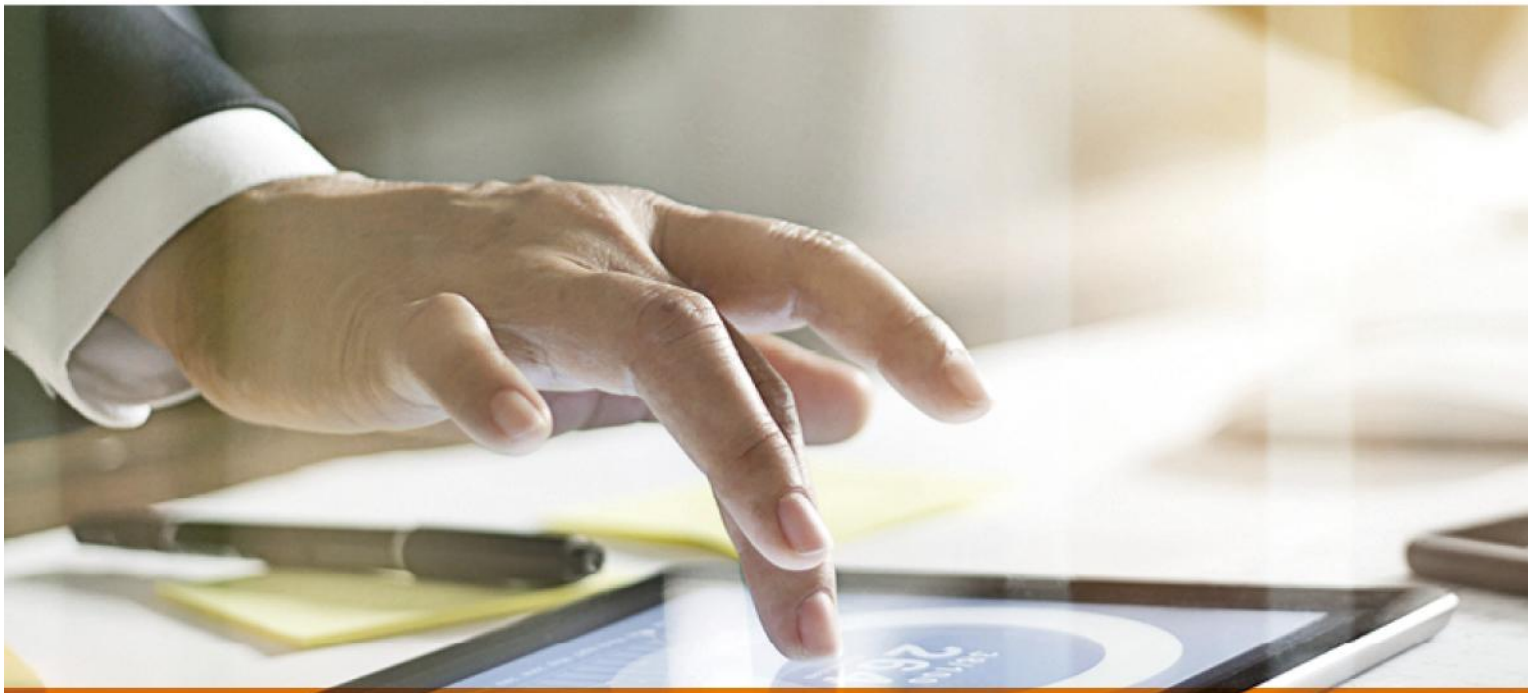
BEIERHOLM
VI SKABER BALANCE



APRIL 2024

IST APS

ISAE 3000 ERKLÆRING

CVR 25545079

Uafhængig revisors erklæring med sikkerhed om informationssikkerhed og foranstaltninger i forhold til databehandleraftale på IST Skoleadministration.

Beierholm
Statsautoriseret Revisionspartnerselskab
Knud Højgaards Vej 9
2860 Søborg
CVR 32 89 54 68
Tlf +45 39 16 76 00

www.beierholm.dk

Erklæringsopbygning

Kapitel 1:

Ledelseserklæring.

Kapitel 2:

Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet.

Kapitel 3:

Beskrivelse af informationssikkerhed og foranstaltninger i forhold til databehandling på IST Skoleadministration.

Kapitel 4:

Kontrolmål, kontrolaktivitet, tests og resultater heraf.

KAPITEL 1:

Ledelseserklæring

IST ApS behandler personoplysninger på vegne af kunder i henhold til databehandleraftale i tilknytning til anvendelse af IST Skoleadministration.

Medfølgende beskrivelse er udarbejdet til brug for kunder og deres revisorer, der har anvendt IST Skoleadministration, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som kunderne dvs. de dataansvarlige selv har udført, ved vurdering af, om kravene til kontrolmiljøet samt databeskyttelsesforordningen er overholdt.

IST ApS bekræfter, at:

(A) Den medfølgende beskrivelse, kapitel 3, giver en retvisende beskrivelse af databehandling i relation til IST Skoleadministration i hele perioden fra 1. april 2023 - 31. marts 2024. Kriterierne for dette udsagn er, at den medfølgende beskrivelse:

(i) Redegør for, hvordan kontrollerne er 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, registrere, behandle samt om nødvendigt korrigere, slette og begrænse behandling af personoplysninger**
- **De processer, der er anvendt for 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 sikringsforanstaltninger for behandlingen af personoplysninger under hensyntagen til de risici, som behandling udgør, navnlig ved såvel hændelige som ulovlige handlinger som 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 IST Skoleadministrations 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 de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger**

(ii) Indeholder relevante oplysninger om ændringer til IST Skoleadministration i forbindelse med behandling af personoplysninger foretaget i perioden 1. april 2023 - 31. marts 2024.

