

Databehandleraftale

Standardkontraktsbestemmelser

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

mellem

Den kunde, institution, skole, kommune, virksomhed eller anden juridiske enhed, der indgår aftale med Danskfaglighed om brug af Danskfagligheds digitale undervisningsplatform, institutionsabonnement eller tilknyttede ydelser

herefter "den dataansvarlige"

og

Danskfaglighed

CVR 41554665

Aastrupvej 83

6100 Haderslev

Danmark

herefter "databehandleren"

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

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

Disse Bestemmelser gælder alene i det omfang, databehandleren behandler personoplysninger på vegne af den dataansvarlige, herunder oplysninger om den dataansvarliges brugere, administratorer, lærere, medarbejdere, elever eller andre registrerede i forbindelse med institutionsaftale, platformadgang eller tilknyttede ydelser. Databehandlerens behandling af egne kunde-, betalings-, fakturerings-, support- og markedsføringsoplysninger som selvstændig dataansvarlig er ikke omfattet af disse Bestemmelser, men reguleres af databehandlerens privatlivspolitik og handelsbetingelser.

1. Indhold

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

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 adgang til Danskfagligheds digitale undervisningsplatform til institutioner/skoler, herunder digitale undervisningsmaterialer, institutionsabonnement, bruger- og adgangsadministration, aktivering og deaktivering af brugere, teknisk drift, support, fejlfinding, sikkerhedsopdateringer, licensadministration og eventuel samlet statistik over brugere/adgange, behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.
4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.
5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.
6. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.
7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.
8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.
9. Bilag D indeholder bestemmelser vedrørende andre aktiviteter, som ikke er omfattet af Bestemmelserne.
10. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk, af begge parter.
11. Disse Bestemmelser frigør ikke databehandleren fra forpligtelser, som databehandleren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

3. Den dataansvarliges rettigheder og forpligtelser

1. Den dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelsesforordningen (se forordningens artikel 24), databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes¹ nationale ret og disse Bestemmelser.

2. Den dataansvarlige har ret og pligt til at træffe beslutninger om, til hvilke(t) formål og med hvilke hjælpemidler, der må ske behandling af personoplysninger.
3. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

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.
3. Hvis databehandleren underretter den dataansvarlige efter pkt. 4.2, skal den dataansvarlige uden unødigt forsinkelse bekræfte, ændre eller trække instruksen tilbage skriftligt. Databehandleren kan udsætte den pågældende behandling, indtil instruksen er afklaret, og må ikke udføre en instruks, der åbenbart strider mod databeskyttelseslovgivningen.

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.

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

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. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes overholdelse af den dataansvarliges forpligtelse efter forordningens artikel 32, ved bl.a. at stille den nødvendige information til rådighed for den dataansvarlige vedrørende de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren allerede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.

Hvis imødegåelse af de identificerede risici – efter den dataansvarliges vurdering – kræver gennemførelse af yderligere foranstaltninger end de foranstaltninger, som databehandleren allerede har gennemført, skal den dataansvarlige angive de yderligere foranstaltninger, der skal gennemføres, i bilag C.

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 eller generel skriftlig godkendelse fra den dataansvarlige som beskrevet nedenfor.

3. Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftligt underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere med mindst 30 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den dataansvarlige allerede har godkendt, fremgår af bilag B.

4. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt

eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.

5. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.

6. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82, over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

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. Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tredjeland, herunder det eventuelle overførselsgrundlag i databeskyttelsesforordningens kapitel V, som overførslen er baseret på, skal angives i bilag C.6.

5. Disse Bestemmelser skal ikke forveksles med standardkontraktsbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre

et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.

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. indsigtsretten
- d. retten til berigtigelse
- e. retten til sletning ("retten til at blive glemt") f. retten til begrænsning af behandling
- g. underretningspligten i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
- h. retten til dataportabilitet i. retten til indsigelse j. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering

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

3. Parterne skal i bilag C angive de fornødne tekniske og organisatoriske foranstaltninger, hvormed databehandleren skal bistå den dataansvarlige samt i hvilket omfang og udstrækning. Det gælder for de forpligtelser, der følger af Bestemmelse 9.1. og 9.2.

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 24 timer efter, at denne er blevet bekendt med bruddet, sådan at den dataansvarlige kan overholde sin forpligtelse til at anmelde bruddet på persondatasikkerheden til den kompetente tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 33.
3. I overensstemmelse med Bestemmelse 9.2.a skal databehandleren bistå den dataansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndighed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse af bruddet til den kompetente tilsynsmyndighed:
 - a. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
 - b. de sandsynlige konsekvenser af bruddet på persondatasikkerheden
 - c. de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.
4. Parterne skal i bilag C angive den information, som databehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

11. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger er databehandleren forpligtet til at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige, og bekræfte over for den dataansvarlige, at oplysningerne er slettet, medmindre den dataansvarlige skriftligt har instrueret databehandleren i fortsat opbevaring, eller 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. Procedurerne for den dataansvarliges revisioner, herunder inspektioner, med databehandleren og underdatabehandlere er nærmere angivet i Bilag C.7. og C.8.
3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivningen har adgang til den dataansvarliges eller databehandlerens faciliteter, eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

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. Disse Bestemmelser træder i kraft ved parternes skriftlige godkendelse i forbindelse med indgåelse af aftalen mellem parterne, herunder ved elektronisk godkendelse, ordreaccept, e-mailbekræftelse eller anden dokumenteret skriftlig accept.

