Deloitte

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

Telefon: 36102030
www.deloitte.dk

Styrelsen for IT og Læring – Unilogin

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

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 "Bekendtgørelse om den digitale identifikationsløsning Unilogin og opgaver og ansvar for de dataansvarlige og for Styrelsen for It og Læring som databehandler", herefter 'Unilogin-bekendtgørelsen'

Til: Styrelsen for IT og Læring og Sektoren, som anvender systemet Unilogin

Omfang

Vi har fået til opgave at afgive erklæring om Styrelsen for IT og Lærings (herefter 'STIL') beskrivelse i afsnit 3 af STIL's services i henhold til bekendtgørelsen med Sektoren, der anvender STIL's services for 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 serviceunderleverandørerne Nine (udviklingsleverandør) og Statens IT ('SIT' - vedrørende housing). STIL's systembeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos serviceunderleverandørerne. Nærværende erklæring omfatter således ikke kontroltest af kontroller hos underleverandørerne, hvorfor vi ikke har vurderet, hvorvidt relevante kontroller var hensigtsmæssigt udformet, implementeret og fungerede effektivt for perioden 1. januar 2023 til 31. december 2023.

Nogle af de kontrolmål, der er anført i STIL's beskrivelse af sit system, kan kun nås, hvis de komplementerende kontroller hos Sektoren 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, 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 funktionen 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 sit system Unilogin, 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 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 services, 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 services, således som denne var udformet og implementeret i hele perioden 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 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 opnået 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 tests 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 services, 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 system Unilogin, 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 system Unilogin, der har behandlet personoplysninger for dataansvarlige, der er omfattet af databeskyttelsesforordningen for perioden 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 systemet 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 systemets 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 system Unilogin til behandling af personoplysninger foretaget i perioden 1. januar 2023 til 31. december 2023

   (iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af det beskrevne system 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 perioden 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 perioden 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 Unilogin inkl. støttesystemerne Elevadministration, Hugo og Skolegrunddata – herefter alene omtalt som Unilogin, hvor STIL er databehandler for Sektoren (statslige institutioner, privat- og offentligt selvejende institutioner, private institutioner, kommuner og regioner).

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

Hjemlen for anvendelse af Unilogin findes under Bekendtgørelse om den digitale identifikationsløsning Unilogin og opgaver og ansvar for de dataansvarlige og for Styrelsen for It og Læring som databehandler (BEK nr. 529 af 02/05/2019), herefter alene omtalt som Unilogin-bekendtgørelsen.

