

DATABEHANDLERAFTALER  
MELLEM  
INSTITUTIONER OG IT-LEVERANDØRER  
- version 1.2 af 9. april 2018 (med ændringer af GO Forlag)

## **DATABEHANDLERAFTALE**

Mellem

Haslev Privatskole  
Jens Chr. Skous Vej 3  
4690 Haslev  
CVR 45768414  
(herefter "Institutionen")

og

GO Forlag A/S  
Anker Heegaards Gade 2, 3. tv.  
1572 København V  
CVR. Nr.: 73315913  
(herefter "Leverandøren")

er der indgået nedenstående databehandleraftale (herefter "Aftalen") om  
Leverandørens behandling af personoplysninger på vegne af Institutionen:

## 1. Generelt

**1.1** Aftalen vedrører Leverandørens forpligtelse til at efterleve de sikkerhedskrav, som fremgår af Lov nr. 429 af 31/05/2000 med senere ændringer om behandling af personoplysninger (Persondataloven) § 42, jf. § 41, stk. 3-5. Kravene er beskrevet i:

- (i) Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (Sikkerhedsbekendtgørelsen).
- (ii) Vejledning nr. 37 af 02/04/2001 til bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (Sikkerhedsvejledningen).

**1.2** Den 25. maj 2018 erstattes Persondataloven af Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 (herefter Databeskyttelsesforordningen) således, at Aftalens pkt. 1.1 (i) – (ii) herefter erstattes med Databeskyttelsesforordningen.

**1.3** I Aftalen er indarbejdet de krav, som såvel Persondataloven som de kommende regler i Databeskyttelsesforordningen stiller til databehandleraftaler.

**1.4** De produkter og ydelser, som Leverandøren leverer til Institutionen fremgår af den som bilag 4 vedhæftede ydelsesbeskrivelse ("Ydelsesbeskrivelsen"), som tillige beskriver Leverandørens behandling af personoplysninger og dertil hørende ydelser. Ydelsesbeskrivelsen omfatter følgende:

- (i) En generel beskrivelse af produkterne,
- (ii) De typer af databehandling der foregår,
- (iii) Formålet med behandling,
- (iv) Typen af personoplysninger,
- (v) Lokationer hvorfra databehandlingen foretages,
- (vi) Sikkerhed og særlige sikkerhedsforanstaltninger,
- (vii) Underdatabehandlere,
- (viii) Overførsler til tredjelande og overførselsgrundlag.

Ydelsesbeskrivelsen opdateres løbende ved ændringer af de processer og vilkår hvorunder behandling af personoplysninger foregår.

**1.5** Leverandøren skal behandle personoplysninger i overensstemmelse med god databehandlingsskik, jf. de til enhver tid gældende regler og forskrifter for behandling af personoplysninger. En beskrivelse af Leverandørens behandling

af personoplysninger og sikkerhedsforanstaltningerne vedrørende behandlingen fremgår af Ydelsesbeskrivelsen (Bilag 4).

## **2. Formål**

- 2.1** Leverandøren behandler i medfør af aftale med Institutionen under en eller flere aftaler (sådanne aftaler herefter betegnet "Hovedaftalen") personoplysninger for Institutionen som dataansvarlig. Leverandørens behandlinger og formålet med behandlingerne er beskrevet i Ydelsesbeskrivelsen.

## **3. Institutionens rettigheder og forpligtelser**

- 3.1** Institutionen er dataansvarlig for de personoplysninger, som Institutionen instruerer Leverandøren om at behandle. Institutionen har ansvaret for, at de personoplysninger, som Institutionen instruerer Leverandøren om at behandle, må behandles af Leverandøren, herunder at behandlingen er nødvendig og saglig i forhold til Institutionens opgavevaretagelse.
- 3.2** Institutionen har de rettigheder og forpligtelser, som er givet en dataansvarlig i medfør af lovgivningen, jf. Aftalens pkt. 1.1 og 1.2.

