoplysninger er at levere og drifte telefoni- og kommunikationsløsninger, herunder oprettelse, administration og support af telefoni-løsninger, samt sikring af stabil og sikker drift af den dataansvarliges telefoni og tilhørende tjenester.

A.14.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)

Behandlingen omfatter registrering, lagring, overførsel, visning, ændring og sletning af personoplysninger i forbindelse med oprettelse og administration af brugere, telefonnumre, kontakt-oplysninger, samt logning af opkald og supporthenvendelser.

A.14.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Behandlingen kan omfatte følgende typer af personoplysninger:

Almindelige personoplysninger:

- Identifikationsoplysninger (f.eks. navn, brugernavn, e-mailadresse)
- Kontaktoplysninger (f.eks. telefonnummer, adresse)
- Oplysninger om brug af telefoni (f.eks. opkaldslog, varighed, tidspunkt, destination)
- Tekniske data (f.eks. IP-adresse, enhedsoplysninger)
- Support- og henvendelsesdata

A.14.4. Behandlingen omfatter følgende kategorier af registrerede

- **Kunder** Personer, som er eller har været kunder/medlemmer/klienter/patienter hos den dataansvarlige, eller er potentielle kunder/medlemmer/klienter/patienter
- **Ansatte** Personer, som er eller har været ansatte/bestyrelses-medlemmer hos den dataansvarlige, eller er nye jobansøgere.
- **Leverandører** Personer som er eller har været forretningsforbindelser, herunder leverandører og samarbejdspartnere hos den dataansvarlige, eller er potentielle forretningsforbindelser

A.14.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen har følgende varighed

Behandlingen er ikke tidsbegrænset og varer, indtil Bestemmelserne opsiges eller ophæves af en af partner. Bestemmelserne skal dog forblive i kraft frem til det tidspunkt, hvor databehandleren ikke længere behandler personoplysninger på vegne af den dataansvarlige.

A.15.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Formålet med databehandlerens behandling af personoplysninger er at levere og drifte SOC-tjenester (Security Operations Center), herunder overvågning, detektion og håndtering af sikkerhedshændelser, trusselsjagt, logning og rapportering.

Tjenesten understøtter den dataansvarliges behov for løbende beskyttelse af IT-miljøet, herunder hurtig reaktion på sikkerhedstrusler.

A.15.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)

Behandlingen omfatter indsamling, overvågning, analyse, lagring og rapportering af sikkerhedsrelevante data, herunder logfiler, hændelsesdata, netværkstrafik og brugeraktiviteter. Derudover indgår trusselsvurdering, hændeshåndtering, teknisk support og samarbejde med den dataansvarlige ved konstaterede eller mistænkte sikkerhedshændelser.

A.15.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Behandlingen kan omfatte følgende typer af personoplysninger:

Almindelige personoplysninger:

- Identifikationsoplysninger (f.eks. navn, brugernavn, e-mailadresse)
- Kontaktoplysninger (f.eks. telefonnummer, arbejdssted)
- Logdata og hændelsesdata (f.eks. IP-adresse, loginhistorik, adgangsforsøg, netværkstrafik)
- Metadata om systemadgang, enheder og applikationer
- Oplysninger om brugeradfærd og sikkerhedshændelser

A.15.4. Behandlingen omfatter følgende kategorier af registrerede

- **Ansatte** Personer, som er eller har været ansatte/bestyrelsesmedlemmer hos den dataansvarlige, eller er nye jobansøgere.
- **Leverandører** Personer som er eller har været forretningsforbindelser, herunder leverandører og samarbejdspartnere hos den dataansvarlige, eller er potentielle forretningsforbindelser

A.15.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen har følgende varighed

Behandlingen er ikke tidsbegrænset og varer, indtil Bestemmelserne opsiges eller ophæves af en af partner. Bestemmelserne skal dog forblive i kraft frem til det tidspunkt, hvor databehandleren ikke længere behandler personoplysninger på vegne af den dataansvarlige.

A.16.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Formålet med databehandlerens behandling af personoplysninger er at levere og drifte managed videoovervågningstjenester, herunder overvågning, optagelse, lagring og adgang til video- og eventuelt lydoptagelser fra kameraer installeret hos den dataansvarlige.

Tjenesten understøtter den dataansvarliges behov for sikkerhed og kriminalitetsforebyggelse.

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

Behandlingen omfatter indsamling, lagring, visning, overførsel, sletning og eventuel analyse af billed- og lydoptagelser fra videoovervågningsudstyr. Derudover indgår logning af adgang til optagelser, teknisk support og sikkerhedsovervågning.

