Bilag A: Databehandleraftale

AX VI itm8 Holding ApS
CVR: 42520292
(i det følgende benævnt den ”Dataansvarlige”)

og

Uniqkey A/S
CVR: 39004127
(i det følgende benævnt ”Databehandleren”)

1. Formål

1.1. Denne Databehandleraftale har til formål at regulere Databehandlerens behandling af personoplysninger i forbindelse med aktivering af Uniqkey appen hos den Dataansvarlige, som nærmere beskrevet i handelsbetingelserne, accepteret af den Dataansvarlige (”Handelsbetingelserne”) ved aktivering af Uniqkey appen.

1.2. Ved eventuelle konflikter mellem Handelsbetingelserne og Databehandleraftalen, har Databehandleraftalen forrang.

1.3. Databehandleraftalens formål er at sikre, at Databehandleren til enhver tid overholder sine forpligtelser i henhold til de til enhver tid gældende regler og forskrifter for behandling af persondata, herunder Europa-Parlamentets og Rådets forordning 1016/679 af 27. april 2016 (”Persondataforordningen”) samt til enhver tid sikre overholdelse af de særregler der er implementeret i Danmark.

1.4. Databehandleraftalen finder anvendelse for den Dataansvarlige og dennes koncernselskaber samt hertil knyttede selskaber.

2. Dataansvarlige og Databehandleren forholdet

2.1. Forholdet mellem den Dataansvarlige og Databehandleren hvad angår kategorier af registrerede brugere og personoplysninger, som behandles i henhold til nærværende Databehandleraftale er beskrevet i Bilag 1.

2.2. Databehandleren må kun behandle personoplysningerne efter dokumenteret instruks fra den Dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Databehandleren er underlagt. I så fald underretter Databehandleren den Dataansvarlige om dette retlige krav inden behandlingen, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

2.3. Databehandleren er forpligtet til at sikre, at de personoplysninger som Databehandleren modtager som led i Databehandleraftalen ikke benyttes til andre formål eller behandles på anden måde, end hvad der fremgår af Databehandleraftalen.

2.4. Hvis den Dataansvarliges instruks, efter Databehandlerens opfattelse, er eller bliver i strid med Persondataforordningen, skal Databehandleren uden ugrundet ophold meddele dette til den Dataansvarlige.

3. Underdatabehandleraftaler

3.1. Ved en underdatabehandler forstås en underleverandør, som forestår behandling af hele eller dele af den behandling, som Databehandleren foretager på vegne af den Dataansvarlige.

3.2. Databehandleren må kun gøre brug af underdatabehandlere med den dataansvarliges forudgående specifikke skriftlig godkendelse. Databehandleren skal indgive anmodningen om en specifik godkendelse mindst 60 dage inden anvendelsen af den pågældende underdatabehandler. Den Dataansvarlige kan ikke nægte en ny underdatabehandler, men hvis den nye underdatabehandler stiller kunden væsentlig dårligere, har Dataansvarlige ret til at opsige samarbejdet med 30 dages varsel. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag 5.

3.3. Alle underdatabehandleraftaler skal som minimum pålægge de samme forpligtelser vedrørende behandling af et givet forhold, som der påhviler Databehandleren efter Databehandleraftalen, samt efter den til enhver tid gældende lovgivning.

3.4. Databehandleren er fuldt ansvarlig overfor den Dataansvarlige for enhver underdatabehandler, der ikke opfylder sine forpligtelser i henhold til lovgivning eller underdatabehandleraftalen.

3.5. Den Dataansvarlige kan til enhver tid forlange dokumentation fra Databehandleren vedrørende underdatabehandleraftaler.

3.6. "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 databeskyttelsesforpligtigelser 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.

3.7. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtigelser, forbliver databehandleren fuldt ansvarlig overfor den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtigelser. 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.

4. Sikkerhed og databrud

4.1. 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.

4.2. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.5, 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 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.
e. Parterne skal i bilag 5 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 5.1. og 5.2.