## **4. Leverandørens forpligtelser**

- 4.1** Leverandøren er databehandler for de personoplysninger, som Leverandøren behandler på vegne af Institutionen, jf. pkt. 6 og bilag 3. [Leverandøren har som databehandler de forpligtelser, som er pålagt en databehandler i medfør af lovgivningen, jf. Aftalens pkt. 1.1 og 1.2.]
- 4.2** Leverandøren behandler alene de overladte personoplysninger efter instruks fra Institutionen, jf. pkt. 6, bilag 3, og alene med henblik på opfyldelse af Hovedaftalen.
- 4.3** Leverandøren skal sikre personoplysningerne via tekniske og organisatoriske sikkerhedsforanstaltninger, som beskrevet i Sikkerhedsbekendtgørelsen og Sikkerhedsvejledningen (frem til 25. maj 2018) og Databeskyttelsesforordningen (fra 25. maj 2018), jf. bilag 1 – Sikkerhed.
- 4.4** Leverandøren skal på opfordring fra Institutionen hjælpe med at opfylde Institutionens forpligtelser i forhold til den registreredes rettigheder, herunder besvarelse af anmodninger fra borgere om indsigt i egne oplysninger, udlevering af borgerens oplysninger, rettelse og sletning af oplysninger, begrænsning af behandling af borgerens oplysninger, samt Institutionens

forpligtelser i forhold til underretning af den registrerede ved sikkerhedsbrud, fra 25. maj 2018 i medfør af Databeskyttelsesforordningens kap. III samt artikel 34.

- 4.5 Leverandøren skal fra 25. maj 2018 hjælpe Institutionen med at efterleve dennes forpligtelser efter Databeskyttelsesforordningens artikel 32-36.
- 4.6 Leverandøren garanterer fra 25. maj 2018 at levere tilstrækkelig ekspertise, pålidelighed og ressourcer til at implementere passende tekniske og organisatoriske foranstaltninger sådan, at Leverandørens behandling af Institutionens personoplysninger opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.
- 4.7 Leverandøren er forpligtet til at oplyse med præcise adresseangivelser i form af by eller lignende, hvor Institutionens personoplysninger opbevares, jf. bilag 2. Leverandøren skal ajourføre oplysningerne over for Institutionen ved enhver ændring.
- 4.8 Hvis Leverandøren er etableret i en anden EU-medlemsstat, skal Leverandøren frem til 25. maj 2018 ligeledes overholde de bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den pågældende medlemsstat.

## **5. Underleverandør (underdatabehandler)**

- 5.1 Ved underdatabehandler forstås en underleverandør, til hvem Leverandøren har overladt hele eller dele af den behandling, som Leverandøren foretager på vegne af Institutionen.
- 5.2 Leverandøren må ikke uden skriftlig godkendelse fra Institutionen anvende andre underdatabehandlere end dem, der er angivet i Ydelsesbeskrivelsen til at behandle de personoplysninger, som Institutionen har overladt til Leverandøren i medfør af Hovedaftalen. Leverandøren vil ved planlagt tilføjelse eller erstatning af underdatabehandlere opdatere Ydelsesbeskrivelsen og underrette Institutionen om sådanne ændringer af Ydelsesbeskrivelsen. Institutionen kan ikke nægte at godkende tilføjelse eller udskiftning af en underdatabehandler medmindre, der foreligger en konkret saglig begrundelse herfor. Institutionens godkendelse eller eventuelle indsigelse skal meddeles Leverandøren inden 30 dage efter at Leverandøren har oplyst om en planlagt ændring af de i Ydelsesbeskrivelsen angivne databehandlere. I modsat fald kan Leverandøren anse ændringerne for godkendt. Hvis Institutionen ikke kan anerkende en underdatabehandler,

betrages Hovedaftalen som annulleret for så vidt angår det eller de produkter eller ydelser for hvilke underdatabehandleren deltager i behandlingsaktiviteter. Institutionen er dog uanset annullationen forpligtet til at betale for ydelsen frem til det tidspunkt, som Institutionen tidligst kunne have opsagt til.

- 5.3 Hvis Leverandøren overlader behandlingen af personoplysninger, som Institutionen er dataansvarlig for, til underdatabehandlere, skal Leverandøren indgå en skriftlig (under)databehandleraftale med underdatabehandleren.
- 5.4 Underdatabehandleraftalen, jf. pkt. 5.3, skal pålægge underdatabehandleren de samme databeskyttelsesforpligtelser, som Leverandøren er pålagt efter Aftalen, herunder, at underdatabehandleren fra 25. maj 2018 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.
- 5.5 Når Leverandøren overlader behandlingen af personoplysninger, som Institutionen er dataansvarlig for, til underdatabehandlere, har Leverandøren over for Institutionen ansvaret for underdatabehandlernes overholdelse af disses forpligtelser, jf. pkt. 5.3.
- 5.6 Institutionen kan til enhver tid forlange dokumentation fra Leverandøren for eksistensen og indholdet af underdatabehandleraftaler for de underdatabehandlere, som Leverandøren anvender i forbindelse med opfyldelsen af sine forpligtelser over for Institutionen.
- 5.7 Al kommunikation mellem Institutionen og underdatabehandleren sker via Leverandøren.