2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.

3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af personoplysninger varer. I denne periode kan Bestemmelserne ikke opsiges, medmindre andre bestemmelser, der regulerer levering af tjenesten vedrørende behandling af personoplysninger, aftales mellem parterne.

4. Hvis levering af tjenesterne vedrørende behandling af personoplysninger ophører, og personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftligt varsel af begge parter.

15. Kontaktpersoner hos den dataansvarlige og databehandleren

Parterne kan kontakte hinanden via nedenstående kontaktpersoner.

Parterne er forpligtet til løbende at orientere hinanden skriftligt om ændringer vedrørende kontaktpersoner.

Kontaktperson hos den dataansvarlige:

Den dataansvarliges kontaktperson er den person, som den dataansvarlige har angivet som administrator, aftalekontakt eller GDPR-kontakt ved aftalens indgåelse, ordreafgivelse, konto-/abonnementsoprettelse eller senere skriftlig meddelelse til databehandleren.

Kontaktperson hos databehandleren:

Navn	Birgitte Lund Thomsen
Stilling	Ejer af Danskfaglighed
Telefonnummer	20 77 16 78
E-mail	info@danskfaglighed.dk

Underskrift

På vegne af databehandleren

Dato

Navn

Birgitte Lund Thomsen

Stilling

Ejer af Danskfaglighed

Telefonnummer

20 77 16 78

E-mail

info@danskfaglighed.dk

Underskrift

Bilag A – Oplysninger om behandlingen

Dette Bilag A beskriver de behandlingsaktiviteter, som databehandleren som databehandler foretager på vegne af institutionen/skolen som dataansvarlig i forbindelse med levering af Danskfagligheds digitale undervisningsplatform, institutionsabonnement og tilknyttede funktioner.

Databehandleren behandler som udgangspunkt egne kunde-, konto-, betalings-, leverings- og supportoplysninger som selvstændig dataansvarlig, jf. handelsbetingelserne. Dette Bilag A omfatter alene de personoplysninger, som databehandleren behandler på vegne af institutionen/skolen, fx oplysninger om institutionens brugere, administratorer, lærere, medarbejdere og eventuelt elever, hvor sådanne oplysninger behandles som led i institutionsaftalen.

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

Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er at levere, administrere, vedligeholde og understøtte den dataansvarliges brug af Danskfagligheds digitale undervisningsplatform og institutionsabonnement.

Behandlingen sker navnlig med henblik på:

1. at oprette, administrere, aktivere og deaktivere brugere tilknyttet institutionens/skolens abonnement,
2. at give institutionens brugere adgang til digitale undervisningsmaterialer og portaladgang inden for det aftalte licensomfang,
3. at administrere institutionens brugere, licenser, samtidige brugere, klasser og adgangsrettigheder,
4. at give institutionens udpegede administrator(er) mulighed for at oprette og deaktivere brugere og modtage drifts- og varslingsmeddelelser,
5. at sikre teknisk drift, adgangsstyring, vedligeholdelse, sikkerhedsopdateringer, fejlfinding og support,
6. at håndtere henvendelser fra institutionen og institutionens brugere vedrørende adgang, konto, tekniske fejl, drift og brug af platformen,
7. at forebygge, opdage og håndtere misbrug, uautoriseret adgang, kompromittering af konti og brud på platformens sikkerhed,
8. at kontrollere og administrere institutionens licensomfang, herunder eventuel samlet statistik over brugere og adgange til brug for institutionens interne kontrol,
9. at understøtte opfyldelse af databehandlerens forpligtelser efter databehandleraftalen, herunder bistand, hændeshåndtering, sletning, dokumentation og tilsyn.

Formålet er afgrænset til levering og administration af institutionsydelsen. Databehandleren må ikke i rollen som databehandler anvende personoplysninger behandlet på vegne af institutionen/skolen til egne formål, herunder selvstændig markedsføring, profilering eller analyse, medmindre dette er særskilt aftalt eller sker på et andet lovligt grundlag uden for denne databehandleraftale.

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

Databehandlerens behandling består primært i teknisk og administrativ behandling af personoplysninger i forbindelse med drift og levering af Danskfagligheds digitale undervisningsplatform til institutioner/skoler.