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne kontroller under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og derfor ikke kan omfatte ethvert aspekt ved kontroller, som den enkelte kunde måtte anse som vigtig efter deres 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. april 2023 - 31. marts 2024. Kriterierne for dette udsagn er, at:**

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

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

(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. april 2023 - 31. marts 2024.**

(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 databehandlere i henhold til databeskyttelsesforordningen.**

Roskilde, den 2. april 2024

Anne Brink Pedersen, Adm. direktør **Janne Veng, Data Security Manager**

IST ApS, Gammel Marbjergvej 9, 4000 Roskilde, CVR 25545079

KAPITEL 2:

Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet

Til brugere af IST Skoleadministration og deres revisorer

Omfang

Vi har fået som opgave at afgive erklæring om beskrivelsen i kapitel 3, som er en beskrivelse af informationssikkerhed og foranstaltninger i forhold til databehandling på IST Skoleadministration i hele perioden fra 1. april 2023 - 31. marts 2024 og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Erklæringen er afgivet efter den partielle metode, hvilket betyder, at denne erklæring ikke omfatter de it-sikkerhedsmæssige kontroller og kontrolaktiviteter, som er tilknyttet i forbindelse med anvendelse af eksterne samarbejdspartnere. Disse underleverandører er nærmere oplistet i databehandleraftaler og tilhørende bilag med kunder.

Erklæringsopgaven dækker ikke kundespecifikke forhold. Desuden dækker erklæringen ikke de komplementerende kontroller og kontrolaktiviteter, som udføres af de dataansvarlige.

Vores konklusion udtrykkes med høj grad af sikkerhed.

IST ApS' ansvar

IST ApS er ansvarlig for udarbejdelsen af beskrivelsen i kapitel 3 og den medfølgende ledelseserklæring i kapitel 1, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen er præsenteret; for leveringen af de ydelser beskrivelsen omfatter, for at anføre kontrolmålene samt for udformningen, implementeringen og effektivt fungerende kontroller for at nå de anførte kontrolmål.

Beierholms uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i FSR – danske revisorers retningslinjer for revisors etiske adfærd (Etiske regler for revisorer), der bygger på de grundlæggende principper om integritet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

Vi er underlagt international standard om kvalitetsstyring, ISQM 1, og anvender og opretholder således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og krav ifølge lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om IST ApS' 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. Denne standard kræver, at vi planlægger og udfører vores handlinger for 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 funktionen af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af IST Skoleadministration 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 sådanne 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 IST ApS har specificeret og beskrevet i kapitel 3.

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

Begrænsninger i kontroller hos IST ApS

IST ApS' beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved systemet, 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 datasikkerheden. Herudover er fremskrivningen af enhver vurdering af funktionaliteten 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 kriterier, der er beskrevet i kapitel 1 i ledelsens erklæring. Det er vores opfattelse,

a) at beskrivelse af informationssikkerhed og foranstaltninger i forhold til databehandling på IST Skoleadministration, således som det var udformet og implementeret i hele perioden fra 1. april 2023 - 31. marts 2024, i alle væsentlige henseender er retvisende, og

b) at kontrollerne, som knyttede sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 1. april 2023 - 31. marts 2024.

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. april 2023 - 31. marts 2024.

Beskrivelse af testede kontroller

De specifikke kontroller, der er testet, samt arten, den tidsmæssige placering og resultater af disse test fremgår af kapitel 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen er udelukkende tiltænkt de kunder, der har anvendt IST Skoleadministration og deres revisorer, som har en tilstrækkelig forståelse til at overveje dem sammen med anden information, herunder information om kontroller, som kunderne dvs. de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen er overholdt.

Søborg, den 3. april 2024

Beierholm
Statsautoriseret Revisionspartnerselskab
CVR-nr. 32 89 54 68

Kim Larsen
Statsautoriseret revisor

Jesper Aaskov Pedersen
IT-auditor, Director

KAPITEL 3:

Beskrivelse af informationssikkerhed og foranstaltninger i forhold til databehandling på IST Skoleadministration

Indledning og omfang

Formålet med nærværende beskrivelse er at levere information til IST ApS′ kunder i forbindelse med leveringen af IST Skoleadministration, hvor IST ApS fungerer som databehandler på vegne af kunderne.

Beskrivelsen giver et retvisende billede af organisationen, systemerne og kontrollerne for indsamling, opbevaring og andre former for behandling af personoplysninger i forbindelse med levering af IST ApS' Service IST Skoleadministration. De udførte kontroller omfatter standardprocesser og -leverancer i IST ApS og med udgangspunkt i IST ApS′ standard databehandleraftale for Servicen, hvorfor kundespecifikke forhold ikke er omfattet af denne erklæring.

Omfanget af beskrivelsen er en afdækning af de tekniske og organisatoriske sikringsforanstaltninger til sikring af personoplysninger, som er implementeret i forbindelse med IST ApS′ Service IST Skoleadministration.

IST Skoleadministration kan omfatte IST ApS′ Servicevarianter, som kan inkludere løsningerne IST Elevadministration, IST Tjenestetid, IST Personkreds, samt moduler, der kan tilknyttes de forskellige løsninger.

Beskrivelse af IST ApS og databehandling

IST ApS er en del af den svenskejede koncern IST Group AB, som blev grundlagt i 1982. IST ApS beskæftiger ca. 105 medarbejdere, som er fordelt på to kontoret i hhv. Roskilde og Midtfyn.

I 2013 opkøbte IST Group AB den danske virksomhed Tabulex ApS, som blev stiftet i 1998, og i 2017 ekspanderede IST ApS med købet af virksomheden UDDATA til også at omfatte ungdomsuddannelser.

IST ApS udvikler, drifter og vedligeholder software-as-a-service (SaaS) løsninger til IST ApS′ kunder, der omfatter offentlige og private uddannelsesinstitutioner, herunder dagtilbud, grundskole, ungdomsuddannelser og FGU. IST ApS tilbyder bl.a. løsninger til elevadministration, skemalægning og medarbejdernes arbejdstid. Med løsningerne fra IST ApS er det nemt for brugerne at samle alt til administrationen af dagtilbuddet eller skolen ét sted.

Leverancen omfatter drift, service og support, konsulentydelser og kurser. Systemerne udvikles løbende, herunder også tilpasning af funktionalitet, således at systemerne lever op til gældende lovgivning og reguleringer. Alle vores systemer udvikles, drives og forvaltes af dygtige medarbejdere med base i Danmark og i samarbejde med vores kollegaer i IST Group AB. IST Group AB har ansatte i Sverige, Norge, Tyskland og Danmark.

IST ApS leverer løsninger til stort set alle 98 kommuner i Danmark, samt mange uddannelsesinstitutioner, og er den førende leverandør på markedet. Udviklingen af løsningerne sker i tæt samarbejde med brugerne, domæneeksperter og udviklere med stor viden om forvaltningsområdet.
Ca. halvdelen af medarbejderne i IST ApS har en baggrund fra uddannelsesverden. Det giver os en god indsigt i brugernes udfordringer og behov og et godt grundlag for at yde god og brugbar support til brugerne.

