

Databehandleraftale

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

mellem

Navn:

CVR:

Adresse:

Postnummer:

By:

Land:

herefter "den dataansvarlige"

og

Navn: Didaktiko ApS

CVR: 40291040

Adresse: Rådyret 58

Postnummer: 9530

By: Støvring

Land: Danmark

herefter "databehandleren"

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

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

1. Indhold

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

2. 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 produkterne 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 tre 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. 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.

3. Den dataansvarliges rettigheder og forpligtelser

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes 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.

4. Databehandleren handler efter instruks

1. Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt. Denne instruks skal være specificeret i bilag A og C. Efterfølgende instruks kan også gives af den dataansvarlige, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Bestemmelser.
2. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

5. Fortrolighed

1. Databehandleren må kun give adgang til personoplysninger, som behandles på den dataansvarliges vegne, til personer, som er underlagt databehandlerens instruktionsbeføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, og kun i det nødvendige omfang. Listen af personer, som har fået tildelt adgang, skal løbende gennemgås. På baggrund af denne gennemgang kan adgangen til personoplysninger lukkes, hvis adgangen ikke længere er nødvendig, og personoplysningerne skal herefter ikke længere være tilgængelige for disse personer.
2. Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de pågældende personer, som er underlagt databehandlerens instruktionsbeføjelser, er underlagt ovennævnte tavshedspligt.

6. Behandlingssikkerhed

1. Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databehandleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder, gennemfører passende tekniske og organisatoriske foranstaltninger for at sikre et beskyttelsesniveau, der passer til disse risici.

Den dataansvarlige skal vurdere risiciene for fysiske personers rettigheder og frihedsrettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

- a. Pseudonymisering og kryptering af personoplysninger
 - b. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
 - c. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
 - d. en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.
2. Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvarlige – også vurdere risiciene for fysiske personers rettigheder som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Med henblik på denne vurdering skal den dataansvarlige stille den nødvendige information til rådighed for databehandleren som gør vedkommende i stand til at identificere og vurdere sådanne risici.
 3. Databehandleren skal 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.

7. Anvendelse af underdatabehandlere

1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).
2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående specifik skriftlig godkendelse fra den dataansvarlige. Listen over underdatabehandlere, som den dataansvarlige har godkendt, fremgår af bilag B.
3. Ved udskiftning af underdatabehandlere eller benyttelse af nye underdatabehandlere, kræves forudgående godkendelse fra den Dataansvarlige.
4. Databehandleren skal sikre sig, at dennes underdatabehandlere overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

8. Overførsel til tredjelande eller internationale organisationer

1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra den dataansvarlige og skal altid ske i overensstemmelse med databeskyttelsesforordningens kapitel V.
2. Hvis overførsel af personoplysninger til tredjelande eller internationale organisationer, som databehandleren ikke er blevet instrueret i at foretage af den dataansvarlige, kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, skal databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende

ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:
 - a. overføre personoplysninger til en dataansvarlig eller databehandler i et tredjeland eller en international organisation
 - b. overlade behandling af personoplysninger til en underdatabehandler i et tredjeland
 - c. behandle personoplysningerne i et tredjeland
4. Disse Bestemmelser skal ikke forveksles med standardkontraktbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

9. Bistand til den dataansvarlige

1. Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel III.

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

- a. oplysningspligten ved indsamling af personoplysninger hos den registrerede
 - b. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
 - c. indsigtretten
 - d. retten til berigtigelse
 - e. retten til sletning ("retten til at blive glemt")
 - f. retten til begrænsning af behandling
 - g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
 - h. retten til dataportabilitet
 - i. retten til indsigelse
 - j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering
2. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3., bistår databehandleren endvidere, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, den dataansvarlige med:
 - a. den dataansvarliges forpligtelse til uden unødigt forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder

- b. den dataansvarliges forpligtelse til uden unødigt forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder
- c. den dataansvarliges forpligtelse til forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)
- d. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet, inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.

10. Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødigt forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.
2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 72 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, Datatilsynet. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge forordningens artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:
 - a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
 - b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden
 - c. de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.
4. Parterne skal i bilag C angive den information, som databehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

11. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databehandleren forpligtet til at tilbagelevere alle personoplysningerne og slette eksisterende kopier, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne.

12. Revision, herunder inspektion

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.
2. Procedurene for den dataansvarliges inspektioner med databehandleren er nærmere angivet i Bilag C.5.
3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

13. Parternes aftale om andre forhold

1. Parterne kan aftale andre bestemmelser vedrørende tjenesten vedrørende behandling af personoplysninger om f.eks. erstatningsansvar, så længe disse andre bestemmelser ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den registreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databeskyttelsesforordningen.