A.16.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Behandlingen kan omfatte følgende typer af personoplysninger:

Almindelige personoplysninger:

- Billed- og lydoptagelser af personer (video og evt. lyd)
- Identifikationsoplysninger (f.eks. navn, brugernavn, hvis adgang til systemet logges)
- Metadata (f.eks. tidspunkt, lokation, kamera-ID, adgangslogs)
- Oplysninger om brugeradfærd og hændelser registreret via overvågningen

A.16.4. Behandlingen omfatter følgende kategorier af registrerede

- **Kunder** Personer, som er eller har været kunder/medlemmer/klienter/patienter hos den dataansvarlige, eller er potentielle kunder/medlemmer/klienter/patienter
- **Ansatte** Personer, som er eller har været ansatte/bestyrelsesmedlemmer hos den dataansvarlige, eller er nye jobansøgere.
- **Leverandører** Personer som er eller har været forretningsforbindelser, herunder leverandører og samarbejdspartnere hos den dataansvarlige, eller er potentielle forretningsforbindelser
- **Øvrige personer** Personer der færdes i eller omkring de overvågede områder.

A.16.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen har følgende varighed

Behandlingen er ikke tidsbegrænset og varer, indtil Bestemmelserne opsiges eller ophæves af en af partner. Bestemmelserne skal dog forblive i kraft frem til det tidspunkt, hvor databehandleren ikke længere behandler personoplysninger på vegne af den dataansvarlige.

A.17.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Formålet med databehandlerens behandling af personoplysninger er at levere og drifte MDM-tjenester, herunder administration, konfiguration, sikring og overvågning af mobile enheder, så den dataansvarlige kan beskytte virksomhedens data effektivt styre den dataansvarliges mobile enheder.

A.17.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)

Behandlingen omfatter lagring, visning, overførsel, opdatering og sletning af personoplysninger i forbindelse med administration af mobile enheder. Dette inkluderer fjernkonfiguration, applikationsstyring, sikkerhedspolitikker, overvågning af enhedsstatus, logning af hændelser, samt mulighed for fjernsletning eller låsning af enheder ved tab eller tyveri.

A.17.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Behandlingen kan omfatte følgende typer af personoplysninger:

Almindelige personoplysninger:

- Identifikationsoplysninger (f.eks. navn, brugernavn, e-mailadresse)
- Enhedsoplysninger (f.eks. enheds-ID, serienummer, model, operativsystem)
- Kontaktoplysninger (f.eks. telefonnummer, adresse)
- Lokationsdata (hvis aktiveret)
- Applikations- og konfigurationsdata
- Logdata og hændelsesdata (f.eks. loginhistorik, sikkerhedshændelser)
- Metadata om brug og status på enheden

A.17.4. Behandlingen omfatter følgende kategorier af registrerede

- **Ansatte** Personer, som er eller har været ansatte/bestyrelsesmedlemmer hos den dataansvarlige, eller er nye jobansøgere.

A.17.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen har følgende varighed

Behandlingen er ikke tidsbegrænset og varer, indtil Bestemmelserne opsiges eller ophæves af en af partner. Bestemmelserne skal dog forblive i kraft frem til det tidspunkt, hvor databehandleren ikke længere behandler personoplysninger på vegne af den dataansvarlige.

Formålet med databehandlerens behandling af personoplysninger er at levere og drifte security awareness training, herunder e-læring, phishing-simulationer og rapportering, med henblik på at styrke medarbejdernes viden om informationssikkerhed og reducere risikoen for menneskelige fejl.

A.18.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Formålet med databehandlerens behandling af personoplysninger er at levere og drifte security awareness training, herunder e-læring, phishing-simulationer og rapportering, med henblik på at styrke medarbejdernes viden om informationssikkerhed og reducere risikoen for menneskelige fejl.

A.18.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)

Behandlingen omfatter lagring, brug og sletning af personoplysninger i forbindelse med oprettelse af brugere, tildeling af kurser, gennemførelse af awareness-træning, afvikling af phishing-simulationer, logging af kursusaktiviteter og udarbejdelse af rapporter til den dataansvarlige.

A.18.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Behandlingen kan omfatte følgende typer af personoplysninger:

Almindelige personoplysninger:

- Identifikationsoplysninger (f.eks. navn, e-mailadresse, brugernavn)
- Kursus- og træningsdata (f.eks. gennemførte kurser, testresultater, kursusfremmøde)
- Logdata og aktivitetsdata (f.eks. tidspunkt for login, gennemførte simulationer, klik på phishing-links)
- Metadata om brugerens adfærd under træning

A.18.4. Behandlingen omfatter følgende kategorier af registrerede

- **Ansatte** Personer, som er eller har været ansatte/bestyrelsesmedlemmer hos den dataansvarlige, eller er nye jobansøgere.

A.18.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser i krafttræden. Behandlingen har følgende varighed

Behandlingen er ikke tidsbegrænset og varer, indtil Bestemmelserne opsiges eller ophæves af en af partner. Bestemmelserne skal dog forblive i kraft frem til det tidspunkt, hvor databehandleren ikke længere behandler personoplysninger på vegne af den dataansvarlige.

Bilag A.19 Oplysninger om behandlingen – Uniconta

A.19.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

Formålet med databehandlerens behandling af personoplysninger er at levere og drifte Uniconta ERP-systemet, herunder bogføring, regnskab, økonomistyring, lagerstyring, fakturering, rapportering og relaterede administrative funktioner.

Behandlingen understøtter den dataansvarliges behov for effektiv økonomistyring.