IST ApS' it-services understøtter kundernes arbejdsprocesser i forbindelse med daginstitutions-, fritids-tilbuds-, ungdomsskole-, folkeskole-, ungdoms- og efteruddannelsesområderne. IST ApS ejer ikke data, som kunderne indsamler, men udvikler og driver de it-services, som kunderne anvender til at udføre den nødvendige persondatabehandling. Ifølge EU Databeskyttelsesforordningen og de danske supplerende bestemmelser (Databeskyttelsesloven) er IST ApS databehandler, og kunden er dataansvarlig. IST ApS samarbejder med juridiske eksperter med henblik på at sikre, at alle relevante juridiske krav er identificeret og imødekommet. IST ApS har også sørget for at have relevante kontrakter med alle nøgleinteressenter (herunder kunder, samarbejdspartnere, nøgleleverandører osv.) med henblik på at sikre overholdelse af loven. Desuden samarbejder IST ApS med sine kunder om at sikre, at kunderne er bekendt med og overholder de relevante GDPR-regler.
Hvilke kategorier af registrerede personer og typer af personoplysninger, der er omfattet af databehandlingen, afhænger af aftalen med den dataansvarlige og hvilken løsning, det drejer sig om.

Al behandling af personoplysninger er styret af politikker og procedurer. IST ApS arbejder med en struktureret metode og er ISO9001 certificeret for at sikre, at alle processer og politikker er beskrevet i vores kvalitetsstyringssystem og ISMS. Sammen med vores ISO27001+2 sikkerhedsarbejde, sikrer dette ensartethed og minimering af fejl, samt sikrer uafhængighed af enkeltpersoner. Incidents eller afvigelser af it-sikkerhedsrelateret karakter behandles løbende og rapporteres på månedlige møder på baggrund af faste procedurer for håndtering af afvigelser.

Forankringen af it-sikkerhedsarbejdet i virksomheden er sikret med ansvaret i ledelsen og informationssikkerhedskonsulenten. Ledergruppen og informationssikkerhedskonsulenten arbejder sammen om at højne opmærksomheden på regler og procedurer blandt medarbejderne.

Kontrolmål

For at støtte vores rolle som databehandler, har IST udviklet og implementeret procedurer og kontroller til at hjælpe os med at overholde Databeskyttelsesforordningen. De indførte procedurer og kontroller er nærmere beskrevet nedenfor.

Behandling af personoplysninger (Kontrolområde A)

IST ApS har etableret procedurer og kontroller som sikre, at personoplysninger behandles i henhold til instruks i databehandleraftalen. Der foretages løbende vurdering af, om procedurerne skal opdateres.

IST ApS indgår databehandleraftaler med sine kunder. Databehandleraftalen indgår som en fastlagt procedure ved kontraktindgåelse, og der benyttes enten IST ApS' egen skabelon, der er baseret på Datatilsynets skabelon, eller kundens skabelon. Disse aftaler beskriver IST ApS' rolle og ansvar som databehandler. Databehandleraftalerne indeholder information om anvendelsen af underdatabehandlere. Alle databehandleraftaler opbevares elektronisk.

Som databehandler arbejder IST ApS med personoplysninger på baggrund af instrukser fra kunderne, der beskriver en formålsafgrænsning for, hvad data må benyttes til. IST ApS er således ansvarlig for, at data indsamlet med ét formål ikke behandles i strid med dette.

Tekniske foranstaltninger (Kontrolområde B)

IST ApS har etableret tekniske foranstaltninger, som er vurderet relevante for behandlingen af personoplysninger for den dataansvarlige.

IST ApS har implementeret passende tekniske foranstaltninger for at tage vare på for vores informationssikkerhed. Dette bliver understøttet gennem implementering af et Information Security Management System (også kaldt ISMS) i overensstemmelse med ISO 27001/2.

IST ApS har ift. it-sikkerhedsstrategien valgt at tage udgangspunkt i ISO27001/2, og har således brugt ISO-metodikken til at implementere de relevante sikringsforanstaltninger inden for følgende områder:

- **Informationssikkerhedspolitikker**
- **Organisering af informationssikkerhed**
- **Medarbejdersikkerhed**
- **Styring af aktiver**
- **Adgangsstyring**
- **Kryptografi**
- **Fysisk sikkerhed og miljøsikring**
- **Driftssikkerhed**
- **Kommunikationssikkerhed**
- **Leverandørforhold**
- **Styring af informationssikkerhedsbrud**
- **Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring**
- **Overensstemmelse med lov- og kontraktkrav**

IST ApS udgiver en revisorerklæring af typen ISAE 3402 type II, hvor der kan findes en dybdegående beskrivelse af områderne ovenfor.

Organisatoriske foranstaltninger (Kontrolområde C)

Det er IST ApS' strategi, at der i forretningen skal være indbygget den nødvendige sikkerhed, så selskabet ikke påføres uacceptable risici.

Som leverandør til offentlige og private uddannelsesinstitutioner arbejder IST ApS med informationssikkerhed på et forretningsstrategisk niveau. Dette grundet de mange personoplysninger, som håndteres i vores systemet. IST ApS' målsætning er at være kundernes professionelle samarbejdspartner, der forsvarligt håndterer data, som de betror til os.

Ledelsen hos IST ApS har det daglige ansvar for it-sikkerhed, og derved sikres det, at de overordnede krav og rammer for it-sikkerhed er overholdt. Gennem den centrale it-sikkerhedspolitik har ledelsen beskrevet IST ApS' struktur for it-sikkerhed. It-sikkerhedspolitikken skal som minimum revideres én gang årligt. It-sikkerhedspolitikken er udarbejdet, så IST ApS har ét fælles regelsæt. Dermed opnår vi et stabilt driftsmiljø og et højt sikkerhedsniveau. Vi foretager løbende forbedringer af både politikker, procedurer og den operationelle drift.

