

DATABASEHANDLERAFTALE

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

mellem

herefter "den dataansvarlige"

og

Ordbogen A/S
CVR. 26404037
Billedskærervej 8
5230 Odense M

herefter "databehandleren"

der hver især er en "part" og sammen udgør "parterne" har aftalt følgende med henblik på at overholde databeskyttelsesforordningen og sikre beskyttelse af privatlivets fred og fysiske personers grundlæggende rettigheder og frihedsrettigheder.

Indhold

1. Præambel.....	3
2. Den dataansvarliges rettigheder og forpligtelser	3
3. Databehandleren handler efter instruks	4
4. Fortrolighed	4
5. Behandlingssikkerhed	4
6. Anvendelse af underdatabehandlere	5
7. Overførsel til tredjelande eller internationale organisationer.....	6
8. Bistand til den dataansvarlige.....	6
9. Underretning om brud på persondatasikkerheden	7
10. Sletning og returnering af oplysninger	8
11. Revision og tilsyn	8
12. Parternes aftale om andre forhold	8
13. Ikrafttræden og ophør	9
14. Kontaktpersoner hos den dataansvarlige og databehandleren.....	10
Bilag A Oplysninger om behandlingen.....	11
Bilag B Underdatabehandlere	15
Bilag C Instruks vedrørende behandling af personoplysninger	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 online ordbøger og undervisningsportaler behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse bestemmelser.
4. Med "Aftalen" menes de forskellige successive ordrer, som den dataansvarlige har afgivet til databehandleren.
5. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.
6. Der hører tre bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.
7. 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.
8. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.
9. 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.
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.

2. 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 medlemsstaters 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.

3. 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.

4. 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.

5. 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.
2. 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.

3. 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.
4. 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.
5. 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.

6. Anvendelse af underdatabehandlere

1. Ved underdatabehandler forstås en underleverandør, til hvem databehandleren har overladt hele eller dele af den behandling, som databehandleren foretager på vegne af den dataansvarlige. 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 ikke uden udtrykkelig skriftlig godkendelse fra den dataansvarlige anvende andre underdatabehandlere end dem, der er angivet i bilag B, herunder foretage udskiftning af disse, til at behandle de personoplysninger, som den dataansvarlige har overladt til databehandleren i medfør af Aftalen. Den dataansvarlige kan ikke nægte at godkende tilføjelse eller udskiftning af en underdatabehandler medmindre, der foreligger en konkret saglig begrundelse herfor.
3. Hvis databehandleren overlader behandlingen af personoplysninger, som den dataansvarlige er ansvarlig for, til underdatabehandlere, skal databehandleren indgå en skriftlig (under)databehandleraftale med underdatabehandleren.
4. Underdatabehandleraftalen, jf. pkt. 3, skal pålægge underdatabehandleren de samme databeskyttelsesforpligtelser, som databehandleren er pålagt efter Aftalen, herunder, at underdatabehandleren garanterer at kunne levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at kunne implementere de passende tekniske og organisatoriske foranstaltninger således, at underdatabehandlerens behandling opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.
5. Når databehandleren overlader behandlingen af personoplysninger, som den dataansvarlige er ansvarlig for, til underdatabehandlere, har databehandleren over for den dataansvarlige ansvaret for underdatabehandlerens overholdelse af disses forpligtelser, jf. pkt. 4.
6. Den dataansvarlige kan til enhver tid forlange dokumentation fra databehandleren for eksistensen og indholdet af underdatabehandleraftaler for de underdatabehandlere, som databehandleren anvender i forbindelse med opfyldelsen af sine forpligtelser over for den dataansvarlige.
7. Al kommunikation mellem den dataansvarlige og underdatabehandleren sker via databehandleren.

7. 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 pågældendes 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.