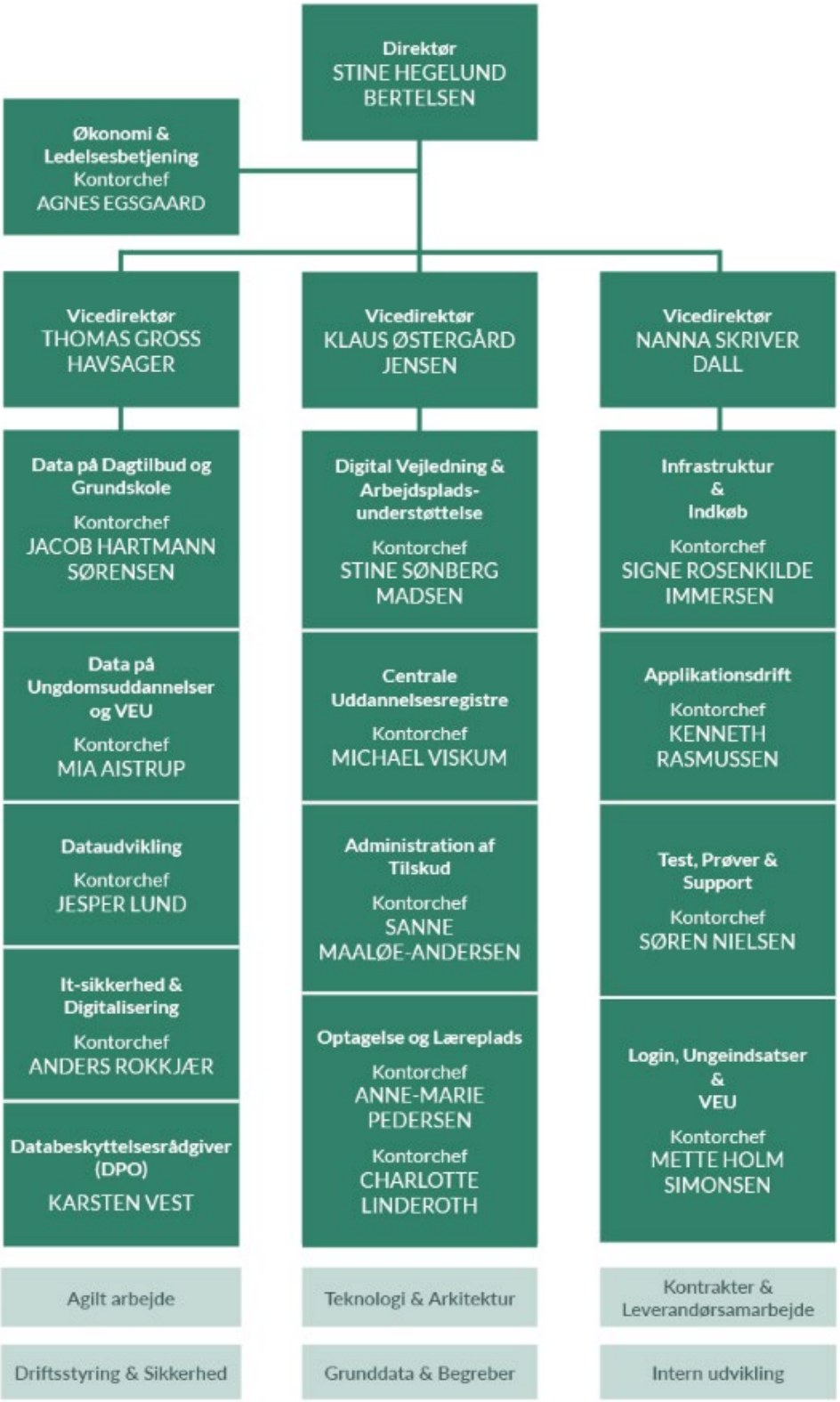
3.1 Ydelsesbeskrivelse

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, herunder Unilogin, for Sektorens behandling af personoplysninger. STIL er databehandler for den behandling, som sker ved brug af Unilogin, da styrelsens behandling af personoplysninger 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

Unilogin har som helt overordnet formål at bidrage til brugervenlig, sikker og fleksibel adgang til den digitale skole og digitale dagtilbud. Unilogin er et digitalt ID for elever, forældre og medarbejdere på institutioner på dagtilbuds- og undervisningsområdet. Det digitale ID styrer elevers, forældres og medarbejderes adgangsrettigheder til pædagogiske og administrative tjenester hos institutionerne.

Unilogin bruges som identifikationsløsning ved en lang række digitale tjenester på Børne- og Undervisningsministeriets område, såsom de nationale tests, digitale prøveafviklingssystemer, de nationale trivselsmålinger m.v. Endvidere bruges Unilogin i institutionernes egne lokale løsninger, såsom digitale læremidler og digitale lærings- og samarbejdsløsninger.
Uddannelses- og dagtilbudsinstitutioner og kommuner er dataansvarlige.

3.2.1 Behandlingen af personoplysninger i Unilogin

Formål
Unilogin er et webbaseret digitalt id for elever, forældre og medarbejdere på institutioner på dagtilbudsområdet og undervisningsområdet. Unilogin giver adgang til nationale tjenester og en lang række pædagogiske services, f.eks. online læremidler.