Vi arbejder med faste procedurer for bl.a. rekruttering, ansættelse og fratrædelser. Nye medarbejdere gennemgår et introduktionsforløb til alle afdelinger i virksomheden. Forløbet omfatter en introduktion i informationssikkerhed, der omhandler it-sikkerhedsregler, introduktion til informationssikkerhedsorganisationen, god it-adfærd, dataklassifikation og særligt fokus på IST ApS' rolle som databehandler. IST ApS indhenter ved ansættelse underskrift fra medarbejderen på en erklæring, hvori medarbejderen tilslutter sig virksomhedens regler for omgang med kundedata, og at medarbejderen er blevet gjort bekendt med hvilket lovgrundlag, der er gældende.

Alle medarbejdere har en fortrolighedsklausul i deres ansættelseskontrakter. Som en del af vores fratrædelsesprocedure indgår en exit-samtale med nærmeste leder, hvor vi minder om, at fortrolighedsklausulen fortsat er gældende efter endt ansættelse. Ved brug af eksterne konsulenter, benytter vi en NDA-skabelon.

For at sikre en kontinuerlig tilgang til informationssikkerhedskulturen har IST ApS en plan for awareness-kampagner. Planen beskriver, hvilke emneområder, der skal arbejdes med i løbet af et år. Planen revurderes årligt af informationssikkerhedsorganisationen.

IST ApS er ejet af IST Group AB, som er en virksomhed med hovedsæde i Växjö i Sverige. IST Group AB har en central forretningsstøtteenhed, Corporate Services, der servicerer de enkelte regioner med funktioner, der understøtter forretningen. Virksomhedens har en fælles ekstern Databeskyttelsesrådgiver.

Sletning og tilbagelevering (Kontrolområde D)

IST ApS må kun slette eller tilbagelevere personoplysninger i overensstemmelse med databehandleraftalen indgået med den dataansvarlige.

IST ApS har etableret procedurer som sikrer, at den dataansvarliges data bliver returneret eller slettet i overensstemmelse med den dataansvarliges instruks som specificeret i databehandleraftalen og i overensstemmelse med IST politikker ved henvendelse fra den dataansvarlige eller ophør af samarbejde.

Opbevaring af personoplysninger (Kontrolområde E)

IST ApS har etableret procedurer og kontroller for at sikre, at databehandleren udelukkende vil opbevare personoplysninger i overensstemmelse med databehandleraftalen med den dataansvarlige. Procedurer revurderes løbende.

IST ApS udarbejder fortegnelser over behandlingsaktiviteter, som løbende opdateres og opbevares elektronisk.

Opbevaring af personoplysninger er kun på lokationer, der er godkendt af kunden, herunder opbevaring af personoplysninger hos underdatabehandlere.

Underdatabehandlere (Kontrolområde F)

IST ApS har implementeret procedurer og kontroller for at sikre, at der udelukkende anvendes underdatabehandlere, der er godkendt af den dataansvarlige.
IST ApS indgår databehandleraftaler med underdatabehandlere og pålægger underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen med de dataansvarlige.
Der føres løbende tilsyn med underdatabehandlere for at sikrer tilstrækkelig behandlingssikkerhed af personoplysninger. Tilsynet er baseret på en vurdering underdatabehandlerens aktiviteter i de pågældende løsninger.

Den dataansvarlige orienteres i overensstemmelse med databehandleraftalen, såfremt det planlægges at anvende en ny underdatabehandler eller ved ændringer i forbindelse med eksisterende underdatabehandlere.

Overførsler til tredjelande / internationale organisationer (Kontrolområde G)

IST ApS har implementeret procedurer og kontroller for at sikre, at der kun overføres personoplysninger til tredjeland eller internationale organisationer i overensstemmelse med aftale med den dataansvarlige. Procedurer revideres løbende.

I databehandleraftalen mellem IST ApS og vores kunder indgår der beskrivelse af, om der må ske overførsel af personoplysninger til tredjeland.

Ved anvendelse af en underdatabehandler anvendes ISTs Data Transfer Location Guidelines, der beskæftiger sig med overførsel af personoplysninger og fastslår, at enhver overførsel udenfor EU/EØS skal være i overensstemmelse med Databeskyttelsesforordningen. Herunder overvejelser om tilstrækkeligt juridisk grundlag og supplerende foranstaltninger.

Bistå den dataansvarlige (Kontrolområde H)

IST ApS har implementeret procedurer og kontroller for at sikre, at vi som databehandler kan assistere den dataansvarlige med at udlevere, korrigere, slette eller begrænse oplysninger om behandlingen af personoplysninger.

IST har defineret interne procedurer og retningslinjer om, hvordan man skal håndtere forespørgsler fra de registrerede. I overensstemmelse med vores procedure imødekommer IST ApS ikke en forespørgsel fra en registreret med mindre den dataansvarlige er underrettet og involveret. Der vil kun blive videregivet oplysninger til den registrerede, hvis der forinden er skriftligt samtykke fra den dataansvarlige.

I overensstemmelse med databehandleraftalen, vil IST ApS bistå den dataansvarlige på anmodning i forbindelse med revision og inspektion af databehandleren, samt hvis den dataansvarlige modtager individuelle forespørgsler fra registrerede, der har forbindelse til IST ApS' behandling af personoplysninger.

Sikkerhedsbrud (Kontrolområde I)

IST ApS har etableret procedurer og kontroller som sikrer, at registrering, håndtering og evaluering af et brud på persondatasikkerheden er i overensstemmelse med databehandleraftalen med den dataansvarlige.

Sikkerhedshændelser og svagheder i IST ApS' systemer skal rapporteres på en sådan måde, at det er muligt at foretage korrektioner rettidigt. Der er etableret procedurer for hændelsesstyring og afvigerapportering, herunder sikkerhedsbrud. Procedurerne sikrer, at der arbejdes systematisk og foretages nødvendig dataindsamling og dokumentation, således at der efterfølgende er et godt grundlag at evaluere ud fra. Afvigerapporteringen er en del af vores Kvalitetsstyringssystem, og det er ledelsen, der er ansvarlig for at definere og koordinere en struktureret ledelsesproces, der sikrer en passende reaktion på sikkerhedshændelser. Herunder orienteringen af den dataansvarlige og bistand til den dataansvarlige i forbindelse med et brud på persondatasikkerheden.

KAPITEL 4:

Kontrolmål, kontrolaktivitet, tests og resultater heraf

Denne rapport har til formål at give de dataansvarlige information om de kontroller hos IST ApS, der kan påvirke behandlingen af personoplysninger, og også at give de dataansvarlige information om driftseffektiviteten af de kontroller, der blev testet.

