



Databehandleraftale

Revision: 2022 version 1

mellem

Virksomhed:

Hovedområde/afdeling (hvis relevant):

Adresse:

CVR nr.:

("den dataansvarlige")

og

UniHelper ApS

Ugelrisvej 40

9632 Møldrup

CVR nr. 39750007

("databehandleren")

(tilsammen benævnt "Parterne")

1. Baggrund for databehandleraftalen

- 1.1 Denne aftale fastsætter de rettigheder og forpligtelser, som finder anvendelse, når databehandleren foretager behandling af personoplysninger på vegne af den dataansvarlige.
- 1.2 Aftalen 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), som stiller specifikke krav til indholdet af en databehandleraftale.
- 1.3 Ved "personoplysning" forstås enhver form for information om en identificeret eller identificerbar fysisk person, jf. artikel 4(1) i databeskyttelsesforordningen. Hvis der som led i opfyldelsen af aftalen behandles andre fortrolige oplysninger end personoplysninger, for eksempel oplysninger som i medfør af parternes aftale, forvaltningsloven eller andet anses for fortrolige, så omfatter enhver henvisning til "personoplysninger" også de øvrige fortrolige oplysninger.
- 1.4 Databehandlerens behandling af personoplysninger sker med henblik på opfyldelse af parternes "hovedaftale"
- 1.5 Databehandleraftalen og "hovedaftalen" er indbyrdes afhængige, og kan ikke opsiges særskilt. Databehandleraftalen kan dog – uden at opsige "hovedaftalen" – erstattes af en anden gyldig databehandleraftale. "Hovedaftalen" kan også erstattes af en lignende hovedaftale uden at parterne behøver underskrive en ny databehandleraftale.
- 1.6 Denne databehandleraftale har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne, herunder i "hovedaftalen".

- 1.7 Til denne aftale hører fem bilag. Bilagene fungerer som en integreret del af databehandleraftalen.
- 1.8 Databehandleraftalens Bilag A indeholder nærmere oplysninger om behandlingen, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.
- 1.9 Databehandleraftalens Bilag B indeholder den dataansvarliges betingelser for, at databehandleren kan gøre brug af eventuelle underdatabehandlere, samt en liste over de eventuelle underdatabehandlere, som den dataansvarlige har godkendt.
- 1.10 Databehandleraftalens Bilag C indeholder en nærmere instruks om, hvilken behandling databehandleren skal foretage på vegne af den dataansvarlige (behandlingens genstand), hvilke sikkerhedsforanstaltninger, der som minimum skal iagttages, samt hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.
- 1.11 Databehandleraftalens Bilag D indeholder parternes eventuelle regulering af forhold, som ikke ellers fremgår af databehandleraftalen eller parternes "hovedaftale".
- 1.12 Databehandleraftalens Bilag E indeholder et skema til underretning af den dataansvarlige ved brud på datasikkerheden.
- 1.13 Databehandleraftalen med tilhørende bilag opbevares skriftligt, herunder elektronisk af begge parter.
- 1.14 Denne databehandleraftale frigør ikke databehandleren for forpligtelser, som efter databeskyttelsesforordningen eller enhver anden lovgivning direkte er pålagt databehandleren.
- 2. Den dataansvarliges forpligtelser og rettigheder**
- 2.1 Den dataansvarlige har over for omverdenen (herunder den registrerede) som udgangspunkt ansvaret for, at behandlingen af personoplysninger sker inden for rammerne af databeskyttelsesforordningen og databeskyttelsesloven.

- 2.2 Den dataansvarlige har derfor både rettighederne og forpligtelserne til at træffe beslutninger om, til hvilke formål og med hvilke hjælpemidler der må foretages behandling.
- 2.3 Den dataansvarlige er blandt andet ansvarlig for, at der foreligger hjemmel til den behandling, som databehandleren instrueres i at foretage.
- 2.4 Det er den dataansvarliges ansvar at sikre, at der alene overlades personoplysninger til databehandleren, som er relevante, nødvendige og begrænset til det formål, som den dataansvarlige har med behandlingen samt, at personoplysningerne er korrekte.

