



Ny Østergade 7, 1. sal

4000 Roskilde

Tlf. 70 20 60 20

www.danskoplysning.dk

post@danskoplysning.dk

Databehandleraftale

Mellem

Dansk Oplysnings Forbund
Ny Østergade 7, 1
4000 Roskilde
CVR Nr. 54 68 63 15
(Databehandler)

Og

DOF's medlemsforening
(Dataansvarlig)

Vedrørende behandlingen af personoplysninger i IT-løsninger.

INDHOLD

1. Baggrund og formål.....	4
2. Instruks	4
3. Tekniske og organisatoriske sikkerhedsforanstaltninger.....	5
4. Underdatabehandler.....	5
5. Overførsel til tredjelande eller internationale organisationer	6
6. Databehandlerens interne procedurer	7
7. Revision og oplysningspligt.....	7
8. Bistand til den dataansvarlige	8
9. Underretningspligt	9
10. Håndtering af data efter aftalens ophør	10
11. Aftalens gyldighed.....	10
12. Tvister.....	10
13. Diverse	10
14. Accept.....	11
Bilag 1: Den Dataansvarliges instruktioner til Databehandleren	12
1.1 Systembeskrivelse.....	12
1.2 Formål med behandlingen.....	12
1.2.1 Formål med den Dataansvarliges behandling af deltagernes persondata	12
1.2.2 Formål med den Dataansvarliges behandling af HR-data	12
1.2.3 Formål med Databehandlerens behandling af persondata	12
1.3 Kategorier af datasubjekter	13
1.4. Kategorier af personoplysninger	13
1.5 Fysisk placering af behandlingen	13
1.6 Godkendte underdatabehandlere.....	13
Bilag 2: Tekniske og organisatoriske sikkerhedskrav	15
2.1 Databehandlerens fysiske sikkerhed.....	15
2.2 Databehandlerens tekniske sikkerhed	15



2.3 Databehandleren organisatoriske sikkerhed..... 15
2.4 Relevante hjemmesider 15



1. Baggrund og formål

1. Denne aftale fastsætter de rettigheder og forpligtelser, som finder anvendelse, når Databehandleren foretager behandling af personoplysninger på vegne af den dataansvarlige.
2. Formål med denne aftale er bl.a. at sikre, at Databehandleren overholder gældende regler om datasikkerhed, Persondatalov og EU Persondataforordningen (GDPR).
3. Til denne aftale hører to bilag. Bilagene fungerer som en integreret del af databehandleraftalen.
4. Databehandleren stiller IT-Løsninger, specificeret i Bilag 1 ("Systembeskrivelse"), til rådighed for den Dataansvarlige til behandling af oplysninger vedr. Dataansvarliges aktiviteter, deltagere, undervisere og personale.
5. Som leverandør af IT-Løsninger, foretager Databehandleren behandling af personoplysninger på vegne af den Dataansvarlige.
6. Den Dataansvarlige er alene ansvarlig for egen behandling af personoplysningerne ved brug af IT-Løsninger, herunder overholdelse af den gældende lovgivning, opfyldelse af afmeldingspligten, uddannelse og vejledning til egne medarbejdere osv.
7. Dataansvarlig har behandlingshjemmel for behandling af personoplysninger og har eneansvar for nøjagtigheden, integriteten, indholdet, pålideligheden og lovligheden af de personoplysninger, der er fremlagt til Databehandleren.
8. Databehandleraftalen med tilhørende bilag opbevares skriftligt, herunder elektronisk af begge parter.

2. Instruks

1. Det er den Dataansvarlige, der afgør, til hvilke formål der må foretages behandling af personoplysninger og Databehandleren handler alene efter instruks fra den Dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som Databehandleren er underlagt.
2. Instruksen er vedlagt aftalen som Bilag 1.
3. Databehandleren må kun behandle personoplysninger til de formål, som er nødvendige for at opfylde aftalen med den Dataansvarlige, og er til enhver tid forpligtet til at overholde de gældende lovgivningsmæssige krav og regler vedr. behandlingen af personoplysninger.