5. Sikkerhed og databrud

5.1. Databehandleren er ansvarlig for implementering af passende tekniske og organisatoriske foranstaltninger, under hensyn til det aktuelle tekniske niveau, implementeringsomkostninger og den aktuelle behandlings karakter, omfang, sammenhæng og formål.

5.2. 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.

5.3. Databehandleren skal opfylde de eventuelle sikkerhedskrav, der påhviler Databehandleren i henhold til de til enhver tid gældende regler og forskrifter for behandling af persondata, herunder Persondataforordningen, og andre gældende sikkerhedskrav i det land, hvor Databehandleren er etableret. De passende tekniske og organisatoriske foranstaltninger udgør som minimum, men ikke begrænset til:

- Pseudonymisering og kryptering af Kundens data,

- Genoprettelse af data i tilfælde af en fysiske eller tekniske hændelser,
- Sikre vedvarende fortrolighed, integritet og tilgængelighed,
- Udarbejdelse og efterlevelse af relevante sikkerhedspolitikker, og
- Efterlevelse af relevante branchestandarder

5.4. 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.

5.5. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtigelse 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 forpligtigelse efter forordningens artikel 32.

5.6. Yderligere beskrivelser af de sikkerhedsforanstaltninger, som skal implementeres af Databehandleren, fremgår af bilag 3.

5.7. 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 tilsynsmyndigheden indenfor 72 timer. Orienteringen skal til følgende e-mailadresse:
gdpr@itm8.com

Orienteringen om databruddet skal så indeholde:

- En beskrivelse af karakteren af bruddet, herunder kategorier af personoplysninger, et estimeret omfang af personoplysninger, samt antal involverede registrerede personer,
- En vurdering af konsekvenserne ved databruddet, og
- En beskrivelse af de foranstaltninger, som Databehandleren eller underdatabehandleren har truffet eller foreslår truffet for at håndtere bruddet, herunder foranstaltninger for at begrænse dets mulige skadevirkninger.

5.8. Såfremt den Dataansvarlige anmoder Databehandleren om at bistå den Dataansvarlige med at besvare anmodninger om udøvelse af de registreredes rettigheder er Databehandleren berettiget til, at fakturere for en sådan bistand.

Databehandleren bistår den Dataansvarlige med, at sikre overholdelse af forpligtelserne i medfør af artikel 32-36 i Persondataforordningen, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for Databehandleren. Databehandleren er berettiget til at fakturere for en sådan bistand

6. Databehandlerens medarbejdere

6.1. Databehandleren er direkte ansvarlig for alle handlinger foretaget af medarbejdere, i strid med Databehandleraftalen, relevant lovgivning eller tilhørende instruks.

6.2. Databehandleren er forpligtet til at begrænse behandlingen af personoplysninger til nødvendigt personale, samt at udføre og opretholde undervisning af personale i håndtering og behandling af persondata.

6.3. Alle medarbejdere underlagt Databehandleren og dennes organisation, som behandler personoplysninger på vegne af den Dataansvarlige, skal være underlagt tavsheds- og fortrolighedsforpligtelser.

6.4. 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.

6.5. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

7. Dokumentation og tilsyn

7.1. Ved skriftlig anmodning fra den Dataansvarlige, skal Databehandleren give den Dataansvarlige eller en uafhængig tilsynsmyndighed tilstrækkelig dokumentation for at påvise overholdelse af Databehandleraftalen, samt de til enhver tid gældende persondataretlige regler. Såfremt Databehandleren er omfattet af kravet om at føre en fortegnelse over behandlingsaktiviteter efter Persondataforordningens artikel 30, skal denne tillige stilles til rådighed for den Dataansvarlige på dennes skriftlige anmodning.

7.2. Den Dataansvarlige kan tillige kræve en sådan information angivet i punkt 8.1 fra Databehandleren vedrørende underdatabehandlere.

