

DATABEHANDLERAFTALE

Mellem

Institution: Haslev privatskole
Adresse 1: Jens Chr. Skovs vej 3
Adresse 2:
Postnr./by: 4690 Haslev
CVR: 45768414

(herefter "Kunden")

og

Ordbogen A/S
Billedskærervej 8
5230 Odense M
CVR. nr.: 26 40 40 37
(herefter "Leverandøren")

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

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 databehandlertaaler.
- 1.4 Leverandøren skal behandle personoplysninger i overensstemmelse med god databehandlingsskik, jf. de til enhver tid gældende regler og forskrifter for behandling af personoplysninger.

2. Formål

- 2.1 Leverandøren behandler i medfør af aftale med Kunden om Adgang til Ordbogen A/S' online ordbøger og undervisningsportaler (herefter "Hovedaftalen") personoplysninger for Kunden, hvor Leverandørens behandling og formålet med behandlingerne er beskrevet.

3. Kundens rettigheder og forpligtelser

- 3.1 Kunden er dataansvarlig for de personoplysninger, som Kunden instruerer Leverandøren om at behandle.
- 3.2 Kunden 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 Kunden, jf. pkt. 6 og bilag 3.
- 4.2 Leverandøren behandler alene de overladte personoplysninger efter instruks fra Kunden, jf. pkt. 6 og bilag 3, og alene med henblik på opfyldelse af Hovedaftalen.
- 4.3 Leverandøren skal fra 25. maj 2018 løbende føre en fortegnelse over behandlingen af personoplysninger samt en fortegnelse over alle sikkerhedsbrud.
- 4.4 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.
- 4.5 Leverandøren skal på opfordring fra Kunden hjælpe med at opfylde Kundens 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 Kundens forpligtelser i forhold til underretning af den registrerede ved sikkerhedsbrud, fra 25. maj 2018 i medfør af Databeskyttelsesforordningens kap. III samt artikel 34.
- 4.6 Leverandøren skal fra 25. maj 2018 hjælpe Kunden med at efterleve dennes forpligtelser efter Databeskyttelsesforordningens artikel 32-36.
- 4.7 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 Kundens personoplysninger opfylder kravene i Databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.
- 4.8 Leverandøren er forpligtet til at oplyse med præcise adresseangivelser, hvor Kundens personoplysninger opbevares, jf. bilag 2. Leverandøren skal ajourføre oplysningerne over for Kunden ved enhver ændring.
- 4.9 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 Kunden.
- 5.2 Leverandøren har ret til at anvende andre underdatabehandlere end dem, som er angivet i bilag 2, herunder at foretage udskiftning af disse, til at behandle de personoplysninger, som Kunden har overladt til Leverandøren i medfør af Hovedaftalen. Leverandøren skal ajourføre oplysningerne om underdatabehandlere i bilag 2 ved enhver ændring.
- 5.3 Kunden kan gøre indsigelse overfor Leverandørens valg af underdatabehandler, og nægte at godkende skift eller tilføjelse af underdatabehandlere, når der foreligger en konkret saglig begrundelse herfor.
- 5.4 Hvis Leverandøren overlader behandlingen af personoplysninger, som Kunden er dataansvarlig for, til underdatabehandlere, skal Leverandøren indgå en skriftlig (under)databehandleraftale med underdatabehandleren.
- 5.5 Underdatabehandleraftalen, jf. pkt. 5.4, 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.
- 5.6 Når Leverandøren overlader behandlingen af personoplysninger, som Kunden er dataansvarlig for, til underdatabehandlere, har Leverandøren over for Kunden ansvaret for underdatabehandlerens overholdelse af disses forpligtelser, jf. pkt. 5.4.
- 5.7 Kunden 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 Kunden.
- 5.8 Al kommunikation mellem Kunden og underdatabehandleren sker via Leverandøren.

6. Instrukser

- 6.1 Leverandørens behandling af personoplysninger på vegne af Kunden sker udelukkende efter dokumenteret instruks, jf. bilag 3. Det er Leverandørens ansvar at sikre, at eventuelle underdatabehandlere, jf. pkt. 5.4, får tilsendt Kundens instruks, jf. bilag 3.