4. Databehandleren må ikke behandle personoplysninger til andre eller egne formål, og må ikke videregive personoplysningerne til tredje part uden forudgående aftale med den Dataansvarlige.
5. 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. Tekniske og organisatoriske sikkerhedsforanstaltninger

1. Databehandleren skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.
2. Databehandleren har udarbejdet IT-sikkerhedspolitikker og er forpligtet til bl.a. at undervise egne medarbejdere i korrekt håndtering af personoplysninger. Databehandleren skal sikre, at alle Databehandlerens medarbejdere er underlagt tavshedspligt. Underdatabehandlere skal ligeledes være underlagt fuld tavshedspligt.
3. Databehandleren forpligter sig til over for uvedkommende at hemmeligholde alle personoplysninger, som Databehandleren får kendskab til som led i opfyldelsen af aftalen med den Dataansvarlige.
4. Databehandleren bemyndiges hermed selv at definere yderligere tekniske og organisatoriske sikkerhedsforanstaltninger, der skal anvendes for at skabe den nødvendige datasikkerhed.
5. For yderligere information henvises til Bilag 2.

4. Underdatabehandler

1. Databehandleren kan gøre brug af underdatabehandlere i det omfang dette er defineret i denne aftales instruks i Bilag 1 eller særskilt aftale med den Dataansvarlige
2. Det er Databehandlerens ansvar at indgå databehandleraftaler med underdatabehandlere og sørge for, at disse aftaler og underdatabehandlere



- efterlever denne aftale og evt. yderligere krav fra den Dataansvarlige vedr. behandlingen af personoplysninger.
3. Databehandleren vil underrette den Dataansvarlige om ændringer vedrørende tilføjelser og udskiftninger af Underdatabehandlere, og Databehandleren vil give den Dataansvarlige mulighed for at opponere mod disse ændringer.
 4. Underdatabehandlere, som Databehandleren anvender fremgår af Bilag 1. Ved accept af nærværende aftale, accepterer den Dataansvarlige Databehandlerens brug af Underdatabehandlere på ovennævnte vilkår.

5. Overførsel til tredjelande eller internationale organisationer

1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisationer (lande uden for EU/EØ) 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 1.
5. Disse Bestemmelser skal ikke forveksles med standardkontraktbestemmelser som omhandlet i databeskyttelsesforordningens artikel 46, stk. 2, litra c og d, og disse Bestemmelser kan ikke udgøre et grundlag for overførsel af personoplysninger som omhandlet i databeskyttelsesforordningens kapitel V.



6. Databehandlerens interne procedurer

1. Databehandleren skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med lov om behandling af personoplysninger.
2. Databehandleren skal sikre, at det kun er autoriserede betroede personer med sagligt formål, der har adgang til personoplysningerne, og at disse enten har underskrevet fortrolighedserklæring eller er underlagt lovbestemt tavshedspligt.
3. Det er Databehandlerens opgave at sikre, at databehandlingen sker i sikre rammer, herunder i det omfang Databehandler gør brug af hjemmearbejdspladser eller andre lokaliteter ud over Databehandlers kontor.
4. Det er også Databehandlers opgave at sikre, at involverede medarbejdere uddannes i korrekt håndtering af personoplysninger.

7. Revision og oplysningspligt

1. Databehandleren skal til enhver tid bistå den Dataansvarlige i at opfylde lovbestemte forpligtelser over for de registrerede. Databehandleren skal på den Dataansvarliges anmodning give den Dataansvarlige tilstrækkelige oplysninger til, at denne kan påse, at de nævnte tekniske og organisatoriske sikkerhedsforanstaltninger er truffet.
2. I tilfælde af, at Tilsynsmyndigheden ønsker at foretage en fysisk inspektion af ovennævnte foranstaltninger, er Databehandleren forpligtet til – med et rimeligt varsel – at stille de nødvendige ressourcer til rådighed.
3. Den Dataansvarlige kan med forudgående aftale med Databehandleren indhente en årlig revisionserklæring fra en tredje part, som får adgang til Databehandleren og underdatabehandlere. Revision og inspektion kan kun ske efter forudgående varsel på minimum 4 uger. Den Dataansvarlige afholder selv alle omkostninger hertil, herunder omkostninger der påføres Databehandleren jf. forbrug af tid og ressourcer.



8. Bistand til den dataansvarlige

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

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. 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 i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den Dataansvarliges overholdelse af sin forpligtelse efter forordningens artikel 32.
 3. I tillæg til Databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 7.2., bistår Databehandleren desuden, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for Databehandleren, den Dataansvarlige med:
 - a. den dataansvarliges forpligtelse til uden unødigt forsinkelse at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, medmindre det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.



- b. den dataansvarliges forpligtelse til uden unødigt forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettigheder
- c. den dataansvarliges forpligtelse til forud for behandlingen at analysere de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)
- d. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, 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.

