Fonden F&P Formidling

ISAE 3000-erklæring omhandlende udvalgte GDPR-kontroller i perioden 1. januar – 31. december 2020 relateret til WebEDI-systemet

Building a better working world

Indhold

1 Beskrivelse af WebEDI-systemet i relation til behandling persondata

1.1 Formål og beskrivelse af systemet

Fonden F&P Formidling (herefter F&P) har udviklet en WebEDI-løsning, der integrerer udveksling via webblanketter, EDIFACT og XML. Systemet afvikles på en Windows-platform med underliggende SQL-databaser.

Udveksling via WebEDI-systemet er baseret på, at de deltagende parter kan udveksle dokumenter enten via en webgrænseflade, webservice/rest-api, en WebEDI-grænseflade eller alternativt via kombinationer af nævnte udvekslingsmetoder. Løsningen sikrer, at alle tilsluttede virksomheder i princippet kan udveksle data elektronisk, således at de tilsluttede virksomheder, der investerer i en elektronisk integreret løsning, ikke parallelt skal håndtere en alternativ manuel arbejdsgang.

F&P's WebEDI-servere udgør den centrale udvekslingsplatform for udveksling af dokumenter for forsikringsselskaber, pensionsselskaber samt banker og leasingselskaber, og alle oplysninger vedrørende ordningerne Opsigelser, Regres, Panthaverdeklarationer, LD-ordninger, §41 mellem pensionsselskaber, §41 mellem bank og pensionsselskaber, Skadehistorik og FP-attester distribueres gennem serveren. Formål

Formålet med WebEDI-systemets behandling af personoplysninger på vegne af de dataansvarlige er at understøtte driften af systemet, herunder udvikling, vedligehold og support på systemet, hvorved person-oplysningerne i systemet tilgås.

Systembeskrivelse

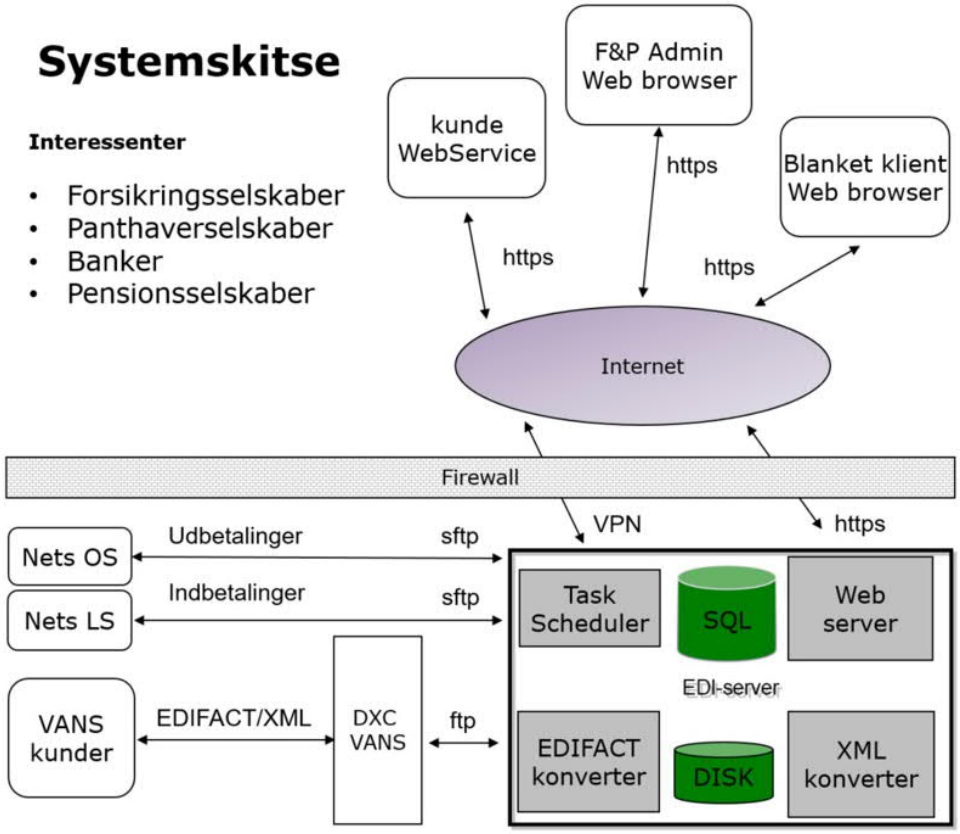
WebEDI-serveren er en service, som de tilsluttede selskaber benytter til elektronisk udveksling af dokumenter mellem selskaberne indbyrdes, samt disses samarbejdspartnere – fx panthavere og læger.

Systemet blev etableret i 1999 med det formål, at mindre selskaber kunne udveksle data med de større selskaber, som benyttede EDIFACT som dataudveksling. Systemet er under løbende udvikling og moder-nisering – nye ordninger er kommet til, og ordninger er udgået.

I dag håndteres otte ordninger via WebEDI-serveren, der har en daglig volumen på godt 12.000 dokumen-ter svarende til otte dokumenter i minuttet.

Udveksling af data foretages via Web, EDIFACT, XML, WebService samt Rest Api.

Skitse af den overordnede komponentmodel af WebEDI-systemet



Databasen er placeret på en separat databaseserver.

WebEDI-serveren består af følgende hovedkomponenter:

- En Web-server, som benyttes til administration af løsningen samt selskabsadministration og sagsbehandling for de mindre selskaber. Web-serveren udstiller desuden en WebService til Pensionsløsningerne samt et Rest Api til Skadehistorik.
- En EDIFACT-konverter, der håndterer og mapper indkommende og udgående EDIFACT.
- En XML-konverter, der håndterer og mapper indkommende og udgående XML.
- Task Scheduler til afvikling af diverse jobs.

Der anvendes følgende front-end-teknologier: jquery, jquery ui, jqgrid, html5.

Der anvendes følgende back-end-teknologier: C#, MVC.NET, EF6, Linq, SOAP WS/WebApi/RestApi.

Der anvendes følgende serverteknologier: Microsoft Windows Server, Microsoft SQL Server.

