

Databehandlersaftale LINU

Standardkontraktsbestemmelser

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

mellem

Lærkeskolen – afd. kompetencecenter
CVR-nr.: 35410538
Præstegårdsvej 30
3660 Stenløse
Danmark

Selene Strube
Tlf. 61303824
Email selene.strube@egekom.dk

og

LINU
(HF&VUC NORD)
CVR-nr.: 29485348
På Sporet 8B, 9000 Aalborg
Danmark

herefter "databehandleren"

der hver især er "part" og sammen udgør "parterne"

har aftalt følgende standardkontraktsbestemmelse (bestemmelserne) 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.	Den dataansvarliges rettigheder og forpligtelser	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, herunder inspektion	8
12.	Parternes aftale om andre forhold	8
13.	Ikrafttræden og ophør	9
14.	Kontaktpersoner hos den dataansvarlige og databehandleren	9
	Bilag A – Oplysninger om behandlingen	11
	Bilag B – Underdatabehandlere	12
	Bilag C – Instruksvedrørende behandling af personoplysninger	13

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 LINU (screeningsværktøj) behandler databehandleren personoplysninger på vegne af den dataansvarlige i overensstemmelse med disse Bestemmelser.
4. Bestemmelserne har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne.
5. Der hører fire bilag til disse Bestemmelser, og bilagene udgør en integreret del af Bestemmelserne.
6. Bilag A indeholder nærmere oplysninger om behandlingen af personoplysninger, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.
7. Bilag B indeholder den dataansvarliges betingelser for databehandlerens brug af underdatabehandlere og en liste af underdatabehandlere, som den dataansvarlige har godkendt brugen af.
8. Bilag C indeholder den dataansvarliges instruks for så vidt angår databehandlerens behandling af personoplysninger, en beskrivelse af de sikkerhedsforanstaltninger, som databehandleren som minimum skal gennemføre, og hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.
9. Bestemmelserne med tilhørende bilag skal opbevares skriftligt, herunder elektronisk af begge parter.
10. Disse Bestemmelser frigør ikke databehandleren for 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 medlemsstaternes¹ 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 bl.a. at sikre, at der er et behandlingsgrundlag for behandlingen af personoplysninger, som databehandleren instrueres i at foretage.

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

3. Den dataansvarliges rettigheder og forpligtelser

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.
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.

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:

- Pseudonymisering og kryptering af personoplysninger
 - evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
 - evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
 - en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.
2. Efter forordningens artikel 32 skal databehandleren – uafhængig 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.

3. 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 forpligtelse efter forordningens artikel 32.

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. 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 således ikke gøre brug af en underdatabehandler til opfyldelse af disse Bestemmelser uden forudgående generel skriftlig godkendelse af den dataansvarlige.

Databehandleren har den dataansvarliges generelle godkendelse til brug af underdatabehandlere. Databehandleren skal skriftlig underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelser eller udskiftning af underdatabehandlere med mindst 14 dages varsel og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer inden brugen af de(n) omhandlede underdatabehandler(e). Længere varsel for underretning i forbindelse med specifikke behandlingsaktiviteter kan angives i bilag B. Listen over underdatabehandlere, som den dataansvarlige allerede er bekendt med, fremgår af bilag B.

3. Når databehandleren gør brug af en underdatabehandler i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, skal databehandleren, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der fremgår af disse Bestemmelser, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen overholder kravene i disse Bestemmelser og databeskyttelsesforordningen.

Databehandleren er derfor ansvarlig for at kræve, at underdatabehandleren som minimum overholder databehandlerens forpligtelser efter disse Bestemmelser og databeskyttelsesforordningen.

4. Underdatabehandleraftale(r) og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom – i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at tilsvarende databeskyttelsesforpligtelser som følger af disse Bestemmelser er pålagt underdatabehandleren. Bestemmelser om kommercielle vilkår, som ikke påvirker det databeskyttelsesretlige indhold i underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.
5. Databehandleren skal i sin aftale med underdatabehandleren indføre den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandlere, som f.eks. gør den dataansvarlige i stand til at instruere underdatabehandleren i at slette eller tilbagelevere personoplysningerne.

6. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette påvirker ikke de registreredes rettigheder, der følger af databeskyttelsesforordningen, herunder særligt forordningens artikel 79 og 82 over for den dataansvarlige og databehandleren, herunder underdatabehandleren.

