Deloitte
Statsautoriseret
Revisionspartnerselskab
CVR-nr.: 33 96 35 56
Weidekampsgade 6
2300 København S

Telefon: 36102030
www.deloitte.dk

Styrelsen for IT og Læring

Uafhængig revisors ISAE 3000-erklæring, type 2, med sikkerhed om informationssikkerhed og foranstaltninger rettet mod databeskyttelse og behandling af personoplysninger i henhold til cirkulæreskrivelsen og databehandleraftalen med STIL's 'kunder', Sektoren (statslige institutioner, privat- og offentligt selvejende institutioner, private institutioner, kommuner og regioner), herefter kaldet 'Sektoren', vedrørende udvalgte systemer.

Erklæringen omfatter perioden 1. januar 2023 til 31. december 2023

Indholdsfortegnelse

1. Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger rettet mod databeskyttelse og behandling af personoplysninger i henhold til databehandleraftale, cirkulæreskrivelse og bekendtgørelse.

Til: Styrelsen for IT og Læring og Sektoren, som anvender udvalgte systemer indeholdt i erklæringen.

Omfang

Vi har fået til opgave at afgive erklæring om Styrelsen for IT og Lærings (herefter "STIL") beskrivelse i afsnit 3 af STIL's systemer i henhold til databehandleraftale, cirkulæreskrivelse og bekendtgørelse med Sektoren, der anvender STIL's systemer i perioden 1. januar 2023 til 31. december 2023 (beskrivelsen) samt om udformningen og funktionaliteten af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Denne erklæring er udarbejdet efter partielmetoden og omfatter således ikke kontroller hos underleverandører. Statens It (SIT) leverer infrastrukturen til STIL's datacentre og er derfor også medtaget som underdatabehandler. STIL anvender underleverandørerne opstillet neden for:

System	**Underdatabehandler - udvikling**	**Underdatabehandler – drift og vedligehold**
EASY P	Intern	Housing hos SIT
EDUP (ElevDataUdvekslingsPunkt)	Netcompany	Housing hos SIT
KOT-systemet	Miracle A/S, Netcompany	Housing hos SIT
Lærepladsen.dk	Intern	Housing hos SIT
Netprøver.dk	Netcompany	Hostes eksternt: Amazon Cloud
Optagelse.dk (Optagelse FTU, samt den del af Elevfordelingen, der foregår i Optagelse.dk)	Miracle A/S	Housing hos SIT
Optagelse,dk (Optagelse KOT)	Miracle A/S, Netcompany	Housing hos SIT
Ordblindetesten	Netcompany	Housing hos SIT
Sprogprøver	Intern	Housing hos SIT
Sprogvurdering	Intern	Housing hos SIT
Testafvikler	Netcompany	Housing hos SIT
Ungedatabasen	Netcompany	Housing hos SIT

STIL's systembeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos underleverandørerne. Nærværende erklæring omfatter således ikke kontroltest af kontroller hos disse underleverandører.

Nogle af de kontrolmål, der er anført i STIL's beskrivelse af sine systemer, kan kun nås, hvis de komplementerende kontroller hos Sektoren (kunderne) er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos STIL. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementerende kontroller.

Styrelsen for IT og Lærings ansvar

STIL er ansvarlig for udarbejdelsen af beskrivelsen og den tilhørende udtalelse i afsnit 2, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret, for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene og for at udforme og implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i IESBA's etiske regler, som er baseret på grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd.

Deloitte anvender International Standard on Quality Management 1, ISQM 1, som kræver, at vi designer, implementerer og driver et kvalitetsstyringssystem, herunder politikker eller procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om STIL's beskrivelse samt om udformningen og funktionaliteten af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000, Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger og yderligere krav ifølge dansk revisorlovgivning, med henblik på at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i STIL's beskrivelse af STIL's systemer samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af udformning og funktionaliteten af de kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået.

En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte mål samt egnetheden af de kriterier, som STIL har specificeret og beskrevet i afsnit 2.

Det er vores opfattelse, at det opnåede bevis er tilstrækkeligt og egnet til at danne grundlag for vores konklusion.

Begrænsninger i kontroller hos en dataansvarlig

STIL's beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved STIL's systemer, som hver enkelt dataansvarlig måtte anse for vigtige efter deres særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden. Herudover er fremskrivning af enhver vurdering af implementering til fremtidige perioder undergivet risikoen for, at kontroller hos en databehandler kan blive utilstrækkelige eller svigte.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i ledelsens udtalelse. Det er vores opfattelse:

(a) at beskrivelsen af STIL's systemer, således som disse var udformet og implementeret i hele perioden fra 1. januar 2023 til 31. december 2023, i alle væsentlige henseender er retvisende
(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 1. januar 2023 til 31. december 2023

(c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene, i beskrivelsen, blev nået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. januar 2023 til 31. december 2023.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultatet af disse test fremgår af afsnit 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller, som fremgår af afsnit 4, er udelukkende tiltænkt de dataansvarlige, der har anvendt STIL's systemer, og som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af om kravene i databeskyttelsesforordningen er overholdt.

København, den 21. juni 2024

Deloitte
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 96 35 56

Thomas Kühn
partner, statsautoriseret revisor

2. Ledelsens udtalelse

Medfølgende beskrivelse er udarbejdet til brug for de dataansvarlige, der anvender STIL's systemer, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af om kravene i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesforordningen") er overholdt.

STIL bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en retvisende beskrivelse af STIL's systemer, der har behandlet personoplysninger for dataansvarlige, der er omfattet af databeskyttelsesforordningen, i hele perioden fra 1. januar 2023 til 31. december 2023. De kriterier, der er anvendt for at give denne udtalelse, var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan STIL's systemer var udformet og implementeret, herunder redegør for:

   - De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger
   - De processer i både it- og manuelle systemer, der er anvendt til at igangsætte og registrere behandling af personoplysninger og om nødvendigt korrigere eller slette personoplysninger og begrænse behandling af personoplysninger
   - De processer, der er anvendt til at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige
   - De processer, der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt
   - De processer, der ved ophør af databehandling sikrer, at der efter den dataansvarliges valg sker sletning eller tilbagelevering af alle personoplysninger til den dataansvarlige, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne
   - De processer, der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underretning til de registrerede
   - De processer, der sikrer passende tekniske og organisatoriske sikkerhedsforanstaltninger for behandlingen af personoplysninger under hensyntagen til de risici, som behandlingen udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet
   - Kontroller, som vi med henvisning til systemernes afgrænsning har forudsat ville være implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen
   - Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger.

   (ii) Indeholder relevante oplysninger om ændringer ved STIL's systemer til behandling af personoplysninger foretaget i perioden fra 1. januar 2023 til 31. december 2023

   (iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne systemer til behandling af personoplysninger, under hensyntagen til at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og derfor ikke kan omfatte ethvert aspekt ved STIL's virke, som den enkelte dataansvarlige måtte anse for vigtigt efter dennes særlige forhold

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 1. januar 2023 til 31. december 2023.

De kriterier, der er anvendt for at give denne udtalelse, var, at:

(i) De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret

(ii) De identificerede kontroller ville, hvis udført som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål

(iii) kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. januar 2023 til 31. december 2023

c) Der er etableret og opretholdt passende tekniske og organisatoriske foranstaltninger med henblik på at opfylde aftalerne med de dataansvarlige, god databehandlerskik og relevante krav til databehandler i henhold til databeskyttelsesforordningen.

København, den 21. juni 2024

På vegne af Styrelsen for IT og Læring

Stine Hegelund Bertelsen
direktør

3. Systembeskrivelse

Denne erklæring omfatter tolv it-systemer, hvor STIL er databehandler på vegne af Sektoren (statslige institutioner, privat- og offentligt selvejende institutioner, private institutioner, kommuner og regioner). Erklæringen omfatter følgende it-systemer:

- EASY-P
- EDUP (ElevDataUdvekslingsPunkt)
- KOT-systemet (Den Koordinerede Tilmelding)
- Lærepladsen.dk
- Netprøver.dk
- Optagelse.dk (Optagelse FTU samt den del af Elevfordelingen, der foregår i Optagelse.dk)
- Optagelse.dk (Optagelse KOT)
- Ordblindetesten
- Sprogprøver.dk
- Sprogvurdering
- Testafvikler
- Ungedatabasen.

Formålet med STIL's (databehandlerens) behandling af personoplysninger på vegne af den dataansvarlige og karakteren af databehandlingen beskrives system for system under afsnit 3.2

Forholdet mellem STIL som databehandler og institutioner, kommuner og regioner som dataansvarlige er reguleret i cirkulæreskrivelse: Cirkulæreskrivelse om Styrelsen for It og Lærings opgaver som databehandler i visse administrative systemer på børne- og undervisningsområdet (CIS nr. 9074 af 07/02/2023)

Herudover er forholdet reguleret af:
- Elevfordeling: Bekendtgørelse om elevfordeling, transporttid og optagelse på de gymnasiale uddannelser (BEK nr. 187 af 27/02/2023)
- KOT-systemet og Optagelse KOT: Her er der indgået en databehandleraftale med Uddannelses- og Forskningsministeriet (UFM)
- Ungedatabasen: Bekendtgørelse om opgaver og ansvar for behandlingen af personoplysninger i det fælles datagrundlag for unges uddannelse og beskæftigelse (BEK nr. 1104 af 08/11/2019)

3.1 Ydelsesbeskrivelse

STIL fremmer den digitale udvikling på undervisningsområdet og udfører opgaver inden for de overordnede målsætninger på ministeriets område. STIL's hovedopgaver er som følger

- STIL understøtter digitalisering på børne- og undervisningsområdet
- STIL udvikler, vedligeholder, drifter og supporterer Børne- og Undervisningsministeriets it-systemer
- STIL indsamler, bearbejder, udstiller og anvender data på børne- og undervisningsområdet
- STIL varetager arbejdet med it-sikkerhed og databeskyttelse internt i Børne- og Undervisningsministeriet og over for Sektoren.

På børne- og undervisningsområdet stiller STIL en række it-systemer til rådighed for sektorens behandling af personoplysninger. STIL er databehandler for den behandling, som sker ved brug af de anførte systemer, da styrelsens behandling af personoplysninger i disse systemer alene sker til sektorens formål og på deres vegne, hvorved de er dataansvarlige for behandlingen af oplysningerne.

STIL's organisationsdiagram:

3.2 Karakteren af behandling og personoplysninger

3.2.1 Behandlingen af personoplysninger i EASY-P

Formål
EASY-P er et administrativt system, der bruges af erhvervsskoler og faglige udvalgs sekretariater til administration af godkendelser af læresteder, uddannelsesaftaler, skoleoplæring, praktik i udlandet, lærepladssøgende samt svendeprøver. EASY-P er under udfasning i takt med, at flere centrale it-funktioner på lærepladsområdet samles på Lærepladsen.dk.

Samtlige lærepladsforhold er således flyttet fra EASY-P til Lærepladsen.dk. Indtil lukningen af EASY-P vil de lærepladsforhold, der er oprettet i EASY-P, være passiverede, men oplysningerne vil fortsat være tilgængelige for brugerne.

EASY-P nedlukkes løbende, hvor den første store del lukkede i 1. kvartal 2023. Lærepladsen.dk, der lige nu sameksisterer med EASY-P, afløser løbende EASY-P. EASY-P forventes lukket helt i 2024.

I EASY-P behandles følgende personoplysninger
- Navn, adresse og kontaktoplysninger
- CPR-nummer
- Praktik- og uddannelsesoplysninger – herunder godkendelser, aftaletype, aftale-id, oplysninger om lærested, afslutningsårsag.

Dataansvarlig myndighed
Uddannelsesinstitutioner og faglige udvalg

Databehandler
Styrelsen for It og Læring

STIL's underdatabehandler - udvikling
Ingen – STIL udvikler selv systemet.

STIL's underdatabehandler – drift, vedligehold
Statens It (SIT) leverer infrastrukturen til STIL's datacentre og er derfor også at betragte som en underdatabehandler. Herudover drifter STIL selv systemet.

Kategorier af registrerede brugere, der har adgang til at behandle data i systemet
- Medarbejdere på skoler og repræsentanter for faglige udvalgs sekretariater har adgang til at behandle og indtaste oplysninger.

Opbevaring af persondata
Personoplysninger i EASY-P slettes ikke af hensyn til sikring af dokumentation for uddannelsesaftaler og uddannelsesbevis. Søgninger slettes og brugerkoder passiveres, hvis de ikke har været brugt i et år.