Fordelingen af volumen (*) mellem Web, EDIFACT, XML/WebService og Rest Api er:

Ordning	Web	EDIFACT	XML/WS	Rest Api
Opsigelser	5,8 %	94,2 %		
Regres	4,6 %	95,4 %		
Panthaverdeklaration	36,1 %	63,9 %		
Pensionsoverførsler – PGF41	36,9 %		63,1 %	
Pensionsoverførsler – UPB	81,3 %		18,7 %	
LD-flytning	33,6 %		66,4 %	
FP-attester	100 %			
Skadehistorik				100%

(*) baseret på tal for 2018.

Selskaberne er opdelt i følgende typer:

Selskabstype	Udveksler	Bemærkninger
Forsikringsselskab	Opsigelser Regres Panthaverdeklarationer FP-attester Skadehistorik	
Panthaverselskab	Panthaverdeklarationer	
Pensionsselskab	Pensionsoverførsler (PGF41, pension-pension) Pensionsoverførsler (UPB, pension-bank) LD-flytning FP-attester	
Bank	Pensionsoverførsler (UPB, pension-bank) LD-Flytning	
Administration		Kun F&P

Organisation

Bag WebEDI står Fonden for F&P Formidling, som står for drift, udvikling og support af løsningen. Databehandleraftalen er indgået mellem de enkelte selskaber, som er tilsluttet WebEDI (forsikrings- og pensionsselskaber, samt pengeinstitutter og leasingselskaber) og Fonden F&P Formidling.

De ansatte i sekretariatet, der bistår WebEDI, er alle ansat i Forsikringsorganisationernes Fællessekretariat.

WebEDI og Fonden F&P formidling har adresse hos Forsikring & Pension på Philip Heymanns Allé 1, 2900 Hellerup.

WebEDI-it-systemet er hosted hos Sentia, der ligger Smedeland 32, 2600 Glostrup.

Sentia får én gang årligt udarbejdet en ISAE 3000-databehandlererklæring af ekstern revisor vedrørende deres behandling af persondata. Seneste erklæring er modtaget i januar og gælder for 2019. Der er ikke handlingskrævende bemærkninger i rapporten.

1.2 Karakteren af behandlingen og de oplysninger, der behandles

WebEDI's behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om udveksling af oplysninger mellem selskaberne, som er tilsluttet systemet (forsikrings- og pensionsselskaber, samt pengeinstitutter og leasingselskaber). Der er også kommunikation med praktiserende læger, hvorfra der indhentes helbredsattester og journaloplysninger.

I systemet behandles både almindelige persondata som navn, adresse, e-mailadresse, postnummer og telefonnummer, samt følsomme persondata som CPR-nummer, pensions- og forsikringsoplysninger (kan være helbredsoplysninger og/eller oplysninger om tilhørsforhold til en fagforening).

De registrerede er forsikringstagere og kunder i de tilsluttede selskaber, samt pårørende eller begunstigede. Der behandles tillige kontaktdata om ansatte og kontaktpersoner i virksomheder med tilslutning til WebEDI i forbindelse med overførsel af data mellem de tilsluttede selskaber.

Behandlingen er reguleret af en aftale

Der er indgået databehandleraftale mellem Fonden for F&P Formidling og de selskaber, der er tilsluttet WebEDI-systemet. Databehandleraftalen er baseret på Datatilsynets oprindelige skabelon og er identisk for samtlige dataansvarlige. Instruksen fra samtlige selskaber er således også enslydende og uden specifikke krav for nogen selskaber.

Databehandleraftalen mellem WebEDI og Fonden for F&P Formidling fastslår og beskriver parternes roller og ansvar som henholdsvis dataansvarlig og databehandler.

Databehandleraftalen sætter således rammen for WebEDI's behandling af persondata og fastslår samtidig WebEDI's forpligtelser i henhold til databehandleraftalen og for overholdelse af de krav, der påhviler den dataansvarlige under databeskyttelsesforordningen og/eller databeskyttelsesloven.

Behandling sker på grundlag af instruks fra de dataansvarlige

Databehandleraftalen indeholder instruks til WebEDI med en beskrivelse af karakteren af databehandlingen, som er omfattet af aftalen, de omfattede kategorier af personoplysninger og registrerede, samt formålet med behandlingen.

I aftalen instruerer de dataansvarlige WebEDI om behandlingen af personoplysninger i overensstemmelse med databehandleraftalens bilag c samt i øvrigt at foretage enhver behandling, der er nødvendig for WebEDI's drift i henhold til hovedaftalen, herunder aftalte services, samt WebEDI's overholdelse af databehandleraftalen.

Krav til behandlingssikkerhed

Instruksen omfatter specifikke krav til tekniske og organisatoriske sikkerhedsforanstaltninger, som WebEDI skal træffe for at sikre mod, at persondata hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med Databeskyttelsesforordningen og/eller Databeskyttelsesloven. Sådanne sikkerhedsforanstaltninger skal afspejle det aktuelle tekniske niveau, være proportionale i forhold til gennemførelsesomkostninger i betragtning af behandlingens karakter, omfang, kontekst og formål, samt risikoen for fysiske personers rettigheder og frihedsrettigheder. WebEDI skal endvidere overholde eventuelt aftalte særlige krav til sikkerhedsforanstaltninger. I praksis håndteres disse foranstaltninger af Sentia og er indskrevet i underdatabehandleraftalen med samme. Kontrol af Sentia sker ved fremsendelse af revisionserklæring én gang årligt.

Opbevaring/sletterutine

Krav til opbevaring og sletterutiner er indeholdt i instruksen.

Instruks vedrørende overførsel af persondata til tredjelande

Der gives ingen særskilt instruks på adgang til overførsel til tredjelande, hvorfor dette som udgangspunktet ikke er tilladt.

Nærmere procedurer for den dataansvarliges tilsyn med behandlingen hos både databehandleren og eventuelle underdatabehandlere

Instruksen omfatter krav om udarbejdelse af revisionserklæringer i form af en ISAE 3402, ISAE 3000 eller lignende standard for både behandlingen hos WebEDI og underdatabehandlere.