A.19.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen)

Behandlingen omfatter registrering, lagring, visning, overførsel, ændring, anonymisering og sletning af personoplysninger i forbindelse med økonomiske transaktioner, kunde- og leverandørstyring, lønadministration, rapportering og teknisk support.

A.19.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede

Behandlingen kan omfatte følgende typer af personoplysninger:

Almindelige personoplysninger:

- Identifikationsoplysninger (f.eks. navn, adresse, e-mail, telefonnummer, CVR/CPR-nummer)
- Økonomiske oplysninger (f.eks. fakturaer, betalingsoplysninger, kontonumre, lønoplysninger)
- Transaktionsdata (f.eks. bilag, posteringer, regnskabsdata)
- Brugerdata (f.eks. brugernavn, adgangsrettigheder, logdata)
- Metadata om brug og status på systemet

Fortrolige personoplysninger:

- CPR-nummer i det omfang det er nødvendigt for at opfylde formålet med behandlingen

A.19.4. Behandlingen omfatter følgende kategorier af registrerede

- **Kunder** Personer, som er eller har været kunder/medlemmer/klienter/patienter hos den dataansvarlige, eller er potentielle kunder/medlemmer/klienter/patienter
- **Ansatte** Personer, som er eller har været ansatte/bestyrelsesmedlemmer hos den dataansvarlige, eller er nye jobansøgere.
- **Leverandører** Personer som er eller har været forretningsforbindelser, herunder leverandører og samarbejdspartnere hos den dataansvarlige, eller er potentielle forretningsforbindelser

A.19.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelser ikrafttræden. Behandlingen har følgende varighed

Side 38 af 52

Behandlingen er ikke tidsbegrænset og varer, indtil Bestemmelserne opsiges eller ophæves af en af partner. Bestemmelserne skal dog forblive i kraft frem til det tidspunkt, hvor databehandleren ikke længere behandler personoplysninger på vegne af den dataansvarlig

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere, der er struktureret ud fra databehandlerens tjenester.

TJENESTER	LEVERANDØR, CVR/ORG.NR, ADRESSE OG KONTAKTPERSON	BEHANDLINGSAKTIVITET	DATAPLACERING	OVERFØRSELSGRUNDLAG/TILSTRÆKKELIGE SIKKERHEDSFORANSTALTNINGER (NON- EU/EEA)
Microsoft 365	Microsoft Org.nr. 256796 One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521 Ireland	Hosting Databehandleren behandler personoplysninger i forbindelse med hosting af e-mail, dokumenter og samarbejdsplatforme. Behandlingen omfatter brugerkontodata, e-mails og dokumenter. Data lagres i EU, medmindre andet er valgt under opsætningen.	Irland	Overførslen sker på baggrund af EU-Kommissionens standardkontraktbestemmelser og EU-U.S. Data Privacy Framework.
Adobe Cloud	Adobe 345 Park avenue San Jose CA 95110-2704 USA	Licenser Datahandleren behandler loginoplysninger og brugerdata i forbindelse med anvendelse af Adobe Cloud. Behandlingen omfatter navn og e-mailadresser.	USA	Overførslen sker på baggrund af EU-Kommissionens standardkontraktbestemmelser og EU-U.S. Data Privacy Framework.
Microsoft Azure	Microsoft Org.nr. 256796 One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521	Hosting Databehandleren behandler personoplysninger i forbindelse med hosting af systemer og data på Microsoft Azure. Behandlingen kan omfatte almindelige og følsomme personoplysninger i det omfang, de indlæses af den dataansvarlige. Data lagres i EU, medmindre andet er valgt under opsætningen.	Irland	Overførslen sker på baggrund af EU-Kommissionens standardkontraktbestemmelser og EU-U.S. Data Privacy Framework.

TJENESTER	LEVERANDØR, CVR/ORG.NR, ADRESSE OG KONTAKTPERSON	BEHANDLINGSAKTIVITET	DATAPLACE-RING	OVERFØRSELSGRUND-LAG/TILSTRÆKKELIGE SIK-KERHEDSFORANSTALTNIN-GER (NON- EU/EEA)
	Ireland			
Webhotel	Curanet CVR-nr. 29412006 Højvangen 4, 8660 Skanderborg GDPR-kontakt: compliance@curanet.dk	Hosting Databehandleren behandler personoplysninger i forbindelse med hosting af hjemmesider og webapplikationer. Behandlingen kan omfatte almindelige oplysninger indtastet via webformularer.	Danmark	N/A
Event	Datto 250 Longwater Avenue, Green Park, Reading RG2 6GB Storbritannien GDPR-kontakt: legal@kaseya.com	Overvågning Databehandleren behandler personoplysninger i forbindelse med overvågning af systemer og hændelser. Behandlingen omfatter logfiler og systembrugerdata. Data lagres i EU.	Storbritan-nien	Overførsel af personoplysninger til Storbritannien sker på baggrund af Europa-Kommissionens tilstrækkelighedsafgørelse for Storbritannien, jf. artikel 45 i databeskyttelsesforordningen (GDPR).
Cloud Backup	Datto 250 Longwater Avenue, Green Park, Reading RG2 6GB Storbritannien GDPR-kontakt: legal@kaseya.com N-Able 30 Corporate Drive, Suite 400, Burlington MA 01803	Backup data via Datto Databehandleren behandler personoplysninger i forbindelse med backup af data via Datto. Behandlingen omfatter kopier af den dataansvarliges system- og brugerdata. Data lagres i Tyskland og Island. Backup data via N-Able Databehandleren behandler personoplysninger i forbindelse med backup af data via N-Able. Behandlingen omfatter kopier	Tyskland og Island Holland	Overførslen sker på baggrund af EU-Kommissionens standardkontraktbestemmelser og EU-U.S. Data Privacy Framework.