- 6.2 Leverandøren giver fra 25. maj 2018 omgående besked til Kunden, 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, jf. bilag 1, iværksætte alle sikkerhedsforanstaltninger, der kræves for at sikre et passende sikkerhedsniveau.
- 7.3 Leverandøren samt dennes ansatte er underlagt forbud mod at skaffe sig oplysninger af enhver art, som ikke har betydning for udførelsen af den pågældendes opgaver.
- 7.4 Leverandøren har pligt til at instruere de ansatte, der har adgang til eller på anden måde varetager behandling af Kundens personoplysninger, om Leverandørens forpligtelser, herunder bestemmelserne om tavshedspligt og fortrolighed, jf. pkt 9.
- 7.5 Leverandøren er forpligtet til straks at underrette Kunden om ethvert sikkerhedsbrud uanset, om dette sker hos Leverandøren eller hos en underdatabehandler.
- 7.6 Leverandøren må ikke hverken offentligt eller til tredjeparter kommunikere om sikkerhedsbrud, jf. pkt 7.5, uden forudgående skriftlig aftale med Kunden 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 Kundens instruks herfor, jf. bilag 3.
- 8.2 Hvis Kundens 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.
- 8.3 Leverandøren er forpligtet til at holde sig ajour med Tilsynsmyndighedens fortegnelse over godkendte 3. lande, samt uden unødigt ophold at give Kunden meddelelse om ændringer heri samt foretage foranstaltninger for lovliggørelse når ændringer i

fortegnelsen har betydning for Leverandørens lovlige behandling af Kundens oplysninger.

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 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 Kunden nødvendige oplysninger til, at Kunden kan sikre sig, at Leverandøren overholder de krav, der følger af denne Aftale.
- 10.2** Kunden, en repræsentant for Kunden 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. Inspektioner og revision skal aftales forud med Leverandøren.
- 10.3** Med mindre der er fastsat et hyppigere interval herfor i Hovedaftalen, skal Leverandøren én gang årligt vederlagsfrit fremsende en erklæring om overholdelse af denne Aftale til Kunden. Erklæringen skal udarbejdes i overensstemmelse med gældende, anerkendte branchestandarder på området og skal omfatte både Leverandørens og eventuelle underdatabehandlers databehandling. Den første erklæring skal foreligge senest den 25. maj 2019.
- 10.4** For Hovedaftaler, hvor der ikke tidligere har været indgået databehandlafter, skal Leverandøren vederlagsfrit fremsende en erklæring om overholdelse af denne Aftale til Kunden senest 12 måneder efter indgåelsen af Aftalen. Når denne særforpligtelse er opfyldt, bortfalder forpligtelsen i afsnit 10.4.
- 10.5** Kunden kan, efter aftale med Leverandøren, en gang årligt foretage et tilsyn om overholdelse af denne Aftale hos Leverandøren. Omfang og proces for tilsyn, herunder Leverandørens pris herfor, aftales i Hovedaftalen, sekundært i separat aftale mellem parterne, såfremt omfang og proces ikke er omfattet af Hovedaftalen. Kundens omkostninger i forbindelse med dette tilsyn afholder Kunden selv.
- 10.6** I tilfælde af, at den Dataansvarlige og/eller relevante offentlige myndigheder, særligt Datatilsynet, ønsker at foretage en uanmeldt fysisk inspektion af de ovennævnte

foranstaltninger, forpligter Databehandleren sig til at stille tid og ressourcer til rådighed herfor.

11. Ændringer i Aftalen

- 11.1** Kunden kan til enhver tid, med et forudgående varsel på 3 måneder, foretage ændringer i Aftalen og instruksen, jf. bilag 3. Ændringsprocessen og omkostningerne herved aftales skriftligt mellem Kunden og Leverandøren i Hovedaftalen, sekundært i separat skriftlig aftale mellem parterne, såfremt vilkår for ændringsprocesser og omkostninger forbundet hermed ikke er reguleret i Hovedaftalen. Leverandøren skal ved sådanne ændringer uden ugrundet ophold sikre, at underdatabehandlerne 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 Kunden berettiget til at foretage ændringer i Aftalen uden varsel, og uden at dette medfører krav om betaling fra Leverandøren.

