Bilag 4- Ydelsesbeskrivelse

1. Ydelsesbeskrivelsens indhold

Ydelsesbeskrivelsen består af dette bilag 4 med tilhørende underbilag.

2. Ændring af Ydelsesbeskrivelsen

2.1 Leverandørens ret til løbende at foretage ændringer

Leverandøren er berettiget til løbende at ændre i Ydelsesbeskrivelsen i de enkelte underbilag i, jf. Aftalens punkt 1.3. Eventuelle opdaterede underbilag til Ydelsesbeskrivelsen findes på www.linu.dk , eller kan rekvireres direkte hos Leverandøren.

Leverandøren underretter Institutionen om væsentlige ændringer i Ydelsesbeskrivelsens underbilag ved fremsendelse af e-mail til den på side to angivne e-mailadresse medmindre andet er oplyst skriftligt.

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 varsle 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 Samarbejdet 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.

Bilag 4. 1. Leverandørens egne produkter

i. Beskrivelse af selve produktet

LINU er et webbaseret Screeningsværktøj, der anvendes i forbindelse med afdækning af ordblindhed og talblindhed samt pædagogiskafdækning indenfor bl.a. dansk, engelsk og matematik.

ii. Typer af databehandling

LINU udfører som databehandler følgende behandlinger af persondata på vegne af Institutionen, der er den dataansvarlige:

1. Opbevaring af de data, som Institutionens brugere inddaterer på den platform, som brugerne har adgang til via den dataansvarliges aftaler hos LINU og LINU's underdatabehandlere.
2. Behandling af anvendelsesdata til brug for rapportering til den dataansvarlige om anvendelsen/udnyttelsen af den dataansvarliges aftaler.
3. I forbindelse med udførelse af support til brugere af LINU eller LINU's underdatabehandleres platforme behandles relevante oplysninger vedrørende brugeren, f.eks. navn, kontakt oplysninger evt. bruger-id eller oplysninger, der identificerer brugeren og den dataansvarlige, brugeren henvender sig på vegne af.

LINU henter og gemmer alene de persondata, som er nødvendige for at levere de ydelser og services, som LINU og Institutionen har indgået aftale om.

Alle personidentificerbare behandlinger, herunder effektuering af den registreredes rettigheder, vil alene blive udført efter dataansvarliges instruks.

iii. Formålet med behandling

Formålet med behandlingen er at levere de ydelser, som Institutionen har aftalt med Leverandøren, og som angivet under afsnit i) og afsnit ii).

iv. Typen af personoplysninger

Almindelige personoplysninger.

v. Kategorier af registrerede

Registrerede:

- Elever
- Lærere
- Andre ansatte/interessenter, som Institutionen måtte give adgang til LINU.

LINU gemmer udelukkende den enkelte brugers bruger-id i sammenhænge, hvor bruger-id'et fungerer som nøgle til:

- brugerens egne data, i forbindelse med screeninger.

vi. Lokationer hvorfra databehandlingen foretages

- Danmark

vii. Sikkerhed og særlige sikkerhedsforanstaltninger

a) Indledning

Dette afsnit 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, således at der skabes et sikkerhedsniveau, som passer til de aftalte behandlinger i aftalen.

b) Sikkerhedskrav

Leverandøren og/eller dennes underleverandører gennemfører følgende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, der passer til de aftalte behandlinger.

Sikkerhedsforanstaltningerne opfylder kravene både i Sikkerhedsbekendtgørelsen (bekg. nr. 528 af 15/6 2000) og tilhørende praksis og i persondataforordningens artikel 32.

Foranstaltningerne fastlægges ud fra en konkret vurdering af den risiko, der er forbundet med den/de pågældende behandling(er). Vurderingen baseres i særdeleshed på:

- Hvad der kan lade sig gøre rent teknisk
- Implementeringsomkostningerne
- Den pågældende behandlings karakter, omfang, sammenhæng og formål, jf. pkt. i-iii i dette bilag
- Konsekvenserne for registrerede ved et sikkerhedsbrud
- 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

c) Generelle sikkerhedsforanstaltninger

Leverandøren har en informationssikkerhedspolitik. Informationssikkerheds- politikken fastlægger bl.a. formål, omfang og organisering for informations- sikkerhed hos Leverandøren.