## **6. Instrukser**

- 6.1 Leverandørens behandling af personoplysninger på vegne af Institutionen sker udelukkende efter dokumenteret instruks, jf. bilag 3. Det er Leverandørens ansvar at sikre, at eventuelle underdatabehandlere, jf. pkt 5.3, handler i overensstemmelse med Institutionens instruks, jf. bilag 3.
- 6.2 Leverandøren giver fra 25. maj 2018 omgående besked til Institutionen, hvis en instruks efter Leverandørens vurdering er i strid med lovgivningen, jf. pkt. 1.2.

## **7. Tekniske og organisatoriske sikkerhedsforanstaltninger**

**7.1** Leverandøren skal frem til 25. maj 2018, jf. bilag 1, træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at personoplysninger:

- (i) tilintetgøres, mistes, ændres eller forringes,
- (ii) kommer til uvedkommendes kendskab eller misbruges, eller
- (iii) i øvrigt behandles i strid med lovgivningen, jf. pkt. 1.1

**7.2** Leverandøren skal fra 25. maj 2018, jf. bilag 1, iværksætte alle sikkerhedsforanstaltninger, der kræves for at sikre et passende sikkerhedsniveau.

**7.3** Leverandøren skal [mindst en gang årligt] gennemgå sine interne sikkerhedsforskrifter og retningslinjer for behandlingen af personoplysninger med henblik på at sikre, at de fornødne sikkerhedsforanstaltninger til stadighed er iagttaget, jf. pkt. 7.1 og 7.2, samt bilag 1.

**7.4** [Leverandøren samt dennes ansatte må ikke skaffe sig oplysninger, som ikke har betydning for udførelsen af den pågældendes opgaver.

**7.5** Leverandøren er forpligtet til straks at underrette Institutionen om ethvert sikkerhedsbrud vedrørende ydelser omfattet af Ydelsesbeskrivelsen uanset, om dette sker hos Leverandøren eller hos en underdatabehandler.

**7.6** Bortset fra kommunikation med myndigheder, rådgivere og leverandører, må Leverandøren ikke hverken offentligt eller til tredjeparter kommunikere om sikkerhedsbrud, uden forudgående skriftlig aftale med Institutionen om indholdet af en sådan kommunikation, medmindre Leverandøren har en retlig forpligtelse til sådan kommunikation.

## **8. Overførsler til andre lande**

**8.1** Leverandørens overførsel af personoplysninger til lande, der ikke er medlem af EU (tredjelande), f.eks. via en cloudløsning eller en underdatabehandler, skal ske i overensstemmelse med Institutionens instruks herfor, jf. bilag 3.

**8.2** Ved overførsel til tredjelande er Leverandøren ansvarlig for, at der foreligger et gyldigt overførselsgrundlag. Institutionen giver Leverandøren fuldmagt til på Institutionens vegne at indgå aftale om ovenstående overførsel af personoplysninger til tredjelande i forbindelse med Samarbejdet med henblik på at kunne etablere et overførselsgrundlag.

- 8.3** Hvis Institutionens personoplysninger overføres til en EU-medlemsstat, er det frem til 25. maj 2018 Leverandørens ansvar, at de til enhver tid gældende bestemmelser om sikkerhedsforanstaltninger, som er fastsat i lovgivningen i den pågældende medlemsstat, overholdes.

## **9. Tavshedspligt og fortrolighed**

- 9.1** Leverandøren er - under og efter Hovedaftalens ophør - pålagt fuld tavshedspligt omkring alle oplysninger, denne bliver bekendt med gennem samarbejdet. Aftalen indebærer, at tavshedspligtsbestemmelserne i straffelovens §§ 152-152f, jf. straffelovens § 152a, finder anvendelse.
- 9.2** Leverandøren skal fra 25. maj 2018 sikre, at alle, der behandler oplysninger omfattet af Aftalen, herunder ansatte, tredjeparter (f.eks. en reparatør) og underdatabehandlere, forpligter sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