3. Behandlingen af personoplysninger

- 3.1 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; i så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.
- 3.2 Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.
- 3.3 Databehandleren iværksætter alle foranstaltninger, som kræves i henhold til databeskyttelsesforordningens artikel 32, hvoraf det bl.a. fremgår, at der under hensyntagen til det aktuelle niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder skal gennemføres passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.
- 3.4 Ovenstående forpligtelse indebærer, at databehandleren skal foretage en risikovurdering, og herefter gennemføre foranstaltninger for at imødegå identificerede risici. Der kan herunder bl.a., alt efter hvad der er relevant, være tale om følgende foranstaltninger:

- 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

3.5 Databehandleren er forpligtet til at foretage databehandlingen rettidigt og i overensstemmelse med aftalen, herunder alene efter den herved afgivne instruks. Databehandleren er endvidere forpligtet til at udføre sine forpligtelser med den kompetence, forsigtighed, omhu og forudseenhed, der normalt kan forventes af en erfaren og kompetent leverandør på området, og på et niveau, der som et minimum svarer til den til enhver tid alment anerkendte branchestandard. De tekniske løsningers kvalitet og funktionalitet såvel som de tilknyttede personers færdigheder og kompetence er omfattet af databehandlerens forpligtelser.

3.6 Databehandleren skal i forbindelse med ovenstående – i alle tilfælde – som minimum iværksætte det sikkerhedsniveau og de foranstaltninger, som er specificeret nærmere i denne aftales Bilag C.

3.7 Parternes eventuelle regulering/aftale om vederlæggelse eller lign. i forbindelse med den dataansvarliges eller databehandlerens efterfølgende krav om etablering af yderligere sikkerhedsforanstaltninger vil fremgå af parternes "hovedaftale" eller af denne aftales Bilag D.

4. Fortrolighed og tavshedspligt

4.1 Databehandleren skal begrænse adgangen til personoplysningerne til de medarbejdere, for hvem det er nødvendigt at have adgang til personoplysninger for at kunne opfylde databehandlerens forpligtelser over for den dataansvarlige.

4.2 Databehandleren sikrer, at de personer, der er autoriseret til at behandle personoplysninger på vegne af den dataansvarlige, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

- 4.3 Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de relevante medarbejdere er underlagt ovennævnte tavshedspligt.
- 4.4 Forpligtelsen til at overholde regler om fortrolighed og tavshedspligt gælder uden tidsbegrænsning. Efter samarbejdets ophør er databehandleren forpligtet til at returnere eller destruere alle data, uanset om dette foreligger i fysisk eller elektronisk form, til den dataansvarlige, og slette eller destruere alle kopier heraf, medmindre EU-retten eller national ret foreskriver opbevaring af personoplysningerne. Oplysninger slettes ikke nødvendigvis fra backups, men det sikres at dataene ikke bliver gendannet senere.

5. Andre databehandlere

- 5.1 Databehandleren må ikke gøre brug af en anden databehandler (underdatabehandler) uden forudgående specifik eller generel skriftlig godkendelse fra den dataansvarlige. I tilfælde af generel skriftlig godkendelse skal databehandleren underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre databehandlere og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer.
- 5.2 Når databehandleren har den dataansvarliges godkendelse til at gøre brug af en underdatabehandler, sørger databehandleren for at pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er fastsat i denne databehandleraftale, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen opfylder kravene i databeskyttelsesforordningen.
- 5.3 Efter anmodning fra den dataansvarlige skal databehandleren levere en kopi af underdatabehandleraftalen senest 30 dage efter, at den dataansvarlige har anmodet databehandleren herom. Fremsendes underdatabehandleraftalen ikke rettidigt eller pålægger denne ikke underdatabehandleren mindst de forpligtelser, som databehandleren er underlagt efter databeskyttelsesreglerne og denne databehandleraftale, kan den dataansvarlige ophæve databehandleraftalen/Kontrakten uden yderligere varsel.
- 5.4 Den dataansvarliges nærmere betingelser for databehandlerens brug af eventuelle underdatabehandlere fremgår af denne aftales Bilag B.