Leverandørens IT-sikkerhedsansvarlige leder det daglige arbejde med IT-sikkerheden hos Leverandøren og har ansvaret for udviklingen af Leverandørens informations sikkerheds-styringspolitik, så det imødegår de aktuelle trusselscenarier og understøtter overholdelsen af de til enhver tid gældende lovkrav.

d) Fysisk sikkerhed

Leverandørens datalokationer er underlagt fysisk adgangskontrol, og der er etableret videoovervågning

e) Kryptering

Alle data er krypterede, når de sendes over offentlige transmissionskanaler, enten via VPN-forbindelser eller via HTTPS protokollen.

f) Pseudonymisering

Kun de medarbejdere hos Leverandøren, som udfører support eller udvikling af de dele af Leverandørens ydelser, der kræver personhenførbare brugerinformationer, har adgang til disse.

g) Autorisation og adgangskontrol

Autorisation og adgangskontrol for dataansvarliges brugere og medarbejdere sker via Leverandørens adgangskontrolsystem. Adgangskontrolsystemet er underlagt Leverandørens regler og procedurer.

Leverandørens medarbejdere og underdatabehandlere

Autorisation og adgangskontrol for Leverandørens medarbejdere og underdatabehandlere sker via Leverandørens adgangskontrolsystem. Adgangskontrolsystemet er underlagt Leverandørens regler og procedurer. Autorisationer, der giver adgang til udvidede rettigheder i systemer og på platforme, er begrænset til få udvalgte medarbejdere.

h) Inddatamateriale som indeholder personoplysninger

Inddatamateriale dannes af brugerne af leverandørens ydelser via brugergrænsefladen.

i) Uddatamateriale som indeholder personoplysninger

Uddatamateriale dannes af brugerne af leverandørens ydelser via brugergrænsefladen. Dataansvarlige kan efter lovlig instruks rekvirere uddatamateriale som omfatter personoplysninger hos databehandler.

j) Eksterne kommunikationsforbindelser

Alle data er krypterede, når de sendes over offentlige transmissionskanaler, enten via VPN-forbindelser eller via HTTPS protokollen.

k) Kontrol med afviste adgangsforsøg

Leverandøren behandler ikke personoplysninger der er anmeldelsespligtige efter lov nr. 429 om behandling af personoplysninger af 31/5 2000, og er derfor ikke omfattet af kravet om kontrol med afviste adgangsforsøg efter kapitel 3 i Sikkerhedsbekendtgørelsen (bekg. nr. 528 af 15/6 2000).

l) Logning

Leverandøren behandler ikke personoplysninger der er anmeldelsespligtige efter lov nr. 429 om behandling af personoplysninger af 31/5 2000, og er derfor ikke omfattet af kravet om logning i kapitel 3 i Sikkerhedsbekendtgørelsen (bekg. nr. 528 af 15/6 2000).

m) Leverandørens behandling af personoplysninger uden for leverandørens lokationer

Leverandørens behandling af personoplysninger uden for leverandørens lokationer, sker ved at udvalgte medarbejdere og underdatabehandlere, er opkoblet via enten VPN-forbindelser eller fra fast IP-adresse med individuel to-faktor-autentifikation.

n) Tilgængelighed og robusthed

Leverandøren har sikret høj tilgængelighed og robusthed af platformene via følgende initiativer:

- Infrastrukturen er en optimal kombination af fysiske- og cloud-baserede servere designet med henblik på høj tilgængelighed.
- Infrastruktur er hostet hos anerkendte leverandører. Dette omfatter både den fysiske infrastruktur og den cloud-løsning, der understøtter ydelserne.

viii. Underdatabehandlere

Leverandører af supplerende services til LINU's løsninger:

ITEM systems
Gammel Gugvej 17 A
DK-9000 Aalborg

Infrastruktur-leverandører:

IT Center Nord
Øster Uttrup Vej 1
DK-9000 Aalborg