7.3. Databehandleren skal efterkomme en sådan anmodning fra den Dataansvarlige jf. punkt 8.1 og 8.2 inden rimelig tid, og senest 5 arbejdsdage efter en anmodning fremsat i henhold til punkt 8.1. En anmodning efter punkt 8.2 kan tage længere tid på grund af sikkerhedskravene kravene hos underdatabehandlere.

7.4. Såfremt den Dataansvarlige, en repræsentant for denne eller en relevant tilsynsmyndighed, ønsker at foretage en fysisk inspektion af Databehandlerens faciliteter, forpligter Databehandleren sig til at give adgang hertil. Anmodning om tilsynsbesøg skal ske med mindst 5 arbejdsdages varsel. Databehandleren er ikke berettiget til særskilt vederlag eller erstatning herfor, medmindre antallet af besøg eller karakteren af disse overstiger, hvad der må anses for sædvanligt for den pågældende type af behandlinger.

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, dem er bemyndiget af den dataansvarlige.I det omfang den Dataansvarlige ønsker, at tilsynsbesøg efter punkt 8.4 skal omfatte den behandling som sker hos underdatabehandlere, aftales dette særskilt (jf. punkt 8.3 ovenfor).

8. Overførsel af personoplysninger til et tredjeland

8.1. Den Dataansvarlige giver herved samtykke til, at Databehandleren kan anvende underdatabehandlere (”Underdatabehandlere”) til opfyldelse af Databehandlerens ydelser i henhold til Aftalen. Det er Databehandlerens ansvar, at Underdatabehandlere opfylder sine databeskyttelsesforpligtelser efter Lovgivningen.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.

8.2. 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.

8.3. 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.

8.4. 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 5

8.5. 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.

9. Ophør af Databehandleraftalen

9.1. Databehandleraftalen kan kun opsiges samtidig med opsigelse af Handelsbetingelserne.

9.2. Databehandlerens bemyndigelse til, at behandle personoplysninger på vegne af den Dataansvarlige bortfalder ved Databehandleraftalens ophør, uanset årsagen hertil.

9.3. Databehandleren og dennes underdatabehandlere skal tilbagelevere alle personoplysninger til den Dataansvarlige ved Databehandleraftalens ophør, i det omfang den Dataansvarlige ikke allerede er i besiddelse af personoplysningerne. Databehandleren er herefter forpligtet til at slette alle personoplysninger modtaget fra den Dataansvarlige. Den Dataansvarlige kan anmode om fornøden dokumentation herfor.

10. Ansvar

10.1. Databehandleren skal skadesløs holde den Dataansvarlige, den Dataansvarliges koncernselskaber eller dennes hertil knyttede selskaber for ethvert tab, som den Dataansvarlige, den Dataansvarliges koncernselskaber eller dennes hertil knyttede selskaber ifalder som følge af overtrædelser af Databeskyttelseslovgivningen, hvis et sådant tab skyldes, at Databehandleren ikke har opfyldt de forpligtelser i Databeskyttelseslovgivningen, som er rettet mod databehandler, eller har undladt at følge eller handlet i strid med den Dataansvarliges lovlige instrukser, jf. artikel 82, stk. 2 i Forordning om Databeskyttelse. Databehandleren skal tage alle fornødne skridt til at forsvare sig mod påstande om overtrædelse af Databeskyttelseslovgivningen.

11. Lovvalg og værneting

11.1. Databehandleraftalen er underlagt dansk lovgivning.

11.2. Enhver tvist, der måtte opstå i forbindelse med Databehandleraftalen, såfremt tvisten ikke kan afgøres i mindelighed, afgøres ved byretten i København.

12. Bilag

12.1. Bilag 1: Kategorier af registrerede brugere og personoplysninger

12.2. Bilag 2: Lokation for behandling af personoplysninger

12.3. Bilag 3: Krav til sikkerhedsforanstaltninger

12.4. Bilag 4: Underdatabehandlere

12.5. Bilag 5: Bilag 5 - Instruks vedrørende behandling af personoplysninger

Underskrifter

Dato: 9. nov. 2023
Email: magnus@uniqkey.eu
Signatur: Magnus Cohn (9. nov. 2023 13:52 GMT+1)

Dato: 8. nov. 2023
Email: mikja@itm8.com
Signatur: Mikael Kjærgaard (8. nov. 2023 21:21 GMT+1)

Bilag 1.