Hvad angår periode har vi i vores test forholdt os til, om IST ApS har levet op til kontrolmålene i perioden 1. april 2023 - 31. marts 2024.

Under det grå felt er tre kolonner:

- **Første kolonne viser de aktiviteter, som IST ApS jf. sin dokumentation har iværksat for at leve op til kravene.**
- **Anden kolonne viser, hvordan vi har valgt at teste, om det forholder sig som beskrevet.**
- **Tredje kolonne viser resultatet af vores test.**

De udførte tests

De udførte tests i forbindelse med fastlæggelsen af kontrollers design, implementering og operationelle effektivitet er foretaget ved metoderne beskrevet nedenfor.

Inspektion	**Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at blive effektive, hvis de implementeres. Endvidere vurderes det, om kontrollerne er implementeret, og om de overvåges og kontrolleret tilstrækkeligt og med passende intervaller.**
Forespørgsler	**Forespørgsel til passende personale hos IST ApS. Forespørgsler har omfattet, hvordan kontroller udføres.**
Observation	**Vi har observeret kontrollens udførelse.**
Genudføre kontrollen	**Gentaget den relevante kontrol. Vi har gentaget udførelsen af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.**

Kontrolmål A: Instruks i forbindelse med behandling

Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgående databehandleraftale.

IST's kontrolaktivitet	Beierholms udførte test	Resultat af test
Databehandleren har procedurer for indgåelse af skriftlige databehandleraftaler, der er i overensstemmelse med de ydelser, som databehandleren leverer. Databehandleren anvender en databehandleraftaleskabelon for indgåelse af databehandleraftaler. Ved indgåelse af skriftlige databehandleraftaler baseret på den dataansvarliges skabelon, anvender databehandleren en tjekliste, som fastlægger hvad databehandleren skal leve op til. Databehandleraftaler indeholder informationer om brugen af underdatabehandlere. Databehandleraftaler underskrives og opbevares elektronisk. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har ved interview forespurgt ledelsen om kontrollen. Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en databehandleraftale med tilhørende instruks. Inspiceret dokumentation for på hvilket grundlag behandling af personoplysninger (skabelon for databehandleraftale) foretages, samt at dette skal godkendes af den dataansvarlige. Det er konstateret, at der anvendes en struktureret arbejdsproces, som fastlægger hvilke krav databehandleren skal efterleve. Inspiceret at skabelonen for indgåelse af databehandleraftale indeholder angivelse af godkendte underdatabehandlere. Inspiceret dokumentationen for, at grundlaget for behandling af personoplysninger sker på baggrund af en underskrevet databehandleraftale, og at aftalen bliver opbevaret i et elektronisk format. Inspiceret, at procedurer er opdateret.	Ingen bemærkninger.
Indgået databehandleraftale indeholder en instruks fra den dataansvarlige. Databehandler indhenter instruks for behandling af personoplysninger fra den dataansvarlige, i forbindelse med indgåelse af databehandleraftale. Databehandler udfører alene behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Vi har ved interview forespurgt ledelsen om kontrollen. Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Inspiceret, at skabelonen for indgåelse af databehandleraftale indeholder angivelse af instruks i forbindelse med databehandlingen.	Ingen bemærkninger.

Kontrolmål B: Tekniske sikringsforanstaltninger

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

IST's kontrolaktivitet	Beierholms udførte test	Resultat af test
Risici minimeres ud fra vurderingen af deres sandsynlighed, konsekvens og afledte implementeringsomkostninger. Risikovurderinger opdateres løbende efter behov, men minimum en gang årligt.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandler foretager en risikovurdering for at opnå en passende sikkerhed. Inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger.	Ingen bemærkninger.
Databehandleren har implementeret forretningsgange for en produktopdelt risikovurdering af behandlingen af personoplysninger på vegne af den dataansvarlige. Der foretages løbende – og mindst én gang årligt – vurdering af, hvorvidt risikovurderingen er opdateret og passende.	Vi har forespurgt ledelsen, om der er implementeret risikovurdering opdelt per SaaS løsning i forhold til behandlingen af personoplysninger på vegne af den dataansvarlige. Vi har ved stikprøvetest inspiceret, at der for IST Skoleadministration bliver udarbejdet en risikovurdering, der omfatter en vurdering af behandling af personoplysninger.	Ingen bemærkninger.
Der er dokumenteret driftsafviklingsprocedurer for forretningskritiske systemer, og de er tilgængelige for personale med et arbejdsbetinget behov. Ledelsen har implementeret politikker og procedurer til sikring af tilfredsstillende funktionsadskillelse. Der er etableret en styring af driftsmiljøet for at minimere risikoen for teknisk betingede nedbrud. Der foretages en løbende kapacitetsfremskrivning baseret på de forretningsmæssige forventninger til vækst og nye aktiviteter og de heraf afledte kapacitetskrav.	Vi har: • forespurgt ledelsen, om alle relevante driftsprocedurer er dokumenteret. • i forbindelse med revisionen af de enkelte driftsområder stikprøvevist kontrolleret, at der foreligger dokumenterede procedurer, samt at der er overensstemmelse mellem disse procedurer og de handlinger, som faktisk udføres. • foretaget inspektion af brugere med administrative rettigheder, til verificering af at adgange er begrundet i et arbejdsbetinget behov og ikke kompromitterer funktionsadskillelsen. • forespurgt ledelsen om de procedurer/ kontrolaktiviteter, der udføres. • stikprøvevist gennemgået, at ressourceforbruget i driftsmiljøet bliver overvåget og tilpasset i forhold til det forventede og nødvendige kapacitetsbehov.	Ingen bemærkninger.