TJENESTER	LEVERANDØR, CVR/ORG.NR, ADRESSE OG KONTAKTPERSON	BEHANDLINGSAKTIVITET	DATAPLACERING	OVERFØRSELSGRUNDLAG/TILSTRÆKKELIGE SIKKERHEDSFORANSTALTNINGER (NON- EU/EEA)
	USA GDPR-kontakt: privacy@n-able.com	af den dataansvarliges system- og brugerdata. Data lagres i Holland.		
BCDR	Datto 250 Longwater Avenue, Green Park, Reading RG2 6GB Storbritannien GDPR-kontakt: legal@kaseya.com	Backup data Databehandleren behandler personoplysninger i forbindelse med backup- og disaster recovery-løsninger. Behandlingen omfatter kopier af kundedata og systemdata. Data lagres i Tyskland og Island.	Tyskland og Island	N/A
Microsoft 365 Backup	Datto 250 Longwater Avenue, Green Park, Reading RG2 6GB Storbritannien GDPR-kontakt: legal@kaseya.com	Backup data Databehandleren behandler personoplysninger i forbindelse med backup af Microsoft 365-data. Behandlingen omfatter e-mails, dokumenter og brugerkontodata. Data lagres i Tyskland.	Tyskland	N/A
Antispam	VIPRE Juridisk navn: Ziff Davis Denmark A/S CVR-nummer: 28117833 Adresse: Delta Park 40, 1.th., 2665 Valensbæk Strand Irsk DPO-kontakt: dpo@vipre.com	Maildata Databehandleren behandler personoplysninger i forbindelse med filtrering og behandling af maildata. Behandlingen omfatter e-mailindhold, metadata samt afsender- og modtageroplysninger. Data lagres i Danmark.	Danmark	N/A

TJENESTER	LEVERANDØR, CVR/ORG.NR, ADRESSE OG KONTAKTPERSON	BEHANDLINGSAKTIVITET	DATAPLACERING	OVERFØRSELSGRUNDLAG/TILSTRÆKKELIGE SIKKERHEDSFORANSTALTNINGER (NON- EU/EEA)
Sikker Mail	<p>Logiva A/S CVR-nr. 21724273 Skæringsvej 110 2, 8520 Lystrup GDPR-kontakt: dpo@j2.com</p> <p>VIPRE Juridisk navn: Ziff Davis Denmark A/S CVR-nummer: 28117833 Adresse: Delta Park 40, 1.th., 2665 Valensbæk Strand</p> <p>Irsk DPO-kontakt: dpo@vipre.com</p>	<p>Maildata via Logiva Databehandleren behandler personoplysninger i forbindelse med sikker mailhåndtering via Logiva. Behandlingen omfatter mailindhold og metadata. Data lagres i Danmark.</p> <p>Maildata via VIPRE Databehandleren behandler personoplysninger i forbindelse med sikker mailhåndtering via VIPRE. Behandlingen omfatter mailindhold og metadata. Data lagres i Danmark.</p>	Danmark	N/A
Email signatur	<p>CodeTwo Wolnosci 16 58-300 Jenia Gora Polen https://www.codetwo.com/form/data-protection/</p> <p>Exclaimer 250 Fowler Avenue, 3rd Floor, Farnborough Hampshire GU14 7JP United Kingdom GDPR: infosec@exclaimer.com</p>	<p>Signaturadministration via CodeTwo Databehandleren behandler personoplysninger i forbindelse med tilføjelse af e-mailsignaturer via CodeTwo. Behandlingen omfatter brugeroplysninger som navn, titel og kontaktoplysninger. Data lagres i Nordeuropa.</p> <p>Signaturadministration via Exclaimer Databehandleren behandler personoplysninger i forbindelse med tilføjelse af e-mailsignaturer. Behandlingen omfatter brugeroplysninger som navn, titel og kontakt-oplysninger. Data lagres i Tyskland.</p>	Nordeuropa Tyskland	N/A