Kategorier af registrerede brugere og personoplysninger.

1. **Kategorier af registrerede brugere**
   - Den Dataansvarliges, den Dataansvarliges koncernselskabers samt hertil knyttede selskabers IT-ansvarlige
   - Den Dataansvarliges, den Dataansvarliges koncernselskabers samt hertil knyttede selskabers medarbejdere
   - Den Dataansvarliges, den Dataansvarliges koncernselskabers samt hertil knyttede selskabers kontaktpersoner
   - Andre som Den Dataansvarliges har givet adgang til Uniqkey appen

2. **Kategorier af personoplysninger**
   - Personligt navn
   - Postadresse
   - Telefon nummer
   - E-mail
   - Anvendte IP-adresser ved adgang/brug af Uniqkey appen.
   - De sidste 4 cifre af et eventuelt tilmeldt betalingskort samt kortets udløbsdato.

3. **Behandlingsaktiviteterne**
   Personoplysningerne vil blandt andet blive genstand for følgende grundlæggende behandling:
   Enhver operation eller et sæt af operationer, der udføres på personoplysninger eller på sæt af personoplysninger, sker udelukkende ved automatiserede midler, såsom indsamling, registrering, organisering, strukturering, opbevaring, tilpasning eller ændring, hentning, konsultation, brug, videregivelse ved transmission, formidling eller på anden måde stille til rådighed, justering eller kombination, begrænsning, sletning eller destruktion.
   Databehandleren behandler kun data automatisk og gemmer Dataansvarlige data. Databehandleren har ikke adgang til og er ikke bekendt med indholdet af kundedata, medmindre kunden specifikt instruerer Databehandleren om at få adgang hertil.
   Databehandler opbevarer og tager back up af tilgængelige data i systemet på vegne af Dataansvarlige så længe at Dataansvarlige har en aktiv kontrakt hos Databehandler. data vil blive sat til sletning ved kontraktudløb og vil blive slettet en måned efter endt periode

Bilag 2.

Lokation for behandling af personoplysninger:

Dette bilag udgør en integreret del af Databehandleraftalen og skal udfyldes af Parterne.

1. LOKATIONER FOR BEHANDLING AF PERSONOPLYSNINGER

Databehandlingen sker på følgende lokationer:

- Lyskær 8 A, 2730 Herlev, Danmark
- ScanNet-datacentre i Danmark

Bilag 3.

Krav til sikkerhedsforanstaltninger

Databehandlerens behandling vil blandt andet være underlagt følgende sikkerhedsforanstaltninger implementeret efter standarder svarende til f.eks. ISO27001:

- Indføre log-in- og adgangskodeprocedurer der sikrer, at alle medarbejdere hos Databehandleren har unikke brugernavne og kodeord. Brugernavnene og kodeord er oprettet og opdateret i overensstemmelse med anerkendte principper.

- Sikre, at alene medarbejderne med arbejdsrelaterede formål hertil har adgang til personoplysningerne omfattet af Databehandleraftalen.
  Medarbejderne modtager passende uddannelse samt fyldestgørende instruktioner i og retningslinjer for behandlingen af personoplysningerne omfattet af Databehandleraftalen. Databehandleren er forpligtet til at sikre, at de medarbejdere, som er involveret i behandlingen af disse personoplysninger, er bekendte med samtlige sikkerhedskrav og indholdet i dette bilag.

  Adgang til systemer og data skal sikres gennem brugerstyring og autorisationer. Databehandlerens medarbejdere er kun autoriseret til at tilgå personoplysninger under denne databehandleraftale for drift eller tekniske formål.

  Databehandleren kontrollerer og opdaterer alle medarbejderes autorisationer periodisk og som minimum en gang årlig.
  Det er ikke muligt at opnå adgang til systemer og data under denne databehandleraftale ved brug af en anonym brugerkonto eller gæstekonto.

