

Timengo DPG A/S

Lautrupvang 1
2750 Ballerup
Denmark



Databehandleraftale

Standardkontraktbestemmelser

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

mellem

{kunde_navn}
{adresse}
{postnr} {by}
CVR: {cvr}

og

Timengo DPG A/S
Lautrupvang 1
2750 Ballerup
CVR 35833684

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..... | 3 |
| 2. Den dataansvarliges rettigheder og forpligtelser | 3 |
| 3. Databehandleren handler efter instruks..... | 4 |
| 4. Fortrolighed | 4 |
| 5. Behandlingssikkerhed | 4 |
| 6. Anvendelse af underdatabehandlere..... | 5 |
| 7. Overførsel til tredjelande eller internationale organisationer | 6 |
| 8. Bistand til den dataansvarlige..... | 6 |
| 9. Underretning om brud på persondatasikkerheden | 7 |
| 10. Sletning og returnering af oplysninger | 8 |
| 11. Revision, herunder inspektion..... | 8 |
| 12. Parternes aftale om andre forhold | 8 |
| 13. Ikrafttræden og ophør | 8 |
| 14. Kontaktpersoner hos den dataansvarlige og databehandleren | 9 |
| Bilag A Oplysninger om behandlingen | 9 |
| Bilag B Underdatabehandlere | 11 |
| Bilag C Instruks vedrørende behandling af personoplysninger | 12 |
| Bilag D Parternes regulering af andre forhold..... | 15 |

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).

I forbindelse med leveringen af DPG-tjenesten til den dataansvarlige, har DPG servicen til formål at behandle Sikkerpost og Digital Post på vegne af den dataansvarlige.

3. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.
4. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.
5. 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.
6. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.
7. 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.
8. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke er omfattet af Bestemmelserne.
9. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
10. 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 medlemsstaternes¹ 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.

1

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

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.
4. 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 fra den dataansvarlige.
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.
5. Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.
6. 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.
7. Databehandleren skal i sin aftale med underdatabehandleren indføre 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.

8. 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

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.
2. Dette indebærer, at databehandleren så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:
 - d. oplysningspligten ved indsamling af personoplysninger hos den registrerede
 - e. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
 - f. indsigtretten
 - g. retten til berigtigelse
 - h. retten til sletning ("retten til at blive glemt")
 - i. retten til begrænsning af behandling

- j. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
 - k. retten til dataportabilitet
 - l. retten til indsigelse
 - m. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering
3. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3., bistår databehandleren desuden, 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 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 analysere de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)
 - d. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet, inden behandling, hvis en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.
4. Parterne skal i bilag C angive de nødvendige 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

- 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 12 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.

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 dataansvarlige, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

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 skriftligt varsel af begge parter.

14. Underskrift

På vegne af den dataansvarlige

Navn {\$aftale_ansvarlig}
Telefonnummer {\$aftale_telefon}
E-mail {\$aftale_email}

Underskrift

På vegne af databehandleren

Navn Ninna Hellqvist
Telefonnummer 20972881
E-mail nhe@timengo.com

Underskrift

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.

Navn {\$aftale_ansvarlig}
Telefonnummer {\$aftale_telefon}
E-mail {\$aftale_email}

Navn Ninna Hellqvist
Telefonnummer 20972881
E-mail nhe@timengo.com

Bilag A Oplysninger om behandlingen

Timengo DPG A/S løsning til sikker-post kommunikation og integration til Digital Post.

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

Formålet er at kunne sende og modtage til/fra digitale postkasser. Kryptering kan foretages både under transport og under lagring.

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

Databehandler stiller DPG løsningen til rådighed der gør det muligt at sende og modtage sikker og Digital post fra Outlook klienter, baseret på Exchange Online (Office365) eller Exchange On-premise.

Behandlingen omfatter følgende typer af personoplysninger om de registrerede:
Navn, adresse, e-mailadresse, telefonnr.

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

Alle oplysninger afsløret i indgående og udgående krypterede e-mails, der behandles af DPG. Dette omfatter, men er ikke begrænset til, navn, e-mail, adresse, telefonnummer.

A.4. Behandlingen omfatter følgende kategorier af registrerede

Alle oplysninger afsløret i indgående og udgående krypterede e-mails, Dette omfatter, men er ikke begrænset til, borgere/kunder, tredjepartskontaktperson samt nuværende og tidligere medarbejdere.

