www.pwc.dk

Sonlinc

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om beskrivelsen af kontroller vedrørende SonWin rettet mod databeskyttelse og behandling af personoplysninger for perioden 1. februar 2019 til 31. januar 2020

Juni 2020

Indholdsfortegnelse

1. Ledelsens udtalelse

Sonlinc varetager databehandling af personoplysninger for vores kunder, der er dataansvarlige i henhold til EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (efterfølgende "databeskyttelsesforordningen") og "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesloven").

Medfølgende beskrivelse er udarbejdet til brug for dataansvarlige, der har anvendt SonWin, 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 databeskyttelsesforordningen og databeskyttelsesloven er overholdt.

Sonlinc bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en retvisende beskrivelse af SonWin, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen og databeskyttelsesloven for perioden 1. februar 2019 til 31. januar 2020. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) redegør for, hvordan SonWin var udformet og implementeret, herunder redegør for:

   - De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger
   - De processer i både it-systemer og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og 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 sikkerhedsforanstaltninger for behandlingen af persondata under hensyntagen til de risici, som behandling 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 SonWins udformning 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 i databehandlerens SonWin til behandling af personoplysninger foretaget for perioden 1. februar 2019 til 31. januar 2020

(iii) ikke udelader eller forvansker oplysninger, der er relevante for omfanget af det beskrevne SonWin 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 SonWin, som den enkelte dataansvarlige måtte anse vigtigt efter sine 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. februar 2019 til 31. januar 2020. Kriterierne 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 for perioden 1. februar 2019 til 31. januar 2020.

b) 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 og databeskyttelsesloven.

Aarhus, den 6. august 2020

Rasmus Dalby Martinussen
Director

2. Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om beskrivelsen af kontroller rettet mod databeskyttelse og behandling af personoplysninger

Til ledelsen i Sonlinc og Sonlincs kunder

Omfang

Vi har fået som opgave at afgive erklæring om Sonlincs opstillede kontrolmål og om udformningen og funktionen af kontroller vedrørende Sonlincs SonWin-system for perioden 1. februar 2019 til 31. januar 2020.

Kontrolmål og kontroller er fastlagt af Sonlinc med udgangspunkt i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesforordningen") og "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesloven") for perioden 1. februar 2019 til 31. januar 2020 (beskrivelsen).

Vores konklusion udtrykkes med høj grad af sikkerhed.

Nærværende erklæring omfatter, om Sonlinc har etableret og udformet hensigtsmæssige kontroller, der knytter sig til de kontrolmål, der fremgår af afsnit 4 i relation til SonWin. Erklæringen omfatter således ikke en vurdering af Sonlincs generelle efterlevelse af ovennævnte lovgivning.

Kontrolmål og tilknyttede kontrolaktiviteter, som vedrører kundernes ansvar i relation til driften af SonWin, indgår ikke i vores erklæring, som ligeledes ikke omfatter kundespecifikke forhold.

Sonlincs ansvar

Sonlinc er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende ledelsesudtalelse, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt 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 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.

PwC er underlagt international standard om kvalitetsstyring, ISQC 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 Sonlincs beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, der er anført i afsnit 4.

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. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen af kontrolmål 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 af kontrolmål og udformningen og funktionaliteten af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for de opstillede kontrolmål og udformede kontroller vedrørende Sonlincs SonWin-system samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at kontrollerne ikke er hensigtsmæssigt udformet.

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

Sonlincs beskrivelse af kontrolmål er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved SonWin, som hver enkelt dataansvarlig måtte anse for vigtige efter sine særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden. 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 de kriterier, der er beskrevet i ledelsens udtalelse. Det er vores opfattelse,

(a) at beskrivelsen af kontrolmål, således som de var udformet og implementeret for perioden 1. februar 2019 til 31. januar 2020, 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 for perioden 1. februar 2019 til 31. januar 2020, idet vi dog har konstateret enkelte afvigelser, jf. afsnit 4

(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 for perioden 1. februar 2019 til 31. januar 2020.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt dataansvarlige, der har anvendt Sonlincs SonWin-system, 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.

Aarhus den 10. august 2020
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab

Jesper Parsberg Madsen
Statsautoriseret revisor

3. Systembeskrivelse

3.1 Beskrivelse af SonWin/Sonlinc

Sonlinc har udelukkende kunder i forsynings- og teleindustrien. Når forsyningen blomstrer, gør vi det også, og derfor prioriterer vi højest af alt at levere løsninger, der smitter positivt af på bundlinjen hos danske forsyningsvirksomheder.

Kundespecifikke forhold er ikke omfattet af denne erklæring.

SonWin

Sonlincs standardløsning går under betegnelsen SonWin. SonWin anvendes til kundeservice, handel og afregning af el, vand, varme, gas, affald og bredbånd. SonWins moduler videreudvikles konstant, som behovene forandrer sig i de forskellige nicher af forsyningssektoren.

SonWin:

- Bruges af flere end 50 danske forsyningsselskaber
- Administrerer over 2 mio. kundeforhold
- Udsender årligt 10 mio. fakturaer til et samlet beløb på mere end 40 mia. kr.
- Afregner fjernvarme for mere end 125.000 forbrugere
- Afregner vand og spildevand hos mere end 250.000 forbrugere
- Fakturerer 60 % af elforbruget i Danmark
- Bruges af over halvdelen af landets gasselskaber
- Faciliterer handel med el på tværs af fem europæiske lande.

Sonlinc som databehandler

Sonlinc er databehandler for vores kunder. Sonlincs kunder er dataansvarlige. Sonlinc har indgået en databehandleraftale med alle kunder. Denne ligger som bilag 3 til de "Generelle Samarbejdsvilkår". I forbindelse med at Sonlinc benytter sig af underleverandører, skal disse godkende og underskrive en underleverandøraftale, "Leverandørens forpligtelse som databehandler for Sonlinc". Det er Sonlincs ansvar at sikre, at underleverandørerne bliver oplært i dels databehandleraftalen og dels i Sonlincs "Procedure for behandling af persondata for kunderne".

Sonlinc som databehandler understøtter følgende artikler i persondataforordningen:

Artikel	Beskrivelse	Sonlinc
Art. 5	Principper for behandling af personoplysninger	Sonlinc efterlever intern skriftlig procedure, der beskriver principperne for behandling af personoplysninger for vores kunder: • Lovlighed, rimelighed og gennemsigtighed • Formålsbegrænsning • Dataminimering • Rigtighed • Opbevaringsbegrænsning • Integritet og fortrolighed.
Art. 6	Lovlig behandling	Sonlinc sikrer gennem sine interne procedurer og kontroller, at der alene sker lovlig behandling af kundernes personoplysninger. Der henvises desuden til de "Generelle Samarbejdsvilkår" samt bilag 3 til disse, "Sonlincs Forpligtelse som Databehandler", hvor "Minimumskrav til de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger" er beskrevet.

Artikel	Beskrivelse	Sonlinc
Art 11 og 12	Behandling, der ikke kræver identifikation, gennemsigtig oplysning, meddelelser og nærmere regler for udøvelsen af den registreredes rettigheder	SonWin understøtter, at opbevaring, indhentelse og behandling af oplysninger til identifikation af den registrerede opretholdes, så længe identifikation er påkrævet.
Art. 15	Den registreredes indsigtsret	SonWin understøtter den registreredes ret til indsigt i egne registrerede personoplysninger, og behandlingen heraf er overholdt.
Art. 16 og 19	Ret til berigtigelse	I SonWin er det muligt at sikre den registreredes ret til berigtigelse af egne registrerede personoplysninger.
Art. 17 og 19	Ret til sletning	SonWin understøtter den registreredes ret til at blive glemt/anonymiseret.
Art. 18 og 19	Ret til begrænsning af behandling	I SonWin er det muligt at sikre den registreredes ret til begrænsning af behandling af egne registrerede personoplysninger.
Art. 20	Ret til dataportabilitet	SonWin understøtter den registreredes ret til at overføre egne registrerede personoplysninger til en anden dataansvarlig.
Art. 24	Den dataansvarliges ansvar – implementering af passende databeskyttelse	Sonlinc har databehandleraftaler med alle kunder, som ligger som bilag 3 til de "Generelle Samarbejdsvilkår".
Art. 25	Databeskyttelse gennem design og standardindstillinger	Sonlinc sikrer, at sikring af personfølsomme data inddrages fra begyndelsen i udviklingen af ny software og nye ydelser. For hvert udviklingsprojekt skal vurderes omfanget af GDPR, herunder "privacy by design".
Art. 28 og 29	Databehandler – behandling af personoplysninger på vegne af den dataansvarlige	Sonlinc skal sikre, at databehandleraftalen med kunderne overholdes. Dette sikres gennem skriftlige procedurer om, hvordan man i Sonlinc efterlever databehandleraftalen, uddannelse af medarbejderne i denne og interne audits, der kontrollerer, at principperne og kontrollerne internt overholdes.
Art. 30	Fortegnelse over behandlingsaktiviteter	Sonlincs databehandleraftale indeholder en fortegnelse over kategorierne af behandlingsaktiviteter, der foretages på vegne af den dataansvarlige. Sonlinc overfører ikke personoplysninger til et tredjeland eller en international organisation. Såfremt dette ændres, skal alle Sonlincs kunder informeres.
Art. 32	Behandlingssikkerhed	Sonlinc har en generel it-risikovurdering, som revideres kvartalsvist af Sonlincs it-sikkerhedsgruppe. Formålet med it-risikovurderingen er at sikre, at der løbende, på baggrund af en evaluering af risici, er truffet de fornødne sikkerhedsforanstaltninger mod hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til registreredes personoplysninger.
Art. 33 og 34	Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden	Sonlinc har de fornødne procedurer og kontroller, der sikrer, at Sonlinc ved brud på persondatasikkerheden kan understøtte den dataansvarliges pligt til rettidig og fyldestgørende anmeldelse til tilsynsmyndigeden samt underrette de registrerede, hvis personoplysninger er omfattet af bruddet.
Art. 35	Konsekvensanalyse vedrørende databeskyttelse	Sonlinc sikrer ved etablering af og løbende opfølgning på it-risikovurderingen, at der løbende foretages konsekvensanalyser vedrørende de registreredes databeskyttelse.
Art. 36	Forudgående høring	I henhold til databehandleraftalen har Sonlinc etableret procedurer samt tekniske og organisatoriske sikkerhedsforanstaltninger, som er påkrævet af tilsynsmyndigheden for behandling af de registreredes personoplysninger.

Artikel	Beskrivelse	Sonlinc
Art 37 og 38 og 39	Databeskyttelsesrådgiver og dennes stilling	Sonlinc vurderer, at det ikke er nødvendigt med en databeskyttelsesrådgiver, og derudover er det ikke et krav som databehandler.
Art. 44, 45, 46, 47, 48, 49 og 50	Overførelse af personoplysninger til tredjeland	Sonlinc overfører ikke de registreredes personoplysninger til tredjeland, Det er desuden ikke accepteret, at medarbejdere i Sonlinc arbejder med de registreredes personoplysninger i tredjeland. Sonlinc har desuden ikke samarbejdspartnere i tredjeland.

Datasikkerhed og risikovurdering

Sonlinc har som databehandler strenge krav til sine medarbejdere om overholdelse af it-sikker-heden. Derfor skal alle medarbejdere ved ansættelsen gennemgå Sonlincs it-sikkerhedspolitik og skrive under på, at de har læst, forstået og accepteret, at de vil efterleve procedurer og principper beskrevet i politikken.

Det er i sidste ende Sonlincs ledelses ansvar at sikre, at Sonlinc behandler persondata i henhold til den gældende lov. Sonlinc er databehandler i henhold til EU's forordning om: "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (efterfølgende "databeskyttelsesforordningen") og "lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesloven").

Sonlincs it-sikkerhedsrisikovurdering lister alle de interne og eksterne risici for it-sikkerheden, og derudover beskriver "Generel Procedure for Sonlinc som databehandler" de interne krav til sikkerhed og fortrolighed, i forbindelse med at Sonlincs medarbejdere arbejder med kundernes persondata.

Kontrolaktiviteter

Sonlinc sikrer, at der bliver gennemført en årlig intern audit. Denne audit har til formål at sikre, at Sonlinc efterlever de krav, der foreligger i persondataforordningen og i Sonlincs forpligtelse som databehandler for kunder. Desuden skal der foreligge dokumentation for, at Sonlinc har foretaget de fornødne kontroller, jf. ovenstående revisorerklæring.

Audit og dokumentation for gennemført audit skal danne baggrund for den efterfølgende ledelsesevaluering, som er beskrevet i "Procedure for Ledelsesevaluering af Sonlincs efterlevelse af Persondataforordningen og Databehandleraftale".

Information og kommunikation

Sonlinc er databehandler for vores kunder. Det betyder, at alle medarbejdere (både fastansatte og eksterne) i Sonlinc på et eller andet tidspunkt kan have adgang til/bliver eksponeret for kundernes kunders persondata. Det er derfor et krav, at alle medarbejdere skriver under på, at de har læst og forstået "Generel procedure for Sonlinc som Databehandler", "Sonlincs Forpligtelse som Databehandler for Kunder" (herefter databehandleraftalen) og it-sikkerhedspolitik i Sonlinc. På underskriftsbilaget skriver medarbejderne under på, hvad der er deres ansvar i forhold til ovenstående. Alle medarbejdere skal have gennemført Sonlinc University-lektionen om "Persondataforordningen og dennes betydning for medarbejderne i Sonlinc". Som opfølgning skal medarbejderne årligt gennemføre en lektion om "Persondataforordningen og hvad det vil sige at være databehandler for vores kunder".

Alle former for personoplysninger, som medarbejderne i Sonlinc har adgang til og bliver eksponeret for, skal anses som dybt fortrolige og skal behandles konfidentielt. Alle ansatte i Sonlinc har tavshedspligt i forhold til de personoplysninger, de har adgang til.

Såfremt en medarbejder oplever, at behandlingen af kundernes personoplysninger strider imod databehandleraftalen (herunder databeskyttelsesforordningen, databeskyttelsesloven eller lovgivning) skal de strakt orientere deres nærmeste chef og sende besked til 'persondata@sonlinc.dk' eller til den ansvarlige for GDPR i Sonlinc (p.t. økonomidirektøren).

Ligeledes skal de informere ovenstående, såfremt de oplever, at der har været en hændelig eller uautoriseret videregivelse af eller adgang til personoplysninger eller mistanke herom.

Som udgangspunkt er det kundens it-afdeling, som kontaktes, såfremt Sonlinc opdager, at der har været brud på sikkerheden for behandlingen af personoplysninger.

Overvågning

Sonlinc har overvågning og logning på alle medarbejderes adgang til de dataansvarliges databaser. Dette kontrolleres og vurderes løbende gennem Sonlincs it-risikovurdering. Det fremgår desuden af Sonlincs it-sikkerhedspolitik, hvor denne overvågning og logning udføres. Der henvises til bilag 1 og til de "Generelle Samarbejdsvilkår" og "IT Revisionserklæring Sonlinc ISAE 3000".

Transformation efter EG's opkøb af Sonlinc

EG's opkøb af Sonlinc den 2. september 2019 medfører en transformation af de interne processer og systemer.

Denne transformation accelereres i 2020, hvilket betyder, at salg, udvikling, support, konsulent og økonomi kommer til at arbejde med nye værktøjer og procedurer fastsat af EG-koncernen.

Dette betyder fx, at:

- Onboarding af medarbejdere, herunder uddannelse ift. it-sikkerhed og GDPR, håndteres af EG.
- Regler for behandling af persondata justeres, når nye interne systemer implementeres.
- De interne processer, hvor der er berøring med persondata, tilrettes til EG's regelsæt.
- Den næste erklæring vil være efter den skabelon, som EG benytter.

Kunderettede kontroller (SonWin)

SonWin understøtter kunderne i overholdelsen af reglerne om persondataforordningen.

Alle persondata i SonWin er kategoriseret og vurderet ud fra deres følsomhed. SonWin indeholder ikke følsomme persondata, medmindre en kundes bruger har indtastet sådanne i et felt, der kan indeholde fritekst.

For hvert felt, der kan indeholde persondata, er det angivet, om det indeholder:

- Almindelige persondata
- Mulige følsomme persondata
- CPR-nummer
- Resultatet af en profilering
- Data, der kan give adgang til persondata, fx pinkode.

Funktionaliteten i SonWin understøtter nedenstående artikler i persondataforordningen:

Artikel	Beskrivelse
Art. 7 og 8	Betingelser for samtykke
Art. 12	Gennemsigtig oplysning, meddelelser og nærmere regler for udøvelsen af den registreredes rettigheder
11 og 12	Behandling, der ikke kræver identifikation, gennemsigtig oplysning, meddelelser og nærmere regler for udøvelsen af registreredes rettigheder
15	Den registreredes indsigtsret
16 og 19	Ret til berigtigelse
17 og 19	Ret til sletning ("Retten til at blive glemt")
18 og 19	Ret til begrænsning af behandling
20	Ret til dataportabilitet

SonWin understøtter, at opbevaring, indhentelse og behandling af oplysninger til identifikation af den registrerede opretholdes, så længe identifikation er påkrævet.

Personoplysningerne kan fremfindes i en gennemsigtig, lettilgængelig og forståelig form, så det er muligt at udlevere dem til den registrerede.

SonWin understøtter den registreredes ret til indsigt i egne registrerede personoplysninger, og om behandlingen heraf er overholdt.

I SonWin er det muligt at sikre den registreredes ret til berigtigelse af egne registrerede personoplysninger.

Ønsker den registrerede at blive glemt, er dette muligt at registrere direkte i SonWin eller indirekte via integrationer fra andre systemer. Når betingelserne for at blive glemt er opfyldt, vil den registrerede blive anonymiseret.

I SonWin er det muligt at sikre den registreredes ret til begrænsning af behandling af egne registrerede personoplysninger.

SonWin understøtter den registreredes ret til at overføre egne registrerede personoplysninger til en anden dataansvarlig.

Med Release 2018.03 er leveret den sidste funktionalitet, der sikrer, at SonWin overholder lovgivningen.

SonWin er udvidet med funktionalitet, der automatiserer ovenstående med den version, der blev frigivet i uge 33 i 2018.

Tiltagene for at SonWin overholder lovgivningen og den efterfølgende automatisering er godkendt af Sonlincs kunder i Erfa-Tilbud #134116 – "Tilretninger til SonWin i forbindelse med Persondataforordning". Desuden har der været kurser, webcast og Erfa-moduler for at understøtte kunderne.

Det er kundernes eget ansvar at eventuelle integrationer til andre systemer overholder lovgivningen.

Dokumenterne, der beskriver, hvordan SonWin understøtter persondataforordningen, er samlet på Sonlincs kundeområder under menupunktet "Vilkår".

Med disse dokumenter og denne erklæring kan kunderne udføre deres kontroller af funktionaliteten i SonWin.

3.2 Komplementerende kontroller hos de dataansvarlige

Sonlinc er udelukkende databehandler. Det er Sonlincs kunder, der som dataansvarlige er ansvarlige for beskyttelsen af deres kunders personoplysninger.

Sonlinc skal som databehandler bistå kunderne med at sikre, at de overholder den dataansvarliges forpligtigelser i forhold til følgende artikler:

Artikel	Beskrivelse
Art. 13 og 14	Oplysningspligt ved indsamling af personoplysninger hos den registrerede
Art. 30	Fortegnelse over behandlingsaktiviteter
Art. 32	Behandlingssikkerhed
Art. 33 og 34	Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden
Art. 35	Konsekvensanalyse vedrørende databeskyttelse
Art. 36	Forudgående høring

Sonlinc er databehandler for vores kunder. Det betyder, at alle medarbejdere (både fastansatte og eksterne) i Sonlinc på et eller andet tidspunkt kan have adgang til/bliver eksponeret for kundernes registreredes personoplysninger. Dette kan være gennem adgang til kundernes databaser eller i forbindelse med kundeservice, hvor medarbejderen hos Sonlinc har adgang til kundernes softwaresystem.

For at sikre dataminimering har Sonlinc indført regler for, hvordan man i Sonlinc må modtage filer, mails og informationer med kundernes registreredes personoplysninger. Såfremt den dataansvarlige kunde har brug for at sende en fil, der indeholder de registreredes personoplysninger, skal disse enten sendes via et sikkert file exchange, eller de skal lægges inde på sagen på Sonlincs kundesite. Såfremt der ikke er oprettet en sag, kan filen vedlægges ved oprettelse af sagen via SWBrugrap.

Sonlinc ønsker ikke at modtage mails, der indeholder de registreredes personoplysninger. Det er de dataansvarliges ansvar, at de ikke sender mails med de registreredes personoplysninger, hverken i mailen eller i vedhæftede filer.

3.3 Kundens ansvar

Processer og kontroller hos kunden er ikke omfattet af nærværende erklæring.

Kunden er selv ansvarlig for at anvende SonWin på en måde, der er i overensstemmelse med lovgivningens krav. Dette omfatter blandt andet:

- At varetage oplysningsforpligtelser over for kundens kunder.
- At sikre, at de personoplysninger, kunderne har registreret om deres kunder, overholder lovgivningen.
- At varetage it-drift og fysisk sikring i den forbindelse.
- At have ansvaret for at etablere betryggende kontroller i forhold til administrationen af egne brugere, herunder, men ikke begrænset til, periodisk gennemgang og vurdering af brugernes adgange samt deres fortsatte anvendelse.
- At sikre, at kommunikationen med Sonlinc følger de officielle kanaler, herunder at e-mail ikke anvendes til udveksling af personoplysninger om kundens kunder.
- At sikre, at eventuelle integrationer til andre systemer overholder lovgivningen.
- At sikre, at de registrerede har givet skriftligt samtykke til behandling af personoplysninger.
- At sikre, at oplysninger om behandling af personoplysninger kan udleveres i en gennemsigtig, letilgængelig og forståelig form til den registrerede.
- At sikre, at udøvelsen af den registreredes rettigheder sker rettidigt, herunder sikre besvarelse af den registreredes anmodninger og begrundelse af eventuelt afslag.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

4.1 Formål og omfang

Vores arbejde er udført i overensstemmelse med ISAE 3000, "Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger".

Vores test af kontrollernes design og implementering har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, der er udvalgt af ledelsen, og som fremgår i afsnit 4.3. Eventuelle andre kontrolmål, tilknyttede kontroller og kontroller hos Sonlincs kunder er ikke omfattet af vores testhandlinger.

4.2 Udførte testhandlinger

Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelser om 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 kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller. På de tekniske platforme, databaser og netværkskomponenter har vi testet den specifikke systemopsætning for at påse, om kontroller er implementeret og fungerer effektivt.
Forespørgsler	Forespørgsel af passende personale. Forespørgslerne har omfattet, hvordan kontrollerne udføres.
Observation	Vi har observeret kontrollens udførelse.
Genudførelse af kontrollen	Gentagelse af den relevante kontrol. Vi har gentaget udførelsen af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

4.3 Kontrolmål, kontrolaktivitet, test og resultat heraf

Principper for behandling af personoplysninger (artikel 5)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at indsamling, behandling og opbevaring af personoplysninger sker i overensstemmelse med principperne for behandling af personoplysninger.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
1	Der foreligger skriftlige procedurer, hvori der er taget stilling til følgende principper for behandling af personoplysninger: • Lovlighed, rimelighed og gennemsigtighed • Formålsbegrænsning • Dataminimering • Rigtighed • Opbevaringsbegrænsning • Integritet og fortrolighed.	Inspiceret, at der foreligger opdaterede skriftlige procedurer for behandling af personoplysninger, der omfatter principper for behandling af personoplysninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
2	Der foretages løbende – og mindst én gang årligt – vurdering af, at principper for behandling af personoplysninger overholdes, og denne vurdering er dokumenteret.	Inspiceret dokumentation for vurdering af principper for behandling af personoplysninger for at sikre, at der minimum en gang årligt foretages vurdering af principper for behandling af personoplysninger samt overholdelsen af disse.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
3	Ledelsen har behandlet og godkendt vurderingen af overholdelse af principperne for behandling af personoplysninger.	Inspiceret dokumentation for ledelsens godkendelse af vurderingen af overholdelse af principper for behandling af personoplysninger.	Vi er informeret om, at ledelsen løbende har været involveret i principperne for behandling af personoplysninger, herunder løbende godkendelse. Der findes dog ikke formel skriftlig dokumentation for denne godkendelse. Vi har ikke ved vores test konstateret yderligere væsentlige afvigelser.

Lovlig behandling (artikel 6)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at der alene sker lovlig behandling af personoplysninger.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger et lovligt grundlag. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer for behandling af personoplysninger, der indeholder krav til lovlig behandling af personoplysninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
2	Der foretages løbende – og mindst én gang årligt – vurdering af, at der ikke er sket ulovlig behandling af personoplysninger, og denne vurdering er dokumenteret.	Inspiceret dokumentation for løbende – og mindst årlig – vurdering af, at der ikke sker eller er sket ulovlig behandling af personoplysninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
3	Ledelsen har behandlet og godkendt vurderingen af, om der er sket ulovlig behandling af personoplysninger.	Inspiceret dokumentation for ledelsens godkendelse af vurderingen af, om der er foretaget ulovlig behandling af personoplysninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
4	Der foreligger skriftlige og af kunden godkendte samarbejdsvilkår mellem Sonlinc og den dataansvarlige kunde. Samarbejdsvilkårene indeholder en oversigt over, på hvilket grundlag behandling af personoplysninger foretages, herunder minimumskrav til de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger.	Inspiceret dokumentation for, på hvilket grundlag behandling af personoplysninger foretages, samt at dette er godkendt af den dataansvarlige.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
5	Der foretages løbende – og mindst én gang årligt – vurdering af, om samarbejdsvilkårene mellem Sonlinc og den dataansvarlige kunde skal opdateres.	Inspiceret dokumentation for, at samarbejdsvilkårene mellem Sonlinc og den dataansvarlige kunde er opdateret og godkendt af den dataansvarlige kunde mindst en gang årligt.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Behandling, der ikke kræver identifikation – Gennemsigtige oplysninger, meddelelser og nærmere regler for udøvelsen af den registreredes rettigheder (artikel 11 og 12)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at opbevaring, indhentelse og behandling af oplysninger til identifikation af den registrerede opretholdes, så længe identifikation er påkrævet. Oplysninger om behandlingen af personoplysninger kan udleveres i en gennemsigtig, lettilgængelig og forståelig form til den registrerede.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
1	Der foreligger skriftlige procedurer, som beskriver, hvordan Sonlinc understøtter registreredes ret til indsigt i registreret data, herunder hvordan det sikres, at oplysninger om behandling af personoplysninger kan udleveres til den registrerede.	Inspiceret, at der foreligger opdaterede skriftlige procedurer, der sikrer, at der er taget stilling til, at opbevaring, indhentelse og behandling af oplysninger til identifikation af den registrerede opretholdes, så længe identifikation er påkrævet.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
2	Funktionalitet i SonWin understøtter registreredes ret til indsigt i registreret data, herunder at opbevaring, indhentelse og behandling af oplysninger til identifikation af den registrerede opretholdes, så længe identifikation er påkrævet. Der er etableret tekniske foranstaltninger i SonWin, som sikrer, at personoplysninger kan udleveres i en gennemsigtig, lettilgængelig og forståelig form til den registrerede.	Inspiceret, at der er funktionalitet i SonWin til understøttelse af registreredes ret til indsigt i registrerede data, herunder at tekniske foranstaltninger i SonWin sikrer, at personoplysninger kan udleveres i en gennemsigtig, lettilgængelig og forståelig form til den registrerede.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
3	Der foreligger skriftlige og af kunden godkendte samarbejdsvilkår mellem Sonlinc og den dataansvarlige kunde. Samarbejdsvilkårene indeholder en oversigt over kriterier for opbevaring, indhentelse og behandling af oplysninger til identifikation af den registrerede.	Inspiceret dokumentation for, at kriterier for opbevaring, indhentelse og behandling af oplysninger til identifikation af den registrerede er godkendt af den dataansvarlige.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
4	Der foretages løbende – og mindst én gang årligt – opdatering af samarbejdsvilkårene mellem Sonlinc og den dataansvarlige kunde.	Inspiceret dokumentation for, at samarbejdsvilkårene mellem Sonlinc og den dataansvarlige kunde er opdateret og godkendt af den dataansvarlige kunde mindst en gang årligt.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at opbevaring, indhentelse og behandling af oplysninger til identifikation af den registrerede opretholdes, så længe identifikation er påkrævet. Oplysninger om behandlingen af personoplysninger kan udleveres i en gennemsigtig, lettilgængelig og forståelig form til den registrerede.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
5	Der foretages løbende – og mindst én gang årligt – vurdering af, at opbevaring, indhentelse og behandling af oplysninger til identifikation af den registrerede sker i henhold til kriterierne fastsat i samarbejdsvilkår mellem Sonlinc og den dataansvarlige kunde.	Inspiceret dokumentation for, at opbevaring, indhentelse og behandling af oplysninger til identifikation af den registrerede sker i henhold til kriterierne fastsat i samarbejdsvilkår mellem Sonlinc og den dataansvarlige kunde.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
6	Ledelsen har behandlet og godkendt vurderingen af, om der foretages opbevaring, indhentelse og behandling af oplysninger til identifikation af den registrerede i henhold til kriterierne fastsat i samarbejdsvilkår mellem Sonlinc og den dataansvarlige kunde.	Inspiceret dokumentation for ledelsens godkendelse af vurderingen af, om der foretages opbevaring, indhentelse og behandling af oplysninger til identifikation af den registrerede, så længe dette er påkrævet i henhold til kriterierne fastsat i samarbejdsvilkår mellem Sonlinc og den dataansvarlige kunde.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Den registreredes indsigtsret (artikel 15)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at den registreredes ret til indsigt i egne registrerede personoplysninger og behandlingen heraf er overholdt.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
1	Der foreligger skriftlige procedurer, der beskriver, hvordan Sonlinc kan bistå den dataansvarlige kunde med at give den registrerede indsigt i egne registrerede personoplysninger og med behandlingen heraf.	Inspiceret, at der foreligger opdaterede skriftlige procedurer, hvori håndtering af de registreredes anmodninger om indsigt i behandlingen af egne personoplysninger er beskrevet.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
2	Funktionalitet i SonWin understøtter, at den dataansvarlige kunde kan give den registrerede indsigt i egne registrerede personoplysninger og i behandlingen heraf. SonWin har et fastdefineret format til udtræk af personoplysninger (kopi af de personoplysninger, som er registreret og behandles), som er godkendt af den dataansvarlige kunde.	Inspiceret, at der er funktionalitet i SonWin til understøttelse af den registreredes ret til indsigt i egne registrerede personoplysninger og i behandlingen heraf, herunder at tekniske foranstaltninger i SonWin sikrer, at personoplysninger kan udleveres i en gennemsigtig, lettilgængelig og forståelig form til den registrerede. Inspiceret, at SonWin har et fastdefineret format til udtræk af personoplysninger (kopi af de personoplysninger, som er registreret og behandles), som er godkendt af den dataansvarlige kunde.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
3	Der foretages løbende – og mindst én gang årligt – vurdering af, hvorvidt udtrækket af personoplysninger til den registrerede samt beskrivelsen af, hvordan Sonlinc kan bistå den dataansvarlige kunde med at give den registrerede indsigt i egne registrerede personoplysninger og i behandlingen heraf, er opdateret og korrekt.	Inspiceret dokumentation for, at udtrækket af personoplysninger til den registrerede og beskrivelsen af, hvordan personoplysningerne bliver behandlet, er opdateret og korrekt.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Ret til berigtigelse (artikel 16 og artikel 19)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at den registreredes ret til berigtigelse af egne registrerede personoplysninger er overholdt, herunder berigtigelse hos modtagere af personoplysningerne.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
1	Der foreligger skriftlige procedurer, der beskriver, hvordan Sonlinc kan bistå den dataansvarlige med håndtering af de registreredes ret til berigtigelse af personoplysninger.	Inspiceret, at der foreligger opdaterede skriftlige procedurer for håndtering af de registreredes ret til berigtigelse af personoplysninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
2	Funktionalitet i SonWin understøtter den dataansvarliges håndtering af de registreredes ret til berigtigelse af personoplysninger. Der er etableret tekniske foranstaltninger i SonWin, som sikrer, at sletning af personoplysninger kan gennemføres.	Inspiceret dokumentation for, at der er etableret tekniske foranstaltninger i de anvendte it-systemer til berigtigelse af personoplysninger. Inspiceret dokumentation for, at berigtigelse af personoplysninger alene sker ved anvendelse af de etablerede tekniske foranstaltninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
3	Der foretages løbende automatisk anonymisering af personoplysninger og relateret data i SonWin. Der foreligger en opdateret beskrivelse af anvendte kriterier ved løbende automatisk anonymisering af personoplysninger og relateret data i SonWin. De anvendte kriterier er godkendt af den dataansvarlige kunde.	Inspiceret dokumentation for, at den løbende automatiske anonymisering er aktiv. Inspiceret, at der foreligger en opdateret beskrivelse af de anvendte kriterier.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
4	Der foretages løbende – og mindst én gang årligt – vurdering af, at de anvendte kriterier ved løbende automatisk anonymisering af personoplysninger er korrekte og tidssvarende.	Inspiceret dokumentation for løbende opdatering af de anvendte kriterier ved løbende automatisk anonymisering af personoplysninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Ret til sletning ("retten til at blive glemt") (artikel 17 og 19)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at den registreredes ret til sletning af egne registrerede personoplysninger er overholdt, herunder sletning hos modtagere af personoplysningerne.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
1	Der foreligger skriftlige procedurer, der beskriver hvordan Sonlinc kan bistå den dataansvarliges håndtering af de registreredes ret til sletning af personoplysninger.	Inspiceret, at der foreligger opdaterede skriftlige procedurer for håndtering af de registreredes ret til sletning af personoplysninger.	Vi har observeret, at der ikke er udarbejdet procedurer for sletning af personoplysninger indeholdt i supportsager. Vi har dog observeret, at personoplysninger slettes i supportsager. Vi har ikke ved vores test konstateret yderligere væsentlige afvigelser.
2	Funktionalitet i SonWin understøtter den dataansvarliges håndtering af de registreredes ret til sletning af personoplysninger. Der er etableret tekniske foranstaltninger i de anvendte it-systemer, som sikrer, at sletning af personoplysninger kan gennemføres.	Inspiceret dokumentation for, at der er etableret tekniske foranstaltninger i de anvendte it-systemer til sletning af personoplysninger. Inspiceret dokumentation for, at sletning af personoplysninger alene sker ved anvendelse af de etablerede tekniske foranstaltninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
3	Der foretages løbende automatisk anonymisering af personoplysninger og relateret data i SonWin. Der foreligger en opdateret beskrivelse af anvendte kriterier ved løbende automatisk anonymisering af personoplysninger og relateret data i SonWin. De anvendte kriterier er godkendt af den dataansvarlige kunde.	Inspiceret dokumentation for, at den løbende automatiske anonymisering er aktiv. Inspiceret, at der foreligger en opdateret beskrivelse af de anvendte kriterier.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
4	Der foretages løbende – og mindst én gang årligt – vurdering af, at de anvendte kriterier ved løbende automatisk anonymisering af personoplysninger er korrekte og tidssvarende.	Inspiceret dokumentation for løbende opdatering af de anvendte kriterier ved løbende automatisk anonymisering af personoplysninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Ret til begrænsning af behandling (artikel 18 og 19)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at den registreredes ret til begrænsning af behandling af egne registrerede personoplysninger er overholdt, herunder begrænsning hos modtagere af personoplysningerne.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
1	Der foreligger skriftlige procedurer, der beskriver, hvordan Sonlinc kan bistå den dataansvarlige med håndtering af de registreredes ret til begrænsning af behandling af personoplysninger, herunder håndtering af adgangsbegrænsning.	Inspiceret, at der foreligger opdaterede skriftlige procedurer for håndtering af de registreredes ret til begrænsning af behandling af personoplysninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
2	Funktionalitet i SonWin understøtter den dataansvarliges håndtering af de registreredes ret til begrænsning af behandling af personoplysninger. Der er etableret tekniske foranstaltninger i SonWin, som sikrer, at begrænsning af behandling af personoplysninger kan gennemføres ved brug af adgangsbegrænsning.	Inspiceret dokumentation for, at der er etableret tekniske foranstaltninger i de anvendte it-systemer til begrænsning af behandling af personoplysninger. Inspiceret dokumentation for, at begrænsning af behandling af personoplysninger alene sker ved anvendelse af de etablerede tekniske foranstaltninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
3	Der foretages løbende – og mindst én gang årligt – vurdering af, at Sonlincs understøttelse af den dataansvarlige kundes håndtering af de registreredes ret til begrænsning af behandling af personoplysninger er korrekt og tidssvarende.	Inspiceret dokumentation for kontrol af, at begrænsning af behandling af personoplysninger er sket korrekt og uden unødig forsinkelse.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Ret til dataportabilitet (artikel 20)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at den registreredes ret til at overføre egne registrerede personoplysninger til en anden dataansvarlig er overholdt.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
1	Der foreligger skriftlige procedurer, der beskriver, hvordan Sonlinc kan bistå den dataansvarlige med behandling af de registreredes ret til overførsel af egne afgivne personoplysninger til en anden dataansvarlig.	Inspiceret, at der foreligger opdaterede skriftlige procedurer for behandling af de registreredes ret til overførsel af egne afgivne personoplysninger til en anden dataansvarlig.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
2	Funktionalitet i SonWin understøtter den dataansvarliges behandling af de registreredes ret til overførsel af egne afgivne personoplysninger til en anden dataansvarlig. SonWin har et fastdefineret format til udtræk af personoplysninger (kopi af de personoplysninger, som er registreret og behandles), som er godkendt af den dataansvarlige kunde.	Inspiceret dokumentation for, at der er etableret tekniske foranstaltninger i de anvendte it-systemer, som sikrer, at overførsel af personoplysninger er mulig. Inspiceret dokumentation for, at udtrækket af personoplysninger til overførsel er godkendt af den dataansvarlige.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
3	Der foretages løbende – og mindst én gang årligt – vurdering af, hvorvidt udtrækket af personoplysninger til den registrerede samt beskrivelsen af, hvordan Sonlinc kan bistå den dataansvarlige med behandling af de registreredes ret til overførsel af egne afgivne personoplysninger til en anden dataansvarlig, er opdateret og korrekt.	Inspiceret dokumentation for, at der foreligger en opdateret beskrivelse af, hvordan Sonlinc kan bistå den dataansvarlige med behandling af de registreredes ret til overførsel af egne afgivne personoplysninger til en anden dataansvarlig.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Den dataansvarliges ansvar – implementering af passende databeskyttelse (artikel 24)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at tekniske og organisatoriske foranstaltninger til beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger fungerer i overensstemmelse med den dataansvarliges retningslinjer.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
1	Sonlinc har indgået en generel databehandleraftale med dataansvarlige kunder, som beskriver de tekniske og organisatoriske sikkerhedsforanstaltninger, som Sonlinc har etableret til beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger.	Inspiceret dokumentation for, at den dataansvarlige har godkendt databehandlerens overordnede skriftlige procedurer og kontroller, herunder tekniske og organisatoriske foranstaltninger, til beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
2	Der foreligger skriftlige og af kunden godkendte samarbejdsvilkår mellem Sonlinc og den dataansvarlige kunde. Samarbejdsvilkårene indeholder en beskrivelse af tekniske og organisatoriske sikkerhedsforanstaltninger til beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger.	Inspiceret dokumentation for, at den dataansvarlige har godkendt databehandlerens overordnede skriftlige procedurer og kontroller, herunder tekniske og organisatoriske foranstaltninger, til beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
3	Sonlinc har etableret tekniske og organisatoriske sikkerhedsforanstaltninger til beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger. De etablerede tekniske og organisatoriske sikkerhedsforanstaltninger svarer til den dataansvarliges krav til passende databeskyttelse og er godkendt af den dataansvarlige.	Inspiceret tekniske og organisatoriske sikkerhedsforanstaltninger til beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger. Inspiceret dokumentation for, at den dataansvarlige har godkendt databehandlerens overordnede skriftlige procedurer og kontroller, herunder tekniske og organisatoriske foranstaltninger, til beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at tekniske og organisatoriske foranstaltninger til beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger fungerer i overensstemmelse med den dataansvarliges retningslinjer.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
4	Databehandleren har en beskrivelse af anvendelsen af underdatabehandlere, herunder beskrivelse af underdatabehandlernes tekniske og organisatoriske foranstaltninger til beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger, som er godkendt af den dataansvarlige.	Inspiceret dokumentation for, at den dataansvarlige har godkendt databehandlerens underdatabehandlere, herunder deres tekniske og organisatoriske foranstaltninger til beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
5	Der foretages løbende – og mindst én gang årligt – vurdering af, at de tekniske og organisatoriske sikkerhedsforanstaltninger og databeskyttelsen er passende og tidssvarende.	Inspiceret dokumentation for kontrol af, at de tekniske og organisatoriske sikkerhedsforanstaltninger og databeskyttelsen er i overensstemmelse med den dataansvarliges krav hertil.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
6	Ledelsen har behandlet og godkendt vurderingen af, om beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger er sket i overensstemmelse med databehandleraftalen og de godkendte procedurer.	Inspiceret dokumentation for, at ledelsen har sikret, at beskyttelse af den registreredes rettigheder og behandlingen af personoplysninger er sket i overensstemmelse med instruksen fra den dataansvarlige og de godkendte procedurer.	Vi er informeret om, at ledelsen løbende har været involveret i principperne for behandling af personoplysninger, herunder løbende godkendelse. Der findes dog ikke formel skriftlig dokumentation for denne godkendelse. Vi har ikke ved vores test konstateret yderligere væsentlige afvigelser.

Databeskyttelse gennem design og standardindstillinger (artikel 25)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at kravene om databeskyttelse gennem design og standardindstillinger i databehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger fungerer effektivt.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
1	Der foreligger skriftlige procedurer, hvori sikring af databeskyttelse gennem design og standardindstillinger er beskrevet, herunder hvordan Sonlinc kan bistå den dataansvarlige med sikring heraf.	Inspiceret, at der foreligger opdaterede skriftlige procedurer for sikring af databeskyttelse gennem design og standardindstillinger, herunder hvordan databehandler kan bistå den dataansvarlige med sikring heraf.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
2	Funktionalitet i SonWin sikrer effektiv og passende databeskyttelse gennem design og standardindstillinger, herunder styring af autentifikation og autorisation til enkelte skærmbilleder og system- og kundedata.	Inspiceret, at der er funktionalitet i SonWin til understøttelse af en effektiv og passende databeskyttelse gennem design og standardindstillinger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
3	Der foretages løbende – og mindst én gang årligt – vurdering af, om design af databeskyttelsen i SonWin er passende og tidssvarende.	Inspiceret dokumentation for kontrol af, at de tekniske og organisatoriske sikkerhedsforanstaltninger og databeskyttelsen er i overensstemmelse med den dataansvarliges krav hertil.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
4	Sonlinc har indgået en generel databehandleraftale med dataansvarlige kunder, som beskriver, hvilke personoplysninger der er nødvendige (dataminimering), og hvordan disse skal behandles i forhold til det/de enkelte specifikke behandlingsformål.	Inspiceret dokumentation for den dataansvarliges instruks til databehandleren om, hvilke personoplysninger der er nødvendige, og hvordan disse skal behandles i forhold til det/de specifikke behandlingsformål.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
5	Der foretages løbende – og mindst én gang årligt – vurdering af, at der alene foretages behandling af de personoplysninger, som er nødvendige i forhold til det enkelte specifikke behandlingsformål og databehandleraftalen.	Inspiceret dokumentation for kontrol af, at behandling af personoplysninger er begrænset til det specifikke formål i overensstemmelse med instruks.	Vi er informeret om, at ledelsen løbende har været involveret i principperne for behandling af personoplysninger, herunder løbende godkendelse. Der findes dog ikke formel skriftlig dokumentation for denne godkendelse. Vi har ikke ved vores test konstateret yderligere væsentlige afvigelser.

Databehandler – behandling af personoplysninger på vegne af den dataansvarlige (artikel 28 og 29)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at behandling af personoplysninger alene sker i henhold til en kontrakt eller et andet retligt bindende dokument (databehandleraftale), samt at databehandlingen alene foretages af databehandlere, som er godkendt af den dataansvarlige.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
1	Sonlinc har indgået en generel databehandleraftale med dataansvarlige kunder, som beskriver de tekniske og organisatoriske sikkerhedsforanstaltninger, som Sonlinc har etableret, for at databehandlingen opfylder kravene i databeskyttelsesforordningen og databeskyttelsesloven samt sikrer beskyttelse af den registreredes rettigheder.	Inspiceret dokumentation for, at databehandleraftalen beskriver de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren har etableret, for at databehandlingen opfylder kravene i databeskyttelsesforordningen og databeskyttelsesloven samt sikrer beskyttelse af den registreredes rettigheder.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
2	Der foretages løbende – og mindst én gang årligt – vurdering af, om databehandleraftalen skal opdateres, herunder om tilstrækkeligheden af de tekniske og organisatoriske sikkerhedsforanstaltninger, som Sonlinc har etableret, for at databehandlingen opfylder kravene i databeskyttelsesforordningen og databeskyttelsesloven samt sikrer beskyttelse af den registreredes rettigheder.	Inspiceret dokumentation for, at databehandleraftalen beskriver de tekniske og organisatoriske sikkerhedsforanstaltninger, som databehandleren har etableret, for at databehandlingen opfylder kravene i databeskyttelsesforordningen og databeskyttelsesloven samt sikrer beskyttelse af den registreredes rettigheder.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
3	Der foretages løbende – og mindst én gang årligt – vurdering af, at Sonlinc har overholdt de tekniske og organisatoriske sikkerhedsforanstaltninger, som er etableret, for at databehandlingen opfylder kravene i databeskyttelsesforordningen og databeskyttelsesloven, samt sikrer beskyttelse af den registreredes rettigheder. Endvidere foretages der vurdering af, at behandling af personoplysninger er foretaget i overensstemmelse med databehandleraftalen.	Inspiceret dokumentation for kontrol af, at databehandler har overholdt de tekniske og organisatoriske sikkerhedsforanstaltninger, som er etableret, for at databehandlingen opfylder kravene i databeskyttelsesforordningen og databeskyttelsesloven, samt sikrer beskyttelse af den registreredes rettigheder, samt at behandling af personoplysninger er foretaget i overensstemmelse med databehandleraftalen.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at behandling af personoplysninger alene sker i henhold til en kontrakt eller et andet retligt bindende dokument (databehandleraftale), samt at databehandlingen alene foretages af databehandlere, som er godkendt af den dataansvarlige.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
4	Ledelsen har behandlet og godkendt vurderingen af overholdelsen af de tekniske og organisatoriske sikkerhedsforanstaltninger og databeskyttelsen, samt at behandlingen af personoplysninger er sket i overensstemmelse med databehandleraftalen.	Inspiceret dokumentation for, at ledelsen har sikret overholdelsen af de tekniske og organisatoriske sikkerhedsforanstaltninger og databeskyttelsen, samt at behandlingen af personoplysninger er sket i overensstemmelse med databehandleraftalen.	Vi er informeret om, at ledelsen løbende har været involveret i principperne for behandling af personoplysninger, herunder løbende godkendelse. Der findes dog ikke formel skriftlig dokumentation for denne godkendelse. Vi har ikke ved vores test konstateret yderligere væsentlige afvigelser.
5	Sonlinc sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer for, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
6	Sonlinc har modtaget en generel godkendelse fra den dataansvarlige kunde af anvendelse af andre underdatabehandlere. Sonlinc underretter den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af underdatabehandlere.	Inspiceret dokumentation for, at den dataansvarlige har godkendt anvendelsen af andre underdatabehandlere. Inspiceret dokumentation for, at den dataansvarlige er blevet underrettet om planlagte ændringer vedrørende tilføjelse eller erstatning af underdatabehandlere.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
7	Der foreligger skriftlige procedurer, som beskriver, at Sonlinc alene må behandle personoplysninger, herunder overføre personoplysninger til et tredjeland eller en international organisation, efter dokumenteret instruks fra den dataansvarlige eller i henhold til EU-ret eller national ret. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer for, at databehandler alene må behandle og overføre personoplysninger efter dokumenteret instruks fra den dataansvarlige eller i henhold til EU-ret eller national ret.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at behandling af personoplysninger alene sker i henhold til en kontrakt eller et andet retligt bindende dokument (databehandleraftale), samt at databehandlingen alene foretages af databehandlere, som er godkendt af den dataansvarlige.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
8	Der foreligger skriftlige procedurer, som – ved Sonlincs brug af underdatabehandlere til udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige kunde – beskriver Sonlincs kontroller til sikring af, at underdatabehandler overholder de samme databeskyttelsesforpligtelser som dem, der er fastsat i databehandleraftalen mellem den dataansvarlige kunde og Sonlinc. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer, som beskriver databehandlers kontroller til sikring af, at underdatabehandlere overholder de samme databeskyttelsesforpligtelser som dem, der er fastsat i databehandleraftalen mellem den dataansvarlige og databehandler.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
9	Der foreligger skriftlige procedurer, som beskriver, hvordan Sonlinc så vidt muligt bistår den dataansvarlige kunde med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder ved hjælp af passende tekniske og organisatoriske foranstaltninger. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer, som beskriver, hvordan databehandler bistår den dataansvarlige med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder ved hjælp af passende tekniske og organisatoriske foranstaltninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
10	Der foreligger skriftlige procedurer, som beskriver, hvordan Sonlinc – under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige – bistår den dataansvarlige med at sikre overholdelse af den dataansvarliges forpligtelser i forhold til: • Behandlingssikkerhed (artikel 32) • Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden (artikel 33) • Underretning om brud på persondatasikkerheden til den registrerede (artikel 34) • Konsekvensanalyse vedrørende databeskyttelse (artikel 35)	Inspiceret, at der foreligger opdaterede skriftlige procedurer, som beskriver, hvordan databehandler bistår den dataansvarlige med at sikre overholdelse af den dataansvarliges forpligtelser.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at behandling af personoplysninger alene sker i henhold til en kontrakt eller et andet retligt bindende dokument (databehandleraftale), samt at databehandlingen alene foretages af databehandlere, som er godkendt af den dataansvarlige.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
	• Forudgående høring (artikel 36). Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.		
11	Der foreligger skriftlige procedurer, som beskriver, hvordan Sonlinc efter den dataansvarliges valg sletter eller tilbageleverer alle personoplysninger til den dataansvarlige, efter at tjenesterne vedrørende behandling er ophørt, og sletter eksisterende kopier, medmindre EU-ret eller national ret foreskriver opbevaring af personoplysningerne. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer, som beskriver, hvordan databehandler efter den dataansvarliges valg sletter eller tilbageleverer alle personoplysninger til den dataansvarlige, efter at tjenesterne vedrørende behandling er ophørt, og sletter eksisterende kopier.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
12	Der foreligger skriftlige procedurer, som beskriver, hvordan Sonlinc stiller alle oplysninger, der er nødvendige for at påvise overholdelse af kravene til databehandler, til rådighed for den dataansvarlige samt giver mulighed for og bidrager til revisioner, inspektioner mv., der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer, som beskriver, hvordan databehandler stiller alle oplysninger, der er nødvendige for at påvise overholdelse af kravene til databehandler, til rådighed for den dataansvarlige samt giver mulighed for og bidrager til revisioner, inspektioner mv.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Fortegnelse over behandlingsaktiviteter (artikel 30)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at databehandleren fører en fortegnelse over kategorier af behandlingsaktiviteter, der foretages på vegne af de dataansvarlige.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
1	Der foreligger hos Sonlinc en generel fortegnelse over kategorier af behandlingsaktiviteter, som indeholder: • It-afdelingen hos hver dataansvarlig og – hvis det er relevant – den dataansvarliges databeskyttelsesrådgiver • De kategorier af behandling, der foretages på vegne af alle dataansvarlige • Kontrol af, at Sonlinc fortsat ikke benytter sig af underleverandører i tredjeland, eller der bliver overført data med persondata til tredjeland eller en international organisation, og i tilfælde af overførsler i henhold til artikel 49, stk. 1, andet afsnit, dokumentation for passende garantier • En generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger.	Inspiceret dokumentation for, at der foreligger en fortegnelse over kategorier af behandlingsaktiviteter for den enkelte dataansvarlige med angivelse af den nødvendige information.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
2	Der foretages løbende – og mindst én gang årligt – vurdering af, hvorvidt fortegnelsen over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige skal opdateres.	Inspiceret dokumentation for, at fortegnelsen over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige er opdateret og korrekt.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
3	Ledelsen har sikret, at fortegnelsen over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige er fyldestgørende, opdateret og korrekt.	Inspiceret dokumentation for, at ledelsen har sikret, at fortegnelsen over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige er fyldestgørende, opdateret og korrekt.	Vi er informeret om, at ledelsen løbende har været involveret i principperne for behandling af personoplysninger, herunder løbende godkendelse. Der findes dog ikke formel skriftlig dokumentation for denne godkendelse. Vi har ikke ved vores test konstateret yderligere væsentlige afvigelser.

Behandlingssikkerhed (artikel 32)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at der på baggrund af en evaluering af risici er truffet passende tekniske og organisatoriske sikkerhedsforanstaltninger mod hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
1	Sonlinc har foretaget en generel risikovurdering af behandlingen af personoplysninger på vegne af dataansvarlige kunder.	Inspiceret dokumentation for, at der er foretaget en generel risikovurdering af behandlingen af personoplysninger på vegne af dataansvarlige kunder.	Vi har observeret, at der er udarbejdet en generel risikovurdering for GDPR, dog ikke specifikt for SonWin-applikationen. Vi har ikke ved vores test konstateret yderligere væsentlige afvigelser.
2	Sonlinc har etableret passende tekniske og organisatoriske sikkerhedsforanstaltninger for at sikre et sikkerhedsniveau, som passer til risiciene i Sonlincs risikovurdering. De etablerede tekniske og organisatoriske sikkerhedsforanstaltninger er godkendt af den dataansvarlige kunde.	Inspiceret dokumentation for, at der er etableret passende tekniske og organisatoriske sikkerhedsforanstaltninger, som sikrer et sikkerhedsniveau, som passer til risiciene i databehandlerens risikovurdering. Inspiceret dokumentation for, at de etablerede tekniske og organisatoriske sikkerhedsforanstaltninger har fungeret effektivt i erklæringsperioden. Inspiceret dokumentation for, at den dataansvarlige har godkendt de etablerede tekniske og organisatoriske sikkerhedsforanstaltninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
3	Der foretages løbende – og mindst én gang årligt – vurdering af, hvorvidt risikovurderingen er opdateret og passende.	Inspiceret dokumentation for, at databehandlers risikovurdering er opdateret og passende.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
4	Der foretages løbende – og mindst én gang årligt – vurdering af, hvorvidt de tekniske og organisatoriske sikkerhedsforanstaltninger afdækker risiciene i Sonlincs opdaterede risikovurdering.	Inspiceret dokumentation for, at de tekniske og organisatoriske sikkerhedsforanstaltninger sikrer et sikkerhedsniveau, som passer til risiciene i databehandlerens opdaterede risikovurdering.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at der på baggrund af en evaluering af risici er truffet passende tekniske og organisatoriske sikkerhedsforanstaltninger mod hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
5	Fysiske personer hos Sonlinc samt underdatabehandlere er instrueret i håndtering af personoplysninger i henhold til databehandleraftaler mellem Sonlinc og dataansvarlige kunder.	Inspiceret dokumentation for, at fysiske personer hos databehandleren og underdatabehandlere er instrueret i håndtering af personoplysninger i henhold til den dataansvarliges instruks.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
6	Ledelsen har behandlet og godkendt risikovurderinger.	Inspiceret dokumentation for, at ledelsen har behandlet og godkendt de risikovurderinger, som har været gældende i revisionsperioden.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
7	Ledelsen har behandlet og godkendt de etablerede tekniske og organisatoriske sikkerhedsforanstaltninger.	Inspiceret dokumentation for, at ledelsen har behandlet og godkendt de etablerede tekniske og organisatoriske sikkerhedsforanstaltninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden (artikel 33 og 34)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at databehandler ved brud på persondatasikkerheden kan understøtte den dataansvarliges pligt til rettidig og fyldestgørende anmeldelse til tilsynsmyndigheden, samt underretning til de registrerede, hvis personoplysninger er omfattet af bruddet.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
1	Der foreligger skriftlige procedurer, hvori håndtering af brud på persondatasikkerheden, herunder rettidig kommunikation til den dataansvarlige, er beskrevet. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger opdaterede skriftlige procedurer for håndtering af brud på persondatasikkerheden, herunder at rettidig kommunikation til den dataansvarlige er beskrevet.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
2	Sonlinc sikrer registrering af alle brud på persondatasikkerheden.	Inspiceret dokumentation for, at alle brud på persondatasikkerheden er registreret hos databehandleren.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
3	Sonlinc fremsender dokumentation omfattende som minimum de faktiske omstændigheder ved bruddet, dets virkning og omfang samt de trufne afhjælpende foranstaltninger til den dataansvarlige.	Inspiceret dokumentation for, at databehandler har fremsendt dokumentation omfattende som minimum de faktiske omstændigheder ved bruddet, dets virkning og omfang samt de trufne afhjælpende foranstaltninger til den dataansvarlige.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
4	Ledelsen har sikret, at alle brud på persondatasikkerheden er kommunikeret rettidigt og fyldestgørende til den dataansvarlige.	Inspiceret dokumentation for, at ledelsen har sikret, at alle brud på persondatasikkerheden er kommunikeret rettidigt og fyldestgørende til den dataansvarlige.	Vi er informeret om, at ledelsen løbende har været involveret i principperne for behandling af personoplysninger, herunder løbende godkendelse af rapportering af brud. Der findes dog ikke formel skriftlig dokumentation for denne godkendelse. Vi har ikke ved vores test konstateret yderligere væsentlige afvigelser.

Konsekvensanalyse vedrørende databeskyttelse (artikel 35)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at databehandler har modtaget resultatet af den dataansvarliges konsekvensanalyse vedrørende databeskyttelse, inden der foretages behandling af personoplysninger, samt at der foretages en fornyet konsekvensanalyse ved ændring i den risiko, som behandlingsaktiviteterne udgør.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
1	Sonlinc har etableret passende procedurer samt tekniske og organisatoriske sikkerhedsforanstaltninger, som sikrer behandling af personoplysninger i overensstemmelse med de dataansvarliges og/eller egne konsekvensanalyser.	Inspiceret dokumentation for databehandlers etablering af procedurer samt tekniske og organisatoriske sikringsforanstaltninger til at sikre, at persondatabehandlingen sker i overensstemmelse med de dataansvarliges og/eller egne konsekvensanalyser.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
2	Sonlincs etablerede procedurer samt tekniske og organisatoriske sikkerhedsforanstaltninger til databeskyttelse er godkendt af den dataansvarlige kunde, inden der foretages behandling af personoplysninger.	Inspiceret dokumentation for, at de af databehandler etablerede procedurer samt tekniske og organisatoriske sikkerhedsforanstaltninger er godkendt af den dataansvarlige.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
3	Der foretages løbende – og mindst én gang årligt – vurdering af, hvorvidt databeskyttelsen er foretaget i overensstemmelse med de dataansvarliges og/eller egne konsekvensanalyser.	Inspiceret dokumentation for, at der foretages løbende – og mindst årlig – vurdering af, hvorvidt databeskyttelsen er foretaget i overensstemmelse med de dataansvarliges og/eller egne konsekvensanalyser.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Forudgående høring (artikel 36)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at databehandler har modtaget resultatet af den dataansvarliges høring hos tilsynsmyndigheden, såfremt konsekvensanalysen viser, at behandlingen af personoplysninger vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen.

Nr.	Databehandlerens kontrolaktivitet	PwC's udførte test	Resultat af test
1	Sonlinc har etableret de procedurer samt tekniske og organisatoriske sikkerhedsforanstaltninger, som er påkrævet af tilsynsmyndigheden for behandling af de specifikke personoplysninger.	Inspiceret dokumentation for, at krav fra tilsynsmyndighederne er indarbejdet i procedurer samt tekniske og organisatoriske sikkerhedsforanstaltninger.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
2	Sonlincs etablerede procedurer samt tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af tilsynsmyndighedens krav er godkendt af den dataansvarlige kunde.	Inspiceret dokumentation for, at den dataansvarlige har godkendt de af databehandler etablerede procedurer samt tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af tilsynsmyndighedens krav.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
3	Der foretages løbende – og mindst én gang årligt – vurdering af, hvorvidt databehandlingen er foretaget i overensstemmelse med tilsynsmyndighedens krav.	Inspiceret dokumentation for løbende opfølgning på overholdelsen af tilsynsmyndighedernes krav til databehandlingen.	Vi har ikke ved vores test konstateret væsentlige afvigelser.