5.5 Den dataansvarliges eventuelle godkendelse af specifikke underdatabehandlere er anført i denne aftales Bilag B.

5.6 Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser.

6. Krav til Databehandleren

6.1 Databehandleren skal på den dataansvarliges anmodning give tilstrækkelige oplysninger til, at den dataansvarlige kan påse, at de nævnte tekniske og organisatoriske sikkerhedsforanstaltninger er truffet. Den dataansvarlige kan påse dette ved enten at udføre et tilsyn med databehandleren eller at indhente en revisionserklæring fra databehandleren.

6.2 Databehandleren skal til myndigheder og den dataansvarliges eksterne rådgivere, herunder revisorer, give alle ønskede oplysninger i relation til udførelsen af databehandlingsopgaven, i det omfang oplysningerne er nødvendige for deres opgavevaretagelse i medfør af EU-retten eller lovgivningen i en medlemsstat.

6.3 Databehandleren er desuden forpligtet til at give myndigheder, der efter den til enhver tid gældende lovgivning har adgang til den dataansvarliges og databehandlerens faciliteter, eller repræsentanter, der optræder på myndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

6.4 Den nærmere procedure for den dataansvarliges tilsyn med databehandleren fremgår af denne aftales Bilag C.

6.5 Den dataansvarliges tilsyn med eventuelle underdatabehandlere sker som udgangspunkt gennem databehandleren. Den nærmere procedure herfor fremgår af denne aftales Bilag C.

6.6 Databehandleren skal på opfordring fra den dataansvarlige hjælpe med at opfylde den dataansvarliges forpligtelser i forhold til den registreredes rettigheder efter databeskyttelsesforordningens kapitel 3, herunder blandt andet besvarelse af anmodninger om indsigt i egne oplysninger, udlevering af egne oplysninger, rettelse og

sletning af oplysninger, begrænsning af behandling af den registreredes oplysninger.

- 6.7 Databehandleren bistår den dataansvarlige med at sikre overholdelse af den dataansvarliges forpligtelser i medfør af databeskyttelsesforordningens artikel 32-36 under hensynstagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren.

7. Overførsel af oplysninger til tredjelande eller internationale organisationer

- 7.1 Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, herunder for så vidt angår overførsel (overladelse, videregivelse samt intern anvendelse) af personoplysninger til tredjelande eller internationale organisationer, 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 behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

- 7.2 Hvis den dataansvarlige har givet tilladelse til en overførsel af personoplysninger til et tredjeland eller til internationale organisationer, påhviler det databehandleren at sikre, at der foreligger et lovligt overførselsgrundlag, for eksempel EU Kommissionens standardkontrakter til overførsel af personoplysninger til tredjelande.

8. Underretning om brud på persondatasikkerheden

- 8.1 Databehandleren har pligt til på eget initiativ at søge eventuel tvivl om sikkerhedskravene og opfyldelsen heraf afklaret, herunder ved henvendelse til den dataansvarlige. Databehandleren underretter straks den dataansvarlige, hvis der konstateres brud på persondatasikkerheden hos denne eller en eventuel underdatabehandler.
- 8.2 For at den dataansvarlige har mulighed for at anmelde sikkerhedsbruddet til datatilsynet inden 72 timer, skal databehandleren uden unødigt forsinkelse og om muligt indenfor 24 timer efter at være blevet opmærksom herpå, skriftligt orientere den dataansvarlige om bruddet.
- 8.3 Databehandleren skal - under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for denne – bistå den dataansvarlige med at foretage anmeldelse af

bruddet til tilsynsmyndigheden. Det kan betyde, at databehandleren blandt andet skal hjælpe med at tilvejebringe nedenstående oplysninger, som efter databeskyttelsesforordningens artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse til tilsynsmyndigheden, jf. Bilag E - skema til anmeldelse af sikkerhedsbrud:

- 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) Sandsynlige konsekvenser af bruddet på persondatasikkerheden.
- c) Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden, herunder hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

9. Ændringer og overdragelser

- 9.1 Den dataansvarlige kan til enhver tid ændre denne databehandleraftale uden varsel, hvis ændringen er nødvendig for at overholde de til enhver tid gældende regler og forskrifter for behandling af personoplysninger.
- 9.2 Parterne kan genforhandle aftalen, hvis lovgivning eller uhensigtsmæssigheder giver anledning hertil.
- 9.3 Databehandleren må ikke overdrage sine rettigheder og forpligtelser i henhold til aftalen uden den dataansvarliges forudgående skriftlige samtykke.