Kontrolmål B: Tekniske sikringsforanstaltninger

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

IST's kontrolaktivitet	Beierholms udførte test	Resultat af test
Alle mobile enheder, som anvendes i arbejdsmæssig sammenhæng, skal have installeret antivirus, som løbende opdateres. Fjernadgang skal foregå via to-faktor autentifikation.	Inspiceret, at der er installeret antivirus-software på mobile enheder, som anvendes i arbejdsmæssig sammenhæng. Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at to-faktor autentifikation anvendes ved brugen af kritiske back-end systemer.	Ingen bemærkninger.
Der udføres dagligt backup af systemer og databaser.	Inspiceret, at der foreligger formaliserede procedurer, der beskriver kravene til håndteringen af backup-aktiviteter. Herunder at rammen indeholder, at backup bliver udført på baggrund af faste parameteropsætninger, i henhold til fastlagte retningslinjer.	Ingen bemærkninger.
For de produktionsmiljøer, der anvendes til behandling af personoplysninger, er der etableret systemovervågning med alarmering.	Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering.	Ingen bemærkninger.
Særligt risikofyldte operativsystemer og netværkstransaktioner eller -aktiviteter bliver overvåget. Afvigende forhold undersøges og løses rettidigt. Systemerne logger, når brugerne logger af og på systemerne. Kun ved mistanke om eller ved konstateret misbrug af systemerne overvåges brugerne aktivt. Der anvendes et centralt overvågningsværktøj, der afgiver alarmer, hvis kendte fejl opstår. Om muligt overvåges for, om en fejl er ved at opstå, for at kunne handle proaktivt.	Vi har: • forespurgt ledelsen, om de procedurer/ kontrolaktiviteter der udføres, og vi har gennemgået systemopsætningen på servere og væsentlige netværksenheder samt påset, at parametre for logning er opsat, således at handlinger, udført af brugere med udvidede rettigheder, bliver logget. • stikprøvevist kontrolleret, at der foretages tilstrækkelig opfølgning på log fra kritiske systemer. • påset, at der anvendes overvågningsværktøj, samt at dette er tilgængeligt for samtlige medarbejdere. • påset, at der afgives alarmer pr. mail og sms ved opståede fejl.	Ingen bemærkninger.

Kontrolmål B: Tekniske sikringsforanstaltninger

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

IST's kontrolaktivitet	Beierholms udførte test	Resultat af test
Ændringer til styresystemer finder sted iht. fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer til styresystemer, herunder håndtering af relevante opdateringer og patches inkl. sikkerhedspatches.	Ingen bemærkninger.
Ændringer af funktionalitet testes, inden de sættes i drift. Udvikling og test udføres i udviklingsmiljøer, som er adskilt fra produktionsmiljøer. Der benyttes et versionsstyringssystem, som registrerer alle ændringer i kildekode. Udviklingsmiljøer og testmiljøer er adskilt fra hinanden.	Vi har forespurgt ledelsen om der: • er udarbejdet en overordnet kvalitetsstyringsmodel for håndteringen af softwareudvikling. • findes procedurer med tilhørende forretningsgange for udrulning af software-ændringer til live-produktionen. • findes procedurer for adskillelse mellem produktionsmiljøet og miljøerne for udvikling og vedligeholdelse. • findes procedurer og forretningsgange for håndtering af versionsændringer samt understøttende system til registrering af ændringer i kildekoden. • findes formaliserede procedurer for adskillelse mellem test- og produktionsmiljøer til brug for softwareudviklingen.	Ingen bemærkninger.
Databehandleren har implementeret procedure for brugeradministration, der sikrer, at brugeroprettelser og -nedlæggelser følger en styret proces, og at alle brugeroprettelser er autoriseret. Brugerrettigheder tildeles ud fra et arbejdsbetinget behov. Privilegerede (administrative) adgangsrettigheder tildeles til systemer og enheder ud fra arbejdsbetinget behov. Der foretages kvartalsvis gennemgang af brugere og brugerrettigheder. Der foretages logning af alle adgange til systemer og data.	Inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger. Inspiceret, at der foreligger formaliserede procedurer for opfølgning på, at brugeres adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov. Inspiceret, at de aftalte tekniske foranstaltninger understøtter opretholdelsen af begrænsningen i brugernes arbejdsbetingede adgang til personoplysninger. Inspiceret, at der foreligger faste arbejdsopgaver for løbende gennemgang af brugere og brugerrettigheder. Inspiceret, at der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter i systemer og databaser, der anvendes til behandling af personoplysninger.	Ingen bemærkninger.

Kontrolmål B: Tekniske sikringsforanstaltninger

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

IST's kontrolaktivitet	Beierholms udførte test	Resultat af test
Databehandleren har implementeret en politik for kryptering af persondata, der definerer styrken og protokollen for kryptering.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at transmission af følsomme og fortrolige oplysninger over internettet er beskyttet af stærk kryptering baseret på en anerkendt algoritme.	Ingen bemærkninger.
Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en sikret firewall. Inspiceret, at firewall er konfigureret i henhold til intern politik herfor.	Ingen bemærkninger.
De etablerede tekniske foranstaltninger testes løbende ved hjælp af sårbarhedsscanninger og penetrationstests.	Inspiceret, at der foreligger formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder gennemførelse af sårbarhedsscanninger og penetrationstests.	Ingen bemærkninger.
Der er fastlagt en ensartet ramme for virksomhedens beredskabsplaner for at sikre, at alle planerne er sammenhængende og tilgodeser alle sikkerhedskrav, samt for at fastlægge prioriteringen af afprøvning og vedligeholdelse.	Vi har forespurgt ledelsen, om der er udarbejdet planer for beredskabsstyring. Vi har ved stikprøvevis inspektion påset, • at der er udarbejdet passende rammer for udarbejdelse af beredskabsstyring. • at der er udarbejdet og implementeret beredskabsplaner. • at planerne har en tværorganisatorisk beredskabsstyring. • at planerne indeholder passende strategi og procedurer for kommunikation med kunder. • at beredskabsplaner afprøves på regelmæssig basis. • at der sker en løbende vedligeholdelse og revurdering af det samlede grundlag for beredskabsstyringen.	Ingen bemærkninger.

Kontrolmål C: Organisatoriske sikringsforanstaltninger

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

IST's kontrolaktivitet	Beierholms udførte test	Resultat af test
Databehandleren har udarbejdet og implementeret en informationssikkerhedspolitik. Databehandlerens informationssikkerhedspolitik bliver gennemgået og opdateret minimum en gang årligt.	Vi har ved interview forespurgt ledelsen om kontrollen. Inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.	Ingen bemærkninger.
Databehandleren har etableret og dokumenteret ledelsesstyring af informationssikkerhed.	Vi har ved interview forespurgt ledelsen om kontrollen. Inspiceret, at der foreligger en formaliseret arbejdsramme for ledelsen til den løbende håndtering og styring af informationssikkerhed.	Ingen bemærkninger.
Databehandleren udfører screening af potentielle medarbejdere før ansættelse.	Vi har ved interview forespurgt til ledelsen om kontrollen. Inspiceret, at der foreligger formaliserede procedurer, der sikrer screening af databehandlerens medarbejdere i forbindelse med ansættelse.	Ingen bemærkninger.
Databehandleren har udarbejdet og implementeret en procedure for fratrædelse af medarbejdere ved ophør af ansættelse.	Vi har ved interview forespurgt ledelsen om kontrollen. Inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. tilbageleveres.	Ingen bemærkninger.
Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende.	Vi har ved interview forespurgt ledelsen om kontrollen. Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på, at den underskrevne fortrolighedsaftale fortsat er gældende.	Ingen bemærkninger.