- Opsætning og vedligeholdelse af firewalls, anti-virus/anti-malware software og andre tekniske løsninger skal sikre beskyttelse mod uautoriseret adgang samt at uautoriseret adgang opdages og rapporteres til den Dataansvarlige uden unødig forsinkelse.

- Enhver adgang til systemer og data relateret til ydelsen vil automatisk blive logget. Tidspunkt, brugernavn, type af applikation og personen, den pågældende data vedrører eller de søgekriterier, der er brugt, bliver logget. Loggen opbevares i minimum seks måneder, og slettes efter maksimum tooghalvfjerds måneder.

  Den Dataansvarlige kan udbede sig en udskrift af loggen ved anmodning herom.
  Når data er tilgået i forbindelse tekniske spørgsmål, support, fejlsøgning eller andre tekniske grunde, vil sådan adgang blive logget.

- Opbevaring af datalagermedier sker på forsvarlig vis, således at disse ikke er tilgængelige for tredjemand, Data der indeholder personoplysninger under denne databehandleraftale opbevares fysisk eller logisk adskilt fra data tilhørende andre af Databehandlerens kunder. Sikring af bygninger samt adgangsforhold ved implementering af foranstaltninger til at forhindre uautoriserede personer i at få adgang til it-systemer samt fysisk materiale der indeholder personoplysninger omfattet af Databehandleraftalen.

- For systemer der anvendes i forbindelse med databehandlingen sikres det, at der anvendes hardware og software af høj kvalitet, som opdateres løbende samt er supporteret af leverandøren.

  I tilfælde af genbrug, kassering, udbedring eller service på disk-medier brugt i relation til den Dataansvarliges data, er det sikret, at tredjeparter ikke kan opnå adgang til den Dataansvarliges data på sådanne medier. Sikkerhedsprocedurer udføres enten via kryptering eller via sletning eller overskrivning, svarende til standarden DOD 5220-22- M, for at sikre, at tidligere opbevarede data for Dataansvarlige ikke kan genskabes.

  Hvis det er muligt, skal harddiske makuleres ved bortskaffelse, hvis disse har indeholdt personoplysninger, der behandles under denne databehandleraftale.

  Alle manuelle registre, der indeholder Dataansvarliges data (f.eks. fysiske dokumenter) vil blive afviklet eller slettet på en sikker måde, når de fysiske dokumenter har opfyldt deres formål. Dette kan ske via makulering eller andre måder, der sikrer, at adgang til Dataansvarliges data ikke er mulig.

- Kryptering der er baseret på generelt anerkendte algoritmer, der som minimum vil svare til SSL 256bit., benyttes som standard ved transmission af data.

  Benytter Databehandleren trådløse forbindelser, er disse sikret ved anvendelse af anerkendte krypteringsalgoritmer.

  Der udarbejdes og implementeres politikker og procedurer for fjernarbejde, hvor dette giver adgang til personoplysninger under denne databehandleraftale. Fjernadgang sikres ved anvendelse af VPN eller lignende.

Databehandleren skal en gang årligt afgive revisionserklæring eller tilsvarende dokumentation til den Dataansvarlige, der viser, at de i denne Databehandleraftale nævnte sikkerhedstiltag er varetaget af Databehandleren.

Bilag 4 - Underdatabehandlere

4.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere:

NAVN/ADRESSE	CVR	LOKATION FOR BEHANDLING	BESKRIVELSE AF BEHANDLING
team.blue Denmark A/S (ScanNet) Højvangen 4 8660 Skanderborg	CVR: 29412006	Højvangen 4 8660 Skanderborg	Housing, drift og support af servere.

Listen over anvendte underdatabehandlere ved aftaleindgåelse er indsat i ovenstående skema, og bliver reguleret ved tilkøb eller ændringer i services.