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 over 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 pågældende 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 overholdelse 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 6.3 bistår databehandleren desuden 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, medmindre det er usandsynligt, at bruddet på persondatasikkerheden indebærer risiko for fysiske personers rettigheder eller frihedsrettigheder.
 - b) den dataforpligtelse 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 til forud for behandlingen at analysere de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger (en konsekvensanalyse)
 - d) den dataansvarliges forpligtelse til at høre den kompetente tilsynsmyndighed, Datatilsynet inden behandling, hvis en konsekvensanalyse 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 nødvendige, tekniske og organisatoriske foranstaltninger, hvorved 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.
2. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 48 timer efter, at denne er blevet bekendt med bruddet, så 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.
4. Parterne skal i bilag C angive den information, som databehandleren skal tilvejebringe i forbindelse med sin bistand til den dataansvarlige i dennes forpligtelse til at anmelde brud på persondatasikkerheden til den kompetente tilsynsmyndighed.

10. Sletning og returnering af oplysninger

1. Ved ophør af tjenesterne vedrørende behandling af personoplysninger er databehandleren forpligtet til at slette alle personoplysninger, der er blevet behandlet på vegne af den dataansvarlige og bekræfte over for den dataansvarlige, at oplysningerne er slettet, medmindre EU-retten eller medlemsstaternes nationale ret foreskriver opbevaring af personoplysningerne. Se i øvrigt pkt. C.4 for opbevaringsperiode samt sletterutine.

Databehandleren forpligter sig alene til at behandle personoplysningerne til de(t) formål, i den periode og under de betingelser, som disse regler foreskriver.

11. Revision, herunder inspektion

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. Procedurerne for den dataansvarliges revisioner, herunder inspektioner med databehandleren og underdatabehandlere er nærmere angivet i bilag C.7. og C.8.
3. Databehandleren er forpligtet til at give tilsynsmyndigheder, som efter gældende lovgivninger 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 mod 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 personoplysningerne er slettet eller returneret til den dataansvarlige i overensstemmelse med Bestemmelse 10.1 og bilag C.4., kan Bestemmelserne opsiges med skriftligt varsel af begge parter.
5. Underskrift

På vegne af den dataansvarlige

Navn:
Stilling:
Telefonnummer:
E-mail:
Dato:
Underskrift:

På vegne af databehandleren

Navn:	Mette Flohr
Stilling:	Forstander
Telefonnummer:	+45 21187808
E-mail:	mrc@hfvucnord.dk
Dato:	
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.

Navn:
Stilling:
Telefonnummer:
E-mail:

Navn: Anders Bruhn Larsen
Stilling: IT-supporter
Telefonnummer: +45 21186420
E-mail: abl@hfvucnord.dk

Bilag A – Oplysninger om behandlingen

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

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

Databehandleren skal understøtte den dataansvarlige i brugen af LINU som et screeningsværktøj.

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

Databehandleren foretager support efter behov fra dataansvarlige samt hosting af personoplysninger, som genereres via test samt login i LINU.

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

Der behandles almindelige personoplysninger efter databeskyttelsesforordningen artikel 6.

- Fødselsår, for- og efternavn, postnummer og by, uddannelsesniveau, dansk modersmål eller ej, login-oplysninger.

Der behandles følsomme personoplysninger efter databeskyttelsesforordningens artikel 9.

- Helbredsoplysninger i form af testresultater, idet en læsevejleder vil kunne identificere ordblindhed herudfra.

A.4. Behandlingen omfatter følgende kategorier af registrerede

De registrerede i LINU er elever og medarbejdere.

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

Behandlingen er ikke tidsbegrænset og varer ind til aftalen opsiges eller ophæves af en af parterne.

Bilag B – Underdatabehandlere

B.1. Godkendte underdatabehandlere

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

NAVN	CVR	ADRESSE	BESKRIVELSE AF BEHANDLING
It Center Nord	46994051	Øster Uttrup Vej 1, 9000 Aalborg	Hosting

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

Hvis databehandleren ikke har modtaget svar (i form af en godkendelse eller indsigelse) indenfor 14 dage fra varslingens afsendelse, anses det som en accept af ændringen for brug af underdatabehandlere.

Bilag C – Instruksvedrørende behandling af personoplysninger

C.1. Behandlingens genstand / instruks

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

Stiller en webløsning til rådighed, hvor personoplysninger lagres i systemet. Der udføres support i forbindelse med løsning af udfordringer i LINU.