TJENESTER	LEVERANDØR, CVR/ORG.NR, ADRESSE OG KONTAKTPERSON	BEHANDLINGSAKTIVITET	DATAPLACE-RING	OVERFØRSELSGRUND-LAG/TILSTRÆKKELIGE SIK-KERHEDSFORANSTALTNIN-GER (NON- EU/EEA)
MFA	Cisco 3098 Olsen Drive San Jose CA 95134 USA https://privacyrequest.cisco.com/	Brugeroplysninger Databehandleren behandler personoplysninger i forbindelse med multifaktor-login og identitetssikring. Behandlingen omfatter brugeridentitet, loginoplysninger og evt. mobilnummer eller token. Data lagres i Irland.	Irland	Overførslen sker på baggrund af EU-Kommissionens standardkontraktbestemmelser og EU-U.S. Data Privacy Framework.
Datto Work-place	Datto 250 Longwater Avenue, Green Park, Reading RG2 6GB Storbritannien GDPR-kontakt: legal@kaseya.com	Data Databehandleren behandler personoplysninger i forbindelse med cloud-baseret fildeling og samarbejde. Behandlingen omfatter brugerkontodata, filer og dokumenter. Data lagres i Storbritannien.	Storbritannien	Overførsel af personoplysninger til Storbritannien sker på baggrund af Europa-Kommissionens tilstrækkelighedsafgørelse for Storbritannien, jf. artikel 45 i databeskyttelsesforordningen (GDPR).
Flexfone Tele-foni	Flexfone CVR-nr. 34042985 Danmarksvej 26, 8660 Skanderborg GDPR-kontakt: gdpr@flexfone.dk	Telefoniadministration Databehandleren behandler personoplysninger i forbindelse med telefoni- og kommunikationsløsninger. Behandlingen omfatter telefonnumre, samtalelogs og eventuelle voicemails. Data lagres i Danmark.	Danmark	N/A
SOC	Datto 250 Longwater Avenue, Green Park, Reading RG2 6GB Storbritannien	Aktivitetslogs Databehandleren behandler personoplysninger i forbindelse med overvågning af systemaktiviteter. Behandlingen omfatter logfiler og aktivitetsdata. Data lagres i Storbritannien.	Storbritannien	Overførsel af personoplysninger til Storbritannien sker på baggrund af Europa-Kommissionens tilstrække-

TJENESTER	LEVERANDØR, CVR/ORG.NR, ADRESSE OG KONTAKTPERSON	BEHANDLINGSAKTIVITET	DATAPLACE-RING	OVERFØRSELSGRUND-LAG/TILSTRÆKKELIGE SIKKERHEDSFORANSTALTNINGER (NON- EU/EEA)
	GDPR-kontakt: legal@kaseya.com			lighedsafgørelse for Storbritannien, jf. artikel 45 i databeskyttelsesforordningen (GDPR).
Managed Video-overvågning	Cisco 3098 Olsen Drive San Jose CA 95134 USA https://privacyrequest.cisco.com/	Optagelser Databehandleren behandler personoplysninger i forbindelse med drift af videoovervågning. Behandlingen omfatter videooptagelser af personer. Data lagres i SUA og overførslen sker på baggrund af EU-Kommissionens standardkontraktbestemmelser.	USA	Overførslen sker på baggrund af EU-Kommissionens standardkontraktbestemmelser og EU-U.S. Data Privacy Framework.
MDM	Miradore Laserkatu 8 53850 Lappeenranta Finland Kontakt Support omkring GDPR: https://support.goto.com/contact? ics=1760342196131&ir-clickid=~16406bhja6156-gmlmcja343QSUXOR-HCINKLBCrpgcb4WPlyugh	Enhedsadministration Databehandleren behandler personoplysninger i forbindelse med Mobile Device Management. Behandlingen omfatter bruger- og enhedsdata, herunder login, device ID og konfigurationsoplysninger. Data lagres i Tyskland.	Tyskland	N/A
Security Awareness Training	VIPRE Juridisk navn: Ziff Davis Denmark A/S CVR-nummer: 28117833	Brugeroplysninger Databehandleren behandler personoplysninger i forbindelse med sikkerhedstræning og simulering af sikkerhedsadfærd.	Danmark	N/A

TJENESTER	LEVERANDØR, CVR/ORG.NR, ADRESSE OG KONTAKTPERSON	BEHANDLINGSAKTIVITET	DATAPLACERING	OVERFØRSELSGRUNDLAG/TILSTRÆKKELIGE SIKKERHEDSFORANSTALTNINGER (NON- EU/EEA)
	Adresse: Delta Park 40, 1.th., 2665 Valensbæk Strand Irsk DPO-kontakt: dpo@vipre.com	Behandlingen omfatter oplysninger om brugere såsom navn, e-mail og træningsdata. Data lagres i Danmark.		
Uniconta	Uniconta A/S CVR-nr. 33266928 Ørestads Boulevard 73, 2300 København S GDPR-ansvarlig: info@uniconta.com	Økonomidata Databehandleren behandler personoplysninger i forbindelse med økonomisystemet Uniconta. Behandlingen omfatter økonomidata, kundedata og leverandørdata. Data lagres i Danmark.	Danmark	N/A

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandlere for den beskrevne behandlingsaktivitet. Databehandleren må ikke – uden den dataansvarliges skriftlige godkendelse – gøre brug af en underdatabehandler til en anden behandlingsaktivitet end den beskrevne og aftalte eller gøre brug af en anden underdatabehandler til denne behandlingsaktivitet

Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker i overensstemmelse med denne instruks samt de til enhver tid gældende salgs- og leveringsbetingelser, som udgør en integreret del af hovedaftalen mellem parterne.

