

Fonden F&P Formidling

ISAE 3000-erklæring omhandlende
udvalgte GDPR-kontroller i perioden 1.
januar – 31. december 2021 relateret til
WebEDI-systemet



Indhold

1	Beskrivelse af WebEDI-systemet i relation til behandling af persondata	2
1.1	Systembeskrivelse og dataflow	2
1.2	Behandlingen af persondata og grundlaget herfor	4
1.3	Revision og kontrol af WebEDI og eventuelle underdatabehandlere	4
1.4	Test og kontrol af WebEDI og eventuelle underdatabehandlere	7
1.5	Risikovurdering	7
1.6	Kontrolforanstaltninger	7
1.7	Kontrolmål	8
2	Udtalelse fra ledelsen	13
3	Uafhængige revisors erklæring	15
4	Tests udført af EY	18
4.1	Formål og omfang	18
4.2	Udførte tests	18
4.3	Resultater af tests	19
5	Supplerende information	34

1 Beskrivelse af WebEDI-systemet i relation til behandling af persondata

WebEDI-systemet er et elektronisk system til udveksling af oplysninger forsikrings- og pensionselskaberne imellem og mellem selskaberne og deres forskellige samarbejdspartnere, herunder banker og praktiserende læger og speciallæger. WebEDI-systemet omfatter 8 forskellige løsninger for udveksling af oplysninger, der bl.a. understøtter opsigelser, regres, panthaverdeklarationer, LD-ordninger, skadeshistorik og FP-attester. Udvekslingen omfatter personoplysninger. WebEDI-systemet ejes og driftes af Fonden F&P Formidling.

1.1 Systembeskrivelse og dataflow

Udveksling af oplysninger i WebEDI-systemet er baseret på, at de deltagende parter kan udveksle dokumenter via Webblanketter, EDIFACT og XML. Udvekslingen sker 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 forsikringselskaber, pensionselskaber samt banker og leasingselskaber.

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 modernisering – nye ordninger er kommet til, og ordninger er udgået.

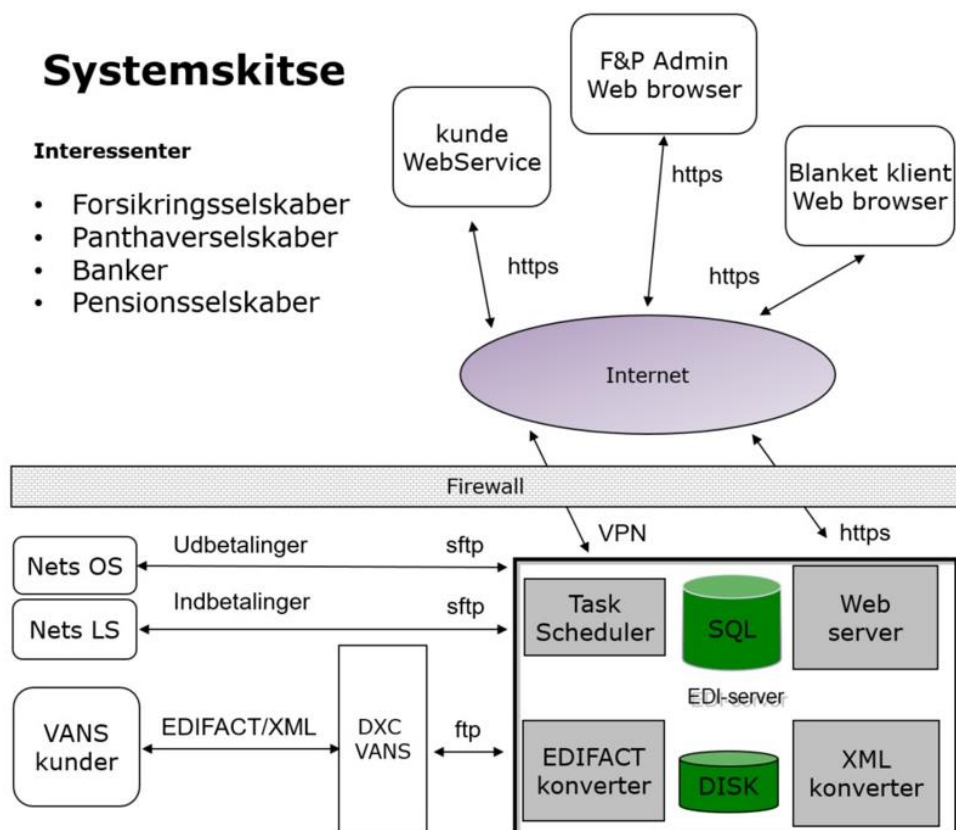
I dag håndteres som nævnt otte ordninger via WebEDI-serveren, der har en daglig volumen på godt 12.000 dokumenter svarende til otte dokumenter i minuttet.