## **10. Kontroller og erklæringer**

- 10.1** Leverandøren er forpligtet til at give Institutionen nødvendige oplysninger til, at Institutionen kan sikre sig, at Leverandøren overholder de krav, der følger af denne Aftale.
- 10.2** Institutionen, en repræsentant for Institutionen eller dennes revision (såvel intern som ekstern) har adgang til at foretage inspektioner og revision hos Leverandøren, med henblik på at konstatere, at Leverandøren overholder de krav, der følger af denne Aftale.
- 10.3** Leverandøren skal én gang årligt vederlagsfrit til Institutionen fremsende en erklæring, som skal udarbejdes i overensstemmelse med gældende, anerkendte branchestandarder på området. Den første erklæring skal foreligge [12] måneder efter Aftalens indgåelse.
- 10.4** I tilfælde af, at Institutionen og/eller relevante offentlige myndigheder, særligt Datatilsynet, ønsker at foretage en inspektion af de ovennævnte foranstaltninger i henhold til denne aftale, forpligter Leverandøren og Leverandørens underleverandører sig til for Institutionen at stille tid og ressourcer til rådighed herfor mod betaling i henhold til Hovedaftalen.



## **11. Ændringer i Aftalen**

- 11.1** Institutionen kan til enhver tid foreslå ændringer i Aftalen og instruksen, jf. bilag 3. Ændringsprocessen og omkostningerne aftales skriftligt mellem Institutionen og Leverandøren i Hovedaftalen. Leverandøren skal ved sådanne ændringer uden ugrundet ophold sikre, at underdatabehandlere tillige forpligtes af ændringerne.
- 11.2** I det omfang ændringer i lovgivningen, jf. pkt 1.1 og 1.2, eller tilhørende praksis, giver anledning til dette, er Institutionen med et varsel på 90 dage og uden at dette medfører krav om betaling fra Leverandøren, berettiget til at foretage ændringer i Aftalen. Omkostninger som påføres Leverandøren eller dennes underdatabehandlere i den anledning afholdes af Institutionen.

## **12. Sletning af data**

- 12.1** Institutionen træffer beslutning om, hvorvidt der skal ske sletning eller tilbagelevering af personoplysningerne efter, at behandlingen af personoplysningerne er ophørt i medfør af Hovedaftalen.
- 12.2** Institutionen skal senest 30 dage inden Hovedaftalens ophør skriftligt meddele Leverandøren, hvorvidt alle personoplysningerne skal slettes eller tilbageleveres til Institutionen. I det tilfælde, hvor personoplysningerne tilbageleveres til Institutionen, skal Leverandøren ligeledes slette eventuelle kopier. Leverandøren skal sikre, at eventuelle underdatabehandlere ligeledes efterlever Institutionens meddelelse.

## **13. Misligholdelse og tvistigheder**

- 13.1** Misligholdelse og tvistigheder er reguleret i Hovedaftalen.

## **14. Erstatning og forsikring**

- 14.1** Erstatnings- og forsikrings spørgsmål er reguleret i Hovedaftalen.

## **15. Ikrafttræden og varighed**

- 15.1** Aftalen indgås ved begge parter underskrift og løber indtil der ikke længere behandles data af Leverandøren.

## **16. Formkrav**

**16.1** Aftalen skal foreligge skriftligt, herunder elektronisk, hos Institutionen og Leverandøren.

## **Bilag 1 – Sikkerhed**

### **1. Indledning**

Dette bilag indeholder en beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger, som Leverandøren i medfør af Aftalen har ansvar for at gennemføre, overholde og sikre overholdelse af hos dennes underdatabehandlere, som er angivet i bilag 2.

### **2. Sikkerhedskrav indtil 25. maj 2018**

Leverandøren gennemfører følgende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der opfylder kravene i Sikkerhedsbekendtgørelsen og tilhørende praksis.

Foranstaltningerne gennemføres for at undgå, at personoplysninger:

- tilintetgøres, mistes, ændres eller forringes,
- kommer til uvedkommendes kendskab eller misbruges,
- eller i øvrigt behandles i strid med lovgivningen, jf. Aftalens pkt. 1.1

#### **Generelle sikkerhedsforanstaltninger**

Se Ydelsesbeskrivelsens punkt (vi).

#### **Autorisation og adgangskontrol**

Se Ydelsesbeskrivelsens punkt (vi).

#### **Inddatamateriale som indeholder personoplysninger**

Se Ydelsesbeskrivelsens punkt (vi).

