|  |
| --- |
|  |
| DATABEHANDLERAFTALE |

Standardkontraktsbestemmelser

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

mellem

<INSTITUTION>

CVR <CVR>

<ADRESSE>

 <POSTNR.> <BY> <LAND>

herefter ”den dataansvarlige”

og DeiC

CVR 30 06 09 46

DTU | Asmussens Alle | bygning 305 2800 Kgs Lyngby

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 per- soners grundlæggende rettigheder og frihedsrettigheder

**1.Indhold**

2.Præambel 3

1. [Den dataansvarliges rettigheder og forpligtelser 3](#_TOC_250015)
2. [Databehandleren handler efter instruks 4](#_TOC_250014)
3. [Fortrolighed 4](#_TOC_250013)
4. [Behandlingssikkerhed 4](#_TOC_250012)
5. [Anvendelse af underdatabehandlere 5](#_TOC_250011)
6. [Overførsel til tredjelande eller internationale organisationer 6](#_TOC_250010)
7. [Bistand til den dataansvarlige 7](#_TOC_250009)
8. [Underretning om brud på persondatasikkerheden 8](#_TOC_250008)
9. [Sletning og returnering af oplysninger 8](#_TOC_250007)
10. [Revision, herunder inspektion 8](#_TOC_250006)
11. [Parternes aftale om andre forhold 9](#_TOC_250005)
12. [Ikrafttræden og ophør 9](#_TOC_250004)
13. [Kontaktpersoner hos den dataansvarlige og databehandleren 10](#_TOC_250003)

[Bilag A Oplysninger om behandlingen 11](#_TOC_250002)

[Bilag B Underdatabehandlere 12](#_TOC_250001)

[Bilag C Instruks vedrørende behandling af personoplysninger 13](#_TOC_250000)

Bilag D Parternes regulering af andre forhold………..…………………………………………..16

1. **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 WAYF-tjenesten 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, her- under om behandlingens formål og karakter, typen af personoplysninger, kategori- erne af registrerede og varighed af behandlingen.
	7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af un- derdatabehandlere 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 databehand- leren er pålagt efter databeskyttelsesforordningen eller enhver anden lovgivning.

# 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.

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

* 1. 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.
	2. Den dataansvarlige er ansvarlig for, blandt andet, at sikre, at der er et behandlings- grundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

# 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 medlemssta- ternes nationale ret, som databehandleren er underlagt. Denne instruks skal være specificeret i bilag A og C. Efterfølgende instruks kan også gives af den dataansvar- lige, mens der sker behandling af personoplysninger, men instruksen skal altid være dokumenteret og opbevares skriftligt, herunder elektronisk, sammen med disse Be- stemmelser.
		2. Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter vedkommendes mening er i strid med denne forordning eller databeskyttelsesbe- stemmelser i anden EU-ret eller medlemsstaternes nationale ret.

# Fortrolighed

* + 1. Databehandleren må kun give adgang til personoplysninger, som behandles på den dataansvarliges vegne, til personer, som er underlagt databehandlerens instruktions- beføjelser, som har forpligtet sig til fortrolighed eller er underlagt en passende lovbe- stemt 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 nødven- dig, 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.

# Behandlingssikkerhed

* + 1. Databeskyttelsesforordningens artikel 32 fastslår, at den dataansvarlige og databe- handleren, under hensyntagen til det aktuelle tekniske niveau, implementeringsom- kostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers ret- tigheder 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 friheds- rettigheder, som behandlingen udgør og gennemføre foranstaltninger for at imødegå disse risici. Afhængig af deres relevans kan det omfatte:

* + - 1. pseudonymisering og kryptering af personoplysninger
			2. evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og ro- busthed af behandlingssystemer og -tjenester
			3. evne til rettidigt at genoprette tilgængeligheden af og adgangen til personop- lysninger i tilfælde af en fysisk eller teknisk hændelse
			4. en procedure for regelmæssig afprøvning, vurdering og evaluering af effek- tiviteten af de tekniske og organisatoriske foranstaltninger til sikring af be- handlingssikkerhed.
		1. Efter forordningens artikel 32 skal databehandleren – uafhængigt af den dataansvar- lige – også vurdere risiciene for fysiske personers rettigheder som behandlingen ud- gør 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.
		2. Derudover skal databehandleren bistå den dataansvarlige med vedkommendes over- holdelse 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 alle- rede har gennemført i henhold til forordningens artikel 32, og al anden information, der er nødvendig for den dataansvarliges overholdelse af sin forpligtelse efter forord- ningens artikel 32.

