Standardkontraktbestemmelser

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

mellem

IT Relation A/S
CVR 27001092
Dalgas Plads 7B 1. 2.
7400 Herning

herefter "den dataansvarlige"

og

Tricent Security Group A/S
CVR 38450255
Meldahlsgade 3
1613 København V

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. Præambel

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 software as a service værktøj til at give overblik over både interne og eksterne deling af filer i Onedrive, Sharepoint og Teams. 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 af 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.

2. 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 medlemsstaternes[1] nationale ret og disse Bestemmelser.

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.

3. 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.

4. 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

1

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.

5. 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.

6. 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 specifik skriftlig godkendelse.

3. Databehandleren må kun gøre brug af underdatabehandlere med den dataansvarliges forudgående specifikke skriftlige godkendelse. Databehandleren skal indgive anmodningen om en specifik godkendelse mindst 30 dage inden anvendelsen af den pågældende underdatabehandler. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

4. 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.

5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som derigennem 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 underdatabehandler aftalen, skal ikke sendes til den dataansvarlige.

6. Databehandleren skal i sin aftale med underdatabehandleren indføje den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandlere, som f.eks. gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.

7. 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.

7. 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.

8. Bistand til den dataansvarlige

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. Indsigtsretten

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

I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3., bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:

1. den dataansvarliges forpligtelse til uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder

2. den dataansvarliges forpligtelse til uden unødig forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder

3. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)

4. den dataansvarliges forpligtelse til at høre 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.

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.

9. Underretning om brud på persondatasikkerheden

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

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.

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.

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.

10. Sletning og returnering af oplysninger

Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at tilbagelevere alle personoplysningerne og slette eksisterende kopier, 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.

11. 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. Procedurerne 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.

12. 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.

13. Ikrafttræden og ophør

1. Bestemmelserne træder i kraft på datoen for begge parters 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. Underskrifter

På vegne af den dataansvarlige:

Navn: Lars Nielsen

Stilling: Cloud Transformation Manager

Telefon: +45 2389 5612

E-mail: lanie@itrelation.dk

Dato: 09 / 20 / 2022

Underskrift: 

På vegne af databehandleren:

Navn:	Michael Hove
Stilling:	Data Protection Officer
Telefon:	+45 23 66 53 55
Email:	mh@tricent.com
Dato:	08 / 26 / 2022
Underskrift	Michael Hove

14. Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

For datansvarlig:

Navn: Compliance & Security
E-mail: compliance@itm8.com

Ved underretning om brud på persondatasikkerheden skal følgende mailadresse altid kopieres: compliance@itm8.com

For databehandler:

Navn: Michael Hove

Stilling: Data Protection Officer

E-mail: mh@tricent.com

Bilag A Oplysninger om behandlingen

A.1. Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige:

1. Levering af data sharing compliance software løsning til dataansvarlig som processerer data i dataansvarlig's Microsoft 365 tenant.

A.2. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen):

1. At gøre Tricent for Microsoft 365 software løsning tilgængelig for dataansvarlig hvilket kræver processering af dataansvarlig's data i Microsoft 365 tenant.

A.3. Behandlingen omfatter følgende typer af personoplysninger om de registrerede:

Behandlingerne indeholder personoplysninger i de nedenfor afkrydsede kategorier.

Almindelige personoplysninger (jf. Databeskyttelsesforordningens artikel 6):

Navn, Email adresse, Adresse

Herunder almindelige personoplysninger, som behandles fortrolig, jf. straffelovens § 152 sammenholdt med forvaltningslovens § 27:

Ingen

Følsomme personoplysninger om, (jf. Databeskyttelsesforordningens artikel 9):

Ingen

Oplysninger om enkeltpersoners rent private forhold (jf. Databeskyttelsesforordningens artikel 10 samt Databeskyttelseslovens § 8):

Ingen

Oplysninger om cpr-nummer (jf. Databeskyttelseslovens § 11, jf. hjemlen til fastansættelse af national lovgivning herom i Databeskyttelsesforordningens artikel 87):

Ingen

A.4. Behandlingen omfatter følgende kategorier af registrerede

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

- Ansatte, leverandører, slutbrugere der anvender dataansvarligs Microsoft 365 tenant til at lagre data.