3.2.2 Behandlingen af personoplysninger i EDUP (ElevDataUdvekslingsPunkt)

Formål
EDUP er et beskedudvekslingssystem til brug for sektorens uddannelsesinstitutioner i forbindelse med deres håndtering af den tværgående uddannelsesadministration. EDUP muliggøre udveksling af data på tværs af uddannelsesinstitutioner – herunder også på tværs af studieadministrative systemer.

STIL's persondatabehandling består i at tage imod beskeder, opbevare disse, samt sikre at disse alene kan afhentes af beskedens retmæssige modtager.

Beskedudvekslingen sker asynkront og løst koblet mellem uddannelsesinstitutionernes studieadministrative systemer, hvilket gør det muligt for uddannelsesinstitutionerne at hente og sende data på eget initiativ.

Kommunikation til og fra EDUP sker udelukkende ved brug af webservicekald via STIL's integrationsplatform.

De administrative opgaver, som EDUP understøtter, udføres af medarbejdere på de enkelte uddannelsesinstitutioner. Den uddannelsesinstitution, der indlæser en personoplysning i dens studieadministrative system, som herefter transmitteres til EDUP, er derfor dataansvarlig for denne personoplysning. EDUP understøtter udveksling af data på følgende områder:

- Elevflytning, dvs. når en elev flytter fra en institution til en anden.
- Elevudlån, dvs. når en elev tager dele af sin uddannelse på en anden institution.
- Elevdeling, dvs. når en elev får undervisning på to forskellige institutioner ifm. uddannelsen, fx når erhvervsuddannelseselever har gymnasiale fag, der gennemføres på et nærliggende teknisk gymnasium.
- Booking af skolehjem, dvs. booking af skolehjemsværelse for erhvervsuddannelseselever der bor langt fra deres uddannelsesinstitution.
- AMU-udlån, dvs. når en institution udlåner en AMU-godkendelse til en anden institution og herefter skal udveksle data til brug for indberetning af tilskudsudløsende aktiviteter.

Dataansvarlig myndighed
Uddannelsesinstitutioner

Databehandler
Styrelsen for It og Læring

STIL's underdatabehandler - udvikling
Netcompany

STIL's underdatabehandler – drift, vedligehold
Statens It (SIT) leverer infrastrukturen til STIL's datacentre og er derfor også at betragte som en underdatabehandler. Herudover drifter STIL selv systemet.

I EDUP behandles følgende personoplysninger
- Navn, adresse og kontaktoplysninger
- CPR-nummer
- Værge
- Elevens resultater og undervisningsforløb.

Kategorier af registrerede brugere, der har adgang til at behandle data i systemet
- Data udstilles og behandles via uddannelsesinstitutionernes studieadministrative systemer. EDUP udstiller ingen brugergrænseflade, men tilbyder udelukkende kommunikation via webservicekald.

Opbevaring af persondata
Personoplysninger i EASY P vises på EDUP. Disse data slettes ikke af hensyn til sikring af dokumentation for uddannelsesaftaler og uddannelsesbevis. Søgninger slettes, og brugerkoder passiveres, hvis de ikke har været brugt i et år.

Af hensyn til uddannelsesinstitutionernes udtrædelse af EASY-A og overgang til nye studieadministrative systemer, slettes data ikke i EDUP for nuværende.

3.2.4 Behandlingen af personoplysninger i KOT-systemet (Den Koordinerede Tilmelding)

Formål
KOT-systemet anvendes med det hovedformål at understøtte fordelingen af studiepladser på landets videregående uddannelser. Fordelingen af studiepladserne foregår i en såkaldt clearing, der på baggrund af indberetninger fra uddannelsesinstitutionerne og ansøgernes prioriteringslister finder frem til, hvilke ansøgere der får tildelt en plads på de enkelte uddannelser. Som led i denne fordeling af studiepladser har systemet desuden mulighed for en række manuelle og automatiske kontrolfunktioner. Derudover kan der på baggrund af data i KOT-systemet udtrækkes diverse statistikker til at fordele pladserne på de

videregående uddannelser efter ansøgningsfristen er udløbet (clearing). Sekundært trækkes statistikker over fordelingen af uddannelsespladser mv på de videregående uddannelser.

Der er også mulighed for at oprette nye ansøgninger i modulet, hvorfor det kan håndtere data fra både Optagelse.dk og fra andre datakilder, eksempelvis manuel indtastning.

Selve clearing-processen i KOT-systemet sikrer, at ansøgerne får tildelt en studieplads med det højest mulige prioriteringsønske, under hensyntagen til adgangskrav og antal pladser på de enkelte uddannelser.

Clearing-processen indgår som en del af en samlet optagelsesproces, der spænder fra, at ansøgerne på Optagelse.dk påbegynder en ansøgning til en videregående uddannelse, til de modtager et tilbud fra en videregående uddannelsesinstitution om optagelse eller et afslag fra Den Koordinerede Tilmelding. Da de opgaver, den koordinerede tilmelding udfører i KOT-systemet, ligger i umiddelbar forlængelse af processerne i KOT-delen af Optagelse.dk, har Uddannelses- og Forskningsministeriet bedt STIL om at bistå med drift og udvikling af KOT-systemet.

Dataansvarlig myndighed
Uddannelses- og Forskningsministeriet ved Uddannelses- og forskningsstyrelsen (UFS)

Databehandler
Styrelsen for It og Læring (STIL)

STIL's underdatabehandler - udvikling
Miracle (ejet af Knowit) med dennes underdatabehandlere og Netcompany

STIL's underdatabehandler – drift, vedligehold
Statens It (SIT) leverer infrastrukturen til STIL's datacentre og er derfor også at betragte som en underdatabehandler. Herudover drifter STIL selv systemet.

I KOT-systemet behandles følgende personoplysninger
- Navn, kontaktoplysninger
- Personnummer
- Adgangsgrundlag
- Beviser
- Uddannelsesønsker, prioritering af uddannelsesønsker
- Institutionens vurdering af ansøgers optagelsesberettigelse
- Resultat af styrelsens koordination af ansøgningerne.

Kategorier af registrerede brugere, der har adgang til at behandle data i systemet
- Brugerne, forstået som ansøgere og medarbejdere på institutionerne, kan ikke logge på systemet.
- Få medarbejdere i KOT-sekretariatet (UFS) behandler data.

Opbevaring af persondata
Data arkiveres i systemet, indtil UFS giver besked om sletning, forventelig efter 10 år.

3.2.5 Behandlingen af personoplysninger i Lærepladsen.dk

Formål
Lærepladsen.dk er en online portal for virksomheder, faglige udvalg, erhvervsskoler og elever på erhvervsskoler. Elever/lærlinge, virksomheder, faglige udvalg og erhvervsskoler bruger Lærepladsen.dk til at:

- Skabe overblik over og dokumentere elevens lærepladssøgning
- Matche elever/lærlinge og virksomheder til et lærepladsforløb
- Varetage indgåelse af lærepladstilsagn
- Varetage indgåelse, tillæg, ændring og ophævelse af uddannelsesaftaler
- Følge med i uddannelsesforløbet, når uddannelsesaftalen er indgået

- Understøtte det lærepladsopsøgende arbejde.

Social- og sundhedsskoler samt kommuner bruger desuden Lærepladsen.dk til at:
- Registrere en fraværsrisiko på elever, der uddanner sig som enten social- og sundhedshjælper eller social- og sundhedsassistent
- Registrere en begrundelse for afslag om læreplads.

Lærepladsen.dk stiller desuden oplysninger til rådighed til Børne-og Undervisningsministeriets statistiske og videnskabelige formål i Ministeriets statistikberedskab.

Dataansvarlig myndighed
Styrelsen for It og Læring (STIL) er *kun* dataansvarlig for personoplysninger i delløsningen "Lærepladstilsagn".
Uddannelsesinstitutionerne er dataansvarlige for alle øvrige personoplysninger i Lærepladsen.dk.

Databehandler
STIL er databehandler for alle personoplysninger i Lærepladsen.dk. Endvidere er STIL ansvarlig for behandlingssikkerheden.

STIL's underdatabehandler - udvikling
Ingen – STIL udvikler selv systemet

STIL's underdatabehandler – drift, vedligehold
Statens It (SIT) leverer infrastrukturen til STIL's datacentre og er derfor også at betragte som en underdatabehandler. Herudover drifter STIL selv systemet.

I Lærepladsen.dk behandles følgende personoplysninger:
Elever/lærlinge:

- CPR-nummer, navn og adresse
- Oplysninger om kvalifikationer, personlige beskrivelse og lærepladsønsker
- Mailadresse, telefon/mobilnummer
- Administrative oplysninger om uddannelse og gennemførelse af uddannelse
- Oplysninger om fravær (ikke fraværsårsager)
- Indhold i evt. uddannelsesaftale (bl.a. arbejdssted, løn, arbejdstid, ansættelsesvilkår, overenskomst)
- Navn og mailadresse på forælder / værge, såfremt eleven/lærlingen er under 18 år, når uddannelsesaftalen indgås
- Signeringsidentifikation i forbindelse med digital underskrift.

Medarbejdere på en erhvervsskole, i en virksomhed eller i et fagligt udvalg:

- Navn
- Adresse, mailadresse, mobilnummer, lærepladsønsker og personlig beskrivelse – angivet af eleven selv. Oplysningerne kan, med elevens samtykke, tillige indtastes/redigeres af en skolemedarbejder
- Stamdata indberettes til Lærepladsen.dk via erhvervsskolernes studieadministrative systemer. Oplysning om elevers fravær og skoleophold indberettes af skolerne via de studieadministrative systemer i overensstemmelse med STIL's revisionsbekendtgørelse og grænsefladebeskrivelser.

Kategorier af registrerede brugere, der har adgang til at behandle data i systemet
- Medarbejdere på erhvervsskolen har adgang til at se elevers profil og kan – med elevens accept – redigere i profilen.
- Virksomheder, der søger lærlinge, har læseadgang til en anonymiseret version af profilen. Virksomheder kan således ikke se elevernes navn, adresse og kontaktoplysninger, men kan kontakte elever gennem portalen. Persondata for elever, som har indgået en uddannelsesaftale med en virksomhed, kan ses af den pågældende virksomhed, elevens skole og af eleven selv.

Opbevaring af persondata
Personoplysninger, som eleven selv indtaster på Lærepladsen.dk, slettes automatisk af STIL, når profilen har været inaktiv i et år.

Eleven kan desuden selv slette profilen ved login. Når eleven har slettet de indtastede personoplysninger fra sin profil, opbevarer STIL ikke længere personoplysningerne på Lærepladen.dk. Stamoplysninger opbevares på Lærepladsen.dk, så længe skolerne indberetter disse til Lærepladsen.dk via de studieadministrative systemer.

3.2.6 Behandlingen af personoplysninger i Netprøver.dk

Formål
Netprøver digitaliserer den samlede proces for prøveafvikling på de gymnasiale uddannelser – lige fra opgavesættet gøres tilgængeligt for eleverne, til eleverne afleverer besvarelsen, til besvarelsen plagiatkontrolleres og censorerne afgiver bedømmelse, og til karakteren overføres til skolernes administrative systemer, som danner eksamensbeviserne. Netprøver benyttes ved afvikling af de centralt stillede skriftlige prøver og de større skriftlige prøver på de gymnasiale uddannelser. Endvidere benyttes Netprøver ved optagelsesprøver til de gymnasiale uddannelser.

Med Netprøver sikres det, at prøveafviklingen foregår på en ensartet, kontrolleret måde på tværs af institutionerne og deres lokale it-setup, hvilket er vigtigt, eftersom afvikling af prøver er en forretningskritisk proces for uddannelsessektoren og for Undervisningsministeriet.

Netprøver har samtidigt fjernet tidligere tiders papirbaserede, manuelle arbejdsgange og store udgifter til forsendelse.

De administrative opgaver, der udføres i Netprøver i henhold til almen eksamensbekendtgørelsen, såsom adgangs- og rettighedsstyring til systemet, bedømmelser og karaktergivning, udføres af medarbejdere på den enkelte uddannelsesinstitution. Den uddannelsesinstitution, der indlæser en personoplysning i det digitale prøveafviklingssystem Netprøver, er derfor dataansvarlig for denne personoplysning. STIL's persondatabehandling består således i at stille et system til rådighed og heri opbevare persondata i Netprøver samt overføre karakterer til de studieadministrative systemer på vegne af de dataansvarlige med det formål at understøtte de opgaver som uddannelsesinstitutionerne har i forbindelse med deres ansvar for afvikling af prøver og eksamener.