WebEDI's forpligtelser i henhold til aftalen i øvrigt

Fortrolighed

Aftalen fastslår endvidere, at medarbejdere hos WebEDI, der er beskæftiget med behandling af personoplysninger, er underlagt tavshedspligt, og at alene medarbejdere, der har arbejdsbetinget behov derfor, må have adgang til personoplysningerne.

Vilkår for anvendelse af underdatabehandlere

Databehandleraftalen regulerer og fastsætter vilkår for WebEDI's anvendelse af underdatabehandlere, herunder forhold vedrørende information og varsling om nye underdatabehandlere, tilsvarende krav til underdatabehandlere, samt forhold vedrørende underdatabehandlere uden for EU/EØS.

Krav om underretning til de dataansvarlige

Instruksen til WebEDI omfatter pligt til at underrette den dataansvarlige:

- Hvis instruks strider mod Databeskyttelsesforordningen og/eller Databeskyttelsesloven.
- Hvis WebEDI ikke kan opfylde forpligtelserne i databehandleraftalen grundet forpligtelser i anden lovgivning.
- I tilfælde af brud på persondatasikkerheden konstateret hos WebEDI eller en af WebEDI's eventuelle underdatabehandlere.

Vilkår for bistand og samarbejde i relation til de dataansvarliges ansvar

Databehandleraftalen fastlægger rammerne for parternes samarbejde, herunder processer for håndtering af sikkerhedsbrud og kundens indsigt og kontrol med behandlingen.

Hvis WebEDI modtager en henvendelse relateret til selskabernes forpligtelser over for den registrerede, informerer WebEDI den registrerede person om, at WebEDI alene er databehandler, og at personen skal rette henvendelse til den dataansvarlige. WebEDI skal efter aftalen assistere de dataansvarlige med håndteringen af de registreredes anmodninger om indsigt, berigtigelse, blokering eller sletning, herunder implementere passende tekniske og organisatoriske foranstaltninger til at understøtte dette.

1.3 Revision og kontrol af WebEDI og eventuelle underdatabehandlere

Denne erklæring udgør WebEDI's rapportering, som har til formål at give de dataansvarlige indsigt i behandlingen af personoplysninger under WebEDI-systemet. WebEDI stiller i øvrigt, efter forudgående skriftlig anmodning og rimeligt varsel, alle oplysninger og dokumentation til rådighed for den dataansvarlige, hvor disse er nødvendige for at påvise WebEDI's overholdelse af databehandleraftalen samt databeskyttelsesforordningens artikel 28.

De dataansvarlige (eller de dataansvarlige repræsenteret af et anerkendt revisionsfirma) er endvidere berettiget til, efter forudgående skriftlig anmodning og rimeligt varsel, at foretage inspektion af WebEDI-lokaliteter under behørig iagttagelse af krav til sikkerhed og fortrolighed. Tilsvarende er den dataansvarlige, jf. databehandleraftalen, berettiget til at foretage inspektion af lokaliteter tilhørende underdatabehandlere, idet den dataansvarlige dog accepterer, at WebEDI i videst muligt omfang vil gennemføre inspektionen på den dataansvarliges vegne.

Både vedrørende inspektion af WebEDI's lokaliteter og underdatabehandlerens lokaliteter gælder, at fysisk inspektion af lokaliteter alene kan finde sted i det omfang formålet med inspektionen ikke kan opfyldes på anden vis, herunder ved WebEDI's/underdatabehandleres fremlæggelse af rapporter, erklæringer eller anden skriftlig dokumentation. Databehandleraftalen fastlægger vilkår for afholdelse af omkostninger i forbindelse med inspektion.

1.4 Risikovurdering

Det er de dataansvarliges ansvar at foretage en vurdering af risikoen for de registreredes rettigheder, herunder en afvejning af disse risici i forhold til de forholdsregler, der bliver truffet for at beskytte disse rettigheder i forbindelse med behandlingen af personoplysninger i WebEDI-systemet.

I forbindelse med større ændringer i systemet gennemfører WebEDI som databehandler en risikovurdering ud fra den registreredes perspektiv som led i den generelle risikovurdering og sikkerhedsvurdering, som WebEDI i øvrigt gennemfører i forbindelse med sådanne aktiviteter.

I de særlige tilfælde, hvor en høj risiko indebærer, at den dataansvarlige skal foretage en konsekvensanalyse vedrørende databeskyttelse, kan WebEDI efter anmodning bistå de dataansvarlige hermed.

1.5 Kontrolforanstaltninger

WebEDI er underlagt den overordnede persondatapolitik for Forsikringsorganisationernes Fællessekretariat. Politikken er godkendt af det interne organ GDPR-styregruppen, som repræsenterer Forsikring & Pensions direktion. Persondatapolitikken revideres efter behov og mindst én gang årligt.

Persondatapolitikken er udmøntet i en række forretningsgange og procedurer, inklusive kontrolmål, for efterlevelse af GDPR specifikt for WebEDI. Procedurerne er ligeledes godkendt af GDPR-styregruppen. Opdatering og kontrol af disse forretningsgange og procedurer er forankret både i it, WebEDI's sekretariat og i JURA.

Der er adgang til data i WebEDI-systemet for de ansatte i Forsikring & Pension, der arbejder med systemet.

Den følgende beskrivelse refererer til de relevante bestemmelser i databeskyttelsesforordningen i forhold til WebEDI's behandling af personoplysninger, der er omfattet af denne erklæring:

Principper for behandling af personoplysninger (Databeskyttelsesforordningen artikel 5, 6 og 9)

WebEDI's medarbejdere er underlagt Forsikringsorganisationernes Fællessekretariats overordnede persondatapolitik, der fastlægger principperne for behandling af persondata i organisationen. Principperne afspejler kravene i databeskyttelsesforordningen og er understøttet af en række praktiske procedurer.

Medarbejderne i organisationen bliver ved ansættelse og efterfølgende løbende undervist i persondatapolitikken og de understøttende procedurer, som de forventes at kende indholdet af.

Lovlighed, rimelighed, gennemsigtighed og dataminimering

I persondatapolitikken og de understøttende procedurer er der fastsat retningslinjer om, at persondata skal behandles ordentligt. Det er præciseret, at behandling kun må ske inden for lovgivningens rammer, og at der skal være et behandlingsgrundlag.