#### **Uddatamateriale som indeholder personoplysninger**

Se Ydelsesbeskrivelsens punkt (vi).

#### **Eksterne kommunikationsforbindelser**

Se Ydelsesbeskrivelsens punkt (vi).

#### **Kontrol med afviste adgangsforsøg**

Se Ydelsesbeskrivelsens punkt (vi).

### **Logning**

Se Ydelsesbeskrivelsens punkt (vi).

### **Hjemmearbejdspladser**

Leverandørens behandling af personoplysninger sker helt eller delvist ved anvendelse af hjemmearbejdspladser i det omfang det følger af Ydelsesbeskrivelsen.

### **Sikkerhedskrav fra 25. maj 2018**

Leverandøren gennemfører følgende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der passer til de aftalte behandlinger, jf. Instruks (bilag 3), og som dermed opfylder Databeskyttelsesforordningens artikel 32.

Foranstaltningerne fastlægges ud fra overvejelser om:

1. Hvad der kan lade sig gøre rent teknisk
2. Implementeringsomkostningerne
3. Den pågældende behandlings karakter, omfang, sammenhæng og formål, jf. Instruksen (bilag 3)
4. Konsekvenserne for borgerne ved et sikkerhedsbrud
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

Se Ydelsesbeskrivelsens punkt (vi).

**Bilag 2 – Oplysninger om lokationer for behandling og underleverandører  
(underdatabehandlere)**

**1. Lokation(er) for behandlingen**

Se Ydelsesbeskrivelsens punkt (vii).

**2. Underdatabehandlere**

Se Ydelsesbeskrivelsens punkt (vii).

## **Bilag 3 – Instruks**

### **Instruks**

Institutionen instruerer hermed Leverandøren om at foretage behandling af Institutionens oplysninger til brug for levering af de ydelser og produkter, der fremgår af Ydelsesbeskrivelsen.

Overlader Leverandøren behandling af Institutionens oplysninger til underdatabehandlere, er Leverandøren ansvarlig for at indgå skriftlige (under)databehandleraftaler med disse, jf. Aftalens pkt 5.3.

#### **1.1 Behandlingens formål**

Behandling af Institutionens oplysninger sker i henhold til formålet i Ydelsesbeskrivelsen.

Leverandøren må ikke anvende oplysningerne til andre formål.

Oplysningerne må ikke behandles efter instruks fra andre end Institutionen.

#### **1.2 Generel beskrivelse af behandlingen**

Leverandøren forestår de typer af behandling og processer, som er nærmere beskrevet i Ydelsesbeskrivelsens punkt (ii).

#### **1.3 Typen af personoplysninger**

Behandlingerne indeholder personoplysninger som det fremgår af Ydelsesbeskrivelsens punkt (iv).

#### **1.4 Kategorier af registrerede**

Der behandles oplysninger om de kategorier af registrerede, som fremgår af Ydelsesbeskrivelsens punkt (iv).

#### **1.5 Tredjelande (ikke EU-medlemslande)**

Leverandøren må overføre personoplysninger til de tredjelande, som er angivet i Ydelsesbeskrivelsens punkt (viii).

Gyldigt overførselsgrundlag for overførslerne er:

EU-Kommissionens standardkontrakter

Privacy Shield og/eller lignende af Kommissionen godkendte andre overførselsgrundlag.

## **Bilag 4 - Ydelsesbeskrivelse**

### **1. Ydelsesbeskrivelsens indhold**

Ydelsesbeskrivelsen består af det i punkt 3 anførte.

### **2. Ændring af Ydelsesbeskrivelsen**

#### **2.1 Leverandørens ret til løbende at foretage ændringer**

Leverandøren er berettiget til løbende at ændre de enkelte elementer i Ydelsesbeskrivelsen, jf. Aftalens punkt 1.4. Leverandøren er dog ikke berettiget til ved ændring af Ydelsesbeskrivelsen at begrænse den generelle funktionalitet og indholdet af produkterne beskrevet i Ydelsesbeskrivelsen.

Leverandøren underretter Institutionen om ændringer i Ydelsesbeskrivelsen ved fremsendelse af email til den af Institutionen udpegede kontaktperson/funktion

#### **2.2 Ændringer af betydning for Instruksen**

I det omfang ændringer af Ydelsesbeskrivelsen har betydning for instruksen anses disse for at være accepteret af Institutionen, medmindre Institutionen gør indsigelse herimod.