Behandlingen omfatter navnlig følgende behandlingsoperationer:

1. indsamling og modtagelse af oplysninger fra den dataansvarlige, institutionens administratorer og institutionens brugere,
2. registrering og oprettelse af brugerprofiler, konti, administratoradgange og adgangsrettigheder,
3. lagring og opbevaring af personoplysninger i systemer, databaser, e-mailmiljøer og backup,
4. organisering, strukturering og ajourføring af bruger-, adgangs- og licensoplysninger,
5. brug af oplysninger til at give adgang til platformen og digitale undervisningsmaterialer,
6. adgangsstyring, autentifikation, loginadministration og deaktivering af brugere,
7. teknisk drift, vedligeholdelse, sikkerhedsopdateringer og systemadministration,
8. support, fejlsøgning, fejlafhjælpning og behandling af henvendelser,
9. logning og kontrol af adgang, drift, sikkerhed og eventuelt misbrug,
10. udarbejdelse og udlevering af samlet statistik over brugere og adgange, hvis institutionen anmoder herom,
11. sikkerhedskopiering og genetablering af data,
12. begrænsning, sletning eller tilbagelevering af personoplysninger efter den dataansvarliges instruks og databehandleraftalens bestemmelser,
13. eventuel videregivelse eller overladelse til godkendte underdatabehandlere i det omfang, det er nødvendigt for at levere platform, hosting, teknisk drift, support, email, database, backup eller tilsvarende funktioner.

Behandlingen er primært almindelig it-drift, adgangsadministration, teknisk support og platformadministration. Den forventes ikke at omfatte behandling af særlige kategorier af personoplysninger efter GDPR artikel 9 eller oplysninger om strafbare forhold efter GDPR artikel 10, medmindre den dataansvarlige særskilt instruerer databehandleren herom og dette er udtrykkeligt aftalt i databehandleraftalen. GDPR artikel 28 kræver, at karakteren og formålet med behandlingen beskrives i databehandleraftalen.

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

Behandlingen kan omfatte følgende typer af personoplysninger, i det omfang oplysningerne er nødvendige for levering, administration, drift, support og sikkerhed i forbindelse med institutionsaftalen:

1. Identifikations- og kontaktoplysninger

- navn,

- e-mailadresse,
- telefonnummer,
- stilling/funktion, fx lærer, medarbejder, administrator eller kontaktperson,
- institutionens/skolens navn,
- afdeling, klasse, team eller organisatorisk tilknytning, hvis dette anvendes i forbindelse med adgangs- eller licensadministration.

2. Konto-, bruger- og adgangsoplysninger

- brugernavn,
- bruger-ID,
- loginoplysninger,
- adgangsrettigheder,
- rolle i systemet, fx administrator, lærer, medarbejder eller anden institutionsbruger,
- oplysninger om oprettelse, aktivering, deaktivering og ændring af brugeradgang,
- oplysninger om tilknytning til institutionsabonnement, licens, klasse, hold eller brugergruppe,
- oplysninger om mistanke om misbrug, uautoriseret adgang eller kompromittering af konto.

3. Brugs-, adgangs- og licensoplysninger

- oplysninger om adgang til platformen,
- oplysninger om anvendelse af licensomfang,
- oplysninger om samtidige brugere, antal brugere, brugergrupper, klasser eller licenser,
- samlet statistik over brugere og adgange, hvis institutionen anmoder om dette,
- oplysninger om overholdelse af adgangs- og licensbegrænsninger.

4. Tekniske oplysninger og sikkerhedsoplysninger

- IP-adresse,
- logoplysninger,
- tidspunkt for login, adgang, fejl eller systemhændelser,
- tekniske identifikatorer,
- browser-, enheds- og systemoplysninger i det omfang, de behandles ved drift, support, fejlfinding eller sikkerhed,
- oplysninger om sikkerhedshændelser, uautoriseret adgang, misbrug eller forsøg på omgåelse af tekniske eller organisatoriske adgangsbegrænsninger.

5. Support- og kommunikationsoplysninger

- navn og kontaktoplysninger på den person, der henvender sig,
- indhold af supporthenvendelser,
- beskeder, beskrivelser af fejl og tekniske problemer,
- eventuelle vedhæftninger eller skærbilleder, som institutionen eller brugeren sender til databehandleren,
- oplysninger, som fremgår af e-mailkorrespondance eller anden supportkommunikation.

6. Eventuelle elev- og personaleoplysninger

Hvis institutionen/skolen anvender platformen på en måde, hvor databehandleren behandler oplysninger om elever eller personale på vegne af institutionen, kan behandlingen desuden omfatte:

- navn,
- e-mailadresse eller anden brugeridentifikator,
- klasse, hold, årgang eller organisatorisk tilknytning,
- rolle eller brugerstatus,
- adgangs- og brugsoplysninger,
- oplysninger, der er nødvendige for at oprette, administrere, deaktivere eller supportere den pågældende bruger. Dette punkt omfatter alene elev- og personaleoplysninger i det omfang, institutionen/skolen stiller oplysningerne til rådighed for databehandleren eller instruerer databehandleren i at behandle dem.