Dataansvarlig myndighed
Uddannelsesinstitutioner

Databehandler
Styrelsen for It og Læring

STIL's underdatabehandler - udvikling
Netcompany

STIL's underdatabehandler – drift, vedligehold
Amazon Web Services (cloud) (i 2023)
Netprøver blev pr. 31. januar 2024 hjemtaget til STIL, hvorfor underdatabehandleren for drift og vedligehold herefter er SIT.

I Netprøver.dk behandles følgende personoplysninger:
- Elever: Navn, CPR-nummer, Unilogin, indhold af besvarelser ved eksamen i de gymnasiale uddannelser og karakterer
- Censorer: CPR-nummer og Unilogin
- Administrativt personale ved institutionen: Navn, CPR-nummer og Unilogin.

Kategorier af registrerede brugere, der har adgang til at behandle data i systemet
- Eksamensansvarlige, prøveansvarlige, prøvevagter, brugeradministratorer og it-ansvarlige.

- Herudover har vejledere og censorer adgang til persondata. Ved prøver der er anonymiserede videregives alene besvarelserne til censorer/bedømmere.

Opbevaring af persondata
Data ældre end 12 måneder vil blive slettet fra Netprøver.dk, når data er indberettet til Rigsarkivet.

3.2.7 Behandlingen af personoplysninger i Optagelse (Optagelse FTU samt Elevfordeling)

Den del af elevfordelingen, der er en del af Optagelse FTU, er indeholdt i dette afsnit.

Formål
Optagelse.dk er en portal til ansøgning om optagelse på en ungdomsuddannelse, 10. klasse samt anden aktivitet, som fx arbejde eller udlandsophold.

Formålet med STIL's behandling af personoplysninger sker i forbindelse med STIL's forpligtelser som databehandler i forhold til at understøtte ansøgning om og optagelse på en ungdomsuddannelse, 10. klasse eller anden aktivitet.

I forhold til parathedsvurderinger skal alle elever, der går i grundskolen (8. – 10. klasse) uddannelsesparathedsvurderes (UPV). UPV'en foretages i Optagelse.dk på baggrund af grundskolernes indberetning af elevoplysninger, karakterer samt personlige- og sociale forudsætninger. Den pågældende kommune er derfor dataansvarlig for behandlingen af de personoplysninger, der finder sted som led i kommunernes vejledning i Optagelse.dk.

STIL's persondatabehandling i denne sammenhæng består således i at stille Optagelse.dk til rådighed og heri opbevare og tilgængeliggøre ansøgninger med persondata for de studieadministrative systemer på ungdomsuddannelserne på vegne af de dataansvarlige med det formål at understøtte de opgaver, som kommunernes KUI-vejledere har i forbindelse med deres uddannelsesvejledning og optagelsesprocessen.

Derudover stiller Styrelsen personoplysningerne fra Optagelse.dk til rådighed for regionerne i overensstemmelse med *Bekendtgørelse om opgaver og ansvar for regionerne som dataansvarlige og for STIL som databehandler i forbindelse med den centrale it-understøttede fordelingsmekanisme, Den Koordinerede Tilmelding til Gymnasiale Ungdomsuddannelser*.

Regionerne anvender personoplysningerne til vurdering af forrang, fordeling af ufordelte ansøgere og fordeling af ansøgere, hvis ansøgning ikke er indgået i fordelingsrunden samt til klagebehandling. Dette gælder for ansøgere til de 3-årige uddannelser til almen, merkantil og teknisk studentereksamen, den 2-årige uddannelse til hf-eksamen og pre-IB.

Derudover behandler Børne- og Undervisningsministeriets personoplysninger til statistiske og videnskabelige formål i Ministeriets statistiskberedskab.

STIL varetager endvidere databehandling i forbindelse med drift og udvikling af Optagelse.dk.

Dataansvarlig
Kommunerne og uddannelsesinstitutionerne er dataansvarlige for behandlingen af de personoplysninger, der finder sted i forbindelse med deres opgaver, som vedrører uddannelsesparathedsvurdering, vejledning og optagelsesprocessen.

I overensstemmelse med Bekendtgørelse om opgaver og ansvar for regionerne er regionerne dataansvarlige i forbindelse med den centrale it-understøttede fordelingsmekanisme, Den Koordinerede Tilmelding til Gymnasiale Ungdomsuddannelser.

Databehandler
STIL er databehandler.

Underdatabehandler – udvikling
Miracle (ejet af Knowit) med dennes underdatabehandlere

STIL's underdatabehandler – drift, vedligehold
Statens It (SIT) leverer infrastrukturen til STIL's datacentre og er derfor også at betragte som en underdatabehandler. Herudover drifter STIL selv systemet.

I Optagelse (Optagelse FTU samt Elevfordeling) behandles følgende personoplysninger
Ansøgere i 8., 9. og 10. klasse og ansøgere uden for skole:

- CPR-nummer
- Navn
- Adresse
- Oplysning om beskyttelse af navn og adresse
- E-mail
- Telefonnummer
- Uddannelsesønsker
- Uddannelse
- Uddannelsesparathedsvurdering, hvis informationen haves
- Standpunkts-, prøvekarakterer og eksamensgennemsnit, hvis informationen haves
- Beviser, hvis informationen haves
- Bilag som studievalgsportfolio, som ansøger uploader til Optagelse.dk
- Transporttid og transportrute mellem bopæl og de gymnasiale uddannelser
- Oplysninger relateret til MitID, hvis ansøger anvender MitID
- Ansøgers forrangsønsker og de bilag, der måtte blive vedhæftet som dokumentation herfor kan indeholde følsomme personoplysninger.

Værge/forældre, hvis ansøger er under 18 år:

- CPR-nummer
- Navn
- Adresse
- Oplysning om beskyttelse af navn og adresse
- E-mail
- Telefonnummer
- Oplysninger relateret til dit MitID, hvis borgeren anvender MitID.

Medarbejdere i regionerne, skolerne og på de kommunale ungeindsatscentre:

- Bruger- og rettighedsstyring via MitID Erhverv.

Kategorier af registrerede brugere, der har adgang til at se og behandle data i systemet

- Forældre/værger til ansøgere, som endnu ikke er fyldt 18 år
  Forældre eller værger har adgang til at se uddannelsesparathedsvurderingen og ansøgningerne. Forældre eller værger skal underskrive ansøgningerne. De kan fjerne underskriften igen og genunderskrive efter behov.

- Grundskoler
  Grundskoler har adgang til at se, rette og slette personoplysninger i uddannelsesparathedsvurderingen. Adgangen gælder for alle skolens elever.

- Den kommunale ungeindsats (vejledere)
  Den kommunale ungeindsats (KUI) har adgang til at se og rette personoplysninger i forbindelse med uddannelsesparathedsvurderingen for de elever, der går på uddannelsesinstitutioner, som er knyttet til det pågældende KUI. Derudover har KUI adgang til at se ansøgningerne fra ansøgere, der har bopæl i de kommuner, hvor KUI har en vejledningsforpligtigelse. Det gælder, hvis ansøgeren har søgt med MitID.

- De ansøgte uddannelsesinstitutioner, fx gymnasier, erhvervsskoler og 10. klasser
  De ansøgte uddannelsesinstitutioner har adgang til at godkende eller afvise forrangsønsker. Institutionerne har adgang til at se de oplysninger, som er nødvendige for at udføre institutionernes opgaver i forbindelse med optagelsesprocessen.

- Regionerne
  Regionerne har adgang til at se de oplysninger, som er nødvendige for at udføre regionens opgaver i forbindelse med optagelsesprocessen, den centrale elevfordeling og eventuel klagebehandling. Reglerne for elevfordeling gælder for de almengymnasiale uddannelser, 3-årig stx og 2-årig hf, og de erhvervsgymnasiale uddannelser, 3-årig hhx og htx. Det gælder uanset, hvilken institutionstype, der udbyder disse uddannelser, med undtagelse af private gymnasier, som ikke er omfattet af reglerne.

  Regionerne har adgang til at godkende eller afvise forrangsønsker vedrørende handicap. Regionerne kan manuelt tildele ansøger en plads.

Derudover har Danmarks Statistik adgang til at se personoplysningerne i pseudonymiseret form som led i det statistiske arbejde.

Opbevaring af persondata
STIL sletter personoplysningerne i Optagelse (Optagelse FTU samt Elevfordeling) tidligst to måneder efter færdigbehandling af ansøgningen, og senest inden der åbnes for en ny ansøgningsrunde.

Styrelsen gemmer dog CPR-nummer og UPV-oplysninger fra eleven går i:
- klasse og indtil 2 år efter, at eleven er gået ud af 9. klasse
- klasse og 1 år efter, at eleven er gået ud af 10. klasse.

Det skyldes det forlængede retskrav om optagelse på en gymnasial uddannelse.

3.2.8 Behandlingen af personoplysninger i Optagelse (Optagelse KOT)

Formål
Optagelse (Optagelse KOT) er en portal til ansøgning om optagelse på videregående uddannelser. STIL varetager databehandling ifm. drift og udvikling af Optagelse.dk til de videregående uddannelser. Ansøgere til videregående uddannelser kan søge med MitID. Har ansøgerne et eller flere beviser i Eksamensdatabasen, tilføjes det automatisk ansøgningen. Oplysningerne i ansøgningen videresendes til ansøgerens ønskede uddannelsesinstitution for, at de kan vurdere om ansøgeren kan optages. Udenlandske ansøgere og personer, der laver ansøgningen på vegne af ansøgeren med fuldmagt, kan søge med e-mail logon (papiransøgning). Udenlandske ansøgere kan desuden søge med Europæisk nationalt ID (eID). eID er dog pt. ikke understøttet, da NemLog-in og eID ikke fungerede sammen ved overgangen til NemLog-in 3.

Dataansvarlig
UFS og de videregående institutioner (UFM's område)

Databehandler
STIL er databehandler.

Underdatabehandler – udvikling
Miracle (ejet af Knowit) med dennes underdatabehandlere og Netcompany

STIL's underdatabehandler – drift, vedligehold
Statens It (SIT) leverer infrastrukturen til STIL's datacentre og er derfor også at betragte som en underdatabehandler. Herudover drifter STIL selv systemet.

I Optagelse (KOT) behandles følgende typer af persondata:
- CPR-nummer
- Kontaktoplysninger
- Adgangsgrundlag
- Beviser
- Uddannelsesønsker
- Prioritering af uddannelsesønsker.

Kategorier af registrerede brugere, der har adgang til at se og behandle data i systemet
- Ansøgere til de videregående uddannelser har adgang til egne oplysninger omkring deres ansøgning.
- Medarbejdere på de videregående uddannelsesinstitutioner har adgang til oplysninger om alle de personer, som har sendt ansøgning til institutionen.
- Medarbejdere ved UFS har adgang til alle ansøgninger og ansøgere.

Opbevaring af persondata
Personoplysningerne på Optagelse (KOT) bliver slettet efter hver optagelsesrunde.

3.2.9 Behandlingen af personoplysninger i Ordblindetesten

Formål
De administrative opgaver, der udføres som led i anvendelsen af Ordblindetesten, såsom indberetninger, administration af testen og tilrettelæggelse af relevante specialpædagogiske undervisningstiltag, som opfylder elevens undervisningsmæssige behov, foretages af medarbejdere på kommunens skoler og medarbejdere på uddannelsesinstitutioner. Opgaven med tilrettelæggelse af undervisningstiltag sker på baggrund af Ordblindetestens automatisk genererede testresultat, som medarbejderne på kommunerne og uddannelsesinstitutionerne (testvejlederne) i sidste ende vurderer selvstændigt. Kommunerne og uddannelsesinstitutionerne er derfor hver især selvstændigt dataansvarlige for behandling af personoplysninger som led i anvendelsen af Ordblindetesten.

STIL's persondatabehandling består således i at stille et system til rådighed og heri opbevare persondata i Ordblindetesten på vegne af de dataansvarlige med det formål at understøtte de opgaver, som kommunernes og uddannelsesinstitutionerne har i forbindelse med deres forpligtelse til at udrede elevers ordblindhed og tilrettelægge et relevant undervisningstiltag.