10. Ikrafttræden og ophør.

- 10.1 Aftalen træder i kraft ved begge parters underskrift.
- 10.2 Parternes eventuelle regulering/aftale om vederlæggelse, betingelser eller lignende i forbindelse med ændringer af denne aftale vil fremgå af parternes "hovedaftale" eller af denne aftales bilag D.
- 10.3 Opsigelse af databehandleraftalen kan ske i henhold til de opsigelsesvilkår, inkl. opsigelsesvarsel, som fremgår af "hovedaftalen".
- 10.4 Aftalen er gældende, så længe behandlingen består. Uanset "hovedaftalens" og/eller databehandleraftalens opsigelse, vil databehandleraftalen forblive i kraft frem til behandlingens ophør og oplysningernes sletning hos databehandleren og eventuelle underdatabehandlere.

- 10.5 En eventuel (særlig) regulering af konsekvenserne af parternes misligholdelse af databehandleraftalen vil fremgå af parternes "hovedaftale" eller af denne aftales Bilag D.
- 10.6 Databehandleren skal straks efter anmodning fra den dataansvarlige overføre eller slette personoplysninger, som databehandleren behandler for den dataansvarlige, med mindre EU-retten eller lovgivningen i en medlemsstat foreskriver opbevaring af personoplysningerne.
- 10.7 Databehandleren er under ingen omstændigheder berettiget til at betinge den fulde og ubegrænsede efterlevelse af den dataansvarliges instrukser af dennes betaling af udestående fakturaer mv., og databehandleren har ingen tilbageholdsret i personoplysningerne.

11. Underskrift

- 11.1 Ved underskrift forpligter databehandleren sig til at overholde denne aftale om behandling af personoplysninger. Underskriver hos databehandler indestår for at have den fornødne fuldmagt til med bindende virkning at indgå denne aftale på vegne af databehandleren.

Navn:

Navn: Gustav Jacobsen Wengel

Dato:

Dato: 06/01/2022

Underskrift:

Underskrift:



På vegne af den dataansvarlige

På vegne af databehandleren

12. Kontaktpersoner

- 12.1 Parterne kan kontakte hinanden via nedenstående kontaktpersoner/kontaktpunkter, og parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersonen/kontaktpunktet:

Den dataansvarlige

Databehandleren

Navn:

Navn: Gustav Wengel

Stilling:

Stilling: CTO

Telefonnummer:

Telefonnummer: +45 25 36 14 07

Email:

Email: gustav@unihelper.dk

Bilag A Oplysninger om behandlingen

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

- At automatisk inddele de studerende i studiegrupper på baggrund af de studerendes indtastede oplysninger.
- At forbedre gruppedannelsesprocessen der udbydes af databehandleren, så den bliver bedre ved senere gruppedannelser.
- At tillade at den dataansvarliges kontaktpersoner i nogen grad kan udføre opgaverne selv vha. UniHelpers selvbetjeningsløsning kaldet Portalen.

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

- at databehandleren stiller UniHelper-systemet til rådighed for den dataansvarlige og herigennem opbevarer og processerer personoplysninger om den dataansvarliges studerende på databehandlerens underdatabehandleres servere.

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

- For dataansvarliges kontaktpersoner:
 - Navn
 - E-mail
 - Korrespondance vedrørende databehandlingen
- For de studerende:
 - Navn
 - E-mailadresse
 - Studienummer
 - Holdnummer
 - Forventninger til studiet
 - Kompetenceprofil
 - Evt. mailkorrespondancer
 - Evt. skræddersyede spørgsmål udvalgt af den dataansvarlige, der er af ikke følsom eller fortrolig karakter.