7. Oplysninger, der som udgangspunkt ikke må behandles under aftalen

Databehandleren må som udgangspunkt ikke behandle følgende oplysninger på vegne af den dataansvarlige, medmindre det er udtrykkeligt aftalt og dokumenteret i en særskilt instruks:

- personnummer,
- særlige kategorier af personoplysninger, herunder oplysninger om helbred, fagforeningsforhold, religion, politisk overbevisning, race eller etnisk oprindelse, biometriske oplysninger eller seksuelle forhold,
- oplysninger om strafbare forhold,
- følsomme elevoplysninger, herunder oplysninger om diagnoser, støttebehov, trivselssager, sociale forhold, disciplinærsager eller tilsvarende forhold.

A.4. Behandlingen omfatter følgende kategorier af registrerede

Behandlingen kan omfatte følgende kategorier af registrerede:

1. institutionens/skolens udpegede administratorer,
2. institutionens/skolens lærere og undervisere,
3. institutionens/skolens medarbejdere, herunder administrative medarbejdere og tekniske kontaktpersoner,
4. institutionens/skolens øvrige autoriserede brugere,
5. elever, kursister eller andre undervisningsdeltagere, hvis institutionen/skolen stiller oplysninger om disse til rådighed for databehandleren eller instruerer databehandleren i at behandle sådanne oplysninger,
6. kontaktpersoner hos institutionen/skolen, herunder personer der modtager drifts-, support-, varslings- eller administrationsmeddelelser,
7. personer, der indgår i support-, fejlretnings- eller sikkerhedshenvendelser på vegne af institutionen/skolen.

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

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes, når disse Bestemmelser er trådt i kraft, og institutionens/skolens aftale om adgang til Danskfagligheds (databehandlerens) digitale undervisningsplatform eller institutionsabonnement er indgået.

Behandlingen varer, så længe det er nødvendigt for at levere, administrere, vedligeholde og supportere institutionsaftalen, herunder i den periode hvor institutionen/skolen har aktiv adgang til platformen, og indtil personoplysningerne er slettet eller tilbageleveret i overensstemmelse med databehandleraftalen og den dataansvarliges dokumenterede instruks.

Ved ophør af institutionsaftalen, udløb af abonnementet eller ophør af tjenesterne vedrørende behandling af personoplysninger skal databehandleren slette eller tilbagelevere personoplysninger behandlet på vegne af den dataansvarlige i overensstemmelse med pkt. 11 og Bilag C, medmindre fortsat opbevaring kræves efter EU-ret eller national ret, eller medmindre den dataansvarlige skriftligt har instrueret databehandleren i fortsat opbevaring. GDPR artikel 28 kræver, at databehandleren efter den dataansvarliges valg sletter eller tilbageleverer alle personoplysninger efter ophør og sletter eksisterende kopier, medmindre EU-ret eller national ret kræver opbevaring.

Backups og sikkerhedskopier slettes eller overskrives efter databehandlerens almindelige backup- og sletterutiner, medmindre andet er skriftligt aftalt i Bilag C. Personoplysninger sikkerhedskopieres via hostingudbyderen Simply.com ifølge de foreliggende oplysninger.

Hvis Databehandleren behandler oplysninger som selvstændig dataansvarlig, fx oplysninger om institutionens køb, betaling, fakturering, levering, support eller retsopfyldelse, er disse behandlinger ikke omfattet af dette Bilag A, men reguleres af Danskfagligheds privatlivspolitik og handelsbetingelser.

Bilag B – Underdatabehandlere

B.1. Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
Simply.com A/S (Curanet)	29412006	Højvangen 4, 8660 Skanderborg	Hosting af hjemmeside, e-mail, databaser, backup og teknisk drift.
IEX ApS	35527710	Roholmsvej 10 R, 2620 Albertslund	Teknisk betalingsintegration mellem webshop og betalingsindløser.
Visma e-conomic A/S	29403473	Gærtorvet 1-5, 1799 København V, Danmark	Bogføring, fakturering og regnskabsmæssig

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
			administration.
UAB "MailerLite"	302942057	J. Basanavičius 15, LT-03108 Vilnius, Litauen	Administration og udsendelse af nyhedsbreve og e-mailkommunikation.
Thagaard ApS	38516736	Søskrænten 31, 8400 Ebeltøft	Teknisk support, udvikling og vedligeholdelse af hjemmeside og webshop.

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

B.2. Varsel for godkendelse af underdatabehandlere

Den dataansvarlige giver ved indgåelse af databehandleraftalen en generel skriftlig godkendelse til, at databehandleren kan anvende de underdatabehandlere, der fremgår af bilag B.1.

Databehandleren skal skriftligt varsle den dataansvarlige mindst 30 dage før tilføjelse eller udskiftning af en underdatabehandler. Varslet skal indeholde navn på underdatabehandleren, dennes ydelse, behandlingssted og de behandlingsaktiviteter, som underdatabehandleren skal udføre.