C.1.1 Behandlingens genstand/instruks – Microsoft 365

Databehandleren behandler personoplysninger på vegne af den dataansvarlige med det formål at levere, drifte, vedligeholde og supportere Microsoft 365-tjenester. Behandlingen omfatter aktiviteter, der skal sikre funktionalitet, sikkerhed, tilgængelighed og løbende optimering af de aftalte Microsoft 365-tjenester.

C.1.2 Behandlingens genstand/instruks – Adobe Cloud

Databehandleren behandler personoplysninger på vegne af den dataansvarlige med det formål at levere og understøtte adgang til Adobe Cloud-tjenester. Behandlingen sker for at muliggøre den dataansvarliges anvendelse af Adobe Cloud i forbindelse med interne forretningsprocesser og kundevedtatte aktiviteter.

C.1.3 Behandlingens genstand/instruks – Microsoft Azure

Databehandleren behandler personoplysninger på vegne af den dataansvarlige med det formål at levere og understøtte adgang til Microsoft Azure-tjenester. Behandlingen sker for at sikre skalerbar, sikker og effektiv databehandling i overensstemmelse med den dataansvarliges instrukser.

C.1.4 Behandlingens genstand/instruks – Webhotel

Databehandleren behandler personoplysninger på vegne af den dataansvarlige med det formål at levere og drifte webhotel-tjenester. Behandlingen sker for at sikre stabil og sikker drift af den dataansvarliges digitale tilstedeværelse.

C.1.5 Behandlingens genstand/instruks – Event

Databehandleren behandler personoplysninger på vegne af den dataansvarlige med det formål at levere og drifte Event Management-tjenester. Behandlingen sker for at sikre stabil drift, identificere fejl og hændelser samt understøtte den dataansvarliges IT-sikkerhed og forretningskontinuitet.

C.1.6 Behandlingens genstand/instruks – Cloud Backup

Databehandleren behandler personoplysninger på vegne af den dataansvarlige med det formål at levere og drifte cloud backup-løsninger, som sikrer kontinuerlig beskyttelse, gendannelse og tilgængelighed af data.

C.1.7 Behandlingens genstand/instruks – BCDR

Databehandleren behandler personoplysninger på vegne af den dataansvarlige med det formål at levere og drifte BCDR-tjenester, herunder backup, gendannelse og sikring af data i tilfælde af systemnedbrud, cyberangreb eller anden form for datatab.

C.1.8 Behandlingens genstand/instruks – Microsoft 365 backup

Databehandleren behandler personoplysninger på vegne af den dataansvarlige med det formål at levere og drifte backup-tjenester for Microsoft 365, herunder Exchange Online, SharePoint, OneDrive og Teams.

C.1.9 Behandlingens genstand/instruks – Antispam

Databehandleren behandler personoplysninger på vegne af den dataansvarlige med det formål at levere og drifte antispam-tjenester. Behandlingen sker for at beskytte e-mailkommunikationen mod uønskede og skadelige beskeder samt sikre dens integritet og tilgængelighed.

C.1.10 Behandlingens genstand/instruks – Sikker mail

Databehandleren behandler personoplysninger på vegne af den dataansvarlige med det formål at levere og drifte sikker mail-tjenester. Behandlingen sker for at beskytte fortrolige og følsomme oplysninger under elektronisk kommunikation.

C.1.11 Behandlingens genstand/instruks – Email signatur

Databehandleren behandler personoplysninger på vegne af den dataansvarlige med det formål at levere og drifte e-mail signaturtjenester. Behandlingen sker for at understøtte den dataansvarliges behov for ensartet branding i e-mailkorrespondance.

C.1.12 Behandlingens genstand/instruks – MFA

Databehandleren behandler personoplysninger på vegne af den dataansvarlige med det formål at levere og drifte MFA-tjenester (Multifaktor-autentifikation). Behandlingen sker for at beskytte adgangen til den dataansvarliges systemer, applikationer og data.

C.1.13 Behandlingens genstand/instruks – Datto Workplace

Databehandleren behandler personoplysninger på vegne af den dataansvarlige med det formål at levere og drifte Datto Workplace-tjenester. Behandlingen sker for at understøtte den dataansvarliges behov for sikker og effektiv håndtering af dokumenter.

C.1.14 Behandlingens genstand/instruks – Flexfone telefoni

Databehandleren behandler personoplysninger på vegne af den dataansvarlige med det formål at levere og drifte telefoni- og kommunikationsløsninger via Flexfone. Behandlingen sker for at sikre stabil og sikker drift af den dataansvarliges telefoni og tilhørende tjenester.

C.1.15 Behandlingens genstand/instruks – SOC

Databehandleren behandler personoplysninger på vegne af den dataansvarlige med det formål at levere og drifte SOC-tjenester (Security Operations Center). Behandlingen sker for at understøtte den dataansvarliges behov for løbende beskyttelse af IT-miljøet, herunder hurtig reaktion på sikkerhedstrusler.