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

# Anvendelse af underdatabehandlere

* + 1. Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesfor- ordningens artikel 28, stk. 2, og stk. 4, for at gøre brug af en anden databehandler (en underdatabehandler).
		2. Databehandleren må således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående specifik skriftlig godkendelse fra den data- ansvarlige.
		3. Databehandleren må kun gøre brug af underdatabehandlere med den dataansvarli- ges forudgående specifikke skriftlige godkendelse. Databehandleren skal indgive an- modningen om en specifik godkendelse mindst to måneder inden anvendelsen af den pågældende underdatabehandler. Listen over underdatabehandlere, som den data- ansvarlige 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 databehand- leren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databe- skyttelsesforpligtelser 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 mi- nimum overholder databehandlerens forpligtelser efter disse Bestemmelser og data- beskyttelsesforordningen.

* + 1. 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 kommer- cielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold af underdatabe- handleraftalen, skal ikke sendes til den dataansvarlige.
		2. Databehandleren skal i sin aftale med underdatabehandleren indføje den dataansvar- lige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gæl- dende over for underdatabehandlere, som f.eks. gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.
		3. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af under- databehandlerens 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 underdatabehandle- ren.

# Overførsel til tredjelande eller internationale organisationer

1. Enhver overførsel af personoplysninger til tredjelande eller internationale organisati- oner må kun foretages af databehandleren på baggrund af dokumenteret instruks herom fra den dataansvarlige og skal altid ske i overensstemmelse med databeskyt- telsesforordningens 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 databehandle- ren er underlagt, skal databehandleren underrette den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underret- ning af hensyn til vigtige samfundsmæssige interesser.
3. Uden dokumenteret instruks fra den dataansvarlige kan databehandleren således ikke inden for rammerne af disse Bestemmelser:
	1. overføre personoplysninger til en dataansvarlig eller databehandler i et tred- jeland eller en international organisation
	2. overlade behandling af personoplysninger til en underdatabehandler i et tred- jeland
	3. behandle personoplysningerne i et tredjeland
4. Den dataansvarliges instruks vedrørende overførsel af personoplysninger til et tred- jeland, 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.

# Bistand til den dataansvarlige

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

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

* 1. oplysningspligten ved indsamling af personoplysninger hos den registre- rede
	2. oplysningspligten, hvis personoplysninger ikke er indsamlet hos den regi- strerede
	3. indsigtsretten
	4. retten til berigtigelse
	5. retten til sletning (”retten til at blive glemt”)
	6. retten til begrænsning af behandling
	7. underretningspligten i forbindelse med berigtigelse eller sletning af person- oplysninger eller begrænsning af behandling
	8. retten til dataportabilitet
	9. retten til indsigelse
	10. retten til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering
1. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 6.3., bistår databehandleren endvidere, under hensyntagen til behand- lingens karakter og de oplysninger, der er tilgængelige for databehandleren, den da- taansvarlige med:
	1. den dataansvarliges forpligtelse til uden unødig forsinkelse og om muligt se- nest 72 timer, efter at denne er blevet bekendt med det, at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed, Datatilsynet i Danmark, medmindre at det er usandsynligt, at bruddet på persondatasik- kerheden indebærer en risiko for fysiske personers rettigheder eller friheds- rettigheder
	2. den dataansvarliges forpligtelse til uden unødig forsinkelse at underrette den registrerede om brud på persondatasikkerheden, når bruddet sandsynligvis vil medføre en høj risiko for fysiske personers rettigheder og frihedsrettighe- der
	3. den dataansvarliges forpligtelse til forud for behandlingen at foretage en ana- lyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)
	4. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndig- hed, Datatilsynet i Danmark, inden behandling, såfremt en konsekvensana- lyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i

mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risi- koen.