Den dataansvarlige kan gøre skriftlig indsigelse mod den varslede ændring inden varslingsfristens udløb, hvis den dataansvarlige har rimelige databeskyttelsesretlige grunde hertil. Hvis der gøres indsigelse, må den nye eller ændrede underdatabehandler ikke anvendes til behandling af personoplysninger for den dataansvarlige, medmindre parterne skriftligt aftaler andet.

Ved akutte ændringer, som er nødvendige af hensyn til driftssikkerhed, informationssikkerhed eller lovkrav, kan databehandleren anvende en ny underdatabehandler med kortere varsel, forudsat at den dataansvarlige underrettes uden unødigt ophold og gives mulighed for at gøre indsigelse.

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:

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren stiller Danskfagligheds digitale platform, hjemmeside, webshop og tilhørende brugeradgang til rådighed for den dataansvarlige og dennes brugere.

Databehandleren instrueres til at behandle personoplysninger i det omfang, det er nødvendigt for at:

1. oprette, administrere og vedligeholde brugerkonti og adgang til platformen,
2. levere digitale undervisningsmaterialer, downloads og/eller portaladgang,
3. administrere institutionsabonnementer, brugerlicenser, administratoradgang og adgangsrettigheder,
4. håndtere support, fejlretning, teknisk drift, sikkerhed, misbrugsforebyggelse og logning,
5. stille relevant brugs- og adgangsstatistik til rådighed for den dataansvarlige, hvis dette er aftalt,
6. administrere betaling, fakturering og regnskab i det omfang behandlingen sker på vegne af den dataansvarlige,
7. foretage nødvendig kommunikation om adgang, drift, support, sikkerhed og ændringer i ydelsen,
8. slette eller tilbagelevere personoplysninger ved ophør i overensstemmelse med databehandlertaften og den dataansvarliges dokumenterede instruks.

Behandlingen omfatter navnlig almindelige personoplysninger om den dataansvarliges brugere, herunder navn, e-mailadresse, institutionstilknytning, rolle, bruger-ID/loginoplysninger, adgangs- og aktivitetslog, ordre-/abonnementsoplysninger, supporthenvendelser og tekniske oplysninger såsom IP-adresse og cookies, i det omfang disse oplysninger er nødvendige for platformens drift og levering af ydelsen.

Databehandleren må alene behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, herunder denne databehandlertaften, bilagene hertil og eventuelle efterfølgende skriftlige instrukser. Hvis databehandleren vurderer, at en instruks er i strid med databeskyttelsesreglerne, skal databehandleren straks underrette den dataansvarlige herom.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle, at behandlingen vedrører en digital undervisningsplatform med brugerkonti, login, adgangsstyring, levering af digitale undervisningsmaterialer, institutionsabonnementer, support, betaling/fakturering og teknisk drift.

Behandlingen omfatter som udgangspunkt almindelige personoplysninger, herunder navn, adresse, telefonnummer, e-mailadresse, konto- og loginoplysninger, ordre- og abonnementsoplysninger, betalings- og faktureringsrelaterede oplysninger, supporthenvendelser, IP-adresse, cookies og bruger-/adgangslog. Behandlingen omfatter ikke som udgangspunkt særlige kategorier af personoplysninger efter GDPR artikel 9.

Sikkerhedsniveauet skal derfor være almindeligt til forhøjet, navnlig fordi der behandles oplysninger om brugerkonti, institutionsbrugere, adgangsrettigheder, supporthenvendelser, betaling/fakturerings og teknisk drift via internettet. Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger der skal gennemføres for at etablere det nødvendige og aftalte sikkerhedsniveau.

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

1. Pseudonymisering og kryptering

Databehandleren skal anvende krypteret kommunikation ved adgang til hjemmeside, webshop, login og betaling. Hjemmesiden og betaling skal som minimum anvende SSL/TLS-kryptering. Hvor det er relevant og teknisk muligt, skal adgangs- og logdata begrænses, adskilles eller pseudonymiseres med henblik på at reducere risikoen for de registrerede.

2. Fortrolighed, integritet, tilgængelighed og robusthed

Databehandleren skal sikre, at behandlingssystemer og -tjenester har passende fortrolighed, integritet, tilgængelighed og robusthed. Dette omfatter adgangskontrol, personlige loginoplysninger, begrænsning af adgang efter sagligt behov, løbende sikkerhedsopdateringer, teknisk vedligeholdelse og foranstaltninger mod uautoriseret adgang, deling af login, scraping, masse-download og andet misbrug.

3. Genopretning ved fysisk eller teknisk hændelse

Databehandleren skal sikre backup og rimelige muligheder for rettidig genetablering af tilgængeligheden af og adgangen til personoplysninger i tilfælde af fysisk eller teknisk hændelse. Dette skal navnlig omfatte data, der behandles i forbindelse med hjemmeside, webshop, e-mail, databaser og teknisk infrastruktur.

4. Regelmæssig afprøvning, vurdering og evaluering

Databehandleren skal regelmæssigt vurdere, om de tekniske og organisatoriske sikkerhedsforanstaltninger er passende i forhold til behandlingens karakter, omfang, sammenhæng, formål og risici. Databehandleren skal arbejde løbende med forebyggelse, opdagelse og håndtering af sikkerhedshændelser.