Dataansvarlig myndighed
Uddannelsesinstitutioner og kommuner

Databehandler
Styrelsen for It og Læring

STIL's underdatabehandler - udvikling
Netcompany

STIL's underdatabehandler – drift, vedligehold
Statens It (SIT) leverer infrastrukturen til STIL's datacentre og er derfor også at betragte som en underdatabehandler. Herudover drifter STIL selv systemet.

I Ordblindetesten behandles følgende typer af persondata:
- Elever: Navn, CPR-nummer, klasse, skoletilhørsforhold, Unilogin og testresultat. Testresultatet indeholder oplysninger om, hvorvidt eleven er ordblind.
- Testvejleder: Navn og skole eller uddannelsesinstitution, hvor ordblindetesten er udført

Registrerede brugere, der har adgang til at se og behandle persondata i systemet
Kun testvejledere hvortil den enkelte elev er tilknyttet, som kan tilgå testen. Testvejlederen skal have adgang via Unilogin for at tilgå testen og data. Testvejlederen åbner op for, at en elev kan tage en ordblindetest og testvejlederen tilgår efter testen resultater for at anvende dette i vurderingen af ordblindhed.

Opbevaring af persondata
Testresultat, herunder oplysninger om ordblindhed, slettes automatisk 15 år efter, at testen er foretaget.

3.2.10 Behandlingen af personoplysninger i Sprogprøver.dk

Formål
Gennemførelse af obligatoriske sprogprøver på grundskoler og afdelinger af grundskoler med en høj andel af børn fra udsatte boligområder. STIL stiller Sprogprøver.dk til rådighed for børnehaveklasserne, som KAN anvende systemet til gennemførelse/administration af prøverne, og som SKAL anvendes til indberetning af sprogprøveresultater for børnehaveklassen og 1.-9. klasse til STIL.

Dataansvarlig myndighed
Kommuner og frie skoler

Databehandler
Styrelsen for It og Læring

STIL's underdatabehandler - udvikling
Ingen – STIL står selv for udvikling.

STIL's underdatabehandler – drift, vedligehold
Statens It (SIT) leverer infrastrukturen til STIL's datacentre og er derfor at betragte som en underdatabehandler. Herudover drifter STIL selv systemet.

I Sprogprøver behandles følgende typer af persondata:
- Navn, CPR-nummer, Unilogin, klasse og skole
- Det gælder for børnehaveklasseelever, børnehaveklasseledere, skoleledere og andre ressourcepersoner tilknyttet børnehaveklassen

Kategorier af registrerede brugere, der har adgang til at behandle data i systemet
- Lærere og pædagoger i børnehaveklasse, der kan hente undervisningsmateriale til sprogprøverne samt registrere elevers resultater
- Skoleledere og sekretærer, der kort tid efter afslutningen af et skoleår skal indberette resultater for deres pågældende skole

Opbevaring af persondata
Data til administrativ brug slettes i systemet Sprogprøver.dk og Indberet.sprogprøver.dk senest 2 måneder efter indberetningsfristen den 5. september årligt. Der er herefter ikke administrative data i Sprogprøver.dk. STIL vil dog bibeholde data, frem til der er taget stilling til arkiveringspligt og evt. indberetning til rigsarkivet er gennemført.

Data, der er indberettet til STIL's statistikberedskab, slettes efter 20 år fra udarbejdelsen som følge af dataetiske hensyn.

3.2.11 Behandlingen af personoplysninger i Sprogvurdering

Formål
Sprogvurdering.dk er et værktøj, som kommuner og andre kan anvende til at løfte opgaven med obligatorisk sprogvurdering i alderen 2-6 år. Den obligatoriske vurdering skal foretages minimum én gang. Systemet vil kunne anvendes af flere omgange, hvis det ønskes. Det afhænger af, hvad kommunen har besluttet. Børnene testes i forskellige områder og vurderingen indgår i grundlaget for, om et barn vil få en fokuseret indsats eller særlig indsats, hvis barnets sproglige udvikling ikke er alderssvarende.

Dataansvarlig myndighed
Kommuner, herunder skoler, institutioner og dagtilbud. Dagtilbuddene omfatter både offentlige og private dagtilbud, som hører ind under den enkelte institutions kommune.

Databehandler
STIL er databehandler for kommuner og uddannelsesinstitutioner.

STIL's underdatabehandler - udvikling
Ingen – STIL udvikler selv systemet.

STIL's underdatabehandler – drift, vedligehold
Statens It (SIT) leverer infrastrukturen til STIL's datacentre og er derfor at betragte som en underdatabehandler. Herudover drifter STIL selv systemet.

I Sprogvurdering behandles følgende typer af persondata:
Børn i 3-årsalderen (både i og uden for dagtilbud) samt elever på folkeskoler og hjemmeunderviste børn:

- Navn, CPR-nummer
- Tilknytning til institution og kommune
- Barnets besvarelser af testens spørgsmål
- Resultatet af testen er ikke diagnosticerende, men vil ligge til grund for et videre forløb for det enkelte barn
- Data i systemet omfatter materialer (vejledninger til testning), registreringsskemaer, der bruges til udførelse af testen og opsummering af sprogvurdering. Derudover data om antal sprogvurderinger barnet har gennemgået.

Medarbejdere (Kommunale konsulenter, pædagoger, lærere, institutionsledere):

- Navn, medarbejderens UniLogin/NemID, og hvor vedkommende arbejder.

Kategorier af registrerede brugere, der har adgang til at behandle data i systemet
- Kommunale konsulenter, pædagoger og institutionsledere har adgang til materialer (vejledninger til testning), registreringsskemaer der bruges til udførelse af testen og opsummering af sprogvurdering samt børnenes testresultater.

Opbevaring af persondata
Dataopbevaringen på Sprogvurdering udvides fra og med 1. klasse til hele elevens grundskoletid.
Der er behov for at kunne tilgå elevens sprogvurderingsresultater i hele den tid, hvor eleven går i grundskolen. Dette skyldes, at nogle vanskeligheder først viser sig sent i skoleforløbet, når det faglige indhold bliver mere komplekst, blandt nogle elever. Det skal i den forbindelse være muligt, både for den enkelte lærer, ressourcepersoner, ledelse og i visse tilfælde klagenævnet for specialundervisning, at kunne gå tilbage og se, hvilke data/udredninger, der er om elevens sproglige vanskeligheder, og hvad der tidligere er gjort i denne sammenhæng.

Efter elevens grundskoletid og en lovpligtig aflevering af data i Rigsarkivet, slettes barnets data.

3.2.12 Behandlingen af personoplysninger i Testafvikler

Formål
Testafvikleren er en generisk afvikler af simple test, herunder multiple choice-test. En vejleder har mulighed for at logge ind via Nemlogin og oprette brugerkoder, som udleveres til testtagere. Brugerkoden giver testtageren adgang til at foretage en test. Når en test er afsluttet, kan resultatet tilgås af vejleder i to år. Testafvikleren understøtter vejledende læsetest og vejledende matematiktest til hhv. FGU og FVU. Disse benyttes til at screene kursister forud for et forløb på FGU eller FVU.

Dataansvarlig myndighed
Kommuner og uddannelsesinstitutioner

Databehandler
STIL er databehandler for kommuner og uddannelsesinstitutioner.

STIL's databehandler - udvikling
Netcompany.

STIL's databehandler – drift, vedligehold
Netcompany. Statens It (SIT) leverer infrastrukturen til STIL's datacentre og er derfor også at betragte som en underdatabehandler. Herudover drifter STIL selv systemet.

I Testafvikler behandles følgende typer af persondata:
Kursist (Testtager):

- Navn, fødselsdato og e-mailadresse
- Tilhørsforhold til vejleder og derigennem til institutionen, som testen er foretaget i forbindelse med
- Kursistens testresultat og besvarelser.

Vejleder:

- Navn og Nemlogin.

Kategorier af registrerede brugere, der har adgang til at behandle data i systemet
- FGU og FVU-kursister: Logger ind med brugerkode udleveret af testvejleder
- Testansvarlig vejleder har mulighed for at logge ind via Nemlogin og oprette brugerkoder, som udleveres til testdeltagende kursister.

Opbevaring af persondata
Alle data knyttet til en testtagning, herunder testbesvarelse samt testtagers navn og fødselsdag, opbevares i systemet i to år. Herefter kasseres de automatisk.

3.2.13 Behandlingen af personoplysninger i Ungedatabasen

Formål
Ungedatabasen stiller data om unge 15-29-åriges uddannelses- og beskæftigelsesmæssige status til rådighed for den kommunale ungeindsats (KUI) og jobcentre, så de kan optimere deres indsats i forhold til den unge.

Formålet med Ungedatabasen er at skabe rammer for en målrettet og aktiv vejledningsindsats over for unge gennem dataudveksling på tværs af myndigheder og institutioner for derigennem at støtte, at 90 % af en ungdomsårgang skal have en ungdomsuddannelse, når de er 25 år. De øvrige 10 pct. af årgangen skal være godt på vej til at få en uddannelse senere eller have fast tilknytning til arbejdsmarkedet. Dataudvekslingen sker på tværs af forvaltninger, uddannelsesinstitutioner, kommuner og stat, herunder registre i jobcentre og kommunale ungeindsatser samt studieadministrative systemer. Herudover indlæses der oplysninger fra e-Indkomstregisteret for at afgøre, om den unge er i beskæftigelse eller modtager sociale ydelser. Oplysningerne i Ungedatabasen må anvendes til administrative og statistiske formål jf. Vejledningsloven.

Dataudvekslingen betyder, at Ungedatabasen systematisk opsamler information om unges uddannelses- og beskæftigelsesaktiviteter på individniveau og videresender disse til aktører, der har vejledningsansvaret for den enkelte unge. Ungedatabasen er dermed et middel til at afgøre, hvem der skal vejledes, hvem der har vejledningsansvaret for den unge og stille information til rådighed for vejlederen. Derved giver løsningen et grundlag for vejlederne til at yde en målrettet service.

Kommunerne får det fulde ansvar for at gøre alle unge under 25 år parate til at gennemføre en ungdomsuddannelse eller komme i beskæftigelse. Alle kommuner skal etablere en sammenhængende, koordineret ungeindsats på tværs af uddannelses-, beskæftigelses- og socialområdet for unge under 25 år uden en ungdomsuddannelse.

Jobcentrene er ansvarlige for indsatsen over for unge mellem 18 og 29 år. En indsats kan være at give den unge uden uddannelse et uddannelsespålæg. Ungedatabasen udveksler data med Beskæftigelsesministeriets system, kaldet Det fælles it-datagrundlag (DFDG). Herfra udveksles igen information med jobcentrene om de unge.

Alle uddannelsesinstitutioner, både inden for og uden for UVM's resort, skal indberette til Ungedatabasen.

Dataansvarlig myndighed
Kommuner

Databehandler
Styrelsen for It og Læring

STIL's underdatabehandler – udvikling
Netcompany

STIL's underdatabehandler – drift, vedligehold
Statens It (SIT) leverer infrastrukturen til STIL's datacentre og er derfor at betragte som en underdatabehandler. Herudover drifter STIL selv systemet.

I Ungedatabasen behandles følgende personoplysninger
For unge op til 25 år:

- I det fælles datagrundlag behandles oplysninger på individniveau, der er nødvendige for tilrettelæggelsen af den kommunale ungeindsats efter den uddannelses- og arbejdsmarkedsrettede lovgivning
- Oplysninger om den unges uddannelsesstatus
- Uddannelsespålæg
- Højst afsluttede uddannelse og planer
- Mål for indsatser, uddannelse og job kan dog indgå i det fælles datagrundlag for unge op til 30 år, når det er nødvendigt for en fortsat arbejdsmarkedsrettet indsats.

For unge efter 9. og 10. klasse:

- CPR-nummer
- Optagelse på en uddannelse
- Resultatet af optagelsesprøver til gymnasiale uddannelser og erhvervsuddannelser
- Afbrud og afbrudsårsagskode
- Gennemførelse af uddannelse
- Risiko for frafald
- Beskæftigelsesmæssig status, jobcenterinitierede aktiviteter, uddannelsespålæg, job- og uddannelsesønsker
- Kontaktoplysninger (navn, telefonnummer og e-mailadresse) på tildelt kontaktperson
- Oplysninger om beskæftigelse ud fra indkomstoplysninger (deltid, fuldtid og offentlig forsørgelse).