Styrelsen for It og Læring stiller som databehandler den digitale identifikationsløsning, Unilogin, til rådighed for institutionerne på undervisningsområdet og dagtilbudsområdet til brug for styring af elevers, forældres og medarbejderes adgangsrettigheder til pædagogiske og administrative tjenester. Styrelsen for It og Lærings behandling består i at opbevare personoplysninger i Unilogins Skolegrunddata samt at give private leverandører af digitale læremidler og værktøjer adgang til personoplysninger i Unilogins Skolegrunddata efter dokumenteret instruks fra den dataansvarlige via en af de webgrænseflader, som styrelsen stiller til rådighed for den dataansvarlige.

Unilogin bruges som identifikationsløsning ved en lang række digitale tjenester på undervisningsområdet, såsom de nationale test, Undervisningsministeriets digitale prøveafviklingssystem, de nationale trivselsmålinger m.v. Endvidere bruges Unilogin i institutionernes egne lokale løsninger, såsom digitale læremidler og digitale lærings- og samarbejdsløsninger.

Da Unilogins Skolegrunddata anvendes til styring af adgangsrettigheder – f.eks. i forbindelse med digitale prøver – er det vigtigt, at der kan ske en entydig identifikation af den pågældende bruger.

Dataansvarlig myndighed
Uddannelsesinstitutioner og kommuner

Databehandler
Styrelsen for It og Læring

STIL's underdatabehandler - udvikling
Nine

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 Unilogin behandles følgende personoplysninger
- Navn, adresse, telefonnummer, e-mail,
- CPR-nummer
- Uddannelsesoplysninger,
- Kontaktpersonstatus samt oplysninger om roller og relation.
- Der behandles personoplysninger om elever, kontaktpersoner og medarbejdere i statsinstitutioner, kommuner, regioner og selvejende institutioner på dagtilbudsområdet og undervisningsområdet.

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

- Brugeradministratorer hos den dataansvarlige har adgang til at indtaste, korrigere og slette personoplysninger
- STIL giver adgang til de dataansvarliges øvrige databehandlere efter dokumenteret instruks fra de dataansvarlige via en af de grænseflader, som styrelsen stiller til rådighed. Dette sker gennem systemet Tilslutning, hvor der ikke behandles persondata.

Opbevaring af data

De dataansvarlige har ansvaret for at vedligeholde oplysninger i Unilogin, herunder sletning af personoplysninger, når en elev eller medarbejder ikke er tilknyttet institutionen.

Af hensyn til evt. skoleskift opbevares UniID og CPR-nummer i 12 måneder, men den tidligere institution har ikke adgang til disse oplysninger. Det sikrer, at eleven kan få samme Unilogin-brugernavn på den nye institution. Alle øvrige personoplysninger slettes i Unilogin, så snart institutionen sletter dem fra deres studieadministrative systemer.

Brugere i SkoleGrunddata, som ikke har haft tilknytning til en institution i 12 måneder, slettes. Ved tilknytning forstås, at brugeren er importeret til SkoleGrunddata fra et administrativt system. Brugerens institutionstilknytning kan fjernes (institutionen nedlægges eller brugeren slettes i institutionens import). Derved har brugeren ingen institutionstilknytning.

Sletning medfører, at alle data slettes permanent fra SkoleGrunddata. Unilogin bruger-ID (UniID) fra en slettet bruger kan ikke genbruges.

Der findes brugere med administratorrettigheder til hjælpesystemet ElevAdgang. Sletning varetages af STIL support på den dataansvarlige instruks som en manuel opgave. Brugere med rettigheden slettes på samme vis som alle øvrige brugere, jf. ovenstående afsnit.

3.2.2 Behandlingen af personoplysninger i Elevadministration

Formål

Elevadministrationen er et værktøj for institutioner som har et - af UVM anerkendt - behov for at administrere elever i forbindelse med BUVM's obligatoriske løsninger, men som ikke har mulighed for at anskaffe et elevadministrativt system selv og dermed generere et Unilogin til at tilgå obligatoriske løsninger som nationale tests.

Skolerne er forpligtet til at udstede et Unilogin til deres elever. Det kan de ikke, fordi skolerne er så små, at de ikke har behov for et elevadministrativt system, som er en forudsætning for udstedelse af Unilogin. De kan derfor anvende Elevadministration til indberetninger af data om deres elever og heri få udstedt et Unilogin. Skolerne indtaster og korrigerer selv data til brug for udstedelse.