Kontrolmål C: Organisatoriske sikringsforanstaltninger

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

IST's kontrolaktivitet	Beierholms udførte test	Resultat af test
Databehandleren afholder awareness-træning af nye medarbejdere i henhold til databeskyttelse og informationssikkerhed, i forlængelse af ansættelsesproceduren.	Vi har ved interview forespurgt ledelsen om kontrollen. Inspiceret, at databehandleren gennemfører awareness-træning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger. Inspiceret ved en stikprøve på 4 medarbejdere, at de pågældende medarbejdere er blevet introduceret til: • Informationssikkerhedspolitikken • Procedurer vedrørende databehandling, samt anden relevant information.	Ingen bemærkninger.
Databehandleren foretager løbende uddannelse af medarbejdere i håndtering af databeskyttelse og informationssikkerhed.	Vi har ved interview forespurgt ledelsen om kontrollen. Inspiceret, at databehandleren afholder løbende uddannelse af medarbejdere om håndtering af databeskyttelse og informationssikkerhed i relation til personoplysninger.	Ingen bemærkninger.
Alle medarbejdere har underskrevet ansættelseskontrakt, der indeholder en bestemmelse om tavshedspligt.	Vi har ved interview forespurgt ledelsen om kontrollen. Inspiceret ved en stikprøve på 5 medarbejdere, at de pågældende medarbejdere har underskrevet en aftale, som indeholder bestemmelse ift. tavshedspligt.	Ingen bemærkninger.

Kontrolmål C: Organisatoriske sikringsforanstaltninger

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

IST's kontrolaktivitet	Beierholms udførte test	Resultat af test
Databehandleren har udpeget en databeskyttelsesrådgiver med passende kompetencer, og dennes kontaktoplysninger er offentliggjort. **Skriftlige procedurer for databeskyttelsesrådgiverens opgaver omfatter:** • **at underrette og rådgive om forpligtelser i henhold til gældende databeskyttelseslovgivning.** • **at overvåge overholdelsen af gældende databeskyttelseslovgivning og af politikker om beskyttelse af personoplysninger.** • **at rådgive med hensyn til konsekvensanalysen vedrørende databeskyttelse og overvåge dens opfyldelse** • **at samarbejde med tilsynsmyndigheden** • **at fungere som tilsynsmyndighedens kontaktpunkt** **Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.**	**Vi har kontrolleret dokumentationen for databehandlerens vurdering af, hvorvidt der skal udpeges en databeskyttelsesrådgiver eller ej.** **Vi har kontrolleret dokumentationen for, at kontaktoplysninger på databeskyttelsesrådgiveren er offentliggjort.** **Vi har kontrolleret dokumentationen for ledelsens behandling og godkendelse af udpegningen af databeskyttelsesrådgiveren, herunder sikring af databeskyttelsesrådgiverens kompetencer.**	**Ingen bemærkninger.**

Kontrolmål D: Sletning af personoplysninger

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

IST's kontrolaktivitet	Beierholms udførte test	Resultat af test
Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.	Ingen bemærkninger.
Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: • Tilbageleveret til den dataansvarlige og/eller • Slettet, hvor det ikke er i modstrid med anden lovgivning.	Inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger.	Ingen bemærkninger.
Ved behandling af data for den dataansvarlige er databehandleren ansvarlig for opsætning af krav til opbevaringsperioder samt sletning af data i henhold til aftalen med den dataansvarlige:	Vi har stikprøvevis kontrolleret dokumentationen for overholdelse af specifikke krav til databehandlerens opbevaringsperioder og sletterutiner i tilknytning til sikkerheds- og tilsynslog, backup og applikationslogs.	Ingen bemærkninger.

Kontrolmål E: Opbevaring af personoplysninger

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

IST's kontrolaktivitet	Beierholms udførte test	Resultat af test
Der foreligger skriftlige procedurer, 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.	Inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Inspiceret ved en stikprøve på 10 databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen sker i henhold til databehandleraftalen. Inspiceret, at procedurerne er opdateret.	Ingen bemærkninger.
Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter og lande.	Ingen bemærkninger.
Databehandleren har etableret en fortegnelse over behandlingsaktiviteter som databehandler.	Vi har ved interview forespurgt ledelsen om fortegnelsen. Inspiceret, at databehandleren har en samlet og opdateret fortegnelse over behandlingsaktiviteter.	Ingen bemærkninger.
Fortegnelsen opdateres løbende ved væsentlige ændringer.	Inspiceret, at oversigten over behandlingsaktiviteter er opdateret og vedligeholdt.	Ingen bemærkninger.
Fortegnelsen opdateres minimum en gang årligt under det årlige review.	Inspiceret, at findes intern opgave for et årligt review af oversigten over behandlingsaktiviteter.	Ingen bemærkninger.
Fortegnelsen opbevares elektronisk i databehandlerens system/ fil-drev.	Inspiceret, at oversigten over behandlingsaktiviteter er opbevaret i elektronisk format.	Ingen bemærkninger.
Databehandleren udleverer fortegnelsen på anmodning fra tilsynsmyndigheden.	Inspiceret, at standard-databehandleraftalen indeholder krav til databehandleren ift. at yde assistance til tilsynsmyndigheden i tilfælde af en henvendelse.	Ingen bemærkninger.

Kontrolmål F: Underdatabehandlere

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.