A.5. Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen har følgende varighed:

- Databehandling gælder så længe kontrakt til levering af Tricent for Microsoft 365 software løsning er aktiv og gældende.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN:	ADRESSE:	BESKRIVELSE AF BEHANDLING:
Microsoft	1 Microsoft Way, Redmond, WA98052 United States	Levering af behandlingsinfrastruktur, der understøtter driften af Tricent for Microsoft 365 SaaS-løsning
Confluent	899 West Evelyn Ave. Mountain View, CA 94041, United States	Levering af meddelelsesinfrastruktur, der understøtter driften af Tricent til Microsoft 365 SaaS-løsning
Sendgrid	375 Beale St Suite 300 San Francisco, CA, United States	Levering af e-mail-infrastruktur, der understøtter driften af Tricent for Microsoft 365 SaaS-løsning

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.

B.2. Varsel for godkendelse af underdatabehandlere

Som beskrevet i afsnit 7, 3 skal databehandleren give et varsel på mindst 30 dage.

Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks:

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende:

Dataansvarlig instruerer databehandler om at foretage behandling af IT Relation A/S personoplysninger til brug for levering af software as a service løsning Tricent for Microsoft 365 til brug for data sharing compliance kontrol af IT Relation A/S data i Mícrosoft 365 tenant.

C.2. Behandlingssikkerhed:

Sikkerhedsniveauet skal afspejle:

Data behandlingen omfatter ved normale omstændigheder udelukkende adgang til ikke særlig følsomme kategorier af persondata hvorfor sikkerhedsniveauet etableres som mellem-højt.

Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal gennemføres for at etableret det nødvendige (og aftalte) sikkerhedsniveau.

Databehandleren skal dog – under alle omstændigheder og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige:

Overordnede instruktioner:

1.1 Databehandleren skal som konsekvens af de forpligtelser, der fremgår af Databehandleraftalen, overholde de anvisninger vedrørende sikkerheds- og informations sikkerhedsforanstaltninger, der fremgår af dette bilag C for de systemer, der anvendes til at behandle Personoplysninger på vegne af den Dataansvarlige.

1.2 Databehandleren skal sikre løbende fortrolighed, integritet, tilgængelighed og modstandsdygtighed af databehandler systemer og -tjenester, som angivet i databehandleraftalen og dette bilag C.

1.3 Databehandleren skal udføre risikoanalyse for systemerne, inden systemerne tages i brug til at behandle personoplysninger på vegne af den dataansvarlige.

2 Fortrolighed:

2.1 Databehandleren skal implementere nedenstående foranstaltninger og processer:

2.1.1 Sikre brug af rollebaseret adgang og login til sektioner med Persondata (herunder mulighed for opfølgning på/justering af rollebaseret adgang) og at kun autoriserede enheder og relevante medarbejdere med et arbejdsrelateret behov for data behandling har adgang til personoplysningerne.

2.1.2 Hvis medarbejdere skifter job, skal Databehandler sikre , at de ikke bevarer adgangen til de personoplysninger, de havde brug for til deres tidligere job. Når Databehandler afskediger medarbejdere, skal det sikres for, at de ikke tager nogen forretningskritisk information, personlige data eller data relateret til personlige data med sig. Sikre, at ingen tidligere medarbejdere eller eksterne konsulenter har adgangsrettigheder til de systemer, der opbevarer personoplysningerne. Databehandler skal sikre sig at der periodisk gennemgås adgangsrettigheder med ejere af systemerne eller tjenesterne.

2.1.3 Sikre brugen af pseudonymisering og kryptering af de personlige data, hvor det er muligt, passende eller påkrævet ved lov.

2.1.4 Brug sikker/krypteret overførsel af de personlige data på det åbne internet, når de overførte personlige data ikke er beregnet til offentligheden.

2.1.5 Fysisk sikkerhed:

2.1.5.1 Monter passende låse eller andre fysiske betjeningsanordninger til døre og vinduer i rum, hvor computere opbevares.