Dataansvarlig myndighed

Uddannelsesinstitutioner og kommuner

Databehandler

Styrelsen for It og Læring

STIL's underdatabehandler - udvikling

Nine

STIL's underdatabehandler – drift, vedligehold

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

I Elevadministration behandles følgende personoplysninger

- Navn
- CPR-nr.
- Adresse

- Klasse
- Klassetrin
- Oplysninger om forældre.

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

- Medarbejdere på en skole, som har en medarbejdersignatur udstedt af skolen eller kommunen og samtidigt har fået tilknyttet rettigheden "Elevadministration" til deres medarbejdersignatur.
- Medarbejdere i STIL kan ikke se data i systemet på brugergrænsefladen – kun data registreret på institutioner med STIL's CVR-nummer (testdata).
- Medarbejdere i STIL kan se alle institutioners data i Brugeroversigt.stil.dk for at kunne understøtte institutionerne i supportsammenhæng.

Opbevaring af persondata

Der er ikke automatisk sletning i systemet. Skolerne kan selv slette eleverne. Det gør de årligt i forbindelse med oprulning af eleverne til de næste klassetrin. Når eleven ikke længere går på skolen, eller når eleven er gået ud af højeste klassetrin (9./10.klasse), kan eleven ikke oprulles mere og bliver derfor slettet af skolens medarbejdere.

3.3 Underdatabehandlere

System	Udviklingsleverandør	Infrastruktur
Unilogin	Nine	Housing hos SIT

3.4 Risikovurdering

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 forelægges løbende information om større risici, samt hvilke tekniske eller organisatoriske sikkerhedsforanstaltninger, der er sat i værk for at mitigere disse. Dertil bliver ledelsen halvårligt forelagt en samlet status på hele risikovurderingsarbejdet. Pågældende kontorchefer og (vice)direktører forholder sig løbende til håndtering af risici, når der er behov for dette.

3.5 Kontrolforanstaltninger

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

- Generelle procedurer for behandling af personoplysninger - Unilogin-bekendtgørelsen (kontrolmål A)
- Tekniske sikkerhedsforanstaltninger (kontrolmål B)
- Organisatoriske foranstaltninger (kontrolmål C)
- Sletning og tilbagelevering af personoplysninger (kontrolmål D)
- Opbevaring af personoplysninger (kontrolmål E)
- Anvendelse af underdatabehandlere (kontrolmål F)
- 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.

3.5.1 Generelle procedurer for behandling af personoplysninger - Unilogin-bekendtgørelsen (kontrolmål A)

Formål
Der efterleves procedurer og kontroller, som sikrer at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med Unilogin-bekendtgørelsen.

Anvendte procedurer og kontroller
STIL har implementeret procedurer og kontroller, der skal sikre, at det juridiske dokument (Unilogin-bekendtgørelsen), som ligger til grund for behandlingen af personoplysninger, løbende opdateres ift. den konkrete behandling. Ved ændringer af systemet, herunder nye/ændrede persondatabehandlinger, er der procedurer for opdatering af fortegnelsen.

Procedurerne tager udgangspunkt i den vedtagne informationssikkerhedspolitik, som er gældende for hele BUVM og herunder STIL, hvor der er angivet de styrende dokumenter i ministeriets ledelsessystem for informationssikkerhed. Herunder kan nævnes en række politikker, retningslinjer, skabeloner og dokumentation for behandling af personoplysninger. De forskellige dokumenter kan tilgås på IT-Kanalen, ministeriets 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 Unilogin-bekendtgørelsen, har STIL udarbejdet en retningslinje og en politik for brugeradministration.

3.5.2 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.