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

Behandlingen er ikke tidsbegrænset og skal udføres, indtil denne aftale opsiges eller opsiges af en af parterne. Aftalen opsiges automatisk ved udløb af aftale på DPG-servicen. Der er reelt tale om Meta data/logs data, på modtager og afsender, tidspunkt, krypterings metode og styrke herpå. Der er ikke tale om indhold i meddelelserne.

Når aftalen opsiges, accepterer DPG at slette alle databehandler relaterede data inden for 14 arbejdsdage.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

| NAVN | ADRESSE | BESKRIVELSE AF BEHANDLING |
|----------------------|---|---|
| Microsoft Azure | Microsoft Ireland Operations, Ltd. One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521, Ireland | Cloud platform der kan hoste DPG løsningen (inden for EU) |
| Microsoft Office 365 | Microsoft Ireland Operations, Ltd. One Microsoft Place South County Business Park Leopardstown Dublin 18, D18 P521, Ireland | Microsoft cloud baseret Office platform. DPG kan benytte OME/AIP eller lign. krypteringsfunktionen (inden for EU) |
| Dansk Cloud | ECIT Solutions A/S Hørkær 12A, 3. Sal 2730 Herlev | Driftscenter der kan hoste DPG løsningen (Inden for Danmark) |

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

Databehandleren indgiver anmodningen om specifik tilladelse mindst 30 dage før den pågældende underbehandlers anvendes.

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:

Kryptering/dekryptering af indgående og udgående mails fra Kundens Microsoft Exchange-mailserveren. Data behandles i hukommelsen og gemmes kun i dataansvarliges Exchange-mailservere. Databehandler gemmer kunde logningsoplysninger i DPG's log løsning.

C.2. Behandlingsikkerhed

Sikkerhedsniveauet skal afspejle:

At DPG-løsningen kan behandle data i e-mails, der omfattes af databeskyttelsesforordningens artikel 9 om "særlige kategorier af personoplysninger", hvorfor der skal etableres et "højt" sikkerhedsniveau."

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

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

Krav til pseudonymisering og kryptering af personoplysninger

Databehandleren opbevarer og behandler så vidt muligt personoplysninger i pseudonymiseret eller krypteret form. I det omfang krypteringsnøglen er mulig og anvendelig, skal den dataansvarlige opbevare krypteringsnøglen. Hvis krypteringsnøglen gemmes af databehandleren, skal nøglen opbevares fysisk inden for EØS.

Krav til sikring af løbende fortrolighed, integritet, tilgængelighed og modstandsdygtighed for behandlingssystemer og -tjenester

Databehandleren skal have formelle procedurer for at sikre, at opdateringer af operativsystemer, databaser, applikationer og anden software vurderes og gennemføres inden for en rimelig frist.

Databehandleren skal have indført formelle procedurer for ændringsstyring for at sikre, at enhver ændring godkendes, testes og godkendes inden gennemførelsen. Sådanne procedurer skal understøttes af en effektiv adskillelse af funktioner eller opfølgning af ledelsen for at sikre, at ingen enkeltperson kan gennemføre en ændring alene.

Databehandleren må kun tillade personer, der er ansat til de formål, hvortil personoplysninger behandles. Individuelle brugere må ikke godkendes til adgang eller brug, bortset fra det, der er nødvendigt for deres engagement. Den autoriserede bruger skal være udstyret med et personligt bruger-id og en adgangskode, der skal anvendes, hver gang den enkelte bruger logger på systemet. Mindst en gang hver sjette måned foretages der en inspektion af de tilladelser, der udstedes, for at sikre, at brugerne kun får tilladelse i det omfang, det er nødvendigt for deres ansættelse.

Databehandleren skal have formelle procedurer for at sikre en effektiv fjernelse af personoplysninger fra elektronisk udstyr, inden udstyret bortskaffes.

Krav til muligheden for at genoprette tilgængeligheden og adgangen til personoplysninger rettidigt i tilfælde af en fysisk eller teknisk hændelse

Databehandleren skal have indført dokumenterede nødprocedurer for at sikre, at tjenesterne genetableres inden for en rimelig frist i tilfælde af afbrydelse af tjenesten.

Databehandleren skal føre en dokumenteret hændelseslog over hændelser med sikkerheds- og personoplysninger, der direkte eller indirekte påvirker de personoplysninger, der behandles på vegne af den dataansvarlige, med hensyn til at sikre fortrolighed, integritet og/eller tilgængelighed.