Leverandøren skal varsles om ændringer i Ydelsesbeskrivelsen så betids, at Institutionen kan nå at gøre indsigelse mod ændringerne inden de træder i kraft, jf. nedenfor.

Institutionen kan ikke gøre indsigelse, medmindre der foreligger en konkret saglig begrundelse herfor.

Institutionens eventuelle indsigelse skal meddeles Leverandøren inden 30 dage efter at Leverandøren har oplyst om en planlagt ændring af Ydelsesbeskrivelsen. I modsat fald kan Leverandøren anse ændringerne for godkendt. Hvis Institutionen ikke kan anerkende ændringen af Ydelsesbeskrivelsen, betragtes Hovedaftalen som annulleret for så vidt angår det produkt i Ydelsesbeskrivelsen, som ændringen vedrører. Institutionen er dog uanset annullationen forpligtet til at betale for ydelsen frem til det tidspunkt, som Institutionen tidligst kunne have opsagt til.

### **3. Ydelsesbeskrivelsen**

#### **(i) En generel beskrivelse af produkterne**

1. Digitale læremidler til grundskolen. Læremidlerne opfylder alle gældende mål og læseplaner. Læremidlerne indeholder læringsforløb med mange forskellige typer opgaver: praktiske aktiviteter, prøv-selv-test med direkte feedback, adaptive test med feedback, selvrettende træningsopgaver m.m. Lærervejledning til alle forløb, oversigter til lærerne over elevernes resultater.

#### **(ii) De typer af databehandling der foregår**

1. Leverandøren anvender fire UNI-Login webservices: (ws03, ws22, ws17, ws71), som indeholder præcis de funktioner, som også anvendes i UNI-Loginservice ws02, som STIL lukker for adgang til i marts 2018.

2. Alle digitale læremidler fra Leverandøren anvender samme data gennem UNI-Login gennem:
  - ws03 (wsaLicens): Denne anvendes fx til bogholderi. Så der gennem abonnementsystemet kan sende fakturaer til institutionen efter antal elever.
  - ws17 (wsiEksport\_LILLE): Denne anvendes bl.a., så læreren kan se elevernes løste opgaver. Med denne service caches data i 24 timer, så data er hentet midlertidigt.
  - ws22 (wsilnst): Hermed gives bl.a. adgang til de rigtige navne på lærere og elever i de rigtige klasser og hold på institutionen. Hermed hentes institutionens brugeroplysninger.
  - ws71 (wsiBruger): Denne giver adgang til brugernes institutioner. Fx at en bruger er tilknyttet en folkeskole, en læreruddannelse eller måske to folkeskoler eller andre tilknytninger.

**(iii) Formålet med behandling**

1. UNI-Login er et digitalt id for elever, forældre og medarbejdere på institutioner. UNI-Login giver i Leverandørens sammenhæng adgang til brug af bestemte læremidler og bl.a. til elevernes gennemførelse af opgaver og test samt lærernes mulighed for at se elevresultaterne.
2. Da UNI-Login anvendes til styring af adgangsrettigheder - f.eks. i forbindelse med digitale opgaver i læremidlerne - er det vigtigt, at der kan ske en entydig identifikation af den pågældende bruger. UNI-Login er det offentlige autorisationssystem, der anvendes til dette formål.
3. UNI-Login anvendes til at registrere oversigter over elevaktiviteter.
4. UNI-Login anvendes til lagring af resultater af elevers arbejde med prøveforberedende materialer, test og opgaver.

**(iv) Typen af personoplysninger**

1. De oplysninger, der anvendes fra UNI-Login-systemet, er alene almindelige personoplysninger: Dvs. identifikationsoplysninger om bl.a. navn, uddannelsesoplysninger (f.eks. skole, afdeling, klasse) om elever og kontaktpersoner (f.eks. forældre eller værger) samt om medarbejdere ved institutionerne. Der behandles ikke følsomme personoplysninger med UNI-Login-systemet.
2. Derudover behandles resultater af elevers arbejde med prøveforberedende materialer, test og opgaver.

**(v) Lokationer hvorfra databehandlingen foretages**

1. Microsoft Azure datacenter i Amsterdam (West EU).
2. Microsoft Azure datacenter i Dublin (North EU).
3. GO Forlag A/S, Anker Heegaards Gade 2, 1572 København V.
4. Jansson Kommunikation A/S, Sivlandvænget 27, 5260 Odense S.
5. Schilling A/S, Baldersbækvej 24-26, 2635 Ishøj.
6. ADM2003 ApS, Baldersbækvej 24-26, 2635 Ishøj.