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 end-point 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 databaseserverne. 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 firewall-ændringer
- **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 eks. 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 penetrationstests:** Der er retningslinjer for sårbarhedsscanninger og penetrationstests. Der gennemføres sårbarhedsscanninger hvert halve år. Det gælder hele

STIL's infrastruktur. Sårbarhedsscanningerne foregår på IP-niveau. og foretages fra "indersiden" dvs. bag ved firewall. Såfremt der identificeres problemstillinger for de enkelte systemer, iværksættes plan for mitigering. Penetrationstest bestilles løbende iht. retningslinje herfor. 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). Ift. hjemmesider, så er det en del af de 20 tekniske minimumskrav, der løbende kontrolleres af STIL
- **Relevante opdateringer og patches, herunder sikkerhedspatches:** STIL varetager installationen og monitoreringen omkring sikkerhedspatches på infrastruktur
- **Fysisk adgangssikkerhed:** Serverne til Unilogin 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 med 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.

Brugeradministrationen af de eksterne konsulenter, der er oprettet hos SIT (X konsulenter), tildeles rettigheder til de enkelte systemer på samme vis som STIL's medarbejdere i ServiceNow. Oprettelse og nedlæggelse af X-konsulenter sker enten ved at kontakte 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 konsulenters/udvikleres tidsbegrænsede adgang 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 datacentrene, der som udgangspunkt ikke tildeles 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 medarbejderens adgang i SIT AD – typisk indenfor 1-1,5 uge. Herefter inaktiveres medarbejderen i ServiceNow, som udsender notifikationer til relevante mhp. brugernedlæggelse i fagsystemer, hvor det er registreret, at den pågældende har adgang.

STIL har for systemernes underliggende databaser gennemført en proces med at centralisere alle databaser på databasehotelservere for at minimere antallet af teknikere, som har adgang til STIL's databaser og for sikre, at der ikke anvendes fælles brugerkonti. Centraliseringen til databasehoteller er gennemført for alle Postgres og Oracle databaser. Centraliseringen af MSSQL-databaser forventes påbegyndt i 2023. Det er kun databaseadministratorer, der har nøglebaseret adgang (certifikater) til databasehotellerne, og al ind logning registreres i lokale logs samt centralt i Nagios logserver.

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 logge 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; f.eks. følsom eller almindelig 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 logge: Hændelseslogning af brugeraktivitet, undtagelser, fejl og tegn på informationssikkerhedshændelser. Den indsamlede log skal opbevares korrekt og fejlmeldinger gennemgås jævnligt. Kontorchefen (kan uddelegeres til PO) 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 ift. risikovurdering eller ved større behov for fejlsøgning. Kontorchefen er ansvarlig for, at det årligt vurderes, hvorvidt længden af opbevaringsperioden fortsat matcher systemets behov.

For at sikre mod manipulation eller sletning, logges alle adgangshændelser på alle miljøer, og disse overføres til SIEM-systemet Nagios (STIL's centrale logserver). Alle logs, som opbevares i Nagios, gemmes i 13 måneder.

3.5.3 Organisatoriske sikkerhedsforanstaltninger (kontrolmål C)

Formål
Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske sikkerhedsforanstaltninger 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 om 3.5.2 om brugerstyring. Samtidigt er der procedurer, der sikrer, at medarbejderens aktiver som pc-udstyr, mobiltelefon, legimitationskort og evt. nøgler til STIL indsamles.

3.5.4 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 politik for informationssikkerhed 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.

STIL har ansvaret for opbevaring af personoplysninger i Unilogin.

3.5.5 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 Unilogin-bekendtgørelsen. Det er kommunikeret til alle relevante medarbejdere i STIL. STIL har udarbejdet procedure for udførte behandlingsaktiviteter i Unilogin.

3.5.6 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 Unilogin-bekendtgørelsen. STIL fører årligt tilsyn med underdatabehandlere gennem indhentning af revisionserklæring, tilsynsrapport og besvarelse af en række tilsynsspørgsmål. Derudover er der løbende dialog med underdatabehandlere i form af statusmøder, afrapportering mv.

3.5.7 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 ift. 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.

3.5.8 Sikkerhedsbrud (kontrolmål I)

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

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 Sektoren om STIL's services og kontroller, som kan påvirke behandlingen af personoplysninger, og samtidig informere de dataansvarlige, for hvem STIL behandler personoplysninger, om implementering 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.