Kategorier af registrerede brugere, der har adgang til at behandle data i systemet
Der er ikke egentlige brugere med adgang til systemet, men følgende kan via webservices se udvalgte persondata:

- STAR (jobcenter) og kommunal ungeindsats (KUI) modtager hændelser på de unge. For KUI's vedkommende er det kun unge med bopæl i KUI's område. KUI får ligeledes, som "skoleKUI", hændelser på unge, der går på grundskoler og i 10. klasse i KUI's område, selvom den unge ikke har bopæl i kommunen
- Uddannelsesinstitutioner modtager i øjeblikket kun kvittering eller fejlbeskeder på deres indberetninger.

Opbevaring af persondata
'STIL sletter senest personoplysninger i det fælles datagrundlag om de registrerede, når den registrerede fylder 30 år. Oplysninger om den registreredes optagelsesprøver slettes dog 2 år efter seneste indlæsning, eller når den unge fylder 25 år. Oplysninger om den registreredes uddannelsesparathedsvurdering slettes 2 år efter seneste indlæsning.

3.3 Underdatabehandlere

Statens It (SIT) leverer infrastrukturen til STIL's systemer og er derfor også at betragte som en underdatabehandler for drift og vedligehold.

System	**Underdatabehandler - udvikling**	**Underdatabehandler – drift og vedligehold**
EASY P	Intern	SIT
EDUP (ElevDataUdvekslingsPunkt)	Netcompany	SIT
KOT-systemet	Miracle A/S, Netcompany	SIT
Lærepladsen.dk	Intern	SIT
Netprøver.dk	Netcompany	Hostes eksternt: Amazon Cloud
Optagelse.dk (Optagelse FTU, samt den del af Elevfordelingen, der foregår i Optagelse.dk)	Miracle A/S	SIT
Optagelse,dk (Optagelse KOT)	Miracle A/S, Netcompany	SIT
Ordblindetesten	Netcompany	SIT
Sprogprøver	Intern	SIT
Sprogvurdering	Intern	SIT
Testafvikler	Netcompany	SIT
Ungedatabasen	Netcompany	SIT

3.4 Risikovurdering

De kontrolmål der beskrives i de følgende afsnit, omfatter alle de systemer, denne erklæring omfatter, medmindre andet er angivet.

Risikovurderingen i STIL består af en overordnet vurdering af modstandskraften mod relevante trusler og sårbarheder, samt en vurdering af efterlevelsen af relevante kontroller. Trusler, sårbarheder og kontroller vurderes med udgangspunkt i STIL's trusselskatalog, som er udarbejdet med afsæt i ISO 27001, GDPR og vejledningsmateriale fra Digitaliseringsstyrelsen og Center for Cybersikkerhed. Trusselskataloget indeholder ligeledes de relevante trusler, sårbarheder og kontroller, som STIL's direktion har vurderet, kræver et særligt fokus.

Risikovurderingens formål er at øge modstandskraften i STIL. Ved prioritering af indsatsen beskyttes informationer på et af ledelsen godkendt og acceptabelt niveau. Risikovurderingen sikrer således, at STIL identificerer de trusler, som STIL's systemer er særligt sårbare overfor. Samtidig muliggør risikovurderingen løbende rapportering og dermed gennemsigtighed til ledelsen, så STIL's ledelse kan være proaktive i deres risikostyring. STIL's direktion orienteres fast hvert halve år om større risici, samt hvilke tekniske eller organisatoriske sikkerhedsforanstaltninger der er sat i værk for at mitigere disse. Dertil bliver pågældende kontorchefer og (vice)direktører løbende orienteret, hvis der er behov for dette.

3.5 Kontrolforanstaltninger

STIL har implementeret kontroller vedr. behandling af personoplysninger, hvor STIL er databehandler inden for følgende områder:

- Cirkulæreskrivelse, bekendtgørelse og databehandleraftale (kontrolmål A)
- Tekniske sikkerhedsforanstaltninger (kontrolmål B)
- Organisatoriske sikkerhedsforanstaltninger (kontrolmål C)
- Sletning og tilbagelevering af personoplysninger (kontrolmål D)
- Opbevaring af personoplysninger (kontrolmål E)
- Anvendelse af underdatabehandlere (kontrolmål F)
- Overførsel til tredjelande eller international organisationer (kontrolmål G)
- Bistand til den dataansvarlige (kontrolmål H)
- Håndtering af sikkerhedsbrud (kontrolmål I).

I afsnit 4 er de kontrolforanstaltninger, STIL anser for relevante for behandlingen af persondata, beskrevet. Nedenfor findes en uddybende beskrivelse af et udvalg af relevante kontrolforanstaltninger.

3.5.5 Generelle procedurer for behandling af personoplysninger (kontrolmål A)

Formål
Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med cirkulæreskrivelsen, Ungedatabasens bekendtgørelse og KOT's databehandleraftale.

Anvendte procedurer og kontroller
STIL har implementeret procedurer og kontroller, der skal sikre, at de juridiske dokumenter, som ligger til grund for behandlingen af personoplysninger, hhv. cirkulæreskrivelsen, Ungedatabasens bekendtgørelse og Optagelse.dk/KOT-systemet databehandleraftale med UFM, løbende opdateres i forhold til den konkrete behandling. Ved ændringer af systemer, herunder nye/ændrede persondatabehandlinger er der procedurer for opdateringer af fortegnelserne.

Procedurerne tager udgangspunkt i den vedtagne informationssikkerhedspolitik, som er gældende for hele BUVM og herunder STIL, hvor de styrende dokumenter i ministeriets ledelsessystem for informationssikkerhed er angivet. Herunder kan nævnes en række politikker, retningslinjer, skabeloner og dokumentation for behandling af personoplysninger. De forskellige dokumenter kan tilgås på ministeries intranet IT-Kanalen, Confluence og ServiceNow. Medarbejdere, der har adgang til personoplysninger, er omfattet af retningslinjer og procedurer, som regulerer adgangen. For at sikre at medarbejderne handler i overensstemmelse med instruksen i ovenstående, har STIL udarbejdet en retningslinje og en politik for brugeradministration.

3.5.6 Tekniske sikkerhedsforanstaltninger (kontrolmål B)

Formål
Der efterleves procedurer og kontroller, som sikrer, at STIL har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.

Anvendte procedurer og kontroller
STIL har implementeret procedurer og kontroller, der sikrer, at de tekniske sikkerhedsforanstaltninger, der er aftalt med sektoren (de dataansvarlige), er opfyldt. Dermed sikrer STIL over for sektoren, at kravene fra cirkulæreskrivelsen, Ungedatabasens bekendtgørelse og KOT's databehandleraftale med UFM er implementeret i de underdatabehandleraftaler, STIL indgår med sine leverandører for at sikre, at der er etableret det fornødne sikkerhedsniveau for it-sikkerhed i STIL's løsninger.

Nedenfor beskrives, hvordan STIL sikrer en række sikkerhedsforanstaltninger.

- **Antivirus:** Klienterne (PC'erne) er underlagt de krav, der fremgår af de tekniske minimumskrav for statslige myndigheder, herunder at der skal anvendes antivirus og endpoint-beskyttelse, at klienterne skal holdes opdateret, og at der skal anvendes VPN med 2-faktor-autentifikation fra

eksterne netværk. Kravene gælder både for SIA Pc'er og ikke SIA PC'er. STIL fører løbende kontrol med ikke SIA PC'er.
Adgang til databaseserverne kun kan ske via STIL's interne netværk og kun via de antivirus sikrede klienter. Databaseserverne er placeret på et databasehotel, der sikrer, at der er et stærkt begrænset antal STIL medarbejdere, der har adgang til databaseserverene. STIL's antivirus beskytter hele vejen rundt om databaseserverne og ikke på selve databaserne, da STIL's RDBMS (relationel database management system) ikke garanterer transaktioner, såfremt RDBMS'en ikke selv har 100% kontrol over filerne

- **Firewall:** Der er etableret firewall på de systemer, STIL har driftsansvaret for. Der er en retningslinje for firewallændringer
- **Segmentering af netværk:** Det interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger
- **Systemovervågning med alarmering:** For hele den grundlæggende infrastruktur, herunder servere og middleware er der etableret systemovervågning med alarmering. Der anvendes som udgangspunkt Nagios Monitor til overvågning, men der anvendes også mere specialiserede løsninger til eksempelvis dele af netværket, virtualiseringsplatforme og storage. Fra Nagios Monitor er der lavet en integration til ServiceNow, hvor der kan oprettes incidents, som håndteres i ServiceNow
- **Sårbarhedsscanninger og penetrationstest:** Der er retningslinjer for sårbarhedsscanninger og penetrationstest. Der gennemføres sårbarhedsscanninger hvert halve år. Det gælder hele STIL's infrastruktur. Sårbarhedsscanningerne foregår på ip-niveau. Dvs. alle systemer med ip-adresser, der er eksponeret for internettet, bliver scannet. Såfremt der identificeres problemstillinger for de enkelte systemer, involveres produktkontoret. Det vurderes løbende med en risikobaseret tilgang hvilke produkter, som udtages til PEN-test.
- **Kryptering:** Mails bliver krypteret centralt hos SIT. Personoplysninger til eksterne skal kommunikeres via sikker post (der er en politik herom). I forhold til hjemmesider, så er det en del af de 20 tekniske minimumskrav, der løbende kontrolleres af STIL
- **Relevante opdateringer og patches, herunder sikkerhedspatches:** STIL varetager løbende installation og monitoreringen af sikkerhedspatches på infrastruktur
- **Fysisk adgangssikkerhed:** Serverne til de systemer, denne erklæring omfatter, er fysisk placeret hos SIT, dvs. al data og housing ligger hos SIT. Opfølgning på den fysiske adgangssikkerhed hos SIT håndteres som en del af STIL's opfølgning på Finansministeriets rapporter om SIT. Der er et stærkt begrænset antal medarbejdere fra STIL, der har adgang til datacenteret, og deres adgang logges
- **Anvendelse af testdata:** Der er implementeret en retningslinje for anvendelse af testdata. Her fremgår, at produktionsdata indeholdende personoplysninger for så vidt muligt skal undgås. Hvis der er behov for anvendelse af produktionsdata i testmiljøerne, skal der ske anonymisering, anvendelse af dummy-data eller pseudonymisering afhængigt af dataklassifikationen (typen af personoplysninger). Er dette ikke muligt, skal der foranstaltes kompenserende sikkerhedsforanstaltninger i form af at have samme sikkerhedsniveau som på produktionsdata med brugerstyring og logning, tidsbegrænsning samt at dette altid skal godkendes af en kontorchef.

Brugeradministration
Brugeradministration er på applikationsniveau formaliseret og systemunderstøttet i STIL via ServiceNow, som er en workflowsoftware-platform. De enkelte medarbejdere bestiller adgange til systemerne via ServiceNow, og bestillingerne videresendes automatisk til deres kontorchef/teamleder, som vurderer, om medarbejderen har et arbejdsbetinget behov, førend de godkender adgangen. Kontorchefen/teamlederen skal løbende følge op på medarbejderens adgang til systemet for at sikre, at der stadig er et arbejdsbetinget behov for adgangen, og at medarbejderen overholder STIL's retningslinjer og procedurer. I Elevadministration og FGU Matematiktest, er der ikke interne STIL-brugere. Her håndteres brugerstyringen via Nemlogin eller Unilogin. For Ordblindetesten og Sprogprøver.dk foregår brugeradministrationen eksternt hos institutionerne.

Brugeradministrationen af de eksterne konsulenter, der er oprettet hos SIT (X-brugere), tildeles rettigheder til de enkelte systemer på samme vis som STIL's medarbejdere i ServiceNow. Oprettelse og nedlæggelse af disse brugere sker enten ved kontakt til de konsulentansvarlige, eller oprettes af kontorerne selv hos SIT. Her følges der månedligt op på, om de fortsat skal være oprettet.

Der er en retningslinje for eksterne konsulenter/udvikleres tidsbegrænsede adgang til services i STIL's datacenter (brugere uden X-konti). Disse tilgår datacenteret via STIL VPN og oprettes som isolerede brugere, der alene har adgang til services i datacenteret. Som udgangspunkt tildeles der ikke rettigheder til produkter, data eller informationer.

HRO har udarbejdet en arbejdsgangsbeskrivelse for fratrædelser. Når en medarbejder stopper og bliver lukket i BUVM's HR-platform, får SIT automatisk besked om fratrædelsesdato og lukker e-mail og brugeradgange. Samtidig orienteres afdelingen om fratrædelsen med henblik på evt. brugernedlæggelse i relevante fagsystemer.