14. Ikrafttræden og ophør

1. Bestemmelserne træder i kraft på datoen for begge parter underskrift heraf.
2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.
3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.
4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.3, kan Bestemmelserne opsiges med skriftligt varsel af begge parter.

15. Underskrift

På vegne af den dataansvarlige

Navn
Stilling
Telefonnummer
E-mail

Underskrift

På vegne af databehandleren

Navn
Stilling
Telefonnummer
E-mail

Underskrift

UDKAST

Bilag A Oplysninger om behandlingen

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

Behandling af den Dataansvarliges personoplysninger sker i overensstemmelse med et eller flere af følgende formål:

- a. at formidle og/eller levere produkter, tjenesteydelser og læringsmidler, som du eller din uddannelsesinstitution har bestilt
- b. at besvare eventuelle spørgsmål eller indsigelser du måtte have
- c. for at underrette dig om ændringer i vores ydelser
- d. for at sende dig direkte markedsføring, herunder for at give dig oplysninger om de produkter og tjenesteydelser, du tidligere har købt hos os, eller som du har rettet forespørgsel om, og for at du kan deltage i konkurrencer eller kampagner
- e. for at forhindre misbrug og svindel
- f. for at forbedre vores hjemmeside, produkter, tjenesteydelser og læremidler
- g. for at opbevare personoplysninger i det omfang, det er nødvendigt for at overholde bogføringsloven, forbrugeraftaleloven og andre retlige forpligtelser Didaktiko ApS måtte have.

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

Databehandleren stiller den digitale portal til rådighed for den Dataansvarlige til brug til undervisning. Databehandleren registrerer og opbevarer herigennem personoplysninger på vegne af den dataansvarlige

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

A.3.1. For brugere af systemet:

UNI-Login brugernavn	Indtastes til login. Bruger oprettes automatisk i systemet med brugernavn tilsvarende UNI-Login brugernavnet til fremtidig login.	<i>Kræver ikke dataaftale</i>
Institutionstilknytning samt rolle	Hentes ved brugeroprettelse for UNI-Login brugernavn via <i>ws71/wsiBRUGER hentBrugersInstitutionstilknytning er</i> Brugerens tilknytning (institution) og rolle (lærer, elev, forældre mv.) gemmes.	<i>Kræver ikke dataaftale</i>
Oplysninger om en institution	Hentes via <i>ws22/wsiINST hentInstitution.</i> Hentes for hver institution som et UNI-Login brugernavn er tilknyttet, hvis ikke allerede oprettet.	<i>Kræver ikke dataaftale</i>

Yderligere information om relevante UNI-Logins webservice:

ws22/wsiINST <https://viden.stil.dk/pages/viewpage.action?pagelid=2360664>

ws71/wsiBRUGER <https://viden.stil.dk/pages/viewpage.action?pagelid=2360665>

Ovennævnte oplysninger trækkes automatisk fra STIL's UNI-Login system, når en bruger logger ind på portal.didaktiko.dk. Brugere af de forskellige apps bliver kun bedt om UNI-Login hvis kontoejeren (eksempelvis læreren) har valgt, at brugerne (eksempelvis eleverne) skal logge ind med UNI-Login. Elever oprettes derfor ikke i systemet automatisk.

A.3.2. For brugere af GeoQuiz:

Vores GeoQuiz bruger Google Maps API til visuelt at præsentere geografisk information. Når Google Maps bruges, opsamles, behandles og bruges Google af Google Maps (Google Inc., 1600 Amphitheater Parkway, Mountain View, California, 94043). Du kan finde detaljerede oplysninger om databehandlingen hos Google fra databeskyttelsesmeddelelser fra Google, som du kan få adgang til på følgende links:

- https://developers.google.com/maps/documentation/android-sdk/play-data-disclosure?fbclid=IwAR0aDDoBbmV89nuD0bXZaHk3GqZ4499Ha_P6FnIHLyVw3N7aiFTQZNUCK9E
- https://policies.google.com/privacy?fbclid=IwAR2FIXY_EW8IUmpO_vJDw9ChUY_J5GFozeNk73o_am-dGUCLTSyY2nkef9l

A.4 Andre behandlinger

Slutbrugerne bliver bedt om følgende i forbindelse med afvikling af forskellige aktivitetstyper:

- QR Quiz - Slutbrugeren skal tillade brugen af kamera i webappen for at gennemføre aktiviteten (scanne QR koder).
Der bliver ikke gemt billeder under aktiviteten.
- GeoQuiz - Slutbrugeren skal tillade lokaltetstjeneste for at anvende GPS-aktiviteten. Dette gøres for at sikre brugeroplevelsen og brugen af aktiviteten generelt.
Didaktiko gemmer ikke slutbrugernes data herfra.
- Evaluering - Slutbrugeren logger ind med UNI-Login. Samme vilkår som pkt. A.3.1.
- Slutbrugernes egne indtastede data, herunder alias og svar på spørgsmål lagres men er ikke personhenførbare.