Det er endvidere præciseret, at data alene må behandles til specifikke og nærmere afgrænsede formål, samt at der ikke må behandles mere data eller i længere tid, end der er behov for. Der skal være gennemsigtighed med behandlingen for den registrerede.

Da WebEDI er databehandler, er det de dataansvarlige, der direkte har ansvaret for at sikre grundlaget for behandlingen af data, herunder også den lovmæssige hjemmel, der fx kan være samtykke, opfyldelse af en kontrakt eller sikre, at den dataansvarlige kan forfølge en anden legitim interesse.

Det fremgår af politikken og de underliggende procedurer, at data behandles efter instruks fra de dataansvarlige. Endvidere fremgår det, at medarbejderne er forpligtede til at gøre opmærksom på, hvis de mener en instruks på en behandling er i strid med lovgivningen.

WebEDI har på baggrund af instruks fra de dataansvarlige taget hensyn til overholdelsen af principperne om lovlighed, rimelighed, gennemsigtighed og dataminimering i forbindelse med indretning af WebEDI-systemet og i de interne processer for kontrol med behandlingen af personoplysninger.

De registreredes rettigheder (Databeskyttelsesforordningen Kap. III, artikel 12-23)

De registreredes rettigheder efter kapitel III i databeskyttelsesforordningen er beskrevet i persondatapolitikken og de underliggende procedurer, der også indeholder retningslinjer for håndteringen heraf.

Som udgangspunkt vil anmodninger fra de registrerede direkte til WebEDI blive henvist til den relevante dataansvarlige efter de fastlagte procedurer.

WebEDI som databehandler (Databeskyttelsesforordningen Kap. IV, artikel 28)

WebEDI agerer som databehandler på vegne de tilsluttede selskaber, og en stor andel af disse er medlemmer af Forsikring & Pension. Der er indgået databehandleraftale mellem parterne, der i en instruks til WebEDI fastsætter genstanden for og varigheden af behandlingen, behandlingens karakter og formål, typen af personoplysninger og kategorier af registrerede, samt den dataansvarliges forpligtelser og rettigheder.

Det fremgår af persondatapolitikken og de understøttende procedurer, at WebEDI alene må behandle data i henhold til databehandleraftale og instruks. Endvidere fremgår det, at medarbejderne er forpligtede til at gøre opmærksom på, hvis de mener en instruks på en behandling er i strid med lovgivningen.

I en erklæring godkendt af GDPR-styregruppen underskriver chefen for WebEDI, at behandling alene er sket inden for instruks.

Databehandleraftalen indeholder krav til WebEDI's brug af underdatabehandlere. Der er i aftalen allerede godkendt forskellige underdatabehandlere. Herudover er der i aftalen givet en generel godkendelse til WebEDI til antagelse af nye underdatabehandlere, efter høring af de dataansvarlige. De interne procedurer for WebEDI omfatter retningslinjer for høring af de dataansvarlige, der skal have mulighed for at gøre indsigelser mod den valgte underdatabehandler.

WebEDI benytter alene underdatabehandlere, der lever op til sikkerhedskravene sat af de dataansvarlige. Der indgås databehandleraftaler med de valgte underdatabehandlere, som pålægger underdatabehandlerne pligter, der understøtter WebEDI's forpligtelser over for de dataansvarlige, samt fører kontrol med behandlingen hos underdatabehandleren.

WebEDI's primære underdatabehandler er Sentia, der hoster WebEDI-systemet. WebEDI har indgået databehandlerkontrakt, som understøtter forpligtelserne, der påhviler WebEDI efter databehandleraftalen med de dataansvarlige. WebEDI har her sikret sig, at de efter underdatabehandleraftalen årligt modtager en ISAE 3402-erklæring på it-systemet og en ISAE 3000-erklæring i forhold til GDPR fra Sentia.

Seneste erklæringer er modtaget for perioden 1. januar til 31. december 2019.

Fortegnelser over behandlingsaktiviteter (Databeskyttelsesforordningens artikel 30)

WebEDI fører fortegnelse over behandlingsaktiviteterne under WebEDI-systemet, der omfatter en beskrivelse af:

- Kategorien af behandlingen.
- Generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger.

Persondatasikkerhed (Databeskyttelsesforordningens artikel 32-34)

Der er for WebEDI-systemet valgt en risikobaserede tilgang i forhold til it-sikkerheden og fastlæggelsen af nødvendige tekniske og organisatoriske sikkerhedsforanstaltninger. Der er foretaget risikovurdering med fokus på persondata og de registrerede, hvor følgende særligt har været i betragtning:

- Behandlingens:
  - Karakter
  - Omfang
  - Sammenhæng
  - Formål
- Risici knyttet til behandlingen
- Konsekvenser for fysiske personers rettigheder

Det er vurderingen af risikoen ved behandling af persondata i WebEDI-systemet er mellem til høj. Der er på grundlag heraf i databehandleraftalen stillet krav til sikkerheden. Kravene ligger inden for rammerne af den it-sikkerhedspolitik, der gælder for PensionsInfo.

WebEDI er omfattet af den overordnede it-sikkerhedspolitik for Forsikringsorganisationernes Fællessekretariat, der er baseret på ISO 27001 og 27002 og implementeret for det underliggende it-system og manuelle processer. It-sikkerhedspolitikken opdateres og godkendes hvert år af bestyrelsen for Forsikringsorganisationernes Fællessekretariat, der er identisk med Forsikring & Pensions bestyrelse.

Implementeringen i it-systemet følger af underdatabehandleraftalen med Sentia, der årligt afgiver både en ISAE 3402-erklæring og en ISEA 3000-erklæring, som nævnt ovenfor.