2.1.5.2 Fysisk sikre uovervågede bærbare computere (for eksempel ved at låse dem i en sikker skuffe eller skab).

2.1.5.3 Sikre kontrol over og sikre alle flytbare medier, såsom flytbare harddiske, cd'er og USB-drev, der indeholder personlige data.

2.1.5.4 Ødelæg eller fjern permanent, uden mulighed for at gendanne, alle personlige data fra medier såsom cd'er, før de bortskaffes.

2.1.5.5 Sørg for, at alle personlige data er permanent fjernet, uden mulighed for gendannelse, fra harddiskene på brugte computere, før de bortskaffes.

2.1.5.6 Opbevar backup af de personlige data enten off-site eller i en brand- og vandtæt beholder.

2.1.6 Adgangskontrol:

2.1.6.1 Adgangskodeprocedurer skal være på plads, herunder brug af stærke adgangskoder, periodisk opdatering af adgangskoder og sikring af, at medarbejderne ikke skriver dem ned.

2.1.7 Logfiler:

2.1.7.1 Log mislykkede loginforsøg, herunder en log over tid, bruger osv., og bloker adgang efter et vist antal mislykkede loginforsøg for hver bruger.

2.1.7.2 Log brugeraktiviteter, herunder en log over tid, bruger, søgning, søgekriterier, adgang, ændring, luk, udskriv, eksport, sletning/sletning osv. og automatisk sletning af log efter et bestemt tidsinterval.

3 Integritet og tilgængelighed:

3.1 Databehandleren skal implementere nedenstående foranstaltninger og processer:

3.1.1 Beskyt netværk, systemer, logfiler og personlige data mod manipulation.

3.1.2 Sikre muligheden for at genoprette tilgængeligheden og adgangen til persondata rettidigt i tilfælde af en fysisk eller teknisk hændelse eller et persondata brud, herunder ved at sikkerhedskopiere data.

4 Modstandsdygtighed:

4.1 Databehandleren skal have et sårbarhedsstyringsprogram, herunder regelmæssig overvågning af potentielle sårbarheder og udførelse af penetrationstest af netværk og systemer, der anvendes til at behandle personoplysningerne.

4.1.1 Programmet til håndtering af sårbarheder skal omfatte, men er ikke begrænset til:

1. Udførelse af sårbarhedsscanninger på interne og eksterne perimeter mindst en gang i kvartalet
2. Udførelse af penetrationstest på eksterne netværksperimetre mindst kvartalsvis eller oftere i tilfælde af hændelser, der afslører et behov for sådanne tests
3. Opfølgning på og afhjælpning af eventuelle svagheder identificeret i forbindelse med sådanne scanninger og tests.

4.2 Databehandleren skal løbende holde netværk og systemer ajour med hensyn til nye versioner, opdateringer og patches.

5 Sikkerheds- og privatlivsteknologier

5.1 Databehandleren skal implementere nedenstående foranstaltninger og processer:

5.1.1 Sørg for, at alle anvendte computere har antivirus- eller anti-malware-software installeret, og virusdefinitionerne skal opdateres mindst en gang om ugen. Al indgående og udgående trafik skal scannes for virus, ligesom enhver disk eller cd, der bruges. Mindst en gang om ugen skal computere scannes for virus.

5.1.2 Hvor computere er forbundet til internettet, implementer en firewall, helst en næste generations firewall, anti-DDOS-detektering og et indtrængnings detekteringssystem.

6 Bevidsthed, træning og sikkerhedstjek i forhold til personale:

6.1 Databehandleren skal implementere nedenstående foranstaltninger og processer:

6.1.1 Udfør integritetstjek på alle nye medarbejdere for at sikre, at de ikke har løjet om deres baggrund, erfaring eller kvalifikationer.

6.1.2 Introducer nye medarbejdere til informationssikkerhed og sørg for, at de læser og forstår informationssikkerhedspolitikken. Sørg for, at medarbejderne ved, hvor de kan finde detaljer om informationssikkerhedsstandarder og -procedurer, der er relevante for deres roller og ansvar.

7 Incident Response Management og forretningskontinuitet:

7.1 Databehandleren skal implementere nedenstående foranstaltninger og processer:

7.1.1 Sørg for, at medarbejderne forstår, hvad et brud på persondatasikkerheden og en sikkerhedshændelse betyder, og træne medarbejderne i at genkende tegnene herpå og reagere passende. Udtrykket "Sikkerhedshændelse" betyder enhver begivenhed, der kan skade eller kompromittere fortroligheden, integriteten eller tilgængeligheden af forretningskritiske oplysninger eller systemer.

7.1.2 Databehandleren skal have en plan på plads for at sikre forretningskontinuitet i tilfælde af en alvorlig sikkerhedshændelse og skal teste planen mindst én gang om året. Efter en hændelse, hvor planen er brugt, og efter hver test, skal den revurderes og opdateres i henhold til erfaringerne.

C.3 Bistand til den dataansvarlige

Databehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

Der henvises til sektion C.2.

C.4 Opbevaringsperiode/sletterutine

Persondata opbevares udelukkende sålænge den kontraktuelle aftale mellem Dataansvarlig og Databehandler om at levere software as a service løsning Tricent for Microsoft 365 fortsat er aktiv og gældende.

Ved ophør af tjenesten vedrørende behandling af personoplysninger, skal databehandleren enten slette eller tilbagelevere personoplysningerne i overensstemmelse med bestemmelse 11.1, medmindre den dataansvarlige – efter underskriften af disse bestemmelser – har ændret den dataansvarlige oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til bestemmelserne."

C.5 Lokalitet for behandling

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

1. Tricent: EEA (Denmark)
2. Tricent medarbejders hjemmekontor: EEA (Denmark)
3. Azure: EEA (Western Europe)
4. Confluent EEA (Western Europe)
5. Sendgrid: EEA (Western Europe)

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Tricent er afhængig af standardkontraktbestemmelser (SCC) for overførsel af personoplysninger til tredjelande i henhold til forordning (EU 20126/679 fra EU-parlamentet og Rådet godkendt af Europa-Kommissionens gennemførelsesafgørelse (EU) 2021/914 af 4. juni 2021, som det pt. er udlagt på 32021D0914 - EN - EUR-Lex

Hvis den dataansvarlige ikke i disse Bestemmelser eller efterfølgende giver en dokumenteret instruks vedrørende overførsel af personoplysninger til et tredjeland, er databehandleren ikke berettiget til inden for rammerne af disse bestemmelser at foretage sådanne overførsler.

C.6.1 Godkendelse af overførsel til specifikke modtagere af personoplysninger i tredjelande, når der er sikret fornødne garantier

Den dataansvarlige instruerer databehandleren til at anvende nedenstående underdatabehandler(e), hvor der sker overførsel af personoplysninger til tredjelande:

NAVN:	ADRESSE:	BESKRIVELSE AF BEHANDLING:	OVERFØRSEL TIL TREDJELAND:
Microsoft	1 Microsoft Way, Redmond, WA98052 United States	Levering af behandlingsinfrastruktur, der understøtter driften af Tricent for Microsoft 365 SaaS-løsning	Overførselsgrundlag: SCC
Confluent	899 West Evelyn Ave. Mountain View, CA 94041	Levering af meddelelsesinfrastruktur , der understøtter driften af Tricent til Microsoft 365 SaaS-løsning	Overførselsgrundlag: SCC
Sendgrid	375 Beale St Suite 300 San Francisco, CA	Levering af e-mail-infrastruktur, der understøtter driften af Tricent for Microsoft 365 SaaS-løsning	Overførselsgrundlag: SCC

Den dataansvarlige har ved indgåelsen af Bestemmelserne givet godkendelse til brugen af ovenstående underdatabehandler(e) samt instruks om overførelse af personoplysninger til tredjelande ved levering af tjenesterne.

Som overførselsgrundlag indgås EU-Kommissionens til enhver tid gældende Standardkontrakter (SCC). Databehandleren og ovenstående underdatabehandler(e) er bemyndiget til at indgå en SCC på vegne af den dataansvarlige. Det betyder, at den dataansvarlige skal anses som dataeksportør i forhold til indgåelse af SCC, og at den dataansvarlige i forbindelse med overførslerne af oplysninger til ovenstående underdatabehandler(e) accepterer at være bundet af de forpligtelser, som SCC pålægger dataeksportøren.

I tilfælde af at EU-Kommissionen udarbejder nye SCC'er efter aftaleindgåelsen, er databehandleren bemyndiget til at udskifte, opdatere og anvende de til enhver tid gældende SCC'er.

Indholdet af denne instruks og/eller Bestemmelserne anses ikke for at ændre indholdet af SCC.

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

"Databehandleren skal årligt for egen regning indhente en revisionserklæring fra en uafhængig tredjepart vedrørende databehandlerens 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 kan anvendes i overensstemmelse med disse Bestemmelser:

1. En SOC-2 for generelle It-kontroller.

Revisionserklæringen fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen og kan i sådanne tilfælde anmode om en ny revisionserklæring under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af erklæringen, 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.

Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når den dataansvarlige finder det nødvendigt."

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

"Databehandleren skal årligt for egen regning indhente en revisionserklæring eller inspektionsrapport 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 eller inspektionsrapporter kan anvendes i overensstemmelse med disse bestemmelser:

2. En SOC-2 for generelle It-kontroller.

Revisionserklæringer eller inspektionsrapporter fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden i erklæringen eller rapporten og kan i sådanne tilfælde anmode om en ny revisionserklæring eller inspektionsrapporter under andre rammer og/eller under anvendelse af anden metode.

Baseret på resultaterne af erklæringen eller rapporten 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.

Databehandleren eller en repræsentant for databehandleren har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner, med lokaliteterne hvorfra underdatabehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når databehandleren (eller den dataansvarlige) finder det nødvendigt.

Dokumentation for sådanne inspektioner fremsendes uden unødig forsinkelse til den dataansvarlige til orientering. Den dataansvarlige kan anfægte rammerne for og/eller metoden af inspektionen og kan i sådanne tilfælde anmode om gennemførelsen af en ny inspektion under andre rammer og/eller under anvendelse af anden metode."

"Den dataansvarlige kan – hvis det findes nødvendigt – vælge at initiere og deltage på en fysisk inspektion hos underdatabehandleren. Dette kan blive aktuelt, hvis den dataansvarlige vurderer, at databehandlerens inspektion hos underdatabehandleren ikke har givet den dataansvarlige tilstrækkelig sikkerhed for, at behandlingen hos underdatabehandleren sker I overensstemmelse med databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Den dataansvarliges eventuelle deltagelse i en inspektion hos underdatabehandleren ændrer ikke ved, at databehandleren også herefter har det fulde ansvar for underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser."

"Databehandlerens og underdatabehandlerens eventuelle udgifter i forbindelse med en fysisk inspektion af underdatabehandlerens lokaliteter er den dataansvarlige uvedkommende – uanset om den dataansvarlige har initieret og deltaget i en sådan inspektion."

HELLOSIGN

Audit trail

TITLE	Tricent IT Relation databehandler aftale version 1
FILE NAME	Tricent IT Relati...ale version 1.pdf
DOCUMENT ID	5672e20b675b3387aee68bc0069e21e111c947fe
AUDIT TRAIL DATE FORMAT	MM / DD / YYYY
STATUS	● Signed

Document history

SENT	**08 / 26 / 2022** 12:10:29 UTC	Sent for signature to Lars Nielsen (lanie@itrelation.dk) from mh@tricent.com IP: 62.243.36.82
VIEWED	**09 / 20 / 2022** 07:25:15 UTC	Viewed by Lars Nielsen (lanie@itrelation.dk) IP: 91.142.136.2
SIGNED	**09 / 20 / 2022** 07:28:09 UTC	Signed by Lars Nielsen (lanie@itrelation.dk) IP: 91.142.136.2
COMPLETED	**09 / 20 / 2022** 07:28:09 UTC	The document has been completed.