Efter Bestemmelsernes ikrafttræden må databehandleren gøre brug af andre underdatabehandlere. Den dataansvarlige vil blive informeret om ændringer i anvendte underdatabehandlere ved tilkøb af nye services eller databehandlerens ændringer af services. Derudover kan et bilag over aktuelt anvendte underdatabehandlere leveres ved forespørgsel.

Databehandlerens meddelelse om planlagte ændringer vedrørende tilføjelse eller erstatning af underdatabehandlere sker som beskrevet i 4.2.

4.2. Varsel for godkendelse af underdatabehandlere

Databehandlerens underretning om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af underdatabehandlere skal være den dataansvarlige i hænde minimum 30 dage, før anvendelsen eller ændringen skal træde i kraft, så vidt dette umiddelbart er muligt.

Uanset ovenstående accepterer den dataansvarlige, at der kan være særlige tilfælde, hvor der kan opstå et konkret behov for, at ændringen vedrørende tilføjelse eller erstatning af underdatabehandlere sker med kortere varsel eller straks. I sådanne tilfælde vil databehandleren underrette den dataansvarlige om ændringen snarest muligt.

Såfremt den dataansvarlige har indsigelser mod ændringerne, skal den dataansvarlige give databehandleren meddelelse herom inden ændringens varslede virkningstidspunkt. Den dataansvarlige kan alene gøre indsigelse, hvis den dataansvarlige har rimelige, konkrete årsager hertil.

Ved den dataansvarliges indsigelse accepterer den dataansvarlige samtidig, at databehandleren kan være forhindret i at levere hele eller dele af de aftalte tjenester. Sådan manglende opfyldelse kan ikke tilskrives databehandlerens misligholdelse. Databehandleren opretholder sit krav på betaling for sådanne ydelser, uanset de ikke kan leveres til den dataansvarlige.

Hvor det er særligt aftalt, at databehandleren ikke må gøre brug af underdatabehandlere uden den dataansvarliges forudgående tilladelse, accepterer den dataansvarlige, at dette kan medføre, at databehandleren kan blive afskåret fra at opfylde Services. Hvis den dataansvarlige har afslået, at der foretages ændringer vedrørende tilføjelse eller erstatning af underdatabehandlere, vil manglende levering af tjenester derfor ikke anses for en misligholdelse af parternes aftale vedrørende levering af Services, som kan tilskrives databehandleren i de tilfælde, hvor den manglende opfyldelse kan henføres til en underdatabehandlers forhold.

Bilag 5 - Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks
Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker i henhold til de indgåede aftaler mellem den dataansvarlige og databehandleren.

Databehandleren baserer sit ledelsessystem for informationssikkerhed på principperne i ISO 27001 sikkerheds-framework og har implementeret de relevante kontroller, standarden definerer. Derudover har databehandleren implementeret et ledelsessystem for sikker behandling af persondata.

Den dataansvarlige har instrueret databehandleren i at behandle data ud fra de Services, der er indgået aftale om og ud fra nedenstående instrukser.

Den dataansvarlige instruerer her med databehandleren at gemme og distribuere brugernavne og passwords, så login informationerne er sikret at være forskellige samt at kunne bruges på tværs af enheder og medarbejdere.

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 5.1 og 5.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

På den dataansvarliges specifikke anmodning bistår databehandleren 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 udøvelse af de registreredes rettigheder som fastlagt i databeskyttelsesforordningen.

Hvis en registreret fremsætter anmodning om udøvelse af sine rettigheder over for databehandleren, giver databehandleren uden ugrundet ophold meddelelse herom til den dataansvarlige.

Under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, bistår databehandleren efter specifik anmodning også den dataansvarlige med at sikre overholdelse af den dataansvarliges forpligtelser i forhold til:
- Gennemførelse af passende tekniske og organisatoriske foranstaltninger
- Sikkerhedsbrud
- Underretning om brud på persondatasikkerheden til den registrerede
- Gennemførelse af konsekvensanalyser
- Forudgående høringer fra tilsynsmyndighederne

C.4 Opbevaringsperiode/sletterutine
Den dataansvarlige disponerer selv over personoplysninger, som databehandleren behandler på vegne af den dataansvarlige. De personoplysninger, der er overladt til databehandlerens behandling, opbevares derfor, indtil den dataansvarlige selv sletter oplysningerne eller indtil ophør af Services vedrørende behandling af personoplysninger.