C.1.16 Behandlingens genstand/instruks – Managed Videoovervågning

Databehandleren behandler personoplysninger på vegne af den dataansvarlige med det formål at levere og drifte managed videoovervågningstjenester. Behandlingen sker for at understøtte den dataansvarliges behov for sikkerhed og kriminalitetsforebyggelse.

C.1.17 Behandlingens genstand/instruks – MDM

Databehandleren behandler personoplysninger på vegne af den dataansvarlige med det formål at levere og drifte MDM-tjenester (Mobile Device Management). Behandlingen sker for at beskytte virksomhedens data og effektivt styre den dataansvarliges mobile enheder.

C.1.18 Behandlingens genstand/instruks – Security Awareness Training

Databehandleren behandler personoplysninger på vegne af den dataansvarlige med det formål at levere og drifte security awareness training. Behandlingen sker for at styrke medarbejdernes viden om informationssikkerhed og reducere risikoen for menneskelige fejl.

C.1.19 Behandlingens genstand/instruks – Uniconta

Databehandleren behandler personoplysninger på vegne af den dataansvarlige med det formål at levere og drifte Uniconta ERP-systemet. Behandlingen sker for at understøtte den dataansvarliges behov for effektiv økonomistyring.

C.2. Behandlingssikkerhed

Databehandleren har implementeret en række generelle tekniske og organisatoriske sikkerhedsforanstaltninger, som gælder på tværs af alle leverede tjenester:

Generelle sikkerhedsforanstaltninger:

Tekniske sikkerhedsforanstaltninger (interne):

- Opdateret antivirus på alle enheder der kan tilgå personoplysninger.
- Opdateret firewall på enheder der kan tilgå personoplysninger samt på servere/driftscentre der måtte holde personoplysninger.
- Passwords udskiftes regelmæssigt eller sikres på anden måde.
- Multifaktor-autentifikation (MFA) ved adgang til systemer og data, hvor det er teknisk muligt og relevant.
- Løbende opdatering af operativsystemer og applikationer
- Ved overførsel af fortrolige, følsomme eller særlige personoplysninger benyttes kryptering
- Operationelt Security Operations Center (SOC)

Organisatoriske sikkerhedsforanstaltninger:

- Alle medarbejdere er instrueret i beskyttelsen af personoplysninger.
- Alle medarbejdere er pålagt tavshedspligt.
- Det overordnede ansvar for overholdelse af sikkerhedskravene, ligger ved databehandlerens ledelse.
- Personoplysninger er kun tilgængelige for de medarbejdere der har en godkendelse og årsag til at skulle kunne tilgå disse data, og skal altid behandles fortroligt.
- Rollebaseret adgang til systemer og data og begrænsning af adgang efter princippet om least privilege.
- Regelmæssig gennemgang og revurdering af adgangsrettigheder
- Løbende træning og uddannelse i informationssikkerhed og databeskyttelse for medarbejdere.
- Leverandørstyring, herunder løbende vurdering og kontrol med underdatabehandlere
Procedurer for incident response og håndtering af brud på persondatasikkerheden.

Fysiske sikkerhedsforanstaltninger hos databehandlerens lokationer:

- Kontorer og bygninger aflåses, når de forlades.
- Sikre at driften kan fortsætte ved strømafbrydelser og evt. redundante kommunikationsforbindelser
- Arkiver med følsomme personoplysninger opbevares altid aflåst, hvor der ligeledes er alarm og overvågning etableret.
- Backup opbevares aflåst (både interne og eksterne), der laves en løbende genindlæsningstest, så det sikres, at backuppen virker og indeholder valide data.
- Alle fysiske medier (papir, USB drev mv.) destrueres på forsvarlig vis, hvis de har været benyttet til at opbevare personoplysninger.

Sikkerhedsforanstaltninger hos underdatabehandlere:

Databehandleren anvender godkendte underdatabehandlere til levering af tjenester. På grund af karakteren af databehandlerens tjenester vil underdatabehandlerne ofte forestå implementering af en væsentlig del af de relevante tekniske og organisatoriske sikkerhedsforanstaltninger.

Dokumentation for underdatabehandlerens sikkerhedsforanstaltninger, herunder relevante revisionsrapporter og certificeringer, kan udleveres til den dataansvarlige efter anmodning.

Underdatabehandlere er typisk:

- ISO/IEC 27001-certificerede, hvilket dokumenterer, at de har et implementeret og auditeret informationssikkerhedsstyringssystem.
- Underlagt relevante og uafhængige revisioner, herunder ISAE 3000, ISAE 3402 eller SOC 2, som dokumenterer deres kontrolmiljø og sikkerhedsforanstaltninger.

C.3 Bistand til den dataansvarlige

Databehandleren bistår den dataansvarlige med at overholde sine forpligtelser i henhold til databeskyttelsesforordningens artikel 32-36 samt kapitel III, i det omfang det er muligt og rimeligt under hensyntagen til behandlingens karakter.