9. Underretningspligt

1. Databehandleren er forpligtet til at underrette den Dataansvarlige skriftligt ved kendskab til enhver afvigelse i forhold til opfyldelse af denne Aftale, herunder ved afvigelse fra instrukser fra den Dataansvarlige.
2. Databehandleren er forpligtet til at underrette den Dataansvarlige uden unødigt forsinkelse i tilfælde af brud på fortrolighedsforpligtelser, misbrug, fortabelse eller forringelse af data.
3. Ved brud på persondatasikkerheden skal Databehandleren ved at underrette den Dataansvarlige gøre det muligt for den Dataansvarlige at overholde kravene i EU GDPR artikel 33 og 34 og anden gældende lovgivning.
4. I overensstemmelse med Bestemmelse 7.3.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.



10. Håndtering af data efter aftalens ophør

1. Det påhviler den Dataansvarlige at oplyse Databehandleren om det tidspunkt, hvor databehandlingen skal ophøre, ligesom det påhviler den Dataansvarlige at informere Databehandleren om, hvad der skal ske med personoplysningerne ved aftalens ophør.
2. Ved ophør af tjenesterne vedrørende behandling, herunder ved aftalens ophør, forpligtes Databehandleren til at slette alle personoplysninger tilhørende den Dataansvarlige, samt at slette eksisterende kopier, medmindre EU-retten eller national ret foreskriver opbevaring af personoplysningerne. Sletning må dog ikke ske før Databehandleren har oplyst den Dataansvarlige om den påtænkte fremgangsmåde for sletning.
3. Den Dataansvarlige har fuld rådighed over personoplysningerne og har ret til at få disse udleveret på begæring, herunder ved aftalens ophør. Databehandleren honoreres for håndtering baseret på timepris for medgået tid.

11. Aftalens gyldighed

1. Aftalen indgås ved begge parters accept og er gældende, så længe den Dataansvarlige anvender af aftalen omfattede IT-Løsninger.
2. Begge parter kan kræve ændringer i aftalen, såfremt ændringerne er nødvendige for at efterleve lovgivningen.

12. Tvister

Aftalen er underlagt gældende lov og værneting, medmindre andet er påkrævet i gældende databeskyttelseslovgivning.

13. Diverse



1. Parterne accepterer, at nærværende aftale erstatter tidligere indgået og/eller eksisterende Databehandleraftaler.
2. I tilfælde af lovændringer, sikkerhedsændringer eller andre praktiske omstændigheder kan der foretages tilpasning af denne aftale. Ved tilpasning af aftalen vil der blive givet skriftlig meddelelse til den anden part. Justeringen vil blive betragtet som accepteret af parten, medmindre den anden part har fremsat lovlige skriftlige indvendinger inden for to uger fra datoen for meddelelsen. Relevante bilag vil blive justeret i overensstemmelse hermed.

14. Accept

I kraft af sit medlemskab af DOF, har den Dataansvarlige betinget adgang til IT-Løsninger beskrevet i Bilag 1.

Ibrugtagning af disse IT-Løsninger betyder automatisk accept af denne Databehandleraftale.



Bilag 1: Den Dataansvarliges instruktioner til Databehandleren

Dette bilag er en integreret del af aftalen og udgør den Dataansvarliges instruks til Databehandleren i forbindelse med anvendelsen af IT-Løsninger, der benyttes af den Dataansvarlige til at opbevare og arbejde med personoplysninger vedrørende den Dataansvarliges kursister og medarbejdere.

1.1 Systembeskrivelse

IT-Løsninger består af:

1. ASA: Benyttes til skole- og kursusadministration samt bogføring.
2. UnderviserNet: Benyttes som underviserens indgang til kursusadministration.
3. Intect (lønkørsel i DOF): Benyttes til lønadministration.
4. VuptiWeb: CMS, benyttes til visning af kurser, online tilmelding og betaling.

1.2 Formål med behandlingen

Databehandleren stiller IT-Løsninger til rådighed for den Dataansvarlige. IT-Løsninger benyttes til at opbevare en række kursus-, deltager- og HR-data samt til at lette administrative processer for den Dataansvarlige.

Databehandleren leverer softwareløsninger, herunder services, support og hosting, til brug for den Dataansvarlige. Som led i leverancen heraf, vil Databehandleren få adgang til personoplysninger vedrørende den Dataansvarliges deltagere og ansatte.