Ved sletning af personoplysninger i den dataansvarliges systemer, vil disse personoplysninger blive slettet i databehandlerens backupsystem ud fra den aftalte opbevaringsperiode (backuphistorik) for hvert enkelt system.

Databehandleren bistår på den dataansvarliges anmodning med sletning eller tilbagelevering af personoplysninger som nærmere instrueret af den dataansvarlige.

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:

Behandlingen af persondata sker på databehandlerens adresser samt de anførte databehandlere og deres underdatabehandleres adresser. Derudover kan der udføres remote arbejde i overensstemmelse med databehandlerens politik for remote arbejde.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande
Den dataansvarlige har bemyndiget og dermed instrueret databehandleren i at overføre personoplysninger til et tredjeland som nærmere specificeret nedenfor. Den dataansvarlige kan herudover ved en efterfølgende skriftlig meddelelse eller aftale angive en instruks eller konkret godkendelse vedrørende overførsel af personoplysninger til et tredjeland.

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.

<u>C.6.1 Generel godkendelse vedrørende overførsel af personoplysninger til sikre tredjelande</u>
Den dataansvarlige giver ved Bestemmelserne sin generelle og forudgående godkendelse (instruks) til, at databehandleren kan foretage overførsel af personoplysninger til tredjelande, hvis Kommissionen har fastslået, at tredjelandet/det relevante område/den relevante sektor har et tilstrækkeligt beskyttelsesniveau.

<u>C.6.2 Godkendelse af overførsel til specifikke modtagere af personoplysninger i tredjelande, når der er sikret fornødne garantier</u>
Den dataansvarlige instruerer databehandleren til at anvende nedenstående underdatabehandler(e), hvor der sker overførsel af personoplysninger til tredjelande:

NAVN	CVR	BESKRIVELSE AF BEHANDLING	OVERFØRSEL TIL TREDJELAND

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 Services.

Såfremt EU-Kommissionens standardkontrakter (”SCC”) for overførsel af personoplysninger til et tredjeland anvendes som overførselsgrundlag, er databehandleren og/eller evt. underdatabehandleren berettiget til at indgå disse SCC’er med den relevante underdatabehandler.

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.

2023 - DPA DK Sep DPA_30052023

Endelig revisionsrapport 2023-11-09

Oprettet:	2023-11-08
Af:	Adam Lindberg (ahl@uniqkey.eu)
Status:	Underskrevet
Transaktions-id:	CBJCHBCAABAAjDNhxRTplBuqDutfIs78wGf8CqEzukbN

Oversigt over "2023 - DPA DK Sep DPA_30052023"

Dokument oprettet af Adam Lindberg (ahl@uniqkey.eu)
2023-11-08 - 12:01:08 GMT

Dokumentet blev sendt til Magnus Cohn (magnus@uniqkey.eu) til underskrivelse
2023-11-08 - 12:06:30 GMT

Dokumentet blev sendt til Mikael Kjærgaard (mikja@itm8.com) til underskrivelse
2023-11-08 - 12:06:30 GMT

E-mail blev vist af Mikael Kjærgaard (mikja@itm8.com)
2023-11-08 - 20:18:44 GMT

Dokumentet blev e-underskrevet af Mikael Kjærgaard (mikja@itm8.com)
Dato for signatur: 2023-11-08 - 20:21:20 GMT - tidskilde: server

E-mail blev vist af Magnus Cohn (magnus@uniqkey.eu)
2023-11-09 - 12:52:02 GMT

Dokumentet blev e-underskrevet af Magnus Cohn (magnus@uniqkey.eu)
Dato for signatur: 2023-11-09 - 12:52:11 GMT - tidskilde: server

Aftale fuldført.
2023-11-09 - 12:52:11 GMT