1. Parterne skal i bilag C angive de fornødne tekniske og organisatoriske foranstaltnin- ger, 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.

# Underretning om brud på persondatasikkerheden

1. Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden.
2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 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 data- ansvarlige med at foretage anmeldelse af bruddet til den kompetente tilsynsmyndig- hed. Det betyder, at databehandleren skal bistå med at tilvejebringe nedenstående information, som ifølge artikel 33, stk. 3, skal fremgå af den dataansvarliges anmel- delse af bruddet til den kompetente tilsynsmyndighed:
	1. karakteren af bruddet på persondatasikkerheden, herunder, hvis det er mu- ligt, kategorierne og det omtrentlige antal berørte registrerede samt katego- rierne og det omtrentlige antal berørte registreringer af personoplysninger
	2. de sandsynlige konsekvenser af bruddet på persondatasikkerheden
	3. de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er rele- vant, 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.

# Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger, er databe- handleren 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 EU-retten eller medlemsstaternes nationale ret foreskriver op- bevaring af personoplysningerne.

# Revision, herunder inspektion

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdel- sen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder in- spektioner, der foretages af den dataansvarlige eller en anden revisor, som er be- myndiget af den dataansvarlige.
2. Procedurerne for 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 lov- givning har adgang til den dataansvarliges eller databehandlerens faciliteter, eller re- præsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehand- lerens fysiske faciliteter mod behørig legitimation.

# 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 bestem- melser ikke direkte eller indirekte strider imod Bestemmelserne eller forringer den re- gistreredes grundlæggende rettigheder og frihedsrettigheder, som følger af databe- skyttelsesforordningen.

# Ikrafttræden og ophør

1. Bestemmelserne træder i kraft på datoen for begge parters underskrift heraf.
2. Begge parter kan kræve Bestemmelserne genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i Bestemmelserne giver anledning hertil.
3. Bestemmelserne er gældende, så længe tjenesten vedrørende behandling af person- oplysninger 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 overensstem- melse med Bestemmelse 11.1 og Bilag C.4, kan Bestemmelserne opsiges med skrift- ligt varsel af begge parter.
5. Underskrift

På vegne af den dataansvarlige Navn

Stilling

Telefonnummer

E-mail

Underskrift

På vegne af databehandleren

Navn

Stilling

Telefonnummer

E-mail

 Underskrift

# Kontaktpersoner hos den dataansvarlige og databehandleren

1. Parterne kan kontakte hinanden via nedenstående kontaktpersoner.
2. Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersoner.

Navn

Stilling

Telefonnummer

E-mail

Navn Mikkel Hald

Stilling konsulent Telefonnummer 0045 3126 9288

E-mail sekretariat@wayf.dk

# Bilag A Oplysninger om behandlingen

## Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige

* + - At drifte et forbindelsesled mellem institutioner (med brugerdata og autentifikations- systemer) og netbaserede services (som kræver login for adgang).

## Databehandlerens behandling af personoplysninger på vegne af den dataansvar- lige drejer sig primært om (karakteren af behandlingen)

* + - Institutionen opbevarer og administrerer selv oplysninger om dens tilknyttede brugere (ansatte, studerende etc.). DeiC formidler med WAYF-tjenesten den tekniske adgang til en række netbaserede services for disse brugere.
		- WAYF dataminimerer, så ikke alle brugerens oplysninger videresendes til den SP (Service Provider) brugeren ønsker adgang til, men kun de oplysninger der er nødvendige for at SP’en kan verificere brugerens adgangsret og i øvrigt levere servicen til brugeren.
	1. **Behandlingen omfatter følgende typer af personoplysninger om de registrerede** De om hver registreret behandlede oplysninger har altovervejende karakter af identifikationsoplysninger. Det varierer med WAYF-føderationens og den dataansvarliges behov hvilke oplysningstyper der konkret behandles; den dataansvarlige instruerer DeiC i at behandle en oplysningstype ved at fremsende den til WAYF fra sit loginsystem efter hver brugers autentifikation. Det er til enhver tid opregnet på WAYFs hjemmeside (ved aftalens indgåelse på adressen https://www.wayf.dk/da/attributter) hvilke typer oplysninger DeiC understøtte at behandle i WAYF; de kan eksempelvis omfatte:
		+ Bruger-ID’er ved institutionen
		+ Den digitale identitets sikringsniveau
		+ E-mailadresser
		+ Fødselsdato
		+ Foretrukne sprog
		+ Fulde navn
		+ Gruppemedlemskaber og systemrettigheder ved institutionen
		+ Institutionens CVR-nummer og kategori
		+ Institutionens identitet og navn
		+ Lokalt identifikationsnummer
		+ Mobiltelefonnummer
		+ Nationale unikke ID (dansk CPR-nummer)
		+ Rolle ved institutionen
		+ Statstilhørsforhold