STIL har for systemernes underliggende databaser iværksat en proces med at centralisere alle databaser på databasehotelservere for at minimere antallet af teknikere, som har adgang til STIL's databaser og sikre, at der ikke anvendes fælles brugerprofiler. Kun seks teknikere har nøglebaseret adgang (certifikater) til databaserne, og al indlogning registreres i Nagios. På databaseniveau er ti ud af tretten systemer på databasehotel. To systemer hostes eksternt og er styret af databehandleraftaler. Et er baseret på VMWare og kan ikke komme på hotel pga. licensudfordringer. Det bliver håndteret særskilt ved, at der kun er tre teknikere, der har adgang til databasen.

Etableret logning
Logning i STIL er udmøntet gennem politik og retningslinjer for hhv. infrastruktur og applikationslogning. Formålet med politikken og retningslinjerne er, at STIL indsamler alle relevante logs og hermed sikrer et troværdigt grundlag for at kunne efterforske sikkerhedsbrud (forensics) og efterleve ISO27001 og GDPR-krav.

På baggrund af den type af data, et system behandler (dataklassifikation: Fx følsomme eller almindelige persondata), er det udspecificeret i retningslinjerne, hvilke særlige krav der er til systemer med specifikke datatyper.

Kontorchefen er ansvarlig for logning af et system, dvs. registrere hændelser og tilvejebringe bevis herfor. Når systemer behandler persondata, stiller det en række krav i forhold til behandling af logs: Hændelseslogning af brugeraktivitet, undtagelser, fejl og tegn på informationssikkerhedshændelser. Den indsamlede log skal opbevares korrekt, og fejlmeldinger gennemgås jævnligt. Kontorchefen (evt. Product Owner) fastlægger de produktspecifikke retningslinjer for logning med udgangspunkt i de fastlagte minimumskrav i politikken og retningslinjerne og øvrige driftsrelaterede krav til logning. Driftsrelaterede krav til logning beskrives af PO. Kontorchefen er ansvarlig for logning i det pågældende system og skal med PO via en risikovurdering aktivt beslutte, hvis produktet ikke skal overholde kravene til logning. Opbevaringsperioden skal som minimum følge de definerede krav i retningslinjerne. Dog kan der opstå tilfælde, hvor opbevaringsperioden forlænges grundet et konkret behov herfor i forhold til risikovurdering eller ved større behov for fejlsøgning. Kontorchefen er ansvarlig for, at det årligt vurderes, hvorvidt længden af opbevaringsperioden fortsat matcher systemets behov.

Logningen håndteres i SIEM-systemet Nagios. Udrulningen af logningen er igangværende og sker i prioriteret rækkefølge. Alle systemerne, på nær de fem nedenstående systemer, har defineret parametrene og opsat alarmer ved anormale hændelser. EASY-P bliver udfaset i 2024/2025, hvorfor det er besluttet, at det er tilstrækkeligt med en applikationsbaseret logning på en lang række af de centrale tabeller, med logning af hvem der senest har ændret data, og hvilken dato det er sket. Netprøver, Sprogprøver, Sprogvurdering og Testafvilker definerer logparametrene i 2024.

3.5.7 Organisatoriske foranstaltninger (kontrolmål C)

Formål
Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.

Anvendte procedurer og kontroller
For at sikre den organisatoriske sikkerhed har STIL en central informationssikkerhedspolitik, der opdateres og godkendes årligt. På STIL's intranet "IT-Kanalen" er der et særskilt afsnit med informationssikkerhed og GDPR. Her findes informationssikkerhedshåndbogen, som alle medarbejdere skal have læst om deres ansvar, sikkerhedsforanstaltninger i BUVM, hjælpeværktøjer, godkendte retningslinjer og vejledninger. Der afholdes løbende awareness-kampagner for at øge fokus og kompetencerne om informationssikkerhed, og alle nye medarbejdere introduceres til informationssikkerhedshåndbogen.

Ved ansættelser kan der indhentes oplysninger fra 1-2 referencer på den ansøger, som overvejes tilbudt en stilling. Referencer tages kun med forudgående accept fra ansøger. Ved ansættelser af medarbejdere med adgang til væsentlige og fortrolige informationssikkerhedsmæssige oplysninger skal vedkommende - efter en konkret vurdering – sikkerhedsgodkendes.

For alle nyansatte er det obligatorisk at tage e-læringskurser i Campus, der udover god adfærd i det offentlige og introduktion til offentlighedsloven e-læringskurserne indeholder: Informationssikkerhed for medarbejdere og Databeskyttelse.

Når en medarbejder fratræder, er der procedurer, der sikrer deaktivering af medarbejderens brugeradgange - se afsnit 3.5.6 om brugerstyring. Samtidig er der procedurer, der sikrer, at medarbejderens aktiver som PC-udstyr, mobiltelefon, legimitationskort og evt. nøgler til STIL indsamles.

3.5.8 Sletning og tilbagelevering af personoplysninger (kontrolmål D)

Formål
Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres, såfremt der indgås aftale herom med den dataansvarlige.

Anvendte procedurer og kontroller
STIL har i cirkulæreskrivelsen og informationssikkerhedspolitikken beskrevet, hvorledes personoplysninger skal behandles. Her er det overordnet beskrevet, hvorledes STIL på anvisning fra institutionerne, kommunerne eller regionerne sletter og tilbageleverer data. Således er det til enhver tid muligt at få slettet eller tilbageleveret data, såfremt dette ikke er i strid med anden lovgivning. Cirkulæreskrivelsen og informationssikkerhedspolitikken opdateres som minimum en gang årligt.

STIL har ansvaret for opbevaring af personoplysninger i de ti systemer i cirkulæreskrivelsen i de tidsperioder, som er anført for hvert system.

Ud over de 9systemer i cirkulæreskrivelsen er håndtering, sletning og tilbagelevering af personoplysninger i de 3 yderligere systemer, Elevfordeling, KOT og Ungedatabasen, beskrevet hver for sig i hovedafsnittet 3.2 i denne revisionserklæring.

3.5.9 Opbevaring af personoplysninger (kontrolmål E)

Formål
Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.

Anvendte procedurer og kontroller
STIL behandler alene personoplysninger i overensstemmelse med cirkulæreskrivelsen, KOT-systemets databehandleraftale med UFM og Ungedatabasens bekendtgørelse. Dette er kommunikeret til alle relevante medarbejdere i STIL.

STIL's databehandling, inklusive opbevaring, finder kun sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.

3.5.10 Anvendelse af underdatabehandlere (kontrolmål F)

Formål
Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.

Anvendte procedurer og kontroller
STIL sikrer, at der er indgået databehandleraftaler med underdatabehandlere, og at underdatabehandlere underlægges samme tekniske og organisatoriske sikkerhedsforanstaltninger som STIL. Endvidere føres der løbende kontrol med underdatabehandlere. Der benyttes udelukkende underdatabehandlere i overensstemmelse med cirkulæreskrivelsen, KOT-systemets databehandleraftale med UFM og Ungedatabasens bekendtgørelse. STIL fører årligt tilsyn med underdatabehandlere gennem indhentning af revisionserklæringer, tilsynsrapport og besvarelse af en række tilsynsspørgsmål. Derudover er der løbende dialog med underdatabehandlere i form af statusmøder, afrapportering mv. Gennemgangen af cirkulæreskrivelsen og underdatabehandlere udføres mindst én gang årligt.

3.5.11 Overførsel til tredjelande (kontrolmål G)

Formål
Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.

Netprøver.dk hostes i Amazon Cloud. Data er placeret i EU. I lyset af problemerne ift. dataoverførsel til tredjelande, har STIL besluttet at hjemtage Netprøver. Netprøver blev flyttet fra Amazon Cloud og hjemtaget til STIL pr. 31. januar 2024.

3.5.12 Bistand til dataansvarlige (kontrolmål H)

Formål
Der efterleves procedurer og kontroller, som sikrer, at databehandleren kan bistå den dataansvarlige med udlevering, rettelse, sletning eller begrænsning af oplysninger om behandling af personoplysninger til den registrerede.

Anvendte procedurer og kontroller
STIL har etableret en overordnet procedure for bistand til de dataansvarlige i forhold til håndtering af de registreredes rettigheder efter GDPR, såsom ret til indsigt, ret til oplysning om behandlingen af personoplysninger, ret til berigtigelse, ret til sletning, ret til begrænsning af behandling og ret til indsigelse i det omfang, de registrerede retter henvendelse herom. Procedurerne opdateres efter behov, eller hvis databeskyttelseslovgivningen ændres.

3.5.13 Sikkerhedsbrud (kontrolmål I)

Formål
Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.

Anvendte procedurer og kontroller
STIL har etableret procedurer til håndtering af sikkerhedshændelser, herunder brud på persondatasikkerheden. Det står overordnet beskrevet på BUVM's intranet "kanalen", og processen er beskrevet i detaljer på STIL's vidensdelingsplatform, Confluence. STIL følger den centrale procedure til håndtering af brud på persondatasikkerheden, hvor der foretages en vurdering af sikkerhedshændelsen. Herefter træffes så vidt muligt omgående tekniske og organisatoriske foranstaltninger for at minimere risikoen for de registrerede.

STIL bistår den dataansvarlige med rettidig anmeldelse til Datatilsynet samt underretning af de registrerede.

STIL arbejder løbende med at højne medarbejdernes awareness i forhold til informationssikkerhed.

3.6 Komplementerende kontroller hos de dataansvarlige

De dataansvarlige institutioner, kommuner og regioner har som dataansvarlige ansvaret for at instruere STIL i behandlingen af persondata, herunder at behandlingen er nødvendig og saglig i forhold til de dataansvarliges opgavevaretagelse.

De dataansvarlige institutioner, kommuner og regioner har desuden ansvaret for at sikre, at de tekniske og organisatoriske sikkerhedsforanstaltninger omkring de dataansvarliges medarbejderes behandling af personoplysningerne er tilstrækkelige, herunder administration af egne brugeres adgange til løsningerne samt registrering af eventuelle sikkerhedsbrud.

4 STIL's kontrolmål, kontroller, test og resultat heraf

4.1 Introduktion

Denne rapport er udformet med henblik på at informere STIL's dataansvarlige om STIL's systemer og kontroller, som kan påvirke behandlingen af personoplysninger, og samtidig informere de dataansvarlige, for hvem STIL behandler personoplysninger, om funktionalitet af de kontroller, der blev efterprøvet. Afsnittet, når det kombineres med en forståelse og vurdering af kontrollerne hos de dataansvarlige, har til hensigt at hjælpe de dataansvarlige til at vurdere risici forbundet med den outsourcede behandling af personoplysninger, som muligvis påvirkes af kontrollerne hos STIL.

Vores test af STIL's kontroller er begrænset til de kontrolmål og relaterede kontroller, som er nævnt i nedenstående kontrolmatrix i denne del af rapporten, og er ikke udvidet til at omfatte alle de kontroller, som er beskrevet i systembeskrivelsen, eller kontroller, som forventes at være implementeret hos de dataansvarlige for at opfylde kontrolmålene.

Det er den dataansvarliges ansvar at evaluere denne information i forhold til de kontroller, som eksisterer hos den dataansvarlige. Hvis bestemte komplementerende kontroller ikke er til stede hos den dataansvarlige, kan STIL's kontroller muligvis ikke kompensere for sådanne svagheder.

STIL's systembeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos underleverandører.

Den dataansvarlige bør vurdere, hvorvidt indhentning af revisionserklæringer fra underleverandøren er relevant for at kunne foretage en samlet vurdering af, om alle nødvendige kontroller er på plads i relation til det samlede kontrolmiljø.

4.2 Test af kontroller

De udførte test i forbindelse med fastlæggelse af kontrollers udformning og funktionalitet består af en eller flere af følgende metoder:

Metode	Beskrivelse
Forespørgsel	Forespørgsel hos udvalgt personale hos STIL
Observation	Observation af kontrollens udførelse
Inspektion	Inspektion af dokumenter og rapporter, som angiver udførelse af kontroller. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er udformet, så de kan forventes at blive effektive, hvis de implementeres. Endvidere vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Genudførelse af kontrollen	Gentagelse af den relevante kontrol med henblik på at verificere, at kontrollen fungerer som forudsat.

4.3 Test af udformning, implementering og funktionalitet

Vores test af kontrollernes udformning, implementering og funktionalitet inkluderer de test, som vi betragter som nødvendige for at vurdere, om de udførte kontroller og overholdelsen heraf er tilstrækkelige til at give høj, men ikke absolut sikkerhed for, at de specificerede kontrolmål blev opnået i perioden 1. januar 2023 til 31. december 2023.