5. Adgang til oplysninger via internettet

Adgang til personoplysninger via internettet skal ske via beskyttet login og adgangsstyring. Loginoplysninger skal være personlige og må ikke deles. Databehandleren skal kunne begrænse eller suspendere adgang ved mistanke om misbrug, uautoriseret adgang eller væsentlig misligholdelse.

6. Beskyttelse under transmission

Personoplysninger skal beskyttes under transmission ved brug af passende kryptering, herunder SSL/TLS ved brug af hjemmeside, webshop og betaling. Oplysninger må ikke sendes eller overføres til uvedkommende, og adgangslinks, loginoplysninger og supportoplysninger skal håndteres på en måde, der reducerer risikoen for uautoriseret adgang.

7. Beskyttelse under opbevaring

Personoplysninger skal opbevares i systemer med passende adgangskontrol, backup og tekniske sikkerhedsforanstaltninger. Oplysninger må kun opbevares, så længe det er nødvendigt til de aftalte formål eller følger af lovkrav, og oplysninger skal slettes eller tilbageleveres ved behandlingens ophør i overensstemmelse med databehandleraftalen.

8. Fysisk sikring af lokaliteter

Databehandleren skal sikre, at lokaler og udstyr, hvorfra der behandles personoplysninger, er passende fysisk sikret mod uvedkommendes adgang. For hosting, e-mail, databaser, backup og teknisk drift kan databehandleren anvende godkendte underdatabehandlere, herunder Simply.com A/S, som led i den tekniske drift.

9. Hjemme- og fjernarbejdspladser

Ved behandling fra hjemme- eller fjernarbejdspladser skal databehandleren sikre, at personoplysninger kun tilgås via sikre enheder, sikre forbindelser og personlige adgangsoplysninger. Personoplysninger må ikke lagres lokalt uden sagligt behov og passende beskyttelse.

10. Logning

Databehandleren skal anvende logning eller tilsvarende kontrol, hvor det er relevant for at kunne forebygge, opdage og håndtere misbrug, uautoriseret adgang, deling af login, supportforløb og sikkerhedshændelser. Logoplysninger skal beskyttes mod uautoriseret adgang og må kun anvendes til saglige drifts-, sikkerheds-, support- og dokumentationsformål.

Databehandleren skal desuden sikre, at personer, der er autoriseret til at behandle personoplysninger, er underlagt fortrolighed, og at databehandleren bistår den dataansvarlige med forpligtelserne vedrørende behandlingssikkerhed, brud på persondatasikkerheden, konsekvensanalyse og eventuel forudgående høring, i det omfang det følger af databehandleraftalen og GDPR artikel 28.

C.3 Bistand til den dataansvarlige

Databehandleren skal så vidt muligt, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og 9.2.

Bistanden omfatter behandling af personoplysninger i forbindelse med Danskfaglighed digitale platform, hjemmeside, webshop, brugeradgang, institutionsabonnementer, support, betaling/fakturering og teknisk drift.

Databehandleren skal navnlig bistå den dataansvarlige med:

1. Anmodninger fra registrerede

Databehandleren skal, i det omfang det er teknisk muligt, bistå med at identificere, fremsøge, rette, begrænse, eksportere eller slette personoplysninger om brugere, som behandles via platformen på vegne af den dataansvarlige.

2. Adgangsadministration

Databehandleren skal bistå med oprettelse, ændring, begrænsning og deaktivering af brugeradgange, administratoradgange og institutionskonti, hvor dette er nødvendigt for den dataansvarliges administration af egne brugere.

3. Sikkerhed og adgangskontrol

Databehandleren skal opretholde passende tekniske og organisatoriske foranstaltninger, herunder loginbeskyttelse, adgangsstyring, krypteret kommunikation, sikker drift, backup, logning hvor relevant og foranstaltninger mod uautoriseret adgang eller misbrug.

4. Brud på persondatasikkerheden

Databehandleren skal uden unødigt forsinkelse bistå den dataansvarlige med oplysninger, der er nødvendige for at vurdere og håndtere et brud på persondatasikkerheden, herunder oplysninger om hændelsens karakter, berørte systemer, berørte kategorier af oplysninger og iværksatte afhjælpende foranstaltninger.

5. Konsekvensanalyse og forudgående høring

Databehandleren skal efter rimelig anmodning bistå den dataansvarlige med relevante oplysninger om behandlingen, sikkerhedsforanstaltninger, underdatabehandlere og teknisk drift, hvis den dataansvarlige skal gennemføre en konsekvensanalyse eller eventuel forudgående høring.

6. Underdatabehandlere

Databehandleren skal stille relevante oplysninger til rådighed om de underdatabehandlere, der anvendes til behandling på vegne af den dataansvarlige, herunder hosting, e-mail, betalingsintegration, bogføring, nyhedsbrev, analyse og teknisk drift, i det omfang de anvendes til den konkrete behandling.