Anmeldelse af brud på persondatasikkerheden til Datatilsynet og underretning til de registrerede (Databeskyttelsesforordningens artikel 33-34)

Konstateres der brud på persondatasikkerheden i WebEDI-systemet, underretter WebEDI de dataansvarlige, der står for den endelige vurdering af risikoen for den registrerede eller andre personers rettigheder eller frihedsrettigheder. Der foreligger procedurer for håndteringen af databrud og underretning til de dataansvarlige med en foreløbig vurdering af:

- Karakteren af bruddet.
- Kategorierne og det omtrentlige antal berørte registrerede.
- Kategorierne og det omtrentlige antal berørte registreringer af personoplysninger.
- Sandsynlige konsekvenser af bruddet.
- Beskrivelse af eventuelle foranstaltninger, som WebEDI har truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

WebEDI dokumenterer på samme måde som øvrige sikkerhedshændelser alle brud på persondatasikkerheden, herunder;

- De faktiske omstændigheder ved bruddet.
- Dets virkning.
- De trufne afhjælpende foranstaltninger.

Processen for anmeldelse og eventuel underretning til de registrerede er en del af Forsikring & Pensions incident-proces, der skal underkastes regelmæssig afprøvning som en del af Forsikring & Pensions overordnede beredskabsplan.

Overførsel af personoplysninger til tredjelande eller internationale organisationer (Databeskyttelsesforordningens artikel 44 ff.)

Der er i databehandleraftalen mellem WebEDI og de dataansvarlige givet mulighed for overførsel af persondata til tredjelande, men der foreligger ikke for nuværende en fornøden instruks herom.

Dataansvarlige og databehandlere skal sikre, at databeskyttelsesforordningens betingelser for overførsler til tredjelande eller internationale organisationer altid bliver overholdt, således at beskyttelsen af de registrerede efter EU-lovgivningen som minimum sikres, uanset hvor i verden data befinder sig.

Der følger af de interne GDPR-procedurer for WebEDI krav om at sikre specifik instruks fra de dataansvarlige forud for eventuel overførsel af data til tredjelande eller internationale organisationer samt at sikre, at der foreligger et overførselsgrundlag.

Komplementerende kontroller hos brugerne

Kontroller hos WebEDI er udformet sådan, at nogle af kontrollerne nævnt i denne erklæring skal suppleres med kontroller hos brugerne af systemet/de dataansvarlige.

Oversigten nedenfor beskriver overordnet fordelingen af kontroller mellem WebEDI og brugerne af WebEDI-systemet i forhold til brugeradministration, passwordpolitik, periodisk gennemgang af brugernes adgangsrettigheder og beredskab.

Brugeradministration (oprettelse, ændring og sletning)	**WebEDI**	**Brugere af WebEDI**
Medarbejdere hos brugere af WebEDI		x
Medarbejdere hos Fonden F&P Formidling	x	
Passwordpolitik	WebEDI	Brugere af WebEDI
Medarbejdere hos brugere af WebEDI		x
Medarbejdere hos Fonden F&P Formidling	x	
Regelmæssig gennemgang af adgangsrettigheder	WebEDI	Brugere af WebEDI
Medarbejdere hos brugere af WebEDI		x
Regelmæssig gennemgang af adgangsrettigheder	WebEDI	Brugere af WebEDI
Medarbejdere hos Fonden F&P Formidling	x	
Kontrol af data, der lægges i systemet	WebEDI	Brugere af WebEDI
Medarbejdere hos brugerne af WebEDI		x

2 Udtalelse fra ledelsen

Fonden F&P Formidling (F&P) behandler personoplysninger på vegne af de dataansvarlige, der anvender WebEDI's services, i henhold til databehandleraftalen.

Medfølgende beskrivelse er udarbejdet til brug for de medlemmer af F&P, der har anvendt WebEDI, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som medlemmerne selv har udført ved vurdering af, om kravene i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesforordningen") er overholdt.

Beskrivelsen angiver, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan opnås, hvis komplementerende kontroller hos F&P, der forudsættes i designet af F&P's kontroller, er passende designet og fungerer effektivt sammen med relaterede kontroller hos F&P. Beskrivelsen omfatter ikke kontrolaktiviteter udført af de dataansvarlige.

F&P anvender Sentia til drift af WebEDI systemet. Beskrivelsen i afsnit 1 medtager de relevante kontrolmål og underliggende kontrolaktiviteter hos Sentia. F&P bekræfter, at:

(a) Den medfølgende beskrivelse i afsnit 1 giver en retvisende beskrivelse af de udvalgte GDPR-relaterede kontroller med relevans for WebEDI, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen i hele perioden fra 1. januar – 31. december 2020. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

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

i. De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger

ii. De processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere, slette og begrænse behandling af personoplysninger

iii. De processer, der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige

iv. 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

v. 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

vi. De processer, der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underrettelse til de registrerede

vii. De processer, der sikrer passende tekniske og organisatoriske sikringsforanstaltninger for behandlingen af personoplysninger 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

viii. Ydelser udført af underleverandører, hvis relevant, herunder om de er medtaget efter helhedsmetoden eller udeladt efter partielmetoden.

ix. Kontroller, som vi med henvisning til GDPR kontroller relateret til WebEDI's 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

x. Kontroller, som vi med henvisning til WebEDI-systemets afgrænsning har forudsat ville være implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen

xi. 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 ved databehandlerens anvendelse af WebEDI-systemet til behandling af personoplysninger foretaget i perioden fra 1. januar – 31. december 2020

(iii) ikke udelader eller forvansker oplysninger, der er relevante for omfanget af det beskrevne system under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af medlemmer af Fonden F&P Formidling og deres revisorer og derfor ikke kan omfatte ethvert aspekt ved kontrollerne, som det enkelte medlem af Fonden F&P Formidling måtte anse for vigtigt 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. januar – 31. december 2020, og kunder har udført de komplementerende kontroller, som forudsættes i designet af F&P's kontroller, i hele perioden fra 1. januar – 31. december 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, 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. januar – 31. december 2020.

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.