12. Sletning af data

- 12.1** Kunden træffer beslutning om, hvorvidt der skal ske sletning eller tilbagelevering af personoplysningerne efter, at behandlingen af personoplysningerne er ophørt i medfør af Hovedaftalen.
Leverandøren skal endvidere sikre, at persondata automatisk slettes, senest efter 3 måneder, når brugere bliver inaktive eller er slettet på UNI-login. Ved sletning på UNI-login, skal leverandøren på brugerens anmodning, foretage sletningen af dennes personoplysninger i umiddelbar forlængelse af anmodningstidspunktet.
- 12.2** Kunden skal inden Hovedaftalens ophør skriftligt meddele Leverandøren, hvorvidt alle personoplysningerne skal slettes eller tilbageleveres til Kunden. I det tilfælde, hvor personoplysningerne tilbageleveres til Kunden, skal Leverandøren ligeledes slette eventuelle kopier. Leverandøren skal sikre, at eventuelle underdatabehandlere ligeledes efterlever Kundens meddelelse.
- 12.3** Leverandøren skal fremsende dokumentation for, at den påkrævede sletning, jf. pkt. 12.2, er foretaget.

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 ophør af Hovedaftalen.

16. Formkrav

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

For Kunden

Dato 15/5-2018



For Leverandøren

Dato 22-5-2018



Bilag:

Bilag 1 – Sikkerhed

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

Bilag 3 – Instruks

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

3. Sikkerhedskrav fra 25. maj 2018

Leverandøren forpligter sig til at udarbejde et særskilt bilag 1 – Sikkerhed, afsnit 3 – under hensyntagen til den løbende implementering af Databeskyttelsesforordningen, således at der foreligger et supplerende delbilag benævnt "Bilag 1 – Sikkerhed, afsnit 3.

I det supplerende delbilag redegør Leverandøren for, hvordan Leverandøren gennemfører de nødvendige 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. instruks (bilag 3)
4. Konsekvenserne for de registrerede 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

Der henvises til Ordbogens IT-sikkerhedspolitik, jf. følgende.

IT-Sikkerhedspolitik, Ordbogen A/S

Redaktør: Michael Walther, IT-Direktør

Godkendt af: Michael Walther & Peter Revsbech 2018-01-22

Version: 2.1

Indledning

Denne IT-Sikkerhedspolitik er den overordnede ramme for informations- og datasikkerhed hos Ordbogen A/S, herefter benævnet "Ordbogen". Denne politik understreger at Ordbogen 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, informationssikkerhedspolitikken op til revurdering. Minimum én gang årligt bliver sikkerhedspolitikken revurderet, så vi sikrer en løbende tilpasning til trusselsniveauet.

Formål

Informationer og databehandling er nødvendige og livsvigtige for Ordbogen, hvorfor IT-sikkerheden har vital betydning for virksomhedens troværdighed og funktionsdygtighed.

Formålet med informationssikkerhedspolitikken er, at definere en ramme for beskyttelse af virksomhedens informationer, og særligt at sikre, at kritiske og følsomme informationer og informationssystemer bevarer deres fortrolighed, integritet og tilgængelighed. Ordbogens 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 informationer og informationssystemer. 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 Ordbogens data, der tilhører virksomheden – samt data, som ikke tilhører virksomheden, men som Ordbogen er ansvarlig for. Dette inkluderer eksempelvis alle data om personale, data om kunder eller data fra 3. part som eksempelvis tjenesten UNI-LOGIN.

Denne politik er gældende for alle ansatte uden undtagelse, både fastansatte og personer, som midlertidigt arbejder for Ordbogen. Eksempelvis praktikanter eller elever. Ved udlicitering af dele af IT-driften skal det sikres i samarbejdet med underleverandøren at Ordbogens sikkerhedsniveau fastholdes således, at leverandøren som minimum lever op til Ordbogens sikkerhedsniveau – herunder EU Persondataforordningens artikel 28 og 29.

Organisering

Det er Ordbogens 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 informationssikkerhedsindsatsen, er placeret hos IT-chefen. Denne sikrer, at de aktiviteter, standarder, retningslinjer, kontroller og foranstaltninger, der er beskrevet, gennemføres og efterleves. Ligeledes er informationssikkerheden 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 Ordbogen. Der er dertil også i udviklingsprocessen indbygget kontroller på tværs af medarbejdere, for at sikre kvaliteten og sikkerheden i produkterne, for derved at undgå 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 Ordbogens sikkerhedspolitik at begrænse adgang til data for såvel udviklere som for administrative medarbejdere.