## Behandlingen omfatter følgende kategorier af registrerede

* + - Ansatte, studerende og andre tjenestebrugere hos den dataansvarlige.

## Databehandlerens behandling af personoplysninger på vegne af den dataansvar- lige kan påbegyndes efter disse Bestemmelsers ikrafttræden. Behandlingen har føl- gende varighed

* + - Behandlingen er ikke tidsbegrænset og varer indtil aftalen opsiges eller ophæves af en af parterne.

# Bilag B Underdatabehandlere

## Godkendte underdatabehandlere

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende un- derdatabehandlere

|  |  |  |  |
| --- | --- | --- | --- |
| **NAVN** | **CVR** | **ADRESSE** | **BESKRIVELSE AF BEHANDLING** |
| NORDUnet A/S | 17490346 | Kastruplundgade 22,1. 2770 Kastrup | Hosting af WAYF’s servere, herunder den maskine, som opbevarer loggen over log-in forsøg igennem WAYF. |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af ovennævnte underdatabehandler 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 under- databehandler til denne behandlingsaktivitet.

## Varsel for godkendelse af underdatabehandlere

Det fremgår af aftalens punkt 7.3, at varslingsperioden for godkendelse af nye underdatabe- handlere af den dataansvarlige er aftalt til at være to måneder.

# Bilag C Instruks vedrørende behandling af personoplysninger

## Behandlingens genstand/instruks

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

* + - Hver gang en kontoindehaver ved Institutionen forsøger at tilgå en til WAYF tilsluttet service, modtager WAYF oplysninger om vedkommende fra Institutionen. WAYF-tjenesten udvælger den delmængde af oplysningerne som en SP (Service Provider) behøver for at kunne levere servicen til brugeren – og videregiver de udvalgte oplysninger til SP’en i det tekniske format som de forventer. WAYF sletter alle modtagne oplysninger umiddelbart herefter.
		- Brugeren kan ansøge samtlige services som er optaget i WAYF, om at blive koblet op til den pågældende service. WAYF vil automatisk sende de kategorier af informa- tioner til den ønskede service som er nødvendige for at logge på servicen. SP’en verificerer brugerens adgangsret til servicen. Det er WAYF uvedkommende, og en sag mellem hver SP (Service Provider) og hver institution, hvilke brugere der skal have brugsret til en bestemt service.
		- Oplysninger om hvordan WAYF er drevet, findes på WAYF’s hjemmeside, [www.wayf.dk](http://www.wayf.dk/), ved aftalens indgåelse særligt på <https://www.wayf.dk/da/politikker>.
		- Oplysninger om hvordan en service (SP) optages i WAYF, fremgår af WAYF’s hjemmeside, ved aftalens indgåelse på https[://www.wayf.dk/da/node/](http://www.wayf.dk/en/node/49)49.

## Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle:

* + - At der er tale om behandling af identifikationsoplysninger, herunder eventuelt CPR- nummer, som skal videregives til andre organisationer.

Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekni- ske og organisatoriske sikkerhedsforanstaltninger der skal gennemføres for at etableret det nødvendige (og aftalte) sikkerhedsniveau.

Databehandleren skal dog – under alle omstændigheder og som minimum – gennemføre føl- gende foranstaltninger, som er aftalt med den dataansvarlige:

* + - Opretholde ISO 27001-efterlevelse for at sikre kravene vedrørende procedurer for
		regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og

organisatoriske foranstaltninger til sikring af behandlingssikkerheden.

* + - Lokationer, hvor der behandles personoplysninger, sikres fysisk ved hjælp af adgangsbegrænsning og aflåsning.
		- Fjernadgang til systemer sikres ved hjælp af sikkert log-in og kryptering.
		- Oplysningerne er krypterede i transmission.
		- Oplysningerne skal signeres ved HSM (hardwarenøgler).
		- Oplysningerne pseudonymiseres i loggen.
		- Failover-mekanisme via to datacentre.
		- WAYF filtrerer informationer om brugeren, så der kun sendes påkrævede log-in informationer til SP (Service Provider).
		- Der informeres løbende om tjenesten på WAYF’s hjemmeside.

## Bistand til den dataansvarlige

Databehandleren skal så vidt muligt – inden for det omfang og den udstrækning som er be- skrevet nedenfor – bistå den dataansvarlige i overensstemmelse med Bestemmelse 9.1 og

* 1. ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

		+ Databehandler skal have en procedure der sikrer at anmodninger fra registrerede vi-

deresendes til den dataansvarlige inden for fem dage efter modtagelse

## Opbevaringsperiode/sletterutine

Personoplysningerne opbevares ikke permanent hos WAYF, men alene helt flygtigt, i størrel- sesordenen få millisekunder, hver gang en bruger fra Institutionen forsøger at tilgå en til WAYF tilsluttet service.

## Lokalitet for behandling

Behandling af de i aftalen omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end de følgende:

* + - Datacentre på to forskellige lokaliteter i Storkøbenhavn.

Underdatabehandleren kan kun overføre personoplysninger til et andet land i Norden efter skriftlig godkendelse af databehandleren, på vegne af den dataansvarlige. Den dataansvarlige kan alene nægte godkendelse, såfremt den dataansvarlige har rimelige, konkrete årsager her- til. Afvisning af godkendelse skal ske senest tre uger fra modtagelse af anmodning.

## Instruks vedrørende overførsel af personoplysninger til tredjelande

Når den dataansvarlige tilmelder sig WAYF-tjenesten, godkender den dataansvarlige overførsel af brugerens personoplysninger til et tredjeland ved log-in-processen når en SP (Service Provider) befinder sig i et tredjeland.
Den dataansvarlige har pligt til at oplyse brugeren om overførsel og sikre hjemmel til overførsel.
WAYF viser på log-in-tidspunktet en generel oplysningsside, som muligvis er egnet til at varetage oplysningspligten og evt. indhentelsen af samtykke til overførsel.

## Procedurer for den dataansvarliges revisioner, herunder inspektioner, med behand- lingen af personoplysninger, som er overladt til databehandleren

Der er enighed mellem parterne om, at følgende typer af tilsyn og certificeringer kan anvendes uden meromkostninger for den dataansvarlige:

* Internt tilsyn
* ISO 27001-certificering

Det interne tilsyn vil blive gennemført hvert 2. år, og dette interne tilsyn er ment som en udvidet service som kan sidestilles med og udgøre dataansvarliges eget tilsyn.
Den dataansvarlige kan i forlængelse af det interne af tilsyn stille yderligere uddybende spørgsmål til WAYF efter behov.

Den dataansvarlige kan gennemføre andre former for tilsyn eller inspektion og afholder alle udgifter forbundet hermed. Databehandleren er dog forpligtet til at afsætte ressourcer i rimeligt omfang (hovedsageligt den tid) der er nødvendige for at den dataansvarlige kan gennemføre sit tilsyn eller inspektion.

I tilfælde af der stilles uforholdsvis stort krav til databehandleren om at afsætte ressourcer i forbindelse med dataansvarliges tilsyn eller inspektion, kan databehandleren forlange at få sine omkostninger dækket af den dataansvarlige.

Rimeligt omfang måles i forhold til hvad der i almindelighed efterspørges i forbindelse med et tilsyn med eller inspektion af lignende virksomheder udført af Datatilsynet eller revisorvirksomheder.

## Procedurer for revisioner, herunder inspektioner, med behandling af personoplys- ninger, som er overladt til underdatabehandlere

WAYF gennemfører tilsyn med underleverandør hvert andet år ved hjælp af interviews og gennemgang af dokumentation.