A.4 Behandlingen omfatter følgende kategorier af registrerede:

- Studerende ved den dataansvarlige, som starter på den uddannelse, som den dataansvarlige har udvalgt til at benytte UniHelper-systemet.

- Kontaktpersoner ved dataansvarlige

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

- Behandlingen er tidsbegrænset fra de studerende starter på uddannelsen, til 8 måneder efter sidste gruppedannelse eller rotation. Dataen beholdes i disse 8 måneder sådan at dataansvarlige har mulighed for grupperotation eller evaluering hvis dette ønskes. Ved skriftlig henvendelse fra dataansvarlige, med henblik på fremtidig brug, kan dataen opbevares i op til 2 år fra sidste rotation eller gruppedannelse.
- Information på databehandlerens kontaktpersoner eller personoplysninger som er sendt mellem dataansvarlige og databehandler via e-mail kan opbevares i op til 2 år. Dette er pga. tekniske foranstaltninger men også for at imødekomme lovkrav ift. registreredes ret til sletning og korrigerings.

Bilag B Betingelser for databehandlerens brug af underdatabehandlere og liste over godkendte underdatabehandlere

B.1 Betingelser for databehandlerens brug af eventuelle underdatabehandlere

Databehandleren må alene gøre brug af underdatabehandlere efter forudgående specifik skriftlig godkendelse fra den dataansvarlige. Databehandlerens anmodning herom skal være den dataansvarlige i hænde minimum 1 måned før anvendelsen eller ændringen skal træde i kraft. Den dataansvarlige kan alene nægte godkendelse, såfremt den dataansvarlige har rimelige, konkrete årsager hertil.

Den dataansvarlige har godkendt, at databehandleren anvender underdatabehandlere beskrevet i afsnit Bilag B.2 i forbindelse med de opgaver, som databehandleren udfører på vegne af den dataansvarlige.

B.2 Godkendte underdatabehandlere

Den dataansvarlige har ved databehandleraftalens ikrafttræden godkendt anvendelsen af følgende underdatabehandlere:

Navn	CVR-nr	Adresse	Kontaktoplysninger	Beskrivelse af behandling	Behandlingslokaltet
TYPEFORM SL	ESB65831836	C/Bac de Roda, 163 (Local), 08018 – Barcelona (Spain)	gdpr@typeform.com	Hosting af spørgeskema som de studerende udfylder, og videresendelse af resultater.	Typeform benytter sig af AWS' datacentre i USA. En Liste over AWS' datacentre kan ses her . Da tjenesten er cloud-baseret er det ikke muligt at angive de præcise adresser hvor dataen befinder sig.
Scaleway SAS	FR35433115904	8 rue de la ville	privacy@scaleway.com	Hosting af UniHelpers services, og opbevaring af de studerendes data, og	Scaleway har data-centre i mange lande i Europa, men vi bruger PARIS-2

		l'Evêque – 75008 Paris, FRANCE		data for dataansvarliges medarbejdere.	regionen som ligger i Paris
Proton Technologies AG	CHE-354.686.492	Route de la Galaisse 32, 1228 Plan-les-Ouates, Geneva, Switzerland	gdpr@protonmail.com	Protonmail bliver brugt til at håndtere mails som indeholder persondata på studerende.	Flere redundante data-centre i Schweiz.
Flowmailer B.V	KvK 62154885	Rotterdam at Van Nelleweg 1, 3044 BC	contact@flowmailer.com	FlowMailer bliver brugt til at sende emails ud i større kvaliteter, eksempelvis når de studerende skal have deres grupper at vide.	3 geografisk spredte datacentre i Amsterdam.

Den dataansvarlige har ved databehandleraftalens ikrafttræden specifikt godkendt anvendelsen af ovennævnte underdatabehandlere til netop den behandling, som er beskrevet ud for parten. Databehandleren kan ikke – uden den dataansvarliges specifikke og skriftlige godkendelse – anvende den enkelte underdatabehandler til en "anden" behandling and aftalt eller lade en anden underdatabehandler foretage den beskrevne behandling.