1.2.1 Formål med den Dataansvarliges behandling af deltagernes persondata

- Kunde- og deltagerhåndtering, herunder tilmeldinger og betalinger.
- Planlægning, gennemførelse og kursusopfølgning.
- Medlemsadministration.
- Opfyldelse af lovkrav vedr. tilskud.
- Bogføringsloven vedr. opbevaring af oplysninger.

1.2.2 Formål med den Dataansvarliges behandling af HR-data

- Arbejdsretlige forpligtelser.
- Opfyldelse af lovkrav, herunder skattelovgivning.
- Udbetaling af løn, refusioner, diæter osv.

1.2.3 Formål med Databehandlerens behandling af persondata

- Drift
- Support og fejlfinding
- Interesseafvejning



- Udbetaling af løn, refusioner, diæter osv.

1.3 Kategorier af datasubjekter

1. Kursusdeltagere
2. HR (undervisere og personale)

1.4. Kategorier af personoplysninger

- For deltagere: Navn, adresse, CPR, fødselsdato, kommune, e-mail, telefon, kursusdeltagelse, betalingsinformationer.
- For HR: Navn, adresse, CPR, ansættelses- og opsigelsesdato, lønoplysninger, telefon, e-mail, CV, kompetencer, ansættelsestype.

1.5 Fysisk placering af behandlingen

Behandling sker på Databehandlers adresse samt godkendte hjemmearbejdspladser.

1.6 Godkendte underdatabehandlere

Databehandleren er parten i samarbejdsfælleskabet OFASA, som på vegne af Databehandleren har relevante databehandleraftaler med følgende underdatabehandlere:

1. Abakion a/s, Lyngbyvej 2, 2100 København Ø.
 - ASA hosting og support. Microsoft partner.
2. EG Danmark a/s, Lautrupvang 24, 2750 Ballerup.
 - ASA udvikling og support.
3. iQi Digital APS, Fruebjergvej 3, 2100 København Ø.
 - ASA API udvikling, hosting og support.
4. Umakers, Tempelvej 7, 4390 Vipperød.
 - UnderviserNet udvikling, hosting og support.

Derudover bruger Databehandleren følgende underdatabehandlere:

5. Microsoft Nederland, Evert van de Beekstraat 354, 1118 CZ Schiphol, Holland.
 - Microsoft Azure – Data hosting og data processing
 - Servere placeret i Holland.
6. Microsoft Ireland Operations Ltd, One Microsoft Place, South County Business Park Leopardstown Dublin 18, D18 P521 Ireland.
 - Microsoft Azure – Data hosting og data processing
 - Servere placeret i Irland
7. Intect ApS, Hørkær 12A, 2730 Herlev.



- Løn - og personalestyringsprogram udvikling, hosting og support.
- 8. Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany
 - UnderviserNet hosting.
 - Servere placeret i Tyskland.
- 9. Novicell, Amerika Plads 19, 2100 København Ø.
 - VuptiWeb udvikling og support.



Bilag 2: Tekniske og organisatoriske sikkerhedskrav

2.1 Databehandlerens fysiske sikkerhed

1. Adgang til Databehandlerens bygning og kontorer er aflåst uden for arbejdstiden.
2. Besøgende skal følges med en Databehandlerens medarbejder.
3. Fysisk materiale opbevares aflåst.

2.2 Databehandlerens tekniske sikkerhed

1. Databehandlerens IT udstyr er beskyttet med opdateret antivirus- og sikkerhedssoftware.
2. Lokal firewall på PC'er og servere er aktiveret og opdateret.
3. Databehandlerens lokale netværk er beskyttet af en opdateret firewall.
4. Databehandlerens medarbejdere har ekstern adgang til netværk via krypterede forbindelser.
5. Udveksling af persondata fra IT systemer til hostningscentre sker via krypterede forbindelser.
6. Hardware- og netværkssikkerhed hos hostningsvirksomheder lever op til de enhver tid gældende krav om passende datasikkerhed.

2.3 Databehandleren organisatoriske sikkerhed

1. Det er kun betroede personer med sagligt formål, som har adgang til personoplysninger.
2. Databehandlerens medarbejdere er underlagt tavshedspligt og undervist i korrekt behandling og beskyttelse af personoplysninger.
3. Databehandleren fører en fortegnelse over egne databehandlingsaktiviteter, som er underlagt Datatilsynets kontrol.
4. Ved destruering eller reparation af IT udstyr, sørges der for, at oplysninger ikke kan komme til uvedkommendes kendskab.

2.4 Relevante hjemmesider

Databehandlerens Persondatapolitik kan læses/hentes på hjemmesiden:

www.danskoplysning.dk