Adgang til administrationssystemer og systemer med dataadgang overvåges. Ligeledes stilles der krav til sværhedsgraden af adgangskoder, samt skift heraf minimum hver 3. måned. Ved stop af centrale medarbejdere, eksempelvis central teknikere, skiftes samtlige adgangskoder til systemerne. Ligeledes er adgangen som standard kun tilgængelig fra leverandørens 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 leverandøren har behov for det til levering af servicen. Der er gennem

de interne administrationssystemer afgrænset hvilke data medarbejdere kan tilgå, således at persondata ikke kan viderebringes eller tilgås uden specifikt formål.

Alle medarbejdere er gennem deres kontrakter pålagt tavshedspligt.

Sletning af data og backup

Persondata fjernes senest 3 måneder efter hovedaftalens ophør, Perioden sikre at evt. data ikke går tabt i forbindelse med en overgang fra en hovedaftale til en ny aftale – eksempelvis i forbindelse med en centralisering af indkøb.

Der laves backup af data døgntligt 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 overvåges døgnet rundt for utilsigtet hændelser, forsøg på indbrud eller forsøg på at kopiere data. Systemerne lukker automatisk ned ved specielle mønstre og advarer teknikkerne, som kan tage nærmere aktion i forhold til hændelsen.

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

1. Lokation(er) for behandlingen

Leverandøren ejer og driver de servere som leverer servicen til fulde. Serverne er placeret på følgende lokationer:

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

2. Underdatabehandlere

Leverandøren benytter ingen underdatabehandlere.

Bilag 3 – Instruks

Instruks

Kunden instruerer hermed Leverandøren om at foretage behandling af Kundens personoplysninger, hentet gennem adgangskontrol, via Uni-login, jf. Hovedaftale Adgang til Ordbogen A/S online ordbøger og undervisningsportaler. Overlader Leverandøren behandling af Kundens oplysninger til underdatabehandlere, er Leverandøren ansvarlig for at indgå skriftlige (under)databehandleraftaler med disse, jf. Aftalens pkt 5.4. Leverandøren er ansvarlig for, at Kundens instruks fremsendes til eventuelle underdatabehandlere.

1.1 Behandlingens formål

Behandling af Kundens oplysninger sker i henhold til formålet i Hovedaftalen.

Leverandøren må ikke anvende oplysningerne til andre formål.

Oplysningerne må ikke behandles efter instruks fra andre end Kunden.

1.2 Generel beskrivelse af behandlingen

Ordbogen A/S behandler med udgangspunkt i STILs webservices *WS22*, *WS71* og *WS17-lille* personoplysninger til brug for adgangskontrol og identifikation af brugere i deres webportaler.

1.3 Typen af personoplysninger

Behandlingerne indeholder personoplysninger i de nedenfor afkrydsede kategorier. Leverandørens og eventuelle underdatabehandlers niveau for behandlingssikkerhed bør afspejle oplysningernes følsomhed, jf. bilag 1.

Almindelige personoplysninger (indtil 25. maj 2018, jf. Persondatalovens § 6, fra 25. maj 2018, jf. Databeskyttelsesforordningens artikel 6)

☒ Almindelige personoplysninger

Følsomme personoplysninger (indtil 25. maj 2018, jf. Persondatalovens § 7, fra 25. maj 2018, jf. Databeskyttelsesforordningens artikel 9):

- ☐ Racemæssig eller etnisk baggrund
- ☐ Politisk overbevisning
- ☐ Religiøs overbevisning
- ☐ Filosofisk overbevisning
- ☐ Fagforeningsmæssige tilhørsforhold

- ☐ Helbredsforhold, herunder misbrug af medicin, narkotika, alkohol m.v.
- ☐ Seksuelle forhold

Oplysninger om enkeltpersoners rent private forhold (indtil 25. maj 2018, jf. Persondatalovens § 8, fra 25. maj 2018, jf. Databeskyttelsesforordningens artikel 6 og 9):

- ☐ Strafbare forhold
 - ☐ Væsentlige sociale problemer
 - ☐ Andre rent private forhold, som ikke er nævnt ovenfor:
-
-

Oplysninger om cpr-nummer (indtil 25. maj 2018, jf. Persondatalovens § 11, fra 25. maj 2018, eventuelt national lovgivning, jf. Databeskyttelsesforordningens artikel 87)

- ☐ CPR-numre

1.4 Kategorier af registrerede

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

- A) Elever
- B) Forældre
- C) Undervisningspersonale

1.5 Tredjelande (ikke EU-medlemslande)

Leverandøren overføre ikke personoplysninger til 3. lande.