Bag WebEDI står som nævnt Fonden F&P Formidling, som står for drift, udvikling og support af løsningen.

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.

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	
Pensionselskab	Pensionsoverførsler (PGF41, pension-pension) Pensionsoverførsler (UPB, pension-bank) LD-flytning FP-attester	
Bank	Pensionsoverførsler (UPB, pension-bank) LD-Flytning	
Administration		Kun F&P

1.2 Behandlingen af persondata og grundlaget herfor

WebEDI's behandling af personoplysninger sker som databehandler på vegne af de til systemet knyttede pensions- og forsikringsselskaber, pengeinstitutter og leasingselskaber, der er dataansvarlige.

Der er indgået databehandleraftale mellem de dataansvarlige og Fonden F&P Formidling, som ejer og driver WebEDI-systemet. Behandlingen sker på grundlag af denne aftale, der omfatter de dataansvarliges instruks til behandlingen.

Behandlingen drejer sig primært om udveksling af oplysninger mellem selskaberne, som er tilsluttet systemet. Der er også kommunikation med praktiserende læger og speciallæger, herunder tandlæger, 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.

1.3 Revision og kontrol af WebEDI og eventuelle underdatabehandlere

Der er indgået databehandleraftale mellem Fonden F&P Formidling og de selskaber, der er tilsluttet WebEDI-systemet. Databehandleraftalen er baseret på Datatilsynets oprindelige skabelon og er identisk for samtlige dataansvarlige. Dog har selskaber, der gør brug af systemet til udveksling af oplysninger og blanketter med privatpraktiserende læger og privatlæger, modtaget opdateret databehandleraftale grundet etableringen af den nye tandlægeordning. Instruksen fra samtlige selskaber er således også enslydende og uden specifikke krav for nogen selskaber.

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 revisorerklæring én gang årligt.

Det er vurderingen, at 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 EDI, som er baseret på ISO 27001-standarden.

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 af sikkerhedsforanstaltninger i it-systemet følger af underdatabehandleraftalen med Sentia.

Krav til 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 udgangspunkt ikke er tilladt.

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

Instruksen omfatter krav om udarbejdelse af revisor erklæringer 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.

Der er i aftalen med de dataansvarlige allerede godkendt en række underdatabehandlere, der teknisk understøtter systemet. Herudover er der i aftalen givet en generel godkendelse for WebEDI til antagelse af nye underdatabehandlere, efter høring af de dataansvarlige. De interne procedurer for behandlingen af persondata i 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 erklæring er modtaget for perioden 1. januar til 31. december 2021.

Udover Sentia benytter EDI følgende underleverandører, der behandler persondata:

- ▶ DXC, der leverer adgang til VANS-netværk for kommunikation mellem parterne
- ▶ Synlab, der understøtter EDI-løsningen for så vidt angår formidling af oplysninger og erklæring mellem selskaberne og de praktiserende læger tilknyttet løsningen.
- ▶ Nasure, der understøtter EDI-løsningen for så vidt angår formidling af oplysninger og erklæring mellem selskaberne og tandlægerne tilknyttet løsningen.