C.2. Behandlingssikkerhed

Sikkerhedsniveauet skal afspejle et passende sikkerhedsniveau set i forhold til mængden og typen af personoplysninger.

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.

Behandlingen omfatter en middel mængde personoplysninger omfattet af databeskyttelsesforordningens artikel 6 og artikel 9, hvorfor der skal etableres et passende højt sikkerhedsniveau.

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

Antivirus og firewall: Til beskyttelse mod virus og anden malware findes en procedure, der sikrer, at der installeres antivirus og firewall på alle domæne computere. Proceduren er automatisk, og der kan ikke kobles på HF&VUC NORDs domæne, medmindre der er installeret antivirus og firewall, og disse er aktive.

For yderligere at beskytte persondata er det sikret, at der altid er en opdateret firewall installeret. Firewall'en beskytter mod indtrængen i både databehandlerens og underdatabehandlerens netværk udefra.

Brugeradministration: Brugeradministration i LINU er administreret af centrale IT-medarbejdere hos HF&VUC NORD. Der udføres kun oprettelse og nedlæggelse af brugere efter henvendelse fra den dataansvarlige.

Oprettelse og nedlæggelse sker efter fastlagte procedurer aftalt med den enkelte dataansvarlige, som beskrevet ovenfor.

Overvågning og logning: Underdatabehandleren, IT Center Nord kan foretage logning og overvåge i de tilfælde, hvor det findes nødvendigt.

Logovervågning har det formål at identificere, når noget unormalt sker på de enheder, som er omfattet af overvågningen. Det kan være virus, malware, forkerte opsætninger, tegn på hacking m.m. Dette gøres ved at indsamle og overvåge relevante sikkerhedslogs for der igennem at kunne alarmere på hændelser.

Det er udelukkende logs med relevante informationer om sikkerhed på enheden, som behandles.

Proces for "alarm":

- En potentiel sikkerhedshændelse sker på en enhed.
- Sikkerhedslog genereres og fremsendes til overvågningssystemet, hvor den sammenholdes med prædefinerede regler.
- Konflikt med regel resulterer i, at der automatisk sendes en notifikation til IT Center Nord-support.

- Her vil der blive analyseret på, hvorfor alarmen er gået, og hvorvidt der er tale om en falsk alarm, eller om årsagen skal undersøges nærmere.
- Hvis der er tale om en reel sikkerhedshændelse, vil IT Center Nord-support håndtere denne.

Løsningen sikrer, at sikkerhedshændelser identificeres og håndteres, således IT-sikkerheden øges.

Databehandleren skal angive en begrundelse for persondataadgangen i tilfælde af, at databehandleren har brug for at tilgå den dataansvarliges personoplysninger.

Sårbarhedsscanninger, change management og backup: Der foretages ugentlige og kvartalsvise sårbarhedsscanninger. Opdateringer og rettelser implementeres løbende.

På Windows-serverplatformen anvendes opdateringer fra Windows Update. De hentes direkte fra Microsoft og installeres automatisk, således systemet altid er helt opdateret.
På Windows arbejdsstationsplatformen anvendes opdateringer fra lokal SCCM og WSUS-server.

Inden større systemændringer kontrolleres det, at der forefindes en tidssvarende backup, således der kan vendes tilbage til fungerende tilstand, skulle opdateringen indfører fejl på systemet.
Der er redundante forbindelser.

Kryptering: Websites er https-krypteret og har derfor et SSL-certifikat.
Alle HF&VUC NORDs medarbejderes computere er krypteret.

To-faktor-godkendelse: Der er hos HF&VUC NORDs medarbejdere indført to-faktor-godkendelse til de systemer og de enheder, hvor det er muligt.

Fysisk adgang: Adgang til serverrum er begrænset til autoriserede medarbejdere hos underdatabehandleren, IT Center Nord. Adgangen nedlægges, når medarbejdere fratræder og afleverer deres nøgler og adgangskort, så der ikke længere kan opnås fysisk adgang til bygningerne.

Organisatoriske sikkerhedsforanstaltninger: Alle databehandlerens medarbejdere følger et awareness-program, som gennemgår både IT-sikkerhed og GDPR-relaterede spørgsmål, og der følges op på, hvorvidt de enkelte medarbejdere har fuldført sessionerne.