IST's kontrolaktivitet	Beierholms udførte test	Resultat af test
Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Inspiceret, at procedurerne er opdateret.	Ingen bemærkninger.
Til behandling af personoplysninger anvender databehandleren udelukkende underdatabehandlere, der er specifikt eller generelt godkendt af den dataansvarlige.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere. Inspiceret ved en stikprøve på 4 stk. underdatabehandlere fra databehandlerens oversigt over underdatabehandlere, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige.	Ingen bemærkninger.
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 fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændring i anvendelse af underdatabehandlerne i erklæringsperioden.	Ingen bemærkninger.
Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Inspiceret, at der foreligger underskrevne underdatabehandleraftaler med de anvendte underdatabehandlere, som fremgår af databehandlerens oversigt. Inspiceret ved en stikprøve på 4 stk. underdatabehandleraftaler, at disse indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Ingen bemærkninger.

Kontrolmål F: Underdatabehandlere

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.

IST's kontrolaktivitet	Beierholms udførte test	Resultat af test
Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: • Navn • CVR-nr. • Adresse • Beskrivelse af behandlingen	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.	Ingen bemærkninger.
Databehandleren 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 eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.	Inspiceret, at der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne. Inspiceret dokumentation for, at der er foretaget en risikovurdering af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne. Inspiceret dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerheden hos de anvendte underdatabehandlere.	Ingen bemærkninger.

Kontrolmål G: Overførsel af personoplysninger til tredjelande mm.

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.

IST's kontrolaktivitet	Beierholms udførte test	Resultat af test
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.	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. Inspiceret, at procedurerne er opdateret	Ingen bemærkninger.
Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over overførsler af personoplysninger til tredjelande eller internationale organisationer. Inspiceret ved en stikprøve på 1 dataoverførsel fra databehandlerens oversigt over overførsler, at der er dokumentation for, at overførslen er aftalt med den dataansvarlige i databehandleraftalen eller senere godkendt.	Ingen bemærkninger.
Databehandleren vurderer og dokumenterer, at der eksisterer et gyldigt overførselsgrundlag i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer.	Inspiceret, at der foreligger formaliserede procedurer for sikring af et gyldigt overførselsgrundlag. Inspiceret, at procedurerne er opdateret. Inspiceret ved en stikprøve på 1 dataoverførsel fra databehandlerens oversigt over overførsler, at der er dokumentation for et gyldigt overførselsgrundlag i databehandleraftalen med den dataansvarlige, samt at der kun er sket overførsler, i det omfang dette er aftalt med den dataansvarlige.	Ingen bemærkninger.

Kontrolmål H: Bistå den dataansvarlige

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.

IST's kontrolaktivitet	Beierholms udførte test	Resultat af test
Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand til den dataansvarlige i relation til de registreredes rettigheder. Inspiceret, at procedurerne er opdateret.	Ingen bemærkninger.
Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	Inspiceret, at der foreligger procedurer for bistand til den dataansvarlige. Inspiceret, at dokumentation for anmodninger om bistand fra den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede er korrekt og rettidigt gennemført.	Ingen bemærkninger.
Databehandler er forpligtet til at få udarbejdet en erklæring om de tekniske og organisatoriske sikkerhedsforanstaltninger, rettet mod behandling og beskyttelse af personoplysninger.	Vi har forespurgt ledelsen, om der er udarbejdet en erklæring om de tekniske og organisatoriske sikkerhedsforanstaltninger vedrørende behandling og beskyttelse af personoplysninger. Inspiceret, at standard-databehandleraftalen indeholder krav til databehandleren ift. at yde bistand til den dataansvarlige i forhold til revision og inspektion.	Ingen bemærkninger.
Databehandleren stiller den fornødne information til rådighed for den dataansvarlige og tilsynsmyndigheden på anmodning i forbindelse med revision og inspektion af databehandleren.	Vi har ved interview forespurgt ledelsen om kontrollen. Inspiceret, at standard-databehandleraftalen indeholder krav til databehandleren ift. at yde bistand til den dataansvarlige i forhold til revision og inspektion.	Ingen bemærkninger.

Kontrolmål I: Brud på datasikkerheden

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

IST's kontrolaktivitet	Beierholms udførte test	Resultat af test
Databehandleren underretter den dataansvarlige om brud på persondatasikkerheden uden unødig forsinkelse. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har ved interview forespurgt ledelsen om kontrollen. Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Inspiceret, at proceduren er opdateret.	Ingen bemærkninger.
Databehandleren har opsat overvågning af system til detektion af brud på persondatasikkerheden.	Vi har ved interview forespurgt ledelsen om kontrollen. Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering. Inspiceret, at databehandler gennemfører awareness-træning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden. Inspiceret dokumentation for, at netværkstrafik overvåges. Inspiceret dokumentation for, at der sker rettidig opfølgning på logning af adgang til personoplysninger.	Ingen bemærkninger.
Databehandleren ajourfører den dataansvarlige med alle relevante og nødvendige oplysninger, når de er til rådighed for databehandleren.	Vi har ved interview forespurgt ledelsen om kontrollen. 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 sandsynlige konsekvenser af bruddet på persondatasikkerheden • Beskrivelse af foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. Inspiceret dokumentation for, at der ved brud på persondatasikkerheden er truffet foranstaltninger, som har håndteret bruddet på persondatasikkerheden.	Ingen bemærkninger.

Kontrolmål I: Brud på datasikkerheden

Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.		
IST's kontrolaktivitet	**Beierholms udførte test**	**Resultat af test**
Kommunikation mellem databehandler og dataansvarlig dokumenteres og gemmes.	Vi har ved interview forespurgt ledelsen om kontrollen. Inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Inspiceret, at databehandleren har medtaget eventuelle brud på persondatasikkerheden hos underdatabehandlere i databehandlerens oversigt over sikkerhedshændelser.	Ingen bemærkninger.
Databehandleren registrerer brud på persondatasikkerheden i databrudsloggen.	Inspiceret databrudsloggen for dokumentation for, at brud på persondatasikkerheden registreres heri.	Ingen bemærkninger.
Databehandleren har udarbejdet og implementeret en procedure for erfaringsopsamling ved brud på persondatasikkerheden.	Inspiceret, at de foreliggende procedurer for håndteringen af brud på persondatasikkerheden indeholder krav ift. erfaringsopsamling.	Ingen bemærkninger.
Der er udarbejdet procedurer for bistand til den dataansvarlige i tilfælde af brud på persondatasikkerheden.	Inspiceret, at der foreligger procedurer for at yde bistand til den dataansvarlige i tilknytning til et brud på persondatasikkerheden.	Ingen bemærkninger.