4.4 Kontrolmål, kontroller og resultater af test

I nedenstående skema er de testede kontrolmål og kontroller anført, ligesom vi har beskrevet, hvilke revisionshandlinger der er udført og resultatet af disse handlinger. I det omfang, vi har konstateret væsentlige kontrolsvagheder, har vi anført dette.

4.5 Kontrolmål, kontrolaktivitet, test og resultat heraf

Kontrolmål A Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med cirkulæreskrivelse, bekendtgørelse og databehandleraftale.			
Nr.	**STIL's kontrolaktivitet**	**Deloittes test**	**Resultat af test**
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Deloitte har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks, og at disse er opdaterede. Deloitte har inspiceret, at procedurerne indeholder krav om mindst en årlig vurdering af behovet for opdatering, herunder ved ændringer i den dataansvarliges instruks eller ændringer i databehandlingen.	Ingen afvigelser konstateret.
A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra den dataansvarlige.	Deloitte har forespurgt, hvordan ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Deloitte har inspiceret, at der er procedurer, der sikrer, at der alene udføres behandling af personoplysninger, som fremgår af instruks. Deloitte har stikprøvevist inspiceret, at behandling af personoplysninger foregår i overensstemmelse med instruks.	Ingen afvigelser konstateret.
A.3	STIL underretter omgående den dataansvarlige, hvis en instruks efter STIL's mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Deloitte har inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning.	Ingen afvigelser konstateret.

Kontrolmål A Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med cirkulæreskrivelse, bekendtgørelse og databehandleraftale.			
Nr.	**STIL's kontrolaktivitet**	**Deloittes test**	**Resultat af test**
		Deloitte har inspiceret, at der er procedurer for underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen.	

Kontrolmål B Der efterleves procedurer og kontroller, som sikrer, at STIL har implementeret tekniske sikkerhedsforanstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	**STIL's kontrolaktivitet**	**Deloittes test**	**Resultat af test**
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres instruerede og aftalte sikkerhedsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige (cirkulæreskrivelse, bekendtgørelse og databehandleraftale). Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Deloitte har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger, og at procedurerne er opdateret. Deloitte har inspiceret cirkulæreskrivelse, bekendtgørelse og databehandleraftale og konstateret, at de instruerede og aftalte sikkerhedsforanstaltninger er etableret.	Ingen afvigelser konstateret.
B.2	STIL har foretaget en risikovurdering og på baggrund heraf taget stilling til de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de med den dataansvarlige aftalte sikkerhedsforanstaltninger.	Deloitte har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at STIL foretager en risikovurdering for at opnå en passende sikkerhed. Deloitte har inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger. Deloitte har inspiceret, at STIL har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen. Deloitte har inspiceret, at STIL har implementeret de sikkerhedsforanstaltninger, der er aftalt med den dataansvarlige og indeholdt i cirkulæreskrivelse og bekendtgørelse.	Ingen afvigelser konstateret.
B.3	Der er for de klienter og systemer, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres. STIL fører løbende kontrol med ikke SIA pc'er med henblik på at undersøge, om antivirus er opdateret.	Deloitte har inspiceret, at der for de klienter og systemer, der anvendes til behandling af personoplysninger, er installeret antivirussoftware.	Ingen afvigelser konstateret.

Kontrolmål B Der efterleves procedurer og kontroller, som sikrer, at STIL har implementeret tekniske sikkerhedsforanstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	**STIL's kontrolaktivitet**	**Deloittes test**	**Resultat af test**
		Deloitte har inspiceret, at der er installeret antivirus på klienter og systemer, som løbende opdateres. Deloitte har stikprøvevist inspiceret, at antivirus-software er opdateret. Deloitte har stikprøvevist udvalgt medarbejdere der anvender ikke SIA pc'er og inspiceret dokumentation for, at STIL har ført kontrol med, at disse har antivirus installeret og opdateret.	
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem en sikret firewall.	Deloitte har inspiceret, at der foreligger en formaliseret procedure for administration af firewalls, og at denne er opdateret. Deloitte har forespurgt, om ekstern adgang til systemer alene tilgås gennem en sikret firewall, for de systemer STIL er ansvarlig for. Deloitte har inspiceret dokumentation for, at ekstern adgang til systemer, der anvendes til behandling af personoplysninger, alene sker gennem en sikret firewall, for de systemer STIL er ansvarlig for.	Ingen afvigelser konstateret.
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Deloitte har forespurgt, om interne netværk er segmenteret med henblik på at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger. Deloitte har inspiceret netværksdiagrammer og anden netværksdokumentation til sikring af behørig segmentering.	Ingen afvigelser konstateret.

Kontrolmål B Der efterleves procedurer og kontroller, som sikrer, at STIL har implementeret tekniske sikkerhedsforanstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	**STIL's kontrolaktivitet**	**Deloittes test**	**Resultat af test**
B.6	Adgang til personoplysninger i de udvalgte systemer er begrænset til interne medarbejdere i STIL, som har et arbejdsbetinget behov for adgang.	Deloitte har inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger, og at der foreligger formaliserede procedurer for opfølgning på, at brugeres adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov. Deloitte har observeret, at applikationerne har tekniske foranstaltninger indbygget, som understøtter opretholdelse af begrænsning i brugernes arbejdsbetingede adgang til personoplysninger. Deloitte har stikprøvevist inspiceret, at autorisation til systemer og data er godkendt og begrænset til medarbejderes arbejdsbetingede behov.	Ingen afvigelser konstateret.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	Deloitte har forespurgt, om der for de systemer og databaser, der anvendes til behandling af personoplysninger, er etableret systemovervågning med alarmering. Deloitte har inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysninger, er etableret systemovervågning med alarmering. Deloitte har stikprøvevist inspiceret, at STIL har modtaget advisering via mail med registrerede alarmer i forbindelse med den etablerede systemovervågning.	Ingen afvigelser konstateret.

Kontrolmål B Der efterleves procedurer og kontroller, som sikrer, at STIL har implementeret tekniske sikkerhedsforanstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	**STIL's kontrolaktivitet**	**Deloittes test**	**Resultat af test**
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet. Ekstern opkobling foregår via anvendelse af VPN med 2-faktor autentifikation.	Deloitte har inspiceret, at der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger over internettet via SSL-kryptering. Deloitte har inspiceret, at certifikater til kryptering har været tilgængelige og aktiveret i erklæringsperioden. Deloitte har inspiceret, at STIL anvender SSL-kryptering og VPN med 2-faktor autentifikation.	Ingen afvigelser konstateret.
B.9	Der er etableret logning af følgende forhold i systemer, hvor personlige data er tilgængelige: • Dataadgang og handlinger udført af systemadministratorer samt andre brugere • Login-information Logoplysninger er beskyttet mod manipulation og tekniske fejl.	Deloitte har inspiceret, at der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter i systemer og databaser, der anvendes til behandling og transmission af personoplysninger, herunder gennemgang og opfølgning på logs. Deloitte har inspiceret, at logning af brugeraktiviteter er konfigureret og aktiveret. Deloitte har inspiceret, at opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod manipulation og sletning. Deloitte har stikprøvevist inspiceret, at logfiler har det forventede indhold i forhold til opsætning, og at der er dokumentation for den foretagne opfølgning og håndtering af evt. sikkerhedshændelser.	Ingen afvigelser konstateret.

Kontrolmål B Der efterleves procedurer og kontroller, som sikrer, at STIL har implementeret tekniske sikkerhedsforanstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	**STIL's kontrolaktivitet**	**Deloittes test**	**Resultat af test**
B.10	Personoplysninger, der anvendes til udvikling, test eller lignende, er i pseudonymiseret eller anonymiseret form. Ved særlige omstændigheder anvendes persondata til test, som foregår på baggrund af godkendelse fra relevant dataansvarlig, og som understøttes af passende tekniske sikkerhedsforanstaltninger. Anvendelse sker alene ved formaliserede procedurer. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.	Deloitte har inspiceret, at der foreligger formaliserede procedurer for anvendelse af personoplysninger til udvikling, test og lignende, der sikrer, at anvendelsen primært sker i pseudonymiseret eller anonymiseret form. Deloitte har forespurgt, om der anvendes produktionsdata til udvikling, test eller lignende. Deloitte har inspiceret dokumentation for, om der indhentes godkendelse ved anvendelse af produktionsdata ved test. Deloitte har stikprøvevist inspiceret, at anvendt data i udviklings- og testmiljø var pseudonymiseret, anonymiseret eller fiktive data.	Ingen afvigelser konstateret.
B.11	De etablerede tekniske foranstaltninger testes løbende gennem sårbarhedsscanninger og penetrationstest.	Deloitte har forespurgt, om der løbende foretages test gennem sårbarhedsscanninger og penetrationstest. Deloitte har stikprøvevist inspiceret, at der er dokumentation for løbende test af de etablerede tekniske foranstaltninger, hvor der løbende foretages sårbarhedsscanning og årlig penetrationstest.	Ingen afvigelser konstateret.
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Deloitte har inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches. Deloitte har stikprøvevist inspiceret, at ændringer er udført i overensstemmelse med proceduren herfor.	Ingen afvigelser konstateret.

Kontrolmål B Der efterleves procedurer og kontroller, som sikrer, at STIL har implementeret tekniske sikkerhedsforanstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	**STIL's kontrolaktivitet**	**Deloittes test**	**Resultat af test**
B.13	STIL har etableret en formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til systemer. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Deloitte har inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang. Deloitte har stikprøvevist inspiceret, at medarbejderes adgange til systemer og databaser er godkendt, og at der er et godkendt arbejdsbetinget behov. Deloitte har stikprøvevist for fratrådte medarbejdere inspiceret, at adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt. Deloitte har inspiceret, at der foreligger dokumentation for regelmæssig - mindst årligt – vurdering og godkendelse af tildelte brugeradgange i systemer.	Ingen afvigelser konstateret.
B.14	Adgang til applikationerne, hvori der sker behandling af personoplysninger, er opsat med password-login.	Deloitte har inspiceret, at der foreligger en procedure for anvendelse af passwords, som ledelsen har behandlet og godkendt inden for erklæringsperioden. Deloitte har inspiceret passwordkonfigurationer til systemer i scope og vurderet, at disse er i overensstemmelse med proceduren herfor.	Ingen afvigelser konstateret.
B.15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Deloitte har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Ingen afvigelser konstateret.

Kontrolmål B Der efterleves procedurer og kontroller, som sikrer, at STIL har implementeret tekniske sikkerhedsforanstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	**STIL's kontrolaktivitet**	**Deloittes test**	**Resultat af test**
		Deloitte har inspiceret dokumentation for, at alene autoriserede personer har haft fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger, frem til erklæringsperioden.	

Kontrolmål C Der efterleves procedurer og kontroller, som sikrer, at STIL har implementeret organisatoriske sikkerhedsforanstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	**STIL's kontrolaktivitet**	**Deloittes test**	**Resultat af test**
C.1	STIL's ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder STIL's medarbejdere. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Deloitte har inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for erklæringsperioden. Deloitte har inspiceret dokumentation for, at disse dokumenter er gjort tilgængelige for alle STIL's medarbejdere.	Ingen afvigelser konstateret.
C.2	STIL's ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftale, cirkulæreskrivelsen og bekendtgørelse.	Deloitte har inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikkerhedsforanstaltninger og behandlingssikkerheden i databehandleraftale, cirkulæreskrivelse og bekendtgørelse. Deloitte har inspiceret, at kravene i databehandleraftale, cirkulæreskrivelse og bekendtgørelse, er dækket af informationssikkerhedspolitikkens krav til sikkerhedsforanstaltninger og behandlingssikkerheden.	Ingen afvigelser konstateret.
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: · Referencer fra tidligere ansættelser · Eksamensbeviser.	Deloitte har inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Deloitte har stikprøvevist inspiceret, at der udføres efterprøvning i forbindelse med ansættelse.	Ingen afvigelser konstateret.