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:

1. Databehandleren stiller en spørgeskema-undersøgelse til rådighed som de studerende har mulighed for at deltage i. Spørgeskemaundersøgelsen danner grundlag for dels at fastlægge den studerendes kompetenceprofil og dels at få fastlagt den studerendes forventninger til studiet. Samtidig skal den studerende også indtaste generelle oplysninger, herunder navn, studienummer, holdnummer og e-mailadresse, så UniHelper kan identificere og efterfølgende kommunikere grupperne ud til den studerende.
 - a. Dataansvarlige har mulighed for at lave ekstra spørgsmål som bliver stillet de studerende, men dog kun noget som ville føre til almindelige personoplysninger.
2. Ud fra besvarelserne vil UniHelper danne studiegrupper til de studerende.
3. Hvis aftalt med den dataansvarlige udsendes en mail til hver enkelt studerende med vedkommendes gruppe. I denne mail vil der stå navne og mails på den studerendes gruppe.
4. Databehandleren giver den dataansvarlige mulighed for at den dataansvarlige kan se hvilke studerende som har svaret, og hvilke grupper de er kommet i.
5. Databehandleren giver den dataansvarlige mulighed for at udsende mails til den studerende, som forklarer hvilken gruppe den studerende er kommet i, og hvordan de kan kontakte deres gruppe.
6. Hvis aftalt med den dataansvarlige vil UniHelper bruge de studerendes navne og mails til at udsende en mail til de studerende for at evaluere processen.
7. Alt afhængig af aftalen med den dataansvarlige kan der udsendes en mail med et evalueringsskema til de studerende. Den dataansvarlige er stadig fuldt ud ansvarlig for den data der indsamles i forbindelse med evalueringen.
8. Databehandleren kan udføre mindre opgaver på dataansvarliges anmodning, såsom at sende en liste over de studerende som har svaret på et spørgeskema, sende en liste over svarprocent mm.

Under processen anerkender Databehandleren at de studerende må kontakte UniHelper direkte hvis de skal have slettet eller korrigeret deres data, eksempelvis hvis de har svaret forkert eller ikke vil have en gruppe alligevel. UniHelper vil assistere de studerende med rimelige ændringer uden at rådføre sig med dataansvarlige.

Databehandleren forpligter sig til at give skriftligt varsel til den dataansvarlige ved ændringer af den ovennævnte procedure. Med mindre ændring af proceduren leder til anvendelse af nye

underdatabehandlere, kræver det ikke en formel ændring af Bilag C, skriftligt varsel via post eller email er tilstrækkeligt.

C.2 Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

- At der er tale om en begrænset behandling af personoplysning af ikke særlig følsom karakter, i en begrænset periode. Der stilles derfor ikke skærpede sikkerhedskrav.

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

Databehandleren skal dog – i alle tilfælde og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige (på baggrund af den risikovurdering den dataansvarlige har foretaget):

- Personoplysningerne er altid krypterede under transmission.
- Personoplysninger slettes når de ikke tjener det aftalte formål længere.
- Adgang til personoplysninger tildeles kun de medarbejdere ved databehandleren, hvor der er et formålstjenesteligt behov. Adgangen fjernes igen, hvis den ikke længere løser det aftalte formål med databehandlingen.
- Adgang til personoplysninger er beskyttet af logins der benytter stærke adgangskoder og 2-faktor-godkendelse hvis muligt.
- Medarbejdere er forpligtet til at beskytte deres personlige computere med adgangskoder og kryptering af data på computeren.

C.3 Opbevaringsperiode/sletterutine

Behandlingen er tidsbegrænset jvf. Bilag A. Personoplysningerne slettes efter den tidsbegrænsede periode hos databehandleren og alle dens underdatabehandlere.