Dette indebærer blandt andet, at databehandleren:

- stiller logfiler, systemoplysninger og sikkerhedsrapporter til rådighed, som kan anvendes i forbindelse med registreredes anmodninger om indsigt, berigtigelse, sletning, begrænsning eller dataportabilitet,
- bistår den dataansvarlige med at tilvejebringe den information, der er nødvendig ved anmeldelse af brud på persondatasikkerheden,
- giver den dataansvarlige adgang til relevante oplysninger, der kan bruges til gennemførelse af konsekvensanalyser (DPIA'er) og forudgående høringer hos Datatilsynet,
- tilvejebringer dokumentation for tekniske og organisatoriske sikkerhedsforanstaltninger samt eventuelle revisionsrapporter fra egne underdatabehandlere, når den dataansvarlige anmoder om dette.

C.4 Opbevaringsperiode/sletterutine

Personoplysninger opbevares hos databehandleren, indtil den dataansvarlige anmoder om at få oplysningerne slettet eller tilbageleveret, medmindre andet er aftalt i Bilag D, hovedaftalen eller i særlige vilkår.

Ved ophør af tjenesten vedrørende behandling af personoplysninger skal databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med bestemmelse 11.1.

For tjenesterne Cloud Backup og BCDR, sker sletning i takt med, at data udfases i henhold til den pågældende tjentes retention-politik. Data slettes endeligt, når backupcyklusser er udløbet, og det er teknisk muligt at fjerne data.

Arbejdet med sletning eller tilbagelevering af personoplysninger ved ophør af tjenester faktureres særskilt til den dataansvarlige efter medgået tid i henhold til databehandlerens til enhver tid gældende timepriser.

C.5 Lokaltet for behandling

Behandling af personoplysninger må alene ske på databehandlerens egne lokationer i Danmark og Grønland samt på de lokaliteter, der fremgår af oversigten over underdatabehandlere i Bilag B.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Databehandleren må alene overføre personoplysninger til tredjelande, når dette sker gennem de underdatabehandlere, der fremgår af Bilag B, og kun i det omfang det er nødvendigt for leveringen af de beskrevne tjenester.

De pågældende overførsler er baseret på EU-Kommissionens standardkontraktbestemmelser eller et andet gyldigt overførselsgrundlag i henhold til databeskyttelsesforordningens kapitel V.

C.7 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren

Databehandleren skal én gang årligt og for egen regning indhente en erklæring eller inspektionsrapport fra en uafhængig tredjepart vedrørende databehandlerens overholdelse af databeskyttelsesforordningen, anden relevant EU-ret eller medlemsstaternes nationale ret samt denne databehandleraftale.

Parterne er enige om, at erklæringen/inspektionsrapporten kan udformes som følger: "En underskrevet erklæring fra en uafhængig tredjepart (navn, adresse, kontaktperson, telefon, e-mail og evt. DPO med angivelse af navn, adresse, telefonnummer og e-mail), der bekræfter at have gennemgået de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren har oplyst til den dataansvarlige i forbindelse med indgåelsen af denne databehandleraftale."

Der er enighed mellem parterne om, at følgende type af revisionserklæring kan anvendes i overensstemmelse med disse bestemmelser:

ISAE 3000.

Erklæringen/inspektionsrapporten skal uden unødigt forsinkelse stilles til rådighed for den dataansvarlige. Den dataansvarlige kan anfægte rammerne eller metoden for erklæringen/inspektionsrapporten og kan i sådanne tilfælde kræve, at der udarbejdes en ny erklæring/rapport efter andre rammer og/eller ved anvendelse af en anden metode.

På baggrund af erklæringen/rapporten er den dataansvarlige berettiget til at anmode databehandleren om yderligere foranstaltninger med henblik på at sikre overholdelse af gældende databeskyttelsesret og denne aftale.

Herudover har den dataansvarlige eller dennes repræsentant adgang til at foretage inspektioner, herunder fysiske inspektioner, af de lokaliteter og systemer, hvorfra databehandleren foretager behandling af personoplysninger. Inspektioner kan iværksættes, når den dataansvarlige finder det nødvendigt, dog baseret på saglige forhold og ikke på baggrund af formodninger.

Fysiske inspektioner kræver forudgående aftale med databehandleren og et varsel på tre uger, således at databehandleren kan afsætte de nødvendige ressourcer. Den dataansvarlige afholder egne omkostninger i forbindelse med inspektionen, mens databehandleren er forpligtet til at stille de nødvendige ressourcer (primært tid) til rådighed for gennemførelsen.

C.8 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere

Databehandleren skal minimum årligt for egen regning indhente en revisionserklæring eller relevant certificering fra en uafhængig tredjepart vedrørende underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Der er enighed mellem parterne om, at følgende typer af revisionserklæringer og certificeringer kan anvendes i overensstemmelse med disse bestemmelser:

ISAE 3000, ISAE 3402, SOC 1, SOC 2 og ISO 27001/27701 certificering.

Revisionserklæring og certificering fremsendes efter anmodning fra den dataansvarlige til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden i revisionserklæringen og kan i sådanne tilfælde anmode om en ny revisionserklæring under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af revisionserklæring, er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Se den mellem parterne indgåede hovedaftale/kontrakt.