Hellerup, den 27. april 2021

Thomas Brenøe
vicedirektør

Torben Weiss Garne
underdirektør

3 Den uafhængige revisors erklæring om beskrivelsen af kontroller og deres udformning

Til: Fonden F&P Formidling

Omfang

Vi har fået som opgave at afgive erklæring om Fonden F&P Formidlings (F&P) beskrivelse i afsnit 1 af udvalgte GDPR-kontroller relateret til WebEDI-systemet i perioden 1. januar – 31. december 2020 (beskrivelsen) og om udformningen og effektiviteten af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

F&P anvender Sentia til drift af WebEDI systemet. Beskrivelsen i afsnit 1 medtager de relevante kontrolmål og underliggende kontrolaktiviteter hos Sentia. Vores handlinger har omfattet test af disse kontrolmål og relaterede kontroller hos Sentia.

Beskrivelsen angiver, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan opnås, hvis komplementerende kontroller hos de dataansvarlige, der forudsættes i designet af F&P's kontroller, er passende designet og fungerer effektivt sammen med relaterede kontroller hos F&P. Vores handlinger har ikke omfattet kontrolaktiviteter udført af de dataansvarlige, og vi har ikke vurderet egnetheden af design eller den operationelle effektivitet af kontrolaktiviteter hos de dataansvarlige.

F&P's ansvar

F&P er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i afsnit 2, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene, identifikation af de risici, der påvirker opnåelsen af kontrolmålene; udvælgelsen af de kriterier, der er præsenteret i ledelsens udtalelse, samt for at udforme, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Vores uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i såvel IESBA's Etiske regler som FSR – danske revisorers retningslinjer for revisors etiske adfærd (etiske regler for revisorer), som er baseret på grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd.

Vi anvender ISQC 1[1] og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder samt gældende krav ifølge lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Fonden F&P Formidlings beskrivelse samt om udformningen og implementeringen af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse. Vi har udført vores arbejde i overensstemmelse med den internationale standard om andre erklæringsopgaver (ISAE 3000) og yderligere krav ifølge dansk revisorlovgivning med henblik på at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed om beskrivelsen, udformningen og funktionaliteten af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller 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.

[1] ISQC 1, Kvalitetsstyring i firmaer, som udfører revision og review af regnskaber, andre erklæringsopgaver med sikkerhed og beslægtede opgaver.

En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte kontrolmål samt hensigtsmæssigheden af de kriterier, som Fonden F&P Formidling har specificeret og beskrevet i afsnit 2.

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

Begrænsninger i kontroller hos en serviceleverandør

Fonden F&P Formidling beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af medlemmer af Fonden F&P Formidling og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved de generelle it-kontroller, som hvert enkelt medlem måtte anse for vigtigt efter deres særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller opdage alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en serviceleverandør 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 afsnit 2. Det er vores opfattelse, at:

(a) beskrivelsen af de udvalgte GDPR-relaterede kontroller hos F&P med relevans for WebEDI, således som de var udformet og implementeret i hele perioden 1. januar – 31. december 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 i hele perioden fra 1. januar – 31. december 2020, hvis kontroller hos underleverandører fungerer effektivt, og hvis dataansvarlige har designet og implementeret de komplementerende kontroller, der forudsættes i designet af F&P's kontroller i hele perioden fra 1. januar – 31. december 2020 og

(c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. januar – 31. december 2020, hvis kontroller hos underleverandører fungerer effektivt, og hvis de komplementerende kontroller hos de dataansvarlige, der forudsættes i designet af F&P's kontroller har fungeret effektivt i hele perioden fra 1. januar – 31. december 2020.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt medlemmer af F&P, der har anvendt WebEDI, og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen er overholdt.

København, den 27. april 2021
EY Godkendt Revisionspartnerselskab
CVR-nr.: 30 70 02 28

Jesper Due Sørensen
Partner

Nils B. Christiansen
statsaut. revisor
mne34106

4 Tests udført af EY

4.1 Formål og omfang

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

Vores test af kontrollers udformning og implementering har omfattet de kontrolmål og tilknyttede kontroller, der er udvalgt af ledelsen, og som fremgår af afsnit 1. Eventuelle andre kontrolmål, tilknyttede kontroller og kontroller hos de medlemmer af Fonden F&P Formidling, der anvender løsningen, beskrevet i afsnit 1, er ikke omfattet af vores test.

Test af design, implementering og effektivitet har omfattet de kontroller, som blev vurderet nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået i perioden 1. januar – 31. december 2020.

4.2 Udførte tests

De udførte tests i forbindelse med fastlæggelsen af kontrollers design og implementering er 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 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 designet, implementeret og fungeret effektiv i perioden 1. januar – 31. december 2020.
Forespørgsler	Forespørgsel af passende personale hos Fonden F&P Formidling. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Vi har observeret kontrollens udførelse.

4.3 Resultater af tests

Pkt.	Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
A		Kontrolmål: Der er procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgående databehandleraftale.		
A	A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der er krav om løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	**F&P:** Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Inspiceret, at procedurerne indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen. Inspiceret, at procedurer er opdateret.	Ingen afvigelser konstateret.
A	A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	**F&P:** Inspiceret, at ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks.	Ingen afvigelser konstateret.
A	A.3	Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	**F&P:** Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at kontrol af behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning. Inspiceret, at der er procedurer for underretning til den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. Forespurgt, om der har været tilfælde af behandling i strid med databeskyttelsesforordningen.	Det har ikke været muligt at teste implementeringen, da vi har fået oplyst, at der ikke har været tilfælde af behandling af personoplysninger, der er vurderet i strid med lovgivningen. Ingen afvigelser konstateret.

Pkt.	Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
B		Kontrolmål: Der er procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.		
B	B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der er krav om løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	**F&P:** Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger. Inspiceret, at procedurer er opdateret. Stikprøvevis inspiceret, at der i databehandleraftalerne er etableret de aftalte sikringsforanstaltninger.	Ingen afvigelser konstateret.
B	B.2	Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de med dataansvarlig aftalte sikringsforanstaltninger.	**F&P:** 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. Inspiceret, at databehandleren har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen. Inspiceret, at databehandleren har implementeret de sikringsforanstaltninger, der er aftalt med de dataansvarlige.	Ingen afvigelser konstateret.

Pkt.	Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
B	B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus som løbende opdateres.	**Sentia:** Forespurgt om proceduren for sikring mod malware. Inspiceret, om personalehåndbogen indeholder beskrivelse af, hvordan medarbejdere skal forholde sig i tilfælde af malware-angreb. Inspiceret, at servere har opdaterede antivirussystemer. Observeret, at det ikke er muligt for brugeren at ændre indstillinger og derved stoppe de implementerede kontroller mod malware.	Ingen afvigelser konstateret.
B	B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	**Sentia:** Forespurgt om procedure for netværksstyring. Inspiceret, at der anvendes MPLS og VLAN til beskyttelse af kundenetværk. Inspiceret netværkstegning for sikkerhed i netværket samt opdeling af brugere og informationssystemer. Inspiceret, at ekstern adgang til systemer og databaser sker gennem sikret firewall.	Ingen afvigelser konstateret.
B	B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	**Sentia:** Forespurgt om procedure for netværksstyring. Inspiceret, at der anvendes MPLS og VLAN til beskyttelse af kundenetværk. Inspiceret netværkstegning for sikkerhed i netværket samt opdeling af brugere og informationssystemer.	Ingen afvigelser konstateret.

Pkt.	Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
B	B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	**F&P:** Forespurgt til proceduren for regelmæssig gennemgang af brugerne med adgang til personoplysninger. Inspiceret, at der hver anden måned afholdes statusmøder, hvor der foretages gennemgang af brugernes adgang.	Ingen afvigelser konstateret.
B	B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering. Overvågningen omfatter kapacitetsovervågning.	**Sentia:** Inspiceret Sentias wiki site for procedure vedrørende kapacitetsstyring. Inspiceret, at der er etableret systemovervågning med alarmering og rapportering af kapacitetsudnyttelse.	Ingen afvigelser konstateret.
B	B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via applikationen.	**F&P:** Forespurgt om proceduren for administration af krypteringsnøgler. Inspiceret informationssikkerhedspolitikken vedrørende procedure for kryptografi. Inspiceret dokumentation for opsætningen af kryptografi, herunder at der foreligger et validt certifikat.	Ingen afvigelser konstateret.

Pkt.	Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
B	B.9	Der er etableret logning i systemer, databaser og netværk af følende forhold: - Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder. - Sikkerhedshændelser omfattende: • Ændringer i logopsætninger herunder deaktivering af logning. • Ændringer i systemrettigheder til brugere. • Fejlede forsøg på log-on til systemer, databaser og netværk. Logoplysninger er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.	**Sentia:** Forespurgt om procedure for hændelseslogning. Stikprøvevist inspiceret, at der er opsat hændelseslogning på servere. Forespurgt om proceduren for beskyttelse af logning. Inspiceret, at der logges, når der logges på servere, hvor log opbevares. Inspiceret, at kun autoriserede personer har adgang til servere, herunder logs. Forespurgt om proceduren for logning af systemadministratorer m.v. Stikprøvevis inspiceret, at der er opsat logning af aktiviteter udført af systemadministratorer m.v. på servere.	Ingen afvigelser konstateret.
B	B.10	Personoplysninger, der anvendes til udvikling, test eller lignede, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål,	**F&P:** Forespurgt om proceduren for sikring af testdata. Inspiceret informationssikkerhedspolitikken for sikring af testdata. Inspiceret, at testdata er pseudonymiseret.	Ingen afvigelser konstateret.
B	B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	**F&P:** Forespurgt om kontrol af informationssystemer og deres overensstemmelse med organisationens informationssikkerhedspolitikker og -standarder. Inspiceret, at der er foretaget en ekstern assessment af Cloud-opsætningen i forhold til udvikling.	Ingen afvigelser konstateret.

Pkt.	Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
B	B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer som sikre vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	**F&P:** Inspiceret, at informationssikkerhedspolitikken indeholder procedure for ændringshåndtering. Inspiceret, at Sentias wiki site indeholder procedure for ændringshåndtering. Stikprøvevis inspiceret, at der afholdes periodiske driftsstatusmøder, hvor ændringer gennemgås. Stikprøvevis inspiceret, at ændringer testes, inden de bliver lagt i produktion, samt at de er afsluttet. **Sentia:** Forespurgt om proceduren for ændringer af organisationen, forretningsprocesser, informationsbehandlingsfaciliteter og -systemer, som påvirker informationssikkerheden. Stikprøvevis inspiceret, at der foreligger dokumentation for ændringer i ticket-systemet på baggrund af en forespørgsel fra F&P.	Ingen afvigelser konstateret.
B	B.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	**F&P:** Inspiceret proceduren for tildeling og afbrydelse af brugeradgange. Inspiceret, at de aktive brugeradgange regelmæssigt vurderes på statusmøder med serviceleverandøren.	Ingen afvigelser konstateret.

Pkt.	Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
B	B.14	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	**Sentia:** Inspiceret Datacenterbeskrivelsen, og at sikkerhedsregler indeholder procedure for fysisk adgangskontrol. Observeret, at der skal bruges adgangsbrik til indgangen til datacentret, personligt adgangskort, irisscanner til sluse samt kort og pinkode til produktionsmiljøerne i datacentret. Inspiceret udtræk over adgange til datacentret for Sentias medarbejdere. Inspiceret, at listen over medarbejdere med adgang til datacentret gennemgås regelmæssigt. Observeret, at tilsvarende standarder for fysisk adgangskontrol også er gældende for fysisk adgang til backup-sitet.	Ingen afvigelser konstateret.
C		Kontrolmål: Der er procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.		
C	C.1	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. It-sikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der er krav om løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	**F&P:** 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 afvigelser konstateret.

Pkt.	Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
C	C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	**F&P:** Inspiceret dokumentation for ledelsens vurdering af, at Informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Stikprøvevis inspiceret, at kravene i databehandleraftalerne er dækket af informationssikkerhedspolitikkens krav til sikringsforanstaltninger og behandlingssikkerheden.	Ingen afvigelser konstateret.
C	C.3	Der udføres en efterprøvning af medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: - Referencer fra tidligere ansættelser. - Straffeattest. - M.m.	**F&P:** Forespurgt, hvordan der foretages efterprøvning af medarbejdere i forbindelse med ansættelse.	Vi har konstateret, at der ikke udføres screening i alle tilfælde, dette er alt efter stillingen, der besættes. Yderligere har vi fået oplyst, at der ikke er ansat personale med adgang til persondata i 2020. Ingen yderligere afvigelser konstateret.
C	C.4	Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.	**F&P:** Inspiceret, at standardkontrakter indeholder afsnit om fortrolighed og informationssikkerheds ansvar.	Ingen afvigelser konstateret.
C	C.5	Ved fratrædelse er der implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	**F&P:** Forespurgt til inddragelse af fratrådte brugeres adgangsrettigheder.	Vi har ikke kunne teste implementeringen af, at brugerrettigheder og aktiver inddrages ved fratrædelse, da vi har fået oplyst, at der ikke har været fratrædelser af brugere med adgang til persondata i 2020. Ingen afvigelser konstateret.

Pkt.	Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
C	C.6	Der gennemføres løbende awareness-træning af medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	**F&P:** Forespurgt, hvordan der gennemføres awareness-træning i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger. Inspiceret dokumentation for afholdt awareness-træning i 2020.	Ingen afvigelser konstateret.
D		Kontrolmål: Der er procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres, såfremt der indgås aftale herom med den dataansvarlige.		
D	D.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der er krav om løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	**F&P:** Inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
D	D.2	Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner: - Data slettes, 3 år efter en kontrakt er afmeldt.	**F&P:** Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner. Observeret, at systemopsætningen af sletterutiner stemmer overens med databehandleraftalen. Inspiceret, at data slettes efter gældende regler.	Ingen afvigelser konstateret.

Pkt.	Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
D	D.3	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.	**F&P:** Inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger. Observeret, at systemopsætningen af sletterutiner stemmer overens med databehandleraftalen. Inspiceret, at data slettes efter gældende regler.	Ingen afvigelser konstateret.
E		Kontrolmål: Der er procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.		
E	E.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der er krav om løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	**F&P:** Inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Inspiceret, at procedurerne er opdateret. Stikprøvevis inspiceret, at der er dokumentation for, at databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, sker i henhold til databehandleraftalen.	Ingen afvigelser konstateret.

Pkt.	Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
E	E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landeområder.	**F&P:** Inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landeområder. Stikprøvevis inspiceret, at der er dokumentation for, at databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, herunder opbevaring af personoplysninger, alene foretages på de lokaliteter, der fremgår af databehandleraftalen – eller i øvrigt er godkendt af den dataansvarlige.	Ingen afvigelser konstateret.
F		Kontrolmål: Der er procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.		
F	F.1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der er krav om løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	**F&P:** Inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.

Pkt.	Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
F	F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	**F&P:** Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere. Stikprøvevis inspiceret, at der er dokumentation for, at underdatabehandlere fra databehandlerens oversigt over underdatabehandlere, fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige.	Vi har konstateret, at der anvendes en underdatabehandler, som ikke fremgår af databehandleraftalerne. Vi har dog inspiceret, at de dataansvarlige er underrettet om denne underdatabehandler. Vi har stikprøvevis konstateret, at 12 ud af 25 databehandleraftaler ikke er underskrevet, heraf er 3 afmeldt i 2020. Ingen yderligere afvigelser konstateret
F	F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underrettes den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	**F&P:** Inspiceret, at der foreligger formaliserede procedurer for underretning til dataansvarlig ved ændringer i anvendelse af underdatabehandlere. Inspiceret dokumentation for, at dataansvarlig er underrettet ved ændring i anvendelse af underdatabehandlerne i erklæringsperioden.	Ingen afvigelser konstateret.
F	F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	**F&P:** Inspiceret, at der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af databehandlerens oversigt. Stikprøvevis inspiceret, at underdatabehandleraftaler indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Ingen afvigelser konstateret.

Pkt.	Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
F	F.5	Databehandleren har en oversigt over godkendte underdatabehandlere, med angivelse af: - Navn - CVR-nr. - Adresse - Beskrivelse af behandlingen	**F&P:** 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.	Vi har konstateret, at der anvendes en underdatabehandler, som ikke fremgår af databehandleraftalerne. Vi har dog inspiceret, at de dataansvarlige er underrettet om denne underdatabehandler. Ingen yderligere afvigelser konstateret.
F	F.6	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 underdatabehandlere.	**F&P:** 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 og behandlingssikkerheden hos de anvendte underdatabehandlere. Inspiceret dokumentation for, at information om opfølgning hos underdatabehandlere meddeles den dataansvarlig, således at denne kan tilrettelægge eventuelt tilsyn.	Ingen afvigelser konstateret.

Pkt.	Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
H		Kontrolmål: Der er 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.		
H	H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der er krav om løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	**F&P:** Inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
H	H.2	Databehandleren har etableret procedurer, som i det omfang, det 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.	**F&P:** Inspiceret, at de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljeret procedurer for: - Udlevering af oplysninger. - Rettelse af oplysninger. - Sletning af oplysninger. - Begrænsning af behandling af personoplysninger. - Oplysning om behandling af personoplysninger til den registrerede. Inspiceret dokumentation for, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer.	Ingen afvigelser konstateret.

Pkt.	Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
I		Kontrolmål: Der er procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.		
I	I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlig ved brud på persondatasikkerheden.	**F&P:** Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning til de dataansvarlige ved brud på persondatasikkerheden. Inspiceret, at proceduren er opdateret.	Ingen afvigelser konstateret.
I	I.2	Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: - Awareness hos medarbejdere.	**F&P:** Forespurgt, om der har været afholdt awareness-træning i 2020. Inspiceret dokumentation for gennemført awareness-træning i 2020.	Ingen afvigelser konstateret.
I	I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	**F&P:** Inspiceret beredskabsplanen for håndtering af brud på persondatasikkerheden. Forespurgt, om der er konstateret nogen brud på persondatasikkerheden i erklæringsperioden	Ingen afvigelser konstateret.

Pkt.	Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
I	I.4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: - Karakteren af bruddet på persondatasikkerheden. - Sandsynlige konsekvenser af bruddet på persondatasikkerheden. - Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	**F&P:** Inspiceret, at de foreliggende procedurer for underretning til 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 de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden.	Ingen afvigelser konstateret.