C.4 Instruks eller godkendelse vedrørende overførsel af personoplysninger til tredjelande

Den Dataansvarlige godkender at databehandleren overfører personoplysninger til tredjelande, hvis der ligger lovligt overførselsgrundlag, såsom EU-kommisionens standardkontrakter.

Databehandleren må endvidere overføre til sikre tredjelande, eller sikre områder i tredjelande.

I de tilfælde, hvor data overføres til tredjelande er databehandleren forpligtet til at indgå SCCer/standardkontraktbestemmelser, som er tilstrækkelige til at dække behovet for de

pågældende overførsler. Den dataansvarlige er til enhver tid berettiget til at påse, at dette er tilfældet.

Ved overførsel til usikre tredjelande skal databehandleren sikre sig at der er udført passende supplerende foranstaltninger. Dette kan eksempelvis være pseudonymisering af persondata eller kryptering hvor krypteringsnøglen ligger indenfor EU's grænser.

Desuden skal der årligt gennemføres en risikovurdering for overførslen, samt redegøres for om de etablerede sikkerhedsforanstaltninger fortsat er tilstrækkelige. Resultatet af denne vurdering skal ved forespørgsel gøres tilgængelig for den dataansvarlige.

C.5 Lokaltet for behandling

Behandling af de i aftalen omfattede personoplysninger sker på databehandlerens kontorer og hjemmearbejdspladser i Aarhus, Danmark og ved databehandlerens underdatabehandlere, som beskrevet i punkt B.2.

C.6 Nærmere procedurer for den dataansvarliges tilsyn med den behandling, som foretages hos databehandleren

Dataansvarlige har ret til at føre digitalt tilsyn med databehandleren, ved eksempelvis at bede om dokumentation for databehandlerens interne kontroller, underdatabehandleraftaler, eller stille et sikkerheds-spørgeskema som databehandleren skal udfylde. Da databehandleren ikke har en fysisk adresse men er i et remote-setup vurderes det ikke at det giver mening at foretage fysisk tilsyn.

Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover adgang til, at føre tilsyn hos databehandleren, når der efter den dataansvarliges vurdering opstår et behov herfor.

C.7 Nærmere procedurer for tilsynet med den behandling, som foretages hos eventuelle underdatabehandlere

På den Dataansvarliges foranledning, skal databehandleren, for den dataansvarliges regning, assistere den dataansvarlige med, at der bliver ført tilsyn hos underdatabehandlere, dog ikke oftere end en gang årligt.

Den dataansvarlige kan – hvis det findes nødvendigt, og for egen regning – vælge at initiere og deltage på en fysisk inspektion hos underdatabehandleren, dog højst en gang årligt.

Den dataansvarliges eventuelle deltagelse i et tilsyn hos underdatabehandleren ændrer ikke ved, at databehandleren også herefter har det fulde ansvar for underdatabehandlerens overholdelse af databeskyttelseslovgivningen og denne databehandleraftale.

Bilag D Parternes regulering af andre forhold

D.1 [Overskrift]

D.2 [Overskrift]

D.3 [Overskrift]

D.4 [Overskrift]

Bilag E Skema til underretning af den dataansvarlige ved brud på datasikkerhed

Nr.	Spørgsmål	Besvarelse
1	Hvornår er bruddet opstået?	
2	Hvornår er bruddet konstateret?	
3	Hvad er der sket (karakteren af bruddet)?	
4	Årsagen til bruddet?	
5	Hvilken type personoplysninger er berørt (almindelige/følsomme)?	
6	Hvilke kategorier af registrerede er berørt?	
7	Hvor mange registrerede er antageligvis blevet berørt (opdelt i kategorier)?	
8	Hvad er der konstateret rent teknisk?	
9	Hvilke sandsynlige konsekvenser har bruddet for de berørte personer?	
10	Hvilke afhjælpende foranstaltninger er truffet?	
11	Har det givet anledning til yderligere internt i organisationen, mhp. at forhindre lignende brud i fremtiden?	
12	Dato for afslutning af bruddet:	

I forbindelse med bruddet kan kontaktpersonen i medfør af databehandleraftalen kontaktes for yderligere informationer.