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 Kontrolmål, kontroller og resultater af test

Vores test af kontrollernes udformning 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 bekendtgørelse.			
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.	Ingen afvigelser konstateret.
A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Deloitte har forespurgt, hvordan ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Deloitte har inspiceret, at instruks fremgår i bekendtgørelse. Deloitte har inspiceret, at der er procedurer, der sikrer, at der alene udføres behandling af personoplysninger, som fremgår af 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. Deloitte har inspiceret, at der er procedurer for underretning af dataansvarlige, i tilfælde hvor behandling af personoplysninger vurderes at være i strid med lovgivningen.	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.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikkerhedsforanstaltninger for behandling af personoplysninger i overensstemmelse med bekendtgørelse. 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 bekendtgørelse og konstateret, at de instruerede sikkerhedsforanstaltninger er etableret.	Ingen afvigelser konstateret.
B.2	STIL har foretaget en risikovurdering med udgangspunkt i Unilogin-applikationen og på baggrund heraf taget stilling til de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed i applikationen.	Deloitte har inspiceret, at den foretagne risikovurdering er opdateret og omfatter forskellige scenarier med udgangspunkt i generel behandlingssikkerhed. Deloitte har inspiceret, at STIL har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen.	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 forespurgt, om der for de systemer, der anvendes til behandling af personoplysninger, er installeret antivirussoftware. Deloitte har inspiceret, at der er installeret antivirus på klienter og systemer, som løbende opdateres. Deloitte har inspiceret, at antivirussoftwaren 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.	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.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. Deloitte har forespurgt, om ekstern adgang til systemer alene tilgås gennem en sikret firewall. Deloitte har inspiceret, at ekstern adgang til systemer, der anvendes til behandling af personoplysninger, alene sker gennem en sikret firewall.	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.
B.6	Adgang til personoplysninger i applikationen Unilogin er begrænset til et antal 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 Unilogin-applikationen har tekniske foranstaltninger indbygget, som understøtter opretholdelse af begrænsning i brugernes arbejdsbetingede adgang til 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 stikprøvevist inspiceret, at autorisationer til systemer og data er godkendt og begrænset til medarbejderes arbejdsbetingede behov.	
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.
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 autentikation.	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	Deloitte har inspiceret, at der er opsat logning af brugeraktiviteter, der anvendes til behandling og transmission af personoplysninger. Deloitte har inspiceret, at logning af brugerak-	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**
	• Login-information. Logoplysninger er beskyttet mod manipulation og tekniske fejl.	tiviteter er konfigureret og aktiveret. Deloitte har inspiceret, at opsamlede oplysninger om brugeraktivitet i logge 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.	
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 penetrationstests.	Deloitte har forespurgt, om der løbende foretages test gennem sårbarhedsscanninger og penetrationstests. Deloitte har inspiceret, at der løbende foretages sårbarhedsscanninger og en gang årligt foretages en penetrationstest.	Vi har konstateret, at der ikke er udført penetrationstest af Unilogin i 2023. Vi har fået oplyst, at Unilogin blev penetrationstestet i 2022, og Unilogin er penetrationstestet igen i Q2 2024.