Kontrolmål C Der efterleves procedurer og kontroller, som sikrer, at STIL har implementeret organisatoriske sikkerhedsforanstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	**STIL's kontrolaktivitet**	**Deloittes test**	**Resultat af test**
C.4	Ved ansættelse underskriver medarbejderen en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til personalehåndbogen samt anden relevant information vedrørende medarbejderens behandling af personoplysninger.	Deloitte har stikprøvevist inspiceret, at nyansatte medarbejdere har underskrevet en fortrolighedsaftale. Deloitte har stikprøvevist inspiceret, at nyansatte medarbejdere er blevet introduceret til informationssikkerhedspolitikken og relevant information for persondatabehandling.	Ingen afvigelser konstateret.
C.5	Ved fratrædelse er der hos STIL implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Deloitte har inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder deaktiveres eller ophører ved fratrædelse, og at aktiver såsom adgangskort, PC, mobiltelefon mv. inddrages. Deloitte har for fratrådte medarbejdere stikprøvevist inspiceret, at rettigheder er deaktiveret eller ophørt, og at aktiver er inddraget i overensstemmelse med proceduren.	Ingen afvigelser konstateret.
C.6	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, og at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, som STIL udfører for de dataansvarlige.	Deloitte har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og deres generelle tavshedspligt. Deloitte har for fratrådte medarbejdere stikprøvevist inspiceret, at der er dokumentation for opretholdelse af fortrolighedsaftale og generel tavshedspligt.	Ingen afvigelser konstateret.

Kontrolmål C Der efterleves procedurer og kontroller, som sikrer, at STIL har implementeret organisatoriske sikkerhedsforanstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	**STIL's kontrolaktivitet**	**Deloittes test**	**Resultat af test**
C.7	STIL gennemfører årlig awareness-træning i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Deloitte har inspiceret, at STIL udbyder awareness-træning til medarbejderne i generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger. Deloitte har inspiceret dokumentation for, at relevante medarbejdere, som enten har adgang til eller behandler personoplysninger, har deltaget i awareness-træning i perioden.	Ingen afvigelser konstateret.

Kontrolmål D Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres, såfremt der indgås aftale herom med den dataansvarlige.			
Nr.	**STIL's kontrolaktivitet**	**Deloittes test**	**Resultat af test**
D.1	STIL har udarbejdet skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Deloitte har inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger, og at procedurerne er opdateret.	Ingen afvigelser konstateret.
D.2	Der er aftalt følgende specifikke krav til STIL's opbevaringsperioder og sletterutiner: • Personoplysninger opbevares hos STIL, indtil den dataansvarlige anmoder om at få oplysningerne slettet eller tilbageleveret. Behandlingen er ikke tidsbegrænset og varer, indtil aftalen opsiges eller ophæves af en af parterne. • Personoplysninger slettes for systemer, hvor sletterfrist er angivet.	Deloitte har inspiceret, at der foreligger procedurer for opbevaring og sletning, som indeholder de specifikke krav til STIL's opbevaringsperioder og sletterutiner ift. cirkulæreskrivelse, bekendtgørelse og databehandleraftale. Deloitte har inspiceret, at der er etableret funktionalitet, som sikrer, at personoplysninger kan slettes i overensstemmelse med de aftalte sletterutiner og opbevares i overensstemmelse med de aftalte opbevaringsperioder.	Ingen afvigelser konstateret.
D.3	Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med STIL: • Tilbageleveret til den dataansvarlige og/eller • Slettet, hvor dette ikke er i strid med anden lovgivning.	Deloitte har inspiceret, at der foreligger formaliserede procedurer for sletning og tilbagelevering af personoplysninger til den dataansvarlige. Deloitte har inspiceret, at procedurerne er opdateret. Deloitte har baseret på forespørgsler fået oplyst, at der ikke har været ophør af behandling i perioden.	Ingen afvigelser konstateret.

Kontrolmål E Der efterleves procedurer og kontroller, som sikrer, at STIL alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.			
Nr.	**STIL's kontrolaktivitet**	**Deloittes test**	**Resultat af test**
E.1	STIL har udarbejdet en skriftlig procedure, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Deloitte har inspiceret, at der foreligger en formaliseret procedure for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftaler og cirkulæreskrivelsen, og at proceduren er opdateret.	Ingen afvigelser konstateret.
E.2	STIL's databehandling, herunder opbevaring, må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Deloitte har inspiceret, at STIL har udarbejdet en procedure, som samlet nævner hvilke behandlingsaktiviteter, der foretages, og at den derudover angiver lokation. Deloitte har inspiceret, at der er dokumentation for, at databehandling, herunder opbevaring af personoplysninger, alene foretages på godkendte lokaliteter.	Ingen afvigelser konstateret.

Kontrolmål F Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, og at STIL ved opfølgning på disses tekniske og organisatoriske sikkerhedsforanstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.			
Nr.	**STIL's kontrolaktivitet**	**Deloittes test**	**Resultat af test**
F.1	STIL har i henhold til den aftalte instruks med den dataansvarlige etableret krav ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks.	Deloitte har inspiceret instruksen med den dataansvarlige, og at der heri foreligger formaliserede krav for anvendelse af underdatabehandlere. Deloitte har stikprøvevist inspiceret, at databehandlingen hos underdatabehandlere alene foretages i henhold til instruksen mellem STIL og dataansvarlige.	Ingen afvigelser konstateret.
F.2	STIL anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Deloitte har inspiceret, at STIL har en samlet og opdateret oversigt over anvendte underdatabehandlere i deres databehandleraftale med den dataansvarlige. Deloitte har inspiceret, at STIL's databehandling fremgår af databehandleraftalerne eller i øvrigt er godkendt af den dataansvarlige.	Ingen afvigelser konstateret.
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underrettes den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Deloitte har forespurgt, om der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Deloitte har forespurgt, om der har været ændringer i anvendelsen af underdatabehandlere frem til erklæringsperioden.	Ingen afvigelser konstateret.

Kontrolmål F Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, og at STIL ved opfølgning på disses tekniske og organisatoriske sikkerhedsforanstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.			
Nr.	**STIL's kontrolaktivitet**	**Deloittes test**	**Resultat af test**
F.4	STIL har pålagt underbehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen eller lignende med den dataansvarlige.	Deloitte har inspiceret, at der foreligger underskreven aftale med anvendt underdatabehandler, som fremgår af oversigten fra databehandleraftalerne. Deloitte har inspiceret at aftale og underlæggende bilag indeholder samme krav og forpligtelser som dem, der er anført i databehandleraftalerne mellem de dataansvarlige og STIL.	Ingen afvigelser konstateret.
F.5	STIL har en oversigt over godkendte underdatabehandlere med angivelse af: • Navn • CVR-nr. • Adresse • Beskrivelse af behandlingen.	Deloitte har inspiceret, at databehandleraftalerne indeholder en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Deloitte har inspiceret, at oversigten som minimum indeholder de påkrævede oplysninger om de enkelte underdatabehandlere.	Ingen afvigelser konstateret.
F.6	STIL foretager på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, et årligt tilsyn heraf: • Netcompany • Miracle • Amazon Web Services • Statens IT.	Deloitte har inspiceret, at der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlere og overholdelse af underdatabehandleraftaler. Deloitte har inspiceret dokumentation for, at der er foretaget risikovurdering af underdatabehandlere og den aktuelle behandlingsaktivitet hos disse. Deloitte har stikprøvevist inspiceret dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstalt-	Vi har konstateret, at opfølgningen hos Amazon Web Services har fundet sted efter erklæringsperioden. Ingen yderligere afvigelser konstateret.

Kontrolmål F Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, og at STIL ved opfølgning på disses tekniske og organisatoriske sikkerhedsforanstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.			
Nr.	**STIL's kontrolaktivitet**	**Deloittes test**	**Resultat af test**
		ninger, behandlingssikkerheden hos de anvendte underdatabehandlere, tredjelands overførselsgrundlag og lignende.	

Kontrolmål G Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.			
Nr.	**STIL's kontrolaktivitet**	**Revisors udførte test**	**Resultat af revisors test**
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres. Data opbevaret i Cloud-tjenester er krypteret med en stærk, anerkendt algoritme og STIL har krypteringsnøglen. Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	Deloitte har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at personoplysninger alene overføres til tredjelande eller internationale organisationer i henhold til aftale med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Deloitte har inspiceret, at procedurerne er opdaterede. Deloitte har inspiceret dokumentation for, at data i Netprøver.dk, er krypterede og STIL har krypteringsnøglen. Deloitte har inspiceret, at anvendt Cloud-leverandør fremgår af EU-U.S. Data Privacy Framework og dermed er omfattet af EU-Kommissionens tilstrækkelighedsafgørelse ved overførsel til internationale organisationer eller tredjelande.	Deloitte har noteret, at STIL har været opmærksom på visse potentielle problemstillinger relateret til anvendelse af cloud-serviceleverandør, der er underlagt amerikansk lovgivning, frem til 10. juli 2023, hvor tilstrækkelighedsafgørelsen trådte i kraft og dermed ikke længere kræver et overførselsgrundlag for den anvendte cloud-serviceleverandør. Deloitte har fået oplyst, at Netprøver blev flyttet fra Amazon Cloud og hjemtaget til STIL pr. 31. januar 2024. Ingen yderligere afvigelser konstateret.

Kontrolmål H Der efterleves procedurer og kontroller, som sikrer, at STIL kan bistå den dataansvarlige med rettelse og sletning af oplysninger om behandling af personoplysninger, udlevering af sådanne oplysninger til den registrerede eller begrænsning af behandling af personoplysninger.			
Nr.	**STIL's kontrolaktivitet**	**Deloittes test**	**Resultat af test**
H.1	STIL har udarbejdet skriftlige procedurer, som indeholder krav om, at STIL skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Deloitte har inspiceret, at der foreligger formaliserede procedurer for STIL's bistand til den dataansvarlige i relation til de registreredes rettigheder, og at procedurerne er opdateret.	Ingen afvigelser konstateret.
H.2	STIL har udarbejdet procedurer, som, i det omfang dette er aftalt, muliggør rettidig bistand til den dataansvarlige i relation til rettelse og sletning af oplysninger om behandling af personoplysninger, udlevering af sådanne oplysninger til den registrerede eller begrænsning af behandling af personoplysninger.	Deloitte har ved interview forespurgt ansvarlig medarbejder til kontrollen. Deloitte har inspiceret, at STIL's procedurer vedrørende bistand til kunder (Sektoren) i relation til de registreredes rettigheder grundet behandlingens karakter og STIL's aftaler med sine kunder omhandler situationer, hvor kunderne henvender sig med specifikke instrukser, da håndtering af en henvendelse fra en registreret påhviler STIL's kunder. Deloitte har på forespørgsel fået oplyst, at der ikke har været anmodninger om bistand til dataansvarlige.	Ingen afvigelser konstateret.

Kontrolmål I Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med cirkulæreskrivelse, bekendtgørelse og databehandleraftale.			
Nr.	**STIL's kontrolaktivitet**	**Deloittes test**	**Resultat af test**
I.1	STIL har udarbejdet skriftlige procedurer, som indeholder krav om, at STIL skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Deloitte har inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden, og at procedurerne er opdateret.	Ingen afvigelser konstateret.
I.2	STIL har etableret følgende kontroller for identificering af eventuelle brud på persondatasikkerheden: • Awareness hos medarbejdere • Overvågning af netværkstrafik.	Deloitte har inspiceret, at STIL udbyder awareness-træning til medarbejderne i identificering af eventuelle brud på persondatasikkerheden. Deloitte har inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysninger, er etableret systemovervågning med alarmering.	Ingen afvigelser konstateret.
I.3	STIL har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos STIL eller en underdatabehandler.	Deloitte har inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Deloitte har inspiceret, at databehandleren har medtaget eventuelle brud på persondatasikkerheden hos underdatabehandlere i databehandlerens oversigt over sikkerhedshændelser. Deloitte har stikprøvevist inspiceret, at registrerede brud på persondatasikkerheden hos databehandleren eller underdatabehandlerne er meddelt de berørte dataansvarlige uden unødig forsinkelse efter, at databehandleren er blevet opmærksom på brud på persondatasikkerheden.	Ingen afvigelser konstateret.

Kontrolmål I Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med cirkulæreskrivelse, bekendtgørelse og databehandleraftale.			
Nr.	**STIL's kontrolaktivitet**	**Deloittes test**	**Resultat af test**
I.4	STIL har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet. Anmeldelsen skal indeholde en beskrivelse af følgende: • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	Deloitte har inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede procedurer for: • Beskrivelse af karakteren af bruddet på persondatasikkerheden • Beskrivelse af de sandsynlige konsekvenser ved bruddet på persondatasikkerheden • Beskrivelse af de foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. Deloitte har inspiceret dokumentation for, at der ved brud på persondatasikkerheden er truffet foranstaltninger, som har håndteret bruddet på persondatasikkerheden.	Ingen afvigelser konstateret.