Ved en fejl var Synlab ikke angivet i den oprindelige databehandleraftale med de dataansvarlige. I forbindelse med udvidelsen med tandlægeløsningen i systemet modtog de dataansvarlige, for hvem det var relevant, underretning om Synlab som underdatabehandler, samt ny underdatabehandleraftale, hvoraf også Nasure fremgik. Der er ikke modtaget indvendinger mod dette fra de dataansvarlige.

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.

Behandlingen af data i WebEDI er alene sket efter instruks givet i databehandleraftalen med de dataansvarlige.

I september 2021 blev der konstateret en fejl i WebEDI-systemet hos en underleverandør (Synlab), der gav anledning til mistanke om databrud. Grundet en serverfejl var en liste over praktiserende læger ikke blevet retmæssigt opdateret, og selskaberne sendte således oplysninger til et forkert lægehus. Fejlen blev konstateret hos et selskab, der rettede henvendelse til EDI-sekretariatet. Herefter blev fejlen rettet umiddelbart efter konstateringen. Der blev i systemet identificeret 20 sager, som kunne være berørt af fejlen, og EDI-sekretariatet underrettede de selskaber, som havde sendt anmodninger til det pågældende lægehus. Et selskab har vurderet fejlen som et databrud og har anmeldt dette til Datatilsynet.

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.

Såfremt 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.

WebEDI er tillige forpligtet til at yde bistand til de dataansvarlige i relation til håndteringen af databrud.

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.

1.4 Test og kontrol af WebEDI og eventuelle underdatabehandlere

Denne erklæring udgør Fonden F&P Formidlings rapportering, som har til formål at give de dataansvarlige indsigt i WebEDI's kontroller i relation til behandling af personoplysninger. Fonden F&P Formidling 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's 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/underdatabehandleres fremlæggelse af rapporter, erklæringer eller anden skriftlig dokumentation. Databehandleraftalen fastlægger vilkår for afholdelse af omkostninger i forbindelse med inspektion.

1.5 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.

Fonden F&P Formidling gennemfører, som databehandler i forbindelse med større ændringer i systemet, 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. Risikovurderinger opdateres årligt.

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. Der er ikke for nuværende konstateret sådan en høj risiko ved behandlingen i WebEDI-systemet.

Der er foretaget samlet risikovurdering af systemet og af de enkelte underdatabehandlere. Risikoen for den registrerede ved behandlingen af persondata i WebEDI-systemet vurderes i udgangspunktet som mellem – høj. Dette skyldes omfanget og karakteren af persondata, der behandles, som både omfatter økonomiske data og journaloplysninger. Når risikoen tangerer høj, skyldes det også dels omfanget af transaktioner og muligheden for at tilføje oplysninger i blanketter, som omfatter helbredsoplysninger. Der er for systemet truffet forskellige foranstaltninger (organisatoriske og tekniske) for håndtering af risici, så risikoen anses samlet for begrænset. Der er ikke sket ændringer i systemet i 2021.

1.6 Kontrolforanstaltninger

WebEDI er underlagt den overordnede persondatapolitik for Forsikring & Pension. 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. Procedureerne er ligeledes godkendt i GDPR-styregruppen. Opdatering og kontrol af forretningsgange og procedurer sker en gang årligt og er forankret både i IT, i WebEDI's sekretariat samt i Rammevilkår og EU.

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 Fonden F&P Formidlings forpligtelser overfor de dataansvarlige, samt kontrol med behandlingen hos underdatabehandleren.

1.7 Kontrolmål

1.7.1 A. Efterlevelse af de dataansvarliges instruks (Databeskyttelsesforordningens artikel 5, 6, 9, 10 og 28)

Behandlingen af persondata i WebEDI sker udelukkende på grundlag af instruks fra de dataansvarlige, der står inde for, at behandlingen er lovlig. Det påhviler dog Fonden F&P Formidling som databehandler at gøre opmærksom på, hvis man vurderer, at instruksen er i strid med lovgivningen.

Instruksen er indeholdt i databehandleraftalen mellem de dataansvarlige og Forsikring & Pension.

Der er for WebEDI indført politikker og procedurer, der understøtter instruksen fra de dataansvarlige og sikrer, at WebEDI's medarbejdere kender til denne. Politikker og procedurer gennemgås mindst en gang årligt med henblik på nødvendig revision, bl.a. som følge af systemændringer og i tilfælde af de dataansvarliges justering af instruksen.

Der synes ikke at være grundlag for at antage, at de dataansvarliges instruks, som den foreligger, skulle være i strid med lovgivningen. Der er ikke i WebEDI sket behandling i strid med instruksen.

1.7.2 B. Tekniske sikkerhedsforanstaltninger (Databeskyttelsesforordningens artikel 24, 32 og 35)

Instruksen omfatter specifikke krav til WebEDI om indførsel af tekniske sikkerhedsforanstaltninger, 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.

De påkrævede tekniske sikkerhedsforanstaltninger er indført for WebEDI. Der udføres løbende risikovurdering af systemet for at sikre et passende beskyttelsesniveau.

I praksis håndteres de tekniske sikkerhedsforanstaltninger af Sentia og er indskrevet i (under)databehandleraftalerne med parterne. Autotaks' kontrol af Sentia sker ved fremsendelse af GDPR-revisorerklæring én gang årligt. Der afholdes yderligere månedlige møder med Sentia omkring projekter, patch, disaster recovery, brugere og drift med mere.

Implementeringen af de tekniske sikkerhedsforanstaltninger er tjekket i forbindelse med it-systemrevisionen, der viser, at de er overholdt i systemet.

1.7.3 C. Organisatoriske sikkerhedsforanstaltninger (Artikel 25 og 32)

Der er ligeledes i overensstemmelse med instruksen fra de dataansvarlige indført organisatoriske sikkerhedsforanstaltninger for behandlingen af persondata.

Medarbejdere med adgang til WebEDI-systemet er underlagt it-sikkerhedspolitikken, som gælder for Forsikring organisationernes fællessekretariat og er godkendt af Forsikring og Pensions bestyrelse. It-sikkerhedspolitikken opdateres årligt, og der føres løbende kontrol med implementeringen heraf, samt at der ikke er konflikt mellem denne og indgåede databehandleraftaler.

Opdatering og godkendelse af it-sikkerhedspolitikken udestår for 2021. Dette skyldes en ingangværende organisationsændring under Forsikring & Pension. Det er forventningen, at it-sikkerhedspolitikken godkendes af bestyrelsen i starten af februar 2022.

Medarbejdere med adgang til WebEDI-systemet er alle underlagt fortrolighed ved deres ansættelse. Der er endvidere indført procedurer, der sikrer, at medarbejdernes rettigheder inddrages ved fratrædelse. Der har ikke i 2021 været ændringer i medarbejderstaben i relation til WebEDI.

Alle medarbejdere modtager introduktion til sikker databehandling, herunder efterlevelse af GDPR, i forbindelse med ansættelsen. De nuværende medarbejdere har således været igennem GDPR-awareness-kursus enten i forbindelse med ansættelse eller det løbende brush-up kursus, der afholdes for alle medarbejdere. Sidstnævnte har ikke været afholdt de sidste par år på pga. corona-situationen. Der er dog en løbende dialog omkring GDPR-problemstillinger mellem medarbejderne i Rammevilkår og EU og medarbejderne i medlemservices, herunder Autotaks, som står for hovedparten af behandlingen af persondata i F&P.

1.7.4 D. Sletning og tilbagelevering af persondata til de dataansvarlige (Databeskyttelsesforordningens artikel 32)

Der er indført sletteprocedurer for systemet på baggrund af instruksen. Disse omfatter alene krav om sletning og ikke tilbagelevering, idet data kommer fra selskaberne, der fortsat har adgang hertil. Det er alene data, der opbevares i systemet, så længe et selskab knyttet til nummeret er tilsluttet systemet.

Data opbevares i EDI-løsningen efter følgende principper:

EDI-løsning	Opbevarings-/sletteregler
Forsikringsopsigelser	Afsluttede sager (opsigelse + accept) og afviste opsigelser slettes efter 3 år. Opsigelser, der aldrig er besvaret, slettes efter 1 år.
Regres	Meddelelser slettes efter 5 år.
Panthaverdeklarationer	Deklarationer slettes 5 år efter, deklarationsdækningen er ophørt.
Skadeshistorik	De oplyste skadesinformationer slettes efter 3 måneder. At der er udvekslet meddelelser mellem selskaberne, slettes efter 18 måneder.
Pensionsoverførsler mellem pensionselskaber	Afsluttede overførsler og forespørgsler slettes efter 10 år. Afviste overførsler, ubesvarede anmodninger eller forespørgsler slettes efter 2 år.
Pensionsoverførsler mellem pensionselskaber og banker	Afsluttede overførsler og forespørgsler slettes efter 10 år. Afviste overførsler, ubesvarede anmodninger eller forespørgsler slettes efter 2 år.
Overførsel af LD-konto	Afsluttede overførsler og forespørgsler slettes efter 10 år. Afviste overførsler, ubesvarede anmodninger eller forespørgsler slettes efter 2 år.
FP-attester og journaloplysninger fra lægerne	Svar fra lægen gemmes ikke i EDI-systemet, men hentes online fra Synlab, der er central dataleverandør for praktiserende læger. Sletteproceduren er sat op til at slette data og adgang til data efter forskellige tidsfrister. Tidsfristerne er: 14 dage: Selskabets adgang til helbredsoplysningerne, som lægen har videregivet, bliver slettet 14 dage efter, at selskabet har hentet helbredsoplysningerne. 3 måneder: Hvis selskabet ikke henter helbredsoplysningerne, som lægen har videregivet, sletter EDI-systemet selskabets adgang til helbredsoplysningerne 3 måneder efter, at selskabet har modtaget oplysningerne i EDI. 6 måneder: Oplysninger om kundens helbred, som selskabet har indtastet i anmodningen, fx skadestidspunkt, bliver slettet efter 6 måneder.

	5 år: Hele sagen bliver slettet i EDI-systemet efter 5 år, herunder kundens samtykke og faktura fra lægen.
TL-attester og journaloplysninger fra tandlægerne	<p>Svar fra tandlægen gemmes ikke i EDI-systemet, men hentes online fra Nasure, der er centrale dataleverandører for tandlægerne, via Synlab.</p> <p>Sletteproceduren er sat op til at slette data og adgang til data efter forskellige tidsfrister. Tidsfristerne er:</p> <p>14 dage: Selskabets adgang til helbredsoplysningerne, som tandlægen har videregivet, bliver slettet 14 dage efter, at selskabet har hentet helbredsoplysningerne.</p> <p>3 måneder: Hvis selskabet ikke henter helbredsoplysningerne, som tandlægen har videregivet, sletter EDI-systemet selskabets adgang til helbredsoplysningerne 3 måneder efter, at selskabet har modtaget oplysningerne i EDI.</p> <p>6 måneder: Oplysninger om kundens helbred, som selskabet har indtastet i anmodningen, fx skadestidspunkt, bliver slettet efter 6 måneder.</p> <p>5 år: Hele sagen, herunder kundens samtykke og faktura fra tandlægen, bliver slettet i EDI-systemet 5 år efter, at tandlægen har meddelt, at sagen og evt. efterfølgende behandling er afsluttet.</p>

1.7.5 E. Opbevaring af data i systemet (Databeskyttelsesforordningens artikel 30)

Data opbevares i systemet i overensstemmelse med instruks, og som ovenfor beskrevet. Data behandles alene på de lokationer, som er angivet i databehandleraftalen og godkendt af de dataansvarlige.

1.7.6 F. Brug af underdatabehandlere (Databeskyttelsesforordningens artikel 32)

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.

Der er i aftalen med de dataansvarlige allerede godkendt underdatabehandlere, der teknisk understøtter systemet. Det gælder Sentia, der drifter systemet, DXC, der leverer forbindelsen til VANS-netværket, Nasure, der leverer løsningen for tandlægerne, og Synlab, der leverer tilsvarende løsning for de praktiserende læger.

Herudover er der i aftalen givet en generel godkendelse for WebEDI til antagelse af nye underdatabehandlere, efter høring af de dataansvarlige. De interne procedurer for behandlingen af persondata i 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.

I forhold til Sentia, der drifter systemet, har WebEDI sikret sig, at de efter underdatabehandleraftalen årligt modtager en ISAE 3402-erklæring på it-systemet. Herudover modtages en ISAE 3000 GDPR-databehandlererklæring, der dog er generisk i forhold til Sentia. GDPR-erklæring for 2021 er modtaget i januar 2022. Erklæringen er givet uden anmærkninger.

Udover Sentia benytter WebEDI følgende underleverandører, der behandler persondata:

- ▶ DXC, der står for forbindelsen til VANS-netværket
- ▶ Nasure, der står for løsningen ud til de praktiserende tandlæger
- ▶ Synlab, der står for løsningen ud til de praktiserende læger.

Der modtages generelle revisionserklæringer fra DXC i relation til it-sikkerheden (SOC II) og en ledelseserklæring i forhold til overholdelsen af databeskyttelsesreglerne. Nasure og Synlab kontrolleres ved fremsendelse af spørgeskema til deres overholdelse af databehandleraftalen.

Der har ikke været ændringer i forhold til listen af underdatabehandlere i 2021.

1.7.7 G. Tredjelandsoverførsler (Databeskyttelsesforordningens artikel 3 og Kap. V)

Der overføres ikke data til tredjelande i forbindelse med WebEDI, og det er umiddelbart heller ikke tilladt efter databehandleraftalen.

1.7.8 H. Understøttelse af de registreredes rettigheder (Databeskyttelsesforordningens artikel 15, 16, 17, 18 og 19)

WebEDI er som databehandler efter Databeskyttelsesforordningen og databehandleraftalen med de dataansvarlige forpligtede til at bistå de dataansvarlige i forhold til at sikre de registreredes rettigheder.

Der er vedtaget en generel databeskyttelsespolitik og procedurer, der understøtter WebEDI's forpligtelser overfor de dataansvarlige.

Når 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.

Der føres log over anmodninger fra de registrerede. WebEDI har ikke i 2021 modtaget anmodninger fra registrerede eller de dataansvarlige om bistand i relation til de registreredes rettigheder.

1.7.9 I. Håndtering af brud på persondatasikkerheden. Databehandleraftalen fastlægger rammer for parternes samarbejde, herunder processer for håndtering af sikkerhedsbrud og anmodninger i relation til de registreredes rettigheder (Databeskyttelsesforordningen artikel 33 og 34)

Databehandleraftalen indeholder instruks om og regulerer Fonden F&P Formidlings forpligtelse overfor de dataansvarlige ved mistanke om eller konstatering af brud på persondatasikkerheden hos WebEDI eller hos en underleverandør.

Der er udarbejdet en generel politik og procedurer, der understøtter WebEDI's forpligtelser overfor de dataansvarlige, herunder håndtering af anmeldelse og underretning.

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	

Brugeradministration (oprettelse, ændring og sletning)	WebEDI	Brugere af WebEDI
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 dataansvarlige, 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 de dataansvarlige selv har udført ved vurdering af, om kravene i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger, og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesforordningen") er overholdt.

F&P anvender Sentia til Drift af WebEDI-systemet. Beskrivelsen i afsnit 1 medtager de relevante kontrolmål og underliggende kontrolaktiviteter hos Sentia.

F&P anvender DXC, Synlab og Nasure til henholdsvis VANS-netværk, udveksling af data mellem praktiserende læger og udveksling af data med tandlæger. Beskrivelsen i afsnit 1 medtager kun kontrolmål og kontrolaktiviteter hos F&P og medtager således ikke kontrolmål og underliggende kontrolaktiviteter hos DXC, Synlab og Nasure. Visse kontrolmål, der er specificeret i beskrivelsen, kan kun nås, hvis underleverandørers kontroller, der forudsættes i designet af vores kontroller, er passende designet og operationelt effektive. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underleverandører.

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

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 2021. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:
- (i) redegør for, hvordan kontrollerne var designet 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 2021
 - (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 dataansvarlige og deres revisorer og derfor ikke kan omfatte ethvert aspekt ved kontrollerne, som den enkelte dataansvarlige 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 designet og operationelt effektive i hele perioden fra 1. januar – 31. december 2021, bortset fra kontrolmål I, hvis relevante kontroller hos underleverandører var operationelt effektive, og de dataansvarlige har udført de komplementerende kontroller, som forudsættes i designet af F&P's kontroller, i hele perioden fra 1. januar – 31. december 2021. 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 designet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. januar – 31. december 2021.
- c) Der er etableret og opretholdt passende tekniske og organisatoriske foranstaltninger med henblik på at opfylde aftalerne med de dataansvarlige, god databehandleriskik og relevante krav til databehandlere i henhold til databeskyttelsesforordningen.

Hellerup, den 10. februar 2022

Thomas Brenøe
vicedirektør

Torben Weiss Garne
underdirektør

3 Uafhængige revisors erklæring

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med de dataansvarlige

Til: Fonden F&P Formidling og dataansvarlige brugere af WebEDI-systemet

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 2021 (beskrivelsen) og om designet og den operationelle effektivitet 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.

F&P anvender DXC, Synlab og Nasure til henholdsvis VANS-netværk, udveksling af data mellem praktiserende læger og udveksling af data med tandlæger. Beskrivelsen i sektion 1 medtager kun kontrolmål og relaterede kontroller hos F&P og medtager således ikke kontrolmål og relaterede kontroller hos DXC, Synlab og Nasure. Visse kontrolmål, der er specificeret i beskrivelsen, kan kun nås, hvis underleverandørers kontroller, der forudsættes i designet af F&P's kontroller, er passende designet og operationelt effektive sammen med de relaterede kontroller hos F&P. Vores handlinger har ikke omfattet kontrolaktiviteter udført af DXC, Synlab og Nasure, og vi har ikke vurderet egnetheden af design eller den operationelle effektivitet af kontrolaktiviteter hos underleverandører.

Visse kontrolmål, der er specificeret i beskrivelsen, kan kun opnås, hvis komplementerende kontroller hos de dataansvarlige, der forudsættes i designet af F&P's kontroller, er passende designet og operationelt effektive 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 designe, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Vores uafhængighed og kvalitetsstyring

EY Godkendt Revisionspartnerselskab er underlagt international standard om kvalitetsstyring, ISQC 1, og anvender således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende krav i lov og øvrig regulering.

Vi har overholdt kravene til uafhængighed og andre etiske krav i International Ethics Standards Board for Accountants' internationale retningslinjer for revisorers etiske adfærd (IESBA Code), der bygger på de grundlæggende principper om integritet, objektivitet, professionel kompetence og fornøden omhu, fortrolighed og professionel adfærd, samt etiske krav gældende i Danmark.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Fonden F&P Formidlings beskrivelse samt om designet og den operationelle effektivitet 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 designet og operationelt effektive.

En erklæringsopgave med sikkerhed om beskrivelsen, designet og den operationelle effektivitet af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i service-

leverandørens beskrivelse af sit system samt for kontrollernes design og operationelle effektivitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt designet eller ikke er operationelt effektive. Vores handlinger har omfattet test af den operationelle effektivitet af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået.

En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, 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 med forbehold.

Begrænsninger i kontroller hos en serviceleverandør

Fonden F&P Formidlings beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved de udvalgte GDPR-relaterede kontroller, som hver enkelt dataansvarlig 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 den operationelle effektivitet til fremtidige perioder undergivet risikoen for, at kontroller hos en serviceleverandør kan blive utilstrækkelige eller svigte.

Grundlag for konklusion med forbehold

Fonden F&P Formidling anfører i afsnit 4, kontrolmål I "Der er procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale".

Vi har konstateret, at F&P ikke har afholdt GDPR-awareness.kurser.

Vi har konstateret, at der har været en situation, hvor der er gået 16 dage, fra et persondatabrud var konstateret, til de dataansvarlige blev orienteret.

Dette gør, at kontrolmål I ikke er opnået.

Konklusion med forbehold

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. Bortset fra indvirkningen af de forhold, der er beskrevet i afsnittet "Grundlag for konklusion med forbehold", er det vores opfattelse, at:

- (a) beskrivelsen af de udvalgte GDPR-relaterede kontroller hos Fonden F&P Formidling med relevans for WebEDI, således som de var designet og implementeret i hele perioden 1. januar – 31. december 2021, i alle væsentlige henseender er retvisende,
- (b) kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt designet i hele perioden 1. januar – 31. december 2021, 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 2021, 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 været operationelt effektive i hele perioden fra 1. januar – 31. december 2021, hvis kontroller hos underleverandører var operationelt effektive, og hvis de komplementerende kontroller hos de dataansvarlige, der forudsættes i designet af F&P's kontroller, har været operationelt effektive i hele perioden fra 1. januar – 31. december 2021.

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.



Fonden F&P Formidling

ISAE 3000-erklæring omhandlende udvalgte GDPR-kontroller i perioden 1. januar – 31. december 2021 relateret til WebEDI-systemet

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt de dataansvarlige, 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 10. februar 2022
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 design og operationel effektivitet 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 operationel 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 2021.

4.2 Udførte tests

De udførte tests i forbindelse med fastlæggelsen af kontrollers design og operationel effektivitet er beskrevet nedenfor:

Inspektion	<p>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.</p> <p>På de tekniske platforme, databaser og netværkskomponenter har vi testet den specifikke systemopsætning for at påse, om kontroller er designet, implementeret og operationelt effektive i perioden 1. januar – 31. december 2021.</p>
Forespørgsler	<p>Forespørgsel af passende personale hos Fonden F&P Formidling. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.</p>
Observation	<p>Vi har observeret kontrollens udførelse.</p>

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 efterleveres 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: Forespurgt, om der har været tilfælde af behandling i strid med databeskyttelsesforordningen. 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.	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. Stikprøvevist 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 antivirus-systemer. 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 arbejdsbehovet herfor.	F&P: Forespurgt til proceduren for regelmæssig gennemgang af brugerne med adgang til personoplysninger. Inspiceret liste af personer med adgang til personoplysninger.	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	<p>Der er etableret logning i systemer, databaser og netværk af følgende forhold:</p> <ul style="list-style-type: none"> - Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder. - Sikkerhedshændelser omfattende: <ul style="list-style-type: none"> • Ændringer i logopsætninger, herunder deaktivering af logning. • Ændringer i systemrettigheder til brugere. • Fejlede forsøg på log-on til systemer, databaser og netværk. <p>Logningsfaciliteter og log-oplysninger er beskyttet mod manipulation og uautoriseret adgang.</p>	<p>Sentia:</p> <p>Forespurgt om procedure for hændelseslogning. Stikprøvevist inspiceret, at der er opsat hændelseslogning på servere.</p> <p>Forespurgt om proceduren for beskyttelse af logning.</p> <p>Inspiceret, at der logges, når der logges på servere, hvor log opbevares.</p> <p>Inspiceret, at kun autoriserede personer har adgang til servere, herunder logs.</p> <p>Forespurgt om proceduren for logning af systemadministratorer m.v.</p> <p>Stikprøvevist inspiceret, at der er opsat logning af aktiviteter udført af systemadministratorer m.v. på servere.</p>	Ingen afvigelser konstateