Standardkontraktsbestemmelser

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

mellem

Kunden

herefter ”den dataansvarlige”

og

Dateco ApS
CVR 26480817
Storgaden 7 A
6052 Viuf
Danmark

herefter ”databehandleren”

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

HAR AFTALT følgende standardkontraktsbestemmelser (Bestemmelserne) med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder

Indhold

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 WebFinance 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.

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

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 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 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 30 dages 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 indføje 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 opsige 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.

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 standardkontraktsbestemmelser 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

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. 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

2. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 5.3., 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 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

   b. 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

   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 8.1. og 8.2.

9. Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødig 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 8.2.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.

10. 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 dataansvarlig, 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.

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 underskrift af abonnementsaftalen

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 10.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftlig varsel af begge parter.

5. Underskrift

   På vegne af databehandleren

Navn	Thomas Hansen
Stilling	Ejer/partner
Telefonnummer	76 700 600
E-mail	kontakt@dateco.dk

   Underskrift

Bilag A Oplysninger om behandlingen

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

Dateco A/S er databehandler i forbindelse med levering af IT-ydelsen:

- WebFinance

Formålet med behandlingen af data, er at kunne stille et økonomisystem til den dataansvarliges rådighed, som er godkendt til bogføringsloven af Erhvervsstyrelsen.

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

Databehandleren stiller økonomiprogrammet WebFinance til rådighed for den dataansvarlige og yder løbende support i forbindelse med ydelsen.

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

I systemet behandles almindelige oplysninger (art. 6) der relaterer sig til økonomihåndtering, herunder:

Navn, titel, e-mail, telefonnummer, adresse mv.

Der behandles som udgangspunkt ikke oplysninger af følsom/særlig karakter.

A.4. Behandlingen omfatter følgende kategorier af registrerede

Den dataansvarliges
- Kunder
- Leverandører
- Ansatte

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

Databehandleren er jf. bogføringsloven forpligtet til at opbevare oplysninger der relaterer sig til bogføring, så længe loven foreskriver det. Herefter vil der ske sletning.

De oplysninger databehandleren behandler for den dataansvarlige, som relaterer sig til bogføring, vil derfor først blive slettet jf. bogføringslovens bestemmelser, selvom kundeforholdet i mellemtiden måtte ophøre.

Oplysninger der ikke relaterer sig til bogføring, eller på anden måde er underlagt en lovbestemt sletteprocedure, slettes eller tilbageleveres når hovedaftalen ophører.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Microsoft		Atrium B, Sandyford Industrial Estate, Carmanhall Rd, Sandyford, Dublin 18, Irland	Licenser
MySupply ApS	25894375	Østre Fælledvej 8, 1. sal, 9400 Nørresundby	Modtagelse og afsendelse af e-dokumenter

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.

C.1. Behandlingens genstand/instruks

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

Den dataansvarlige instruerer databehandleren i at stille økonomisystemet WebFinance til rådighed, og drifte og behandle data der måtte blive uploadet til systemet. Den dataansvarlige instruerer ligeledes databehandleren i at yde support i forbindelse med brugen af systemet.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:
Behandlingen vil som udgangspunkt omfatte personoplysninger efter databeskyttelsesforordningens artikel 6 om almindelige personoplysninger.

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:

Adgangsstyring
Udgangspunktet for tildeling af rettigheder og adgang til systemer og informationer er, at alt er låst ned og at der kun gives adgang, hvor der er et forretningsmæssigt behov. Ledelsen beslutter hvem, der skal have adgang til system og/eller informationer, og tildeler herefter rettighederne ud fra disse beslutninger.

Dateco's servere og bærbare pc'er beskyttes med adgangskode og skærmlås samt opdaterede antivirusprogrammer og lokale firewalls.

Styring af adgangskoder sker via intern politik - minimum 8 karakterer, kombination af store/små bogstaver samt tal og specialtegn.

Dateco's fysiske lokaler er sikret med adgangssystem og alarm. Ledelsen beslutter hvem, der skal have adgang til hvad.

Det kritiske it-udstyr er anbragt i adgangsstyret serverrum, med alarmer, hvor det er sikret mod forsyningssvigt med strømbackup (UPS) og mod miljøskader med temperaturføler samt brandalarm.

Informationer og aktiver
Dateco's informationer findes på it-aktiver som servere, cloud-lagre, samt backupbånd. Sikkerhedspolitikken kræver, at Dateco's informationer er beskyttet i tilfælde af tab, tyveri, kopiering mv.

Når der anvendes kryptering, er det vigtigt at lave en sikkerhedskopi af krypteringsnøglen, hvilket der er vejledning til i systemerne.

Der er mulighed for at anvende kryptering på alle typer medier, men i denne politik vil det være for omfattende at beskrive alle mulighederne.

Kryptering af virksomhedens informationer understøttes af en begrænsning af hvilke personer, der får rettigheder til at læse, rette eller slette informationer. Se afsnit om adgangsstyring.

Medarbejdere i Dateco må som udgangspunkt ikke opbevare firmarelaterede data i et cloud-lager, som Dropbox, medmindre dette er stillet til rådighed af Dateco, eller godkendt af Dateco's ledelse til firmabrug. Hvis der opstår et akut behov for at opbevare firmarelaterede data i et ikke-godkendt cloud-lager, er det medarbejderens ansvar at sørge for, at data er krypterede.

Driftsikkerhed
Der foretages backup af Dateco's systemer og informationer, så de kan genskabes efter et nedbrud. Dette gøres ved backup ud af huset. Backup sker dagligt 4 uger tilbage, ugentligt 6 måneder tilbage og månedligt 5 år tilbage.

Logning af aktiviteter er slået til i Dateco's systemer, og hvor der er persondata, logges adgang og forsøg på adgang til de enkelte informationer også.

Windows Update benyttes på alle Windows-platforme til styring af tekniske sårbarheder, for at forhindre at disse udnyttes ved et angreb. Kritiske Windows-opdateringer installeres hurtigst muligt, og andre Windows-opdateringer en gang pr. måned. Opdatering af tredjeparts applikationer sker løbende.

Ændringer følger en proces med strukturerede tests af løsningerne inden idriftsættelse. Idriftsættelse af ændringer på kritiske systemer foregår i videst muligt omfang i planlagte servicevinduer, for at undgå at eventuelle fejl vil påvirke tilgængeligheden.

Driften sikres yderligere ved at alle servere er dublerede (redundante), med spejlede (Raid-baserede) diske, aftaler med leveringstidsgarantier (Service Level Agreement) på levering af reservedele, samt ekstern opbevaret kopi af backuppen.

Der køres både elektronisk backup og fysisk backup LTO-medie (Kryptereret).

24/7 tilgængeligheden af Dateco's systemer dækker også bemandingen, så viden er dubleret og kritiske funktioner tilgængelige døgnet rundt.

Kommunikationssikkerhed
Dateco's interne netværk er beskyttet med en firewall, der regulerer og logger trafikken mellem Dateco's interne net og Dateco's tele-/internetleverandør (Internet Service Provider, ISP) (internettet), så kun tilladt trafik passerer igennem.

Firewallregler er så vidt muligt konfigureret i henhold til PCI-compliance, hvilket betyder at der kun åbnes for de nødvendige services og kun mellem relevante netværkssegmenter, samt at der er defineret regler for både indgående netværkstrafik.

Adgang til filer, der downloades, bliver scannet for virus og andet malware.

Alle indgående e-mails, der modtages i Dateco's e-mailsystem, bliver scannet for usikre links til eksterne hjemmesider og for om det er en potentiel phishing-mail. Derudover scannes vedhæftede filer for virus og andet malware.

Al ekstern adgang til Dateco's netværk og systemer sker via krypterede forbindelser. Dateco's website og webservices benytter https-kryptering baseret på Transport Layer Security (TLS), ligesom e-mailserveren også håndterer TLS.

Adgang til andre servere/services og Dateco's interne netværk sker via klientkryptering beskyttet af 2-faktor autentifikation.

Overførsel af, eller adgang til, Dateco's informationer til/fra eksterne samarbejdspartnere eller myndigheder må kun ske efter aftale med disse, baseret på informationernes fortrolighed, herunder om evt. brug af kryptering.

PC'er der kobler sig på virksomhedens netværk og systemer eksternt fra, skal overholde virksomhedens retningslinjer. Dette er kun tilladt for virksomhedens udstyr/gælder også medarbejdernes egne pc'er.

Leverandørstyring og outsourcing
Microsoft, der står for drift af Microsoft 365, skal overholde Dateco's krav til it-sikkerhed
Der skal foreligge en aftale, og om nødvendigt også en databehandleraftale, som lever op til kravene i databeskyttelsesloven.

Medarbejdersikkerhed og awareness
I forbindelse med stillingsopslag/ansættelser vurderer ledelsen, om der er særlige sikkerhedsmæssige krav, herunder om det for eksempel er nødvendigt at bede om at se en straffeattest.
Som en del af ansættelsesproceduren, dog senest ved første arbejdsdag, orienteres den nye medarbejder om tavshedspligt og andre sikkerhedskrav.
Når en medarbejder fratræder, gør ledelsen vedkommende opmærksom på, at tavshedspligten og fortroligheden også gælder efter ansættelsens ophør.

Sikkerhedshændelser og it-beredskab
Hvis en medarbejder opdager trusler mod, eller brud på, informationssikkerheden, eller får mistanke om det, skal vedkommende straks underrette ledelsen om dette.

Ledelsen vurderer de rapporterede sikkerhedshændelser hurtigst muligt efter at de er anmeldt. Det vurderes om de kan vente til senere behandling, om de skal håndteres her og nu (eventuelt ved hjælp af ændringer, yderligere awareness eller kontakt til tredjepart) eller om de er så alvorlige, at de kræver aktivering af Dateco's it-beredskabsplan. Er der tale om hændelser med persondata, aktiveres Dateco's procedurer for dette.

Når hændelsen er behandlet, vurderes om sagen kan lukkes eller om der skal ske en opdatering af risikobilledet, som evt. kræver nye sikkerhedstiltag.

Hvis eksterne parter berøres af sikkerhedshændelser hos Dateco, er ledelsen ansvarlig for eventuel kommunikation over for berørte parter.

Vurdering af sikkerhed

De etablerede sikkerhedsforanstaltninger vurderes jævnligt i forhold til ændringer i trusselsniveauet og tilpasses om nødvendigt.

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 8.1 og 8.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

Databehandleren skal bistå den dataansvarlige i forbindelse med de nævnte tilfælde i punkt 8.1 og 8.2. og databehandleren skal igangsætte de fornødne tekniske og organisatoriske foranstaltninger til at opfylde betingelserne i tilfælde af de nævnte forhold i punkt 8.1. og 8.2

C.4 Opbevaringsperiode/sletterutine

Databehandleren er jf. bogføringsloven forpligtet til at opbevare oplysninger der relaterer sig til bogføring, så længe loven foreskriver det. Herefter vil der ske sletning.

De oplysninger databehandleren behandler for den dataansvarlige, som relaterer sig til bogføring, vil derfor først blive slettet jf. bogføringslovens bestemmelser, selvom kundeforholdet i mellemtiden måtte ophøre.

Oplysninger der ikke relaterer sig til bogføring, eller på anden måde er underlagt en lovbestemt sletteprocedure, slettes eller tilbageleveres når hovedaftalen ophører.

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:

- Dateco ApS' adresse: Storgaden 7A, Viuf 6052
- Lokationer for listede underdatabehandlere

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

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.

Den dataansvarlige instruerer databehandleren i at foretage overførsler til tredjelande, hvis dette findes relevant for behandlingen. Der vil kun kunne ske overførsel til en nuværende, eller i fremtiden godkendt underdatabehandler.

Databehandleren er i den forbindelse forpligtet til at sikre lovligheden og sikkerheden af data der måtte overføres.

Der vil være sikret et overførselsgrundlag efter GDPR-kapitel V, i form at en tilstrækkelighedsafgørelse, Standard Contractual Clauses (SCC) og/eller Binding Corporate Rules (BCR).

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

Ved anmodning vil databehandleren fremsende passende dokumentation på at databehandleren overholder nærværende aftale og databeskyttelsesreglerne. Databehandleren vil fremsende et besvaret spørgeskema, som bør betragtes som tilstrækkeligt.

Ønsker den dataansvarlige yderligere dokumentation eller adgang til at føre fysisk audit, skal dette aftales direkte med databehandleren. Databehandleren forbeholder sig retten til at tage sin vanlige timepris for assistance med at fremskaffe yderligere dokumentation samt fysiske inspektioner.

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

Databehandleren fører tilsyn med sine underdatabehandlere. Ønskes materiale herfor udleveret kan dette ske efter aftale. Databehandleren forbeholder sig retten til at tage sin vanlige timepris for assistance med dokumentation for revision ved underdatabehandlerne.