Databehandleren sikrer, at systemer og personoplysninger regelmæssigt understøttes. Sådanne sikkerhedskopieringer skal opbevares sikkert og på en sådan måde, at sikkerhedskopiering ikke går tabt i hændelser, der fører til tab af originale personoplysninger.

Databehandleren kontrollerer og sikrer regelmæssigt, at sikkerhedskopieringen er læsbar.

Krav til processer til regelmæssig afprøvning, vurdering og evaluering af effektiviteten af tekniske og organisatoriske foranstaltninger til sikring af behandlingens sikkerhed

Databehandleren skal have dokumenteret systematiske og varierede prøvninger af interne nødprocedurer. I det omfang sådanne procedurer er baseret på en risikovurdering, skal dette meddeles den registeransvarlige.

Krav til ekstern adgang til data

Databehandleren skal sikre, at ekstern adgang til data kun finder sted i overensstemmelse med metoder og værktøjer, der tidligere er godkendt af den dataansvarlige.

Krav til beskyttelse af data under videregivelse

Databehandleren skal tage skridt til at sikre, at personoplysninger, der overføres via åbne netværk, såsom internettet, ikke går tabt, ændres eller videregives til uautoriserede personer under sådanne overførsler.

Krav til beskyttelse af data under opbevaring

Databehandleren skal så vidt muligt sikre, at data i hvile krypteres.

Data i hvile skal lagres inden for EØS.

Krav til fysisk sikkerhed på steder, hvor personoplysninger behandles

Databehandleren skal have rimelige fysiske adgangs begrænsninger og sikre det samme for alle underbehandlere, der er vært for personoplysninger

Krav til brug af hjemme-/fjernarbejde

Databehandleren skal sikre, at enhver brug af hjemmearbejdssteder eller andre fjerntliggende arbejdspladser kun må finde sted i det omfang, der træffes effektive foranstaltninger for at sikre, at uautoriserede personer ikke kan få adgang til personoplysninger via sådanne forbindelser. Sådanne foranstaltninger kan bl.a. være krypterede forbindelser og to faktor validering af brugere.

Desuden skal databehandleren sikre, at der er skriftlige instruktioner om behandling og lagring af personoplysninger på vegne af den registeransvarlige i forbindelse med brugen af hjemmearbejdssteder og andre fjerntliggende arbejdspladser.

Krav til logføring

Maskinregistrering (logning) skal gøres for al brug af personoplysninger. Logbogen skal som minimum indeholde oplysninger om tid, brugerkonto og brugstype.

I tilfælde af behandling af følsomme personoplysninger skal loggen suppleres med oplysninger om den person, som de pågældende oplysninger er relateret til, eller det anvendte søgekriterium.

Logbogen skal opbevares i seks måneder, hvorefter den slettes, medmindre der fastsættes en længere periode i overensstemmelse med formålet med logbogen.

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:

Forespørgsler fra den dataansvarlige vedrørende spørgsmål, der er omfattet af afsnit 9.1. eller 9.2. besvares hurtigst muligt og senest 24 timer efter modtagelsen af forespørgslen.

Hvis databehandleren modtager en forespørgsel fra en registreret eller en tredjepart vedrørende forhold, der er omfattet af afsnit 9.1. eller 9.2., sendes undersøgelsen til den dataansvarlige hurtigst muligt og senest 24 timer efter modtagelsen af forespørgslen.

C.4 Opbevaringsperiode/sletterutine

Databehandler lagrer ikke personhenførbare data, men kun logning. Denne log slettes indenfor 60 dage, efter ophør af denne aftale.

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. Microsoft Azure datacenter I nord Europa
2. Den dataansvarliges datacenter
3. EC-IT danske hostingcenter i Herlev

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

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

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

Der er enighed mellem parterne om, at en ISAE3402 og ISAE-3000. Type II revisionserklæring kan anvendes som grundlag for revision.

Revisionserklæringen fremsendes uden unødigt forsinkelse til den dataansvarlige til orientering. Baseret på resultaterne af Revisionserklæringen er den dataansvarlige berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelsen af databeskyttelsesforordningen, ifølge dansk lov.

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, og for den dataansvarliges regning.

Bilag D Parternes regulering af andre forhold

Disse bestemmelser er underlagt dansk lovgivning, og enhver tvist vedrørende og opstået som følge af denne aftale skal afgøres af de danske domstole i henhold til danske procedure regler.