A.5. Behandlingen omfatter følgende kategorier af registrerede

Behandlingen omfatter den Dataansvarliges medarbejdere, slutbrugere og kontrakt personer.

A.6. Behandlingens varighed

Aftalen er gældende, så længe Databehandleren behandler personoplysninger på vegne af den Dataansvarlige i forbindelse med den Dataansvarliges brug af applikationen

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	REG. No.	ADRESSE	BESKRIVELSE AF BEHANDLING
team.blue Denmark A/S	CVR-nr.: 29412006	Højvangen 4, 8660 Skanderborg, Danmark	Hosting
tawk.to inc.		187 East Warm Springs Rd, SB298 Las Vegas, NV, 89119	Chat og support system.
Google Maps API*		Google Inc., 1600 Amphitheater Parkway, Mountain View, California, 94043	Sikrer brugeroplevelse samt nøjagtig placering ifm. aktivitet (GeoQuiz)

*Beskrivelse af Google Maps API i GeoQuiz app

Didaktiko GeoQuiz anvender Google Maps API til visuelt at præsentere geografisk information. Når Google Maps bruges, opsamles, behandles og bruges Google af Google Maps (Google Inc., 1600 Amphitheater Parkway, Mountain View, California, 94043). Du kan finde detaljerede oplysninger om databehandlingen hos Google fra databeskyttelsesmeddelelser fra Google, som du kan få adgang til på følgende links:

- https://developers.google.com/maps/documentation/android-sdk/play-data-disclosure?fbclid=IwAR0aDDoBbmV89nuD0bXZaHk3GqZ4499Ha_P6FnIHLYVw3N7aiFTQZNUCK9E
- https://policies.google.com/privacy?fbclid=IwAR2FIXY_EW8IUmpO_vJDw9ChUY_J5GFozeNk73o_am-dGUCLTSyY2nkef9l

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

Bilag C Instruks vedrørende behandling af personoplysninger

C.1. Behandlingens genstand/instruks

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

Generel drift, herunder hosting, visning, organisering, modtagelse, indhentelse, videresendelse, tilpasning, implementering, søgning, lagring, gendannelse, sletning, vedligeholdelse, udvikling, support, fejlfinding og andre it-ydelser forbundet med Databehandlerens levering af en digital portal, som kan benyttes til quizspil og evaluering.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

Databehandleren skal træffe de nødvendige og organisatoriske sikkerhedsforanstaltninger, som måtte være nødvendige, mod at de i bilag A anførte personoplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med databeskyttelseslovgivningen.

Databehandleren skal sikre, at de medarbejdere, der er involveret i at behandle personoplysninger til stadighed er bekendt med og har tilstrækkelig uddannelse og instruktion om databehandlings formål, politikker, arbejdsgange og om deres tavshedspligt.

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.

Kommunikationsforbindelser og kryptering

Databehandleren har passende tekniske foranstaltninger til at beskytte systemer og netværk, herunder beskyttelse data under transmission og adgang via internettet, samt til at begrænse risikoen for uautoriseret adgang og/eller installation af skadelig kode.

Databehandleren anvender passende krypteringsteknologier og andre tilsvarende foranstaltninger i overensstemmelse med kravene i lovgivningen, godkendte standarder for kryptering af klassificeret information samt god databehandlingskik.

Antivirus

Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.

Sikkerhedskopiering

Databehandler skal have interne beredskabsprocedurer, der sikrer genetablering af services uden ugrundet ophold i tilfælde af driftsafbrydelser i henhold til hovedaftalen. Databehandleren sikrer backup.

Anvendelse af hjemme/fjernarbejdspladser Såfremt der foretages databehandling fra ad hoc og/eller hjemmearbejdspladser, sikre Databehandleren at disse lever op til de sikkerhedsmæssige krav i denne Databehandleraftale med bilag og lovgivning i øvrigt.

C.3 Opbevaringsperiode/sletterutine

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

Persondata skal kunne slettes på den Dataansvarliges forespørgsel og inden for rimelige tid.

C.4 Lokaltet for behandling

Behandling af de af Bestemmelserne omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end Didaktiko ApS' hovedkontor, samt ad hoc arbejdspladser

C.5 Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behandlingen af personoplysninger, som er overladt til databehandleren

Den dataansvarlige eller en repræsentant for den dataansvarlige har mulighed for at foretage en fysisk inspektion af lokaliteterne, hvorfra databehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen, med henblik på at fastslå databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Den dataansvarliges eventuelle udgifter i forbindelse med en fysisk inspektion afholdes af den dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer (hovedsageligt den tid), der er nødvendigt for, at den dataansvarlige kan gennemføre sin inspektion.