7. Dokumentation og tilsyn

Databehandleren skal stille de oplysninger til rådighed, der er nødvendige for at dokumentere overholdelse af databehandleraftalen, og skal medvirke til rimelige tilsyns- og revisionsaktiviteter i overensstemmelse med aftalen.

Databehandlerens bistand ydes inden for rammerne af de systemer og oplysninger, som databehandleren faktisk råder over. Bistand, der går ud over almindelig support, drift og opfyldelse af databehandleraftalen, kan faktureres efter parternes aftale, medmindre bistanden skyldes forhold, som databehandleren er ansvarlig for.

C.4 Opbevaringsperiode/sletterutine

Databehandleren må kun opbevare personoplysninger, så længe det er nødvendigt for at levere den aftalte ydelse til den dataansvarlige, herunder brugeradgang, institutionsabonnement, levering af digitale materialer, support, sikkerhed, dokumentation, fakturering og opfyldelse af lovkrav.

For Danskfagligheds behandling gælder følgende sletterutiner, medmindre den dataansvarlige dokumenteret instruerer andet, eller opbevaring er nødvendig efter EU-ret eller national ret:

1. Brugerkonti og adgangsoplysninger

Oplysninger om brugerkonti, login, adgangsrettigheder og institutionsbrugere opbevares, så længe aftalen eller brugeradgangen er aktiv. Ved ophør deaktiveres adgangen, og personoplysninger slettes eller anonymiseres inden rimelig tid, medmindre oplysningerne fortsat er nødvendige af hensyn til dokumentation, sikkerhed, retskrav eller lovkrav.

2. Kunde- og abonnementsoplysninger

Oplysninger i kundekartoteket slettes som udgangspunkt 24 måneder efter kundeforholdets ophør eller inaktivitet, medmindre længere opbevaring er nødvendig efter lovgivningen eller for at fastlægge, gøre gældende eller forsvare retskrav.

3. Faktura- og regnskabsoplysninger

Fakturaer og regnskabsmateriale, hvor personoplysninger kan fremgå, opbevares i 5 år i overensstemmelse med bogføringsreglerne.

4. Kontaktformularer og supporthenvendelser

Oplysninger indsendt via kontaktformularer opbevares i op til 1 år for at kunne henvise til tidligere aftaler, kommentarer og henvendelser. Supporthenvendelser opbevares kun så længe, det er nødvendigt for at behandle henvendelsen, dokumentere forløbet og varetage legitime drifts- eller sikkerhedshensyn.

5. Log- og sikkerhedsoplysninger

Logoplysninger og tekniske oplysninger, der behandles med henblik på drift, sikkerhed, misbrugsforebyggelse og fejlfinding, opbevares kun så længe, det er nødvendigt til disse formål, hvorefter de slettes eller anonymiseres.

6. Nyhedsbrev og e-mailkommunikation

Oplysninger behandlet til nyhedsbreve opbevares, så længe modtageren er tilmeldt, og slettes eller anonymiseres ved afmelding, medmindre fortsat opbevaring er nødvendig som dokumentation for samtykke eller retskrav.

Ved ophør af tjenesten vedrørende behandling af personoplysninger skal Databehandleren efter den dataansvarliges valg slette eller tilbagelevere alle personoplysninger, der behandles på vegne af den dataansvarlige, og slette eksisterende kopier, medmindre EUret eller national ret foreskriver fortsat opbevaring.

Hvis den dataansvarlige efter underskrift af disse Bestemmelser ændrer sit valg om sletning eller tilbagelevering, skal ændringen være dokumenteret og opbevares skriftligt, herunder elektronisk, i tilknytning til databehandleraftalen.

C.5 Lokaltet for behandling

Behandling af de af Bestemmelserne omfattede personoplysninger sker primært i Danmark hos Databehandleren og hos de underdatabehandlere, der anvendes til drift, hosting, support, betaling, fakturering, e-mail, analyse og teknisk vedligeholdelse.

Behandling kan desuden ske på de lokaliteter inden for EU/EØS, som fremgår af bilag B om underdatabehandlere og af den til enhver tid gældende liste over Danskfagligheds under- og databehandlere i privatlivspolitikken.

På tidspunktet for indgåelsen omfatter dette blandt andet underdatabehandlere i Danmark, Litauen og Irland. Behandling uden for EU/EØS må ikke ske uden den dataansvarliges forudgående dokumenterede instruks eller et gyldigt overførselsgrundlag efter databeskyttelsesforordningens kapitel V.

Databehandleren skal underrette den dataansvarlige om planlagte ændringer vedrørende tilføjelse eller udskiftning af underdatabehandlere i overensstemmelse med bilag B.2, så den dataansvarlige kan gøre indsigelse mod ændringen.

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Databehandleren er ikke berettiget til at overføre personoplysninger omfattet af disse Bestemmelser til tredjelande eller internationale organisationer uden den dataansvarliges forudgående dokumenterede instruks.