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**
			Ingen yderligere 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.
B.13	STIL har etableret en formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange, som dækker applikationen Unilogin.	Deloitte har inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang. Deloitte har stikprøvevist på tiltrådte medarbejders adgange til systemer og databaser inspiceret, at tildelte brugeradgange er godkendt, og at der er et 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.	Ingen afvigelser konstateret.
B.14	Adgang til applikationen Unilogin, hvori der sker behandling af personoplysninger, er opsat med password login.	Deloitte har inspiceret, at der foreligger en procedure for anvendelse af passwords, som	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**
		ledelsen har behandlet og godkendt inden for erklæringsperioden. Deloitte har inspiceret passwordkonfigurationen for Unilogin og vurderet, at denne er i overensstemmelse med proceduren herfor.	
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. 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.	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.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 informationssikkerhedspolitik, som ledelsen har behandlet og godkendt indenfor erklæringsperioden. Deloitte har inspiceret, at informationssikkerhedspolitik er gjort tilgængelige for alle STIL's medarbejdere.	Ingen afvigelser konstateret.
C.2	STIL har sikret, at de aftalte sikkerhedsforanstaltninger til enhver tid overholder de gældende organisatoriske og tekniske sikkerhedskrav og ikke er i strid med Unilogin-bekendtgørelsen.	Deloitte har inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikkerhedsforanstaltninger og behandlingssikkerheden i Unilogin-bekendtgørelsen. Deloitte har inspiceret, at kravene i 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.
C.4	Ved ansættelse underskriver medarbejdere 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.	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**
		Deloitte har stikprøvevist inspiceret, at nyansatte medarbejdere er blevet introduceret til informationssikkerhedspolitikken og relevant information for persondatabehandling.	
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 stikprøvevist for fratrådte medarbejdere 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 stikprøvevist for fratrådte medarbejdere inspiceret, at der er dokumentation for opretholdelse af fortrolighedsaftale og generel tavshedspligt.	Ingen afvigelser konstateret.
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.	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**
		Deloitte har inspiceret dokumentation for, at relevante medarbejdere, som enten har adgang til eller behandler personoplysninger, har deltaget i awareness-træning i perioden.	

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. Deloitte har inspiceret, at der er overensstemmelse mellem Unilogin-bekendtgørelsen.	Ingen afvigelser konstateret.
D.2	Der er aftalt følgende specifikke krav til STIL's opbevaringsperioder og sletterutiner: • Personoplysninger opbevares i 12 måneder, hvorefter det slettes i Unilogin.	Deloitte har inspiceret, at der foreligger procedurer for opbevaring og sletning, som indeholder de specifikke krav til STIL's opbevaringsperioder og sletterutiner. Deloitte har inspiceret, at der er etableret funktionalitet i Unilogin, som sikrer, at personoplysninger kan slettes i overensstemmelse med 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 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. STIL har udarbejdet procedure for udførte behandlingsaktiviteter i Unilogin.	Deloitte har inspiceret, at der foreligger formaliserede procedure for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til Unilogin-bekendtgørelsen, og at proceduren er opdateret. Deloitte har inspiceret, at der er dokumentation for, at databehandlingen sker i henhold til Unilogin-bekendtgørelsen. Deloitte har inspiceret, at STIL har udarbejdet en procedure, som samlet nævner, hvilke behandlingsaktiviteter, der foretages i Unilogin.	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 etableret krav ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks, som er i overensstemmelse med de krav, som STIL er underlagt at følge.	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 cirkulæreskrivelse indeholder retningslinjer for STIL's anvendelse af underdatabehandlere. Deloitte har baseret på forespørgsler fået bekræftet, at anvendte underdatabehandlere for Unilogin er i overensstemmelse med gældende retningslinjer og krav.	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 aftaler 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, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring, tilsyn eller lignende. Kontrol udføres for følgende leverandører: • Nine • Statens IT (SIT)	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-	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**
		ninger, behandlingssikkerheden hos de anvendte underdatabehandlere, tredjelands overførselsgrundlag og lignende.	

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 skriftlig procedure, 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. Deloitte har inspiceret, 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 Unilogin-bekendtgørelsen.			
Nr.	**STIL's kontrolaktivitet**	**Deloittes test**	**Resultat af test**
I.1	STIL har udarbejdet skriftlig procedure, 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 proceduren er opdateret. Deloitte har inspiceret, 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	Ingen afvigelser konstateret.

Kontrolmål I Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med Unilogin-bekendtgørelsen.			
Nr.	**STIL's kontrolaktivitet**	**Deloittes test**	**Resultat af test**
		blevet opmærksom på brud på persondatasikkerheden.	
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, at der ved brud på persondatasikkerheden er truffet foranstaltninger, som har håndteret bruddet på persondatasikkerheden.	Ingen afvigelser konstateret.