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. I tillæg til databehandlerens forpligtelse til at bistå den dataansvarlige i henhold til Bestemmelse 5.4., 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 eller hvis udenfor Danmark den kompetente tilsynsmyndighed i det pågældende land, 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 forud for behandlingen at foretage en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger.
 - d. den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet eller hvis udenfor Danmark den kompetente tilsynsmyndighed i det pågældende land, inden behandling, såfremt en analyse 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 8.1. og 8.2.

9. 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 hos databehandleren eller underdatabehandleren.
2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 48 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 8.2.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.

10. Sletning og returnering af oplysninger

1. Styrelsen for It og Læring, STIL, er ansvarlig for den digitale identifikationsløsning UNI-login, som er det digitale ID, der anvendes til styring af adgangsrettigheder til tjenester for brugere. Den dataansvarlige giver databehandleren adgang til UNI-login personoplysninger via en dataaftale, der er indgået mellem den enkelte undervisningsinstitution og databehandleren. Dataaftalen definerer de personoplysninger (services) jf. bilag A, som databehandleren får adgang til via UNI-Login.
Ved ophør af Aftalen (jf. Bestemmelse 1.4) skal den dataansvarlige lukke den enkelte bruger via skoleadministrationssystemet og dermed databehandlerens adgang til UNI-Login, hvorigennem databehandleren ikke længere vil have adgang til personoplysningerne. Databehandleren vil herefter være i besiddelse af bruger-ID og data på den lukkede bruger. Bruger-ID slettes efter tre måneder for at sikre overgangen til evt. ny dataansvarlig. Databehandleren forpligter sig til at slette alle gemte personoplysninger om den enkelte bruger: Elev/studerende/ansat, der afslutter skoleforløb/ansættelse på grundskoler, gymnasier, ungdomsuddannelser, videregående uddannelser, og som har haft adgang til databehandlerens tjenester, tre måneder efter, at adgangen til databehandlerens tjenester er ophørt.

11. Revision og tilsyn

1. Databehandleren stiller alle oplysninger, der er nødvendige for at påvise overholdelsen af databeskyttelsesforordningens artikel 28 og disse Bestemmelser til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.
2. Procedurene for den dataansvarliges revisioner, herunder tilsyn, 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 lovgivning har adgang til Den dataansvarliges eller databehandlerens faciliteter eller repræsentanter, der optræder på tilsynsmyndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

12. 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.

13. 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 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 den dataansvarlige har lukket for adgangen til UNI-Login i overensstemmelse med Bestemmelse 10.1 og Bilag C.4, kan Bestemmelserne opsiges med skriftlig varsel af begge parter.
5. Underskrift

På vegne af den dataansvarlige

På vegne af den databehandleren

Stilling	Adm. direktør
Navn	Peter Revsbech
Telefonnummer	69 12 76 14
E-mail	pet@ordbogen.com
Dato	D. 1. juni 2021
Underskrift	



14. 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.

Kontaktpersoner hos den dataansvarlige:

Databeskyttelsesrådgiver (DPO)

Revisionserklæringer, allonger og henvendelser vedr. databehandleraftaler sendes på anmodning til:

Kontaktpersoner hos databehandleren:

Navn	Annon M. Østergaard
Stilling	DPO
Telefonnummer	66 12 60 00
E-mail	dba@ordbogen.com

Bilag A Oplysninger om behandlingen

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

Behandling af den dataansvarliges oplysninger sker med det formål, at brugerne kan tilgå databehandlerens online ordbøger og læringsportaler. Ligeledes for, at undervisere kan følge den enkelte elevs progression. Databehandleren må ikke anvende oplysningerne til andre formål. Oplysningerne må ikke behandles efter instruks fra andre end den dataansvarlige.

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

Databehandleren behandler med udgangspunkt i STIL-services WS22 og WS17-lille personoplysninger til brug for adgangskontrol og identifikation af brugere i deres webportaler.

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

Data i STIL-service WS22

Der gives adgang til information om en institutions gruppelicens hos udbyderne, medlemskabet af institutions grupper og information om brugere på institutionen. Følgende information udleveres om institutionens brugere:

- Bruger-ID
- Navn
- Brugertype
- Roller
- Gruppemedlemskaber

For ansatte leveres desuden:

- Initialer
- Stilling

For elever:

- Hovedgruppe/klasse
- Elevtrin

Data i STIL-service WS17-lille

- Den lille pakke: Data i skemaet, som er markeret	L
- Mellem pakken: Data i skemaet, som er markeret	M
- Den fulde pakke: Alle data i skemaet - markeret	F
- Myndighedspakken: Alle data i skemaet - markeret	F
Ved beskyttelse udleveres data mærket * kun af myndighedspakken.	*

Data om ansatte, elever, værger og andre kontaktpersoner				
- CPR-nummer	F	M		*
- Fornavn(e)	F	M	L	*

- Efternavn	F	M	L	*
- Privatadresse (Se adresseinformation)	F			*
- Hjemmetelefon (Se telefonnummer-information)	F			
- Arbejdstelefon (Se telefonnummer-information)	F			
- Mobiltelefon (Se telefonnummer-information)	F			
- E-mail	F	M		
- Fødselsdag	F	M		
- Køn	F	M		
- Photold	F	M		
Adresseinformation:				*
- Om adressen er beskyttet	F			*
- Adressens vejnavn, nr. og etage	F			*
- Postnummer	F			*
- By	F			*
- Landekode	F			*
- Land	F			*
- Kommunekode	F			*
- Kommunens navn	F			*
Telefonnummer-information:				
- Om telefonnummeret er beskyttet	F			
- Telefonnummer	F			
Supplerende data om elever				
- Elevrolle (Barn, Elev, Studerende)	F	M	L	
- Studienummer	F	M	L	
- Elevens niveau (for grundskoleelever)	F	M	L	
- Elevens hovedgruppe (klasse)	F	M	L	
- Yderligere grupper elever er tilknyttet	F	M	L	

- Kontaktperson(er)s relation (Far, Mor eller Andet)	F		
- Om kontaktperson(er) har forældremyndighed	F		
- Afdeling, bygning eller værelsesnummer på efterskoler	F	M	L
- ID i det lokale studieadministrative system	F	M	L
Supplerende data om ansatte			
- Ansættelsesroller (fx Lærer, Pædagog, Leder, ...)	F	M	L
- Initialer	F	M	L
- Stilling	F	M	L
- Afdeling, bygning eller værelsesnummer på efterskoler	F	M	L
- Grupper medarbejderen er tilknyttet	F	M	L
- ID i det lokale studieadministrative system	F	M	
Data om UNI-Login for ansatte og elever			
- UNI-Login brugernavn (brugerID)	F	M	L
- Initialpassword	F	M	
- Om initialpassword er gældende password	F	M	
- Brugerens navn i UNI-Login	F	M	
- SkoleKom-navn	F	M	
- Brugerens selvvalgte email-adresse i UNI-Login	F	M	
- Brugerens selvvalgte mobilnummer i UNI-Login	F	M	
Data om grupper på institutionen			
- Gruppeid	F	M	L
- Gruppenavn	F	M	L
- Gruppetype	F	M	L
- Niveau	F	M	L
- Spor	F	M	L
- Startdato	F	M	L
- Slutdato	F	M	L

A.4. Behandlingen omfatter følgende kategorier af registrerede

Der behandles følgende personoplysninger af registrerede (f.eks. borgere, elever, kontanthjælpsmodtagere m.m.):

- A) Elever
- B) Forældre
- C) Undervisere

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

Behandlingen udløber ved ophør af Aftalen eller tre måneder efter, at adgangen for en bruger til databehandlerens tjenester er ophørt, herunder tre måneder efter, at en brugers UNI-login er blevet gjort inaktivt.

Bilag B Underdatabehandlere

B.1. Godkendte underdatabehandlere

Databehandleren benytter ingen underdatabehandlere.

Ved Bestemmelsernes ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere:

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING

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

Databehandleren skal give et varsel på mindst 30 dage.

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:

Den dataansvarlige instruerer hermed databehandleren om at foretage behandling af den dataansvarliges oplysninger, hentet gennem adgangskontrol, via Uni-Login, jf. Aftalen, adgang til databehandlerens online ordbøger og undervisningsportaler.

Ved ophør af Aftalen skal den dataansvarlige sørge for at lukke dataaftalen mellem den dataansvarlige og databehandleren hos STIL, hvorefter databehandleren ikke længere har adgang til personoplysninger.

Overlader databehandleren behandling af den dataansvarliges oplysninger til underdatabehandlere, er databehandleren ansvarlig for at indgå en skriftlig(under)databehandlertaftale med underdatabehandleren jf. Bestemmelse 6.3. Databehandleren er ansvarlig for, at den dataansvarliges instruks fremsendes til eventuelle underdatabehandlere.

C.2. Behandlingssikkerhed

Databehandleren gennemfører følgende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der passer til de aftalte behandlinger, jf. Instruks (bilag A), og som dermed opfylder Databeskyttelsesforordningens artikel 32.

Foranstaltningerne fastlægges ud fra overvejelser om:

1. Det aktuelle tekniske niveau.
2. Implementeringsomkostningerne.
3. Den pågældende behandlings karakter, omfang, sammenhæng og formål.
4. Konsekvenserne for borgerne ved brud på persondatasikkerheden.
5. Den risiko, der er forbundet med behandlingerne, herunder risikoen for:
 - a) tilintetgørelse af oplysningerne.
 - b) tab af oplysningerne.
 - c) ændring af oplysningerne.
 - d) uautoriseret videregivelse af oplysningerne.
 - e) uautoriseret adgang til oplysningerne.

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.

Politik om behandlingssikkerhed

Denne politik er den overordnede ramme for behandlingssikkerheden ved håndtering af personoplysninger hos databehandleren. Politikken er et uddrag af databehandlerens IT-Sikkerhedspolitik, hvor relevante emner omkring behandlingssikkerhed i forhold til den dataansvarlige, er gengivet nedenfor.

Denne politik understreger, at databehandleren er en IT-virksomhed, der med stort ansvar varetager og leverer data til kommunikation og læring.

Som et led i den overordnede sikkerhedsstyring tager ledelsen, gennem den daglige overvågning og rapportering, politikken op til revurdering.

Minimum én gang årligt bliver IT-Sikkerhedspolitikken og denne politik revurderet, så vi sikrer en løbende tilpasning til trusselsniveauet og fastholdelse af behandlingssikkerheden. Ved ændringer i politikken, der vurderes at have betydning for behandlingssikkerheden, underrettes den dataansvarlige af databehandleren.

Formål

Informationer og databehandling er nødvendige og livsvigtige for databehandleren, hvorfor sikkerheden har vital betydning for databehandlerens troværdighed og funktionsdygtighed.

Formålet med politikken er at definere en ramme for beskyttelse af virksomhedens personoplysninger og særligt at sikre, at kritiske og følsomme oplysninger og behandlingssystemer bevarer deres fortrolighed, integritet og tilgængelighed.

Databehandlerens ledelse har derfor besluttet sig for et sikkerhedsniveau, der er afstemt efter risiko og væsentlighed samt overholder lovkrav – herunder EU-Persondataforordningen og indgåede aftaler.

Ledelsen vil oplyse medarbejderne om ansvarlighed i relation til virksomhedens personoplysninger og behandlingssystemer.

Hensigten med politikken er desuden at tilkendegive over for alle, som har en relation til virksomheden, at anvendelse af data og systemer er underkastet retningslinjer. På denne måde forebygges sikkerhedstrusler, eventuelle skader kan begrænses og etablering af informationer kan sikres.

Omfang

Politikken omfatter databehandlerens data, der tilhører databehandleren – samt data, som ikke tilhører databehandleren, men som databehandleren er ansvarlig for. Dette inkluderer eksempelvis al data om personale, data om kunder eller data fra tredjepart som eksempelvis tjenesten UNI-Login.

Denne politik er gældende for alle ansatte uden undtagelse, både fastansatte og personer, som midlertidigt arbejder for databehandleren, eksempelvis praktikanter eller elever. Ved udlicitering af dele af IT-driften skal det sikres, i samarbejdet med underdatabehandleren, at databehandlerens sikkerhedsniveau fastholdes i henhold til EU-Persondataforordningens artikel 28 og 29.

Organisering

Det er databehandlerens politik at beskytte sine data og udelukkende tillade brug, adgang og offentliggørelse af informationer i overensstemmelse med virksomhedens retningslinjer og under hensyntagen til den til enhver tid gældende lovgivning.

Det operationelle ansvar for den daglige styring af behandlingssikkerhedsindsatsen er placeret hos COO. Denne sikrer, at de aktiviteter, standarder, retningslinjer, kontroller og foranstaltninger, der er beskrevet, gennemføres og efterleves. Ligeledes er behandlingssikkerheden en fast del af forretningsgange, driftsopgaver og udviklingsprojekter. Det operationelle fokus sker samtidig gennem et fast hold af udviklere og teknikere, som overvåger og efterprøver sikkerheden hos databehandleren.

Der er dertil også i udviklingsprocessen indbygget kontroller på tværs af medarbejdere for at sikre kvaliteten og sikkerheden i produkterne for derved at imødegå såvel interne som eksterne trusler.

Adgang til data & systemer

Medarbejdere har kun adgang til data, såfremt der er et klart formål med adgangen. Adgang til data er generelt forbeholdt udviklere med formål i udviklingen. Det er en fast del af databehandlerens sikkerhedspolitik at begrænse adgang til data for såvel udviklere som for administrative medarbejdere. Adgang til behandlingssystemer og systemer med dataadgang overvåges. Ligeledes stilles der krav til sværhedsgraden af adgangskoder samt skift heraf minimum hver tredje måned. Ved ansættelsesophør af centrale medarbejdere, eksempelvis centralteknikere, skiftes samtlige adgangskoder til systemerne. Ligeledes er adgangen som standard kun tilgængelig fra databehandlerens fysiske lokation. Fysisk adgang til servere overvåges ved adgangskontrol samt kameraovervågning. Systemerne er adskilt fra resten af opsætningen for at sikre log.

Data og persondata

Persondata er defineret som det data, der kan identificere en person. Persondata bliver kun bibeholdt i det omfang databehandleren har behov - til levering af servicen. Der er gennem de interne behandlingssystemer afgrænset hvilke data medarbejdere kan tilgå, således at persondata ikke kan viderebringes eller tilgås uden specifikt formål.

Alle medarbejdere er gennem deres ansættelseskontrakter pålagt tavshedspligt.

Sletning af data og backup

Persondata slettes efter tre måneder for at sikre overgang fra en hovedaftale til en ny aftale – eksempelvis i forbindelse med en centralisering af indkøb (Jf. Bestemmelse 10.1).

Der laves backup af data døgnet rundt, og enkelt data laves der backup af timevist. Backuppen bliver sikret på dertil indrettet backupfacilitet afkoblet fra resten af systemet. Således har kun få udvalgte medarbejdere adgang til backupdata. Adgang hertil er logget.

Data bliver slettet i produktionen, men bibeholdt i backup i op til 12 måneder. Det er ikke muligt direkte at trække data ud af backups. Fysiske diske bliver destrueret på en sådan måde, at evt. data herpå bliver utilgængelig.

Overvågning af systemer

Alle systemer skal overvåges døgnet rundt for utilsigtede hændelser, f.eks. forsøg på indbrud eller forsøg på at kopiere data. Behandlingssystemerne lukkes ned af teknikerne ved specielle mønstre og tager aktion i forhold til hændelsen.

C.3 Bistand til den dataansvarlige

Databehandleren skal så vidt muligt – inden for det nedenstående omfang og udstrækning – bistå den dataansvarlige i overensstemmelse med Bestemmelse 8.1 og 8.2 ved at gennemføre følgende tekniske og organisatoriske foranstaltninger:

Databehandleren skal på opfordring fra den dataansvarlige hjælpe med at opfylde den dataansvarliges forpligtelser i forhold til den registreredes rettigheder, herunder besvarelse af anmodninger fra brugere om indsigt i egne oplysninger, udlevering af brugerens oplysninger, rettelse og sletning af oplysninger, begrænsning af behandling af brugerens oplysninger samt den dataansvarliges forpligtelser i forhold til underretning af den registrerede ved brud på persondatasikkerheden, i medfør af Databeskyttelsesforordningens kap. III samt artikel 34.

Databehandleren skal hjælpe den dataansvarlige med at efterleve dennes forpligtelser efter Databeskyttelsesforordningens artikel 32-36, jf. Databeskyttelsesforordningens artikel 28, stk. 3, litra f.

C.4 Opbevaringsperiode/sletterutine

Data opbevares i tre måneder, hvorefter de slettes hos databehandleren. Backup opbevares i 12 måneder, hvorefter det ligeledes slettes hos databehandleren.

Ved ophør af Aftalen skal den dataansvarlige lukke adgangen til UNI-Login jf. Bestemmelse 10.1.

C.5 Lokalitet for behandling

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

Lokation(er) for behandlingen

- a. Ordbogen A/S, Billedskærervej 8, 5230 Odense M

Underdatabehandlere

- a. Databehandleren benytter ingen underdatabehandlere

C.6 Instruks vedrørende overførsel af personoplysninger til tredjelande

Databehandleren overfører ikke persondata til tredjelande.

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

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

Databehandleren skal årligt for egen regning indhente revisionserklæring fra en uafhængig tredjepart vedrørende databehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret og disse Bestemmelser.

Der er enighed mellem parterne om, at følgende type revisionserklæring kan anvendes i overensstemmelse med disse Bestemmelser: ISAE 3000

Databehandleren er forpligtet til at give den dataansvarlige nødvendige oplysninger til, at den dataansvarlige kan sikre sig, at databehandleren overholder de krav, der følger af denne Aftale.

Den dataansvarlige, en repræsentant for den dataansvarlige eller dennes revision (såvel intern som ekstern) har adgang til at foretage inspektioner og revision hos databehandleren med henblik på at konstatere, at databehandleren overholder de krav, der følger af denne Aftale. Inspektioner og revision skal aftales forud med databehandleren med 14 dages varsel.

Databehandleren skal, efter anmodning, vederlagsfrit til den dataansvarlige fremsende en erklæring om overholdelse af denne Aftale.

C.8 Procedurer for revisioner, herunder inspektioner, med behandling af personoplysninger, som er overladt til underdatabehandlere

Databehandleren er forpligtet til at give den dataansvarlige nødvendige oplysninger til, at den dataansvarlige kan sikre sig, at underdatabehandleren overholder de krav, der følger af denne Aftale.

Databehandleren, en repræsentant for databehandleren eller dennes revision (såvel intern som ekstern) har adgang til at foretage inspektioner og revision hos underdatabehandleren, med henblik på at konstatere, at underdatabehandleren overholder de krav, der følger af denne Aftale. Inspektioner og revision skal aftales forud med underdatabehandleren med 14 dages varsel.

Databehandleren skal, efter anmodning, vederlagsfrit til den dataansvarlige fremsende en dokumentation for underdatabehandlerens overholdelse af EU-Persondataforordning i forbindelse med databehandling af personoplysninger.