HF&VUC NORDs medarbejdere skal med passende intervaller skifte adgangskoder på computer m.m. Medarbejderne er alle underlagt tavshedspligt, som de har underskrevet i forbindelse med deres ansættelse ved databehandleren.

Anvendelse af hjemme- og fjernarbejdspladser: Der anvendes VPN-forbindelse, når medarbejdere gør brug af hjemme- og fjernarbejdspladser.

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:

I tilfælde af at dataansvarlige og / eller relevante offentlige myndigheder, særligt Datatilsynet ønsker at inspicere de ovennævnte foranstaltninger i henhold til denne aftale, forpligter databehandleren og dennes underdatabehandlere sig til at stille tid og ressourcer til rådighed her for i rimeligt omfang.

Dog forbeholder databehandleren sig ret til at fakturere dataansvarlige på egne og underdatabehandleres vegne for dokumenteret forbrugt tid, som relaterer sig til opgaver opstået som følge af den dataansvarliges selvfor skyldte hændelser. Timesatsen i disse selvfor skyldte tilfælde følger af underleverandørers gældende timesatser.

Hvis tilsynet udspringer af et brud hos databehandleren eller underdatabehandlere, er tilsynet og bistanden vederlagsfrit.

C.4. Opbevaringsperiode / sletterutine

Den dataansvarlige vælger ved oprettelsen af den enkelte screening, i hvilket tidsinterval screeningsdata skal gemmes. Den dataansvarlige har valgmulighed mellem opbevaring i 3, 6 eller 12 måneder, hvor efter alt screeningsdata slettes. Som standard sættes 12 måneders opbevaringsperiode.

Ved ophør af tjenesten vedrørende behandling af personoplysninger skal databehandleren slette personoplysningerne i overensstemmelse med Bestemmelse 10.1., med mindre den dataansvarlige – efter underskriften af disse Bestemmelser – har ændret den dataansvarliges oprindelige valg. Sådanne ændringer skal være dokumenteret og opbevares skriftligt, herunder elektronisk i tilknytning til Bestemmelserne.

C.5. Lokaltet for behandling

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

HF&VUC NORD, På Sporet 8B, 9000 Aalborg

IT Center Nord, Øster Uttrup Vej 1, 9000 Aalborg

ITEM (ITEM SYSTEMS), Gammel Gugvej 17A, 9000 Aalborg

- Second level support. Der gives kun adgang i de tilfælde, hvor det er nødvendigt af hensyn til den enkelte dataansvarliges avancerede supportbehov. Forholdet er reguleret i en fortroligheds-erklæring.

C.6. Instruks vedrørende overførsel af personoplysninger til tredjelande

Der overføres ikke personoplysninger 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 stiller via sin underdatabehandler en ISAE 3402 erklæring til rådighed årligt fra en uafhængig tredjepart vedrørende databehandlerens overholdelse af de tekniske forhold reguleret i databeskyttelsesforordningen.

Databehandleren stiller sig her ud over til rådighed for generel dialog om kontrol af databehandlingens forskellige aspekter.

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

Der er enighed mellem parterne om, at følgende typer af ISAE 3402 og ISAE 3000 erklæringer kan anvendes i overensstemmelse med disse Bestemmelser.

Databehandleren skal årligt indhente en ISAE 3402 samt ISAE 3000 revisionserklæring fra en uafhængig tredjepart vedrørende underdatabehandlerens overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret samt disse Bestemmelser.

ISAE-erklæringerne fremsendes af underdatabehandleren uden unødigt forsinkelse til databehandleren. Databehandleren kan anfægte rammerne for og / eller metoden i erklæringerne, og databehandleren kan i sådanne tilfælde anmode om en ny erklæring under andre rammer og / eller under anvendelse af en anden metode.

Baseret på resultaterne af erklæringerne er databehandleren berettiget til at anmode om gennemførelse af yderligere foranstaltninger med henblik på at sikre overholdelse af databeskyttelsesforordningen, databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret samt disse Bestemmelser.

Databehandleren eller en repræsentant for databehandleren har herudover adgang til at foretage inspektioner, herunder fysiske inspektioner med lokaliteterne, hvor fra underdatabehandleren foretager behandling af personoplysninger, herunder fysiske lokaliteter og systemer, der benyttes til eller i forbindelse med behandlingen. Sådanne inspektioner kan gennemføres, når databehandleren finder det nødvendigt.