Personoplysninger skal som udgangspunkt behandles og opbevares inden for EU/EØS. Dette svarer til Danskfagligheds privatlivspolitik, hvor det fremgår, at der ikke overføres personoplysninger til tredjelande eller internationale organisationer.

Hvis en konkret behandling indebærer overførsel til et tredjeland eller en international organisation, må overførslen kun ske, hvis den dataansvarlige skriftligt har godkendt overførslen, og der foreligger et gyldigt overførselsgrundlag efter GDPR kapitel V.

Dette kan navnlig være:

1. en afgørelse om tilstrækkeligt beskyttelsesniveau efter GDPR artikel 45,
2. EU-Kommissionens standardkontraktbestemmelser efter GDPR artikel 46, eventuelt med nødvendige supplerende foranstaltninger, eller
3. et andet gyldigt overførselsgrundlag efter GDPR kapitel V.

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

Databehandleren skal underrette den dataansvarlige, hvis databehandleren eller en underdatabehandler bliver bekendt med, at behandling, support, hosting, backup, analyse eller anden adgang til personoplysninger vil indebære en tredjelandsoverførsel, før overførslen påbegyndes.

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

Databehandleren skal efter skriftlig anmodning stille de oplysninger til rådighed for den dataansvarlige, som er nødvendige for at påvise databehandlerens overholdelse af databeskyttelsesforordningens artikel 28 og disse Bestemmelser.

Den dataansvarliges tilsyn gennemføres som udgangspunkt ved skriftlig dokumentation. Databehandleren kan blandt andet stille følgende til rådighed, i det omfang det er relevant for den konkrete behandling:

1. gældende databehandleraftale med bilag,
2. beskrivelse af relevante tekniske og organisatoriske sikkerhedsforanstaltninger,
3. opdateret liste over anvendte underdatabehandlere,
4. oplysninger om behandlingslokaliteter og eventuelle overførsler til tredjelande,
5. oplysninger om relevante slette- og backup-rutiner,
6. oplysninger om håndtering af brud på persondatasikkerheden,
7. kopi eller uddrag af relevante databehandleraftaler med underdatabehandlere, dog med mulighed for at udelade kommercielle eller fortrolige vilkår uden databeskyttelsesretlig betydning.

Den dataansvarlige kan én gang årligt anmode om dokumentation for databehandlerens overholdelse af disse Bestemmelser, medmindre der foreligger en konkret og saglig anledning til yderligere tilsyn, herunder ved mistanke om væsentlig misligholdelse, brud på persondatasikkerheden eller påbud fra en tilsynsmyndighed.

Fysisk inspektion hos databehandleren kan kun gennemføres, hvis skriftlig dokumentation ikke med rimelighed er tilstrækkelig til at påvise overholdelse af disse Bestemmelser. Fysisk inspektion skal varsles skriftligt med mindst 30 dages varsel, gennemføres inden for normal arbejdstid og tilrettelægges, så den ikke unødigt forstyrrer databehandlerens drift, sikkerhed eller øvrige kunders fortrolighed.

Den dataansvarlige kan lade en uafhængig revisor eller anden sagkyndig repræsentant gennemføre revision eller inspektion på den dataansvarliges vegne. En sådan repræsentant skal være underlagt sædvanlig fortrolighed og må ikke være konkurrent til databehandleren.

Den dataansvarlige afholder egne omkostninger ved revision og inspektion. Databehandleren afholder egne interne omkostninger ved almindelig og rimelig medvirken. Hvis den dataansvarliges anmodning medfører et væsentligt tidsforbrug eller bistand ud over almindelig dokumentation og rimelig medvirken, kan databehandleren kræve betaling efter medgået tid efter forudgående aftale mellem parterne, medmindre revisionen skyldes forhold, som databehandleren er ansvarlig for.

Revision eller inspektion af underdatabehandlere gennemføres som udgangspunkt ved databehandlerens indhentelse eller videreformidling af relevant dokumentation fra underdatabehandleren. Direkte inspektion hos underdatabehandlere kan kun ske, hvis dette er aftalt med den pågældende underdatabehandler, eller hvis det følger af den relevante underdatabehandleraftale.

Bilag D – Parternes regulering af andre forhold

Der er på tidspunktet for indgåelsen af disse Bestemmelser ikke aftalt særskilt regulering af øvrige forhold mellem parterne.

Eventuelle særskilte vilkår om tjenesten vedrørende behandling af personoplysninger, herunder vilkår om ansvar, betaling for ekstraordinær bistand, særlige sikkerhedskrav, yderligere revision, særlige slettefrister eller andre kundespecifikke forhold, skal aftales skriftligt mellem parterne.

Særskilte vilkår må ikke direkte eller indirekte stride mod disse Bestemmelser, databeskyttelsesforordningen eller forringe de registreredes grundlæggende rettigheder og frihedsrettigheder.

Henvendelse om særskilte vilkår kan ske til databehandleren via de kontaktoplysninger, der fremgår af disse Bestemmelser.