(vi) **Sikkerhed og særlige sikkerhedsforanstaltninger**

**1. Generelle sikkerhedsforanstaltninger**

Leverandørens produkter hostes hos Microsoft Azure. Microsoft Azure er verdens største datacenter med millioner af servere over hele verden. Sikkerhedsforanstaltningerne baserer sig herpå.

**2. Autorisation og adgangskontrol**

Leverandøren sikrer, at kun de personer, som autoriseres hertil, har adgang til de personoplysninger, der behandles. Personer, som er autoriseret til adgang, er kun de, der har et formål med adgangen.

Udviklings-, test- og driftsmiljø er isolerede i forhold til hinanden. Kun systemudviklere har adgang til udviklingsmiljøet med persondata.

Leverandøren har truffet foranstaltninger til at sikre, at kun autoriserede brugere kan få adgang til personoplysninger.

Sikkerheden baserer sig på Microsoft Azure.

**3. Inddatamateriale som indeholder personoplysninger**

Leverandøren benytter STIL's webservices og forskrifter for inddatamateriale. Leverandøren lagrer kun de persondata, der er brug for til opgaven.

**4. Uddatamateriale som indeholder personoplysninger**

Leverandøren leverer ikke uddatamateriale til andre end dataejer. Resultater fra prøver, test og opgaver samt registrerede elevaktiviteter leveres til dataejer. Log over hvem der anvender produkterne kan udleveres til dataejer.

Medarbejderne må ifølge deres aftaler ikke printe persondata eller på anden måde tage persondata ud af systemet.

**5. Eksterne kommunikationsforbindelser**

Der findes en krypteret VPN-forbindelse mellem Leverandørens lokationer og serverne hos Microsoft Azure.

**6. Kontrol med afviste adgangsforsøg**

Der findes en politik for afviste adgangsforsøg.

**7. Logning**

Leverandøren foretager logning af hvilke personer, der tilgår hvad i databaserne.

**8. Hjemmearbejdspladser**

Leverandørens behandling af personoplysninger sker delvist ved anvendelse af hjemmearbejdspladser:

Ved brug af hjemmearbejdsplads anvendes samme rutiner og adfærd som på arbejdspladsen, og som sikrer en forsvarlig behandling af data og med en tilsvarende sikkerhed.

Lokal lagring af personoplysninger sker ikke.

Lokal udskrivning af personoplysninger sker ikke.

Privat anvendelse af hjemme-pc'en er ikke tilladt.

Der anvendes Cisco Umbrella som er en overbygning på de øvrige sikkerhedssystemer med firewall, antivirus og spamfilter.

Cisco Umbrella anvendes til overvågning af sikkerhedssituationen på virksomhedens netværk. Systemet arbejder på forkanten af netværket for at stoppe trusler mod virksomhedens netværksprotokoller og IP-porte.

**(vii) Underdatabehandlere**

Microsoft Azure datacenter i Amsterdam (West EU).

Microsoft Azure datacenter i Dublin (North EU).

Jansson Kommunikation A/S, Sivlandsvænget 27, 5260 Odense S.

Schilling A/S, Baldersbækvej 24-26, 2635 Ishøj.

ADM2003 ApS, Baldersbækvej 24-26, 2635 Ishøj.

**(viii) Overførsler til tredjelande og overførselsgrundlag**

Sker ikke. Ikke relevant.

**Versionshistorik**

Versionsnr.	Dato	Beskrivelse
0.8	25.11.2016	Høringsudkast på <a href="http://www.kombit.dk">www.kombit.dk</a>
1.0	03.04.2017	Tilrettet efter bemærkninger fra høringsrunde.
1.1	02.02.2018	Ændringer indsat af GO Forlag A/S
1.2	09.04.2018	Ændringer indsat af GO Forlag A/S

For Institutionen

Dato 15/5-18

Q. G. N. R.

For Leverandøren

Dato

Tac Tran Jørgensen

**Bilag:**

Bilag 1 – Sikkerhed

Bilag 2 – Oplysninger om lokationer for behandling og underleverandører  
(underdatabehandlere)

Bilag 3 – Instruks

Bilag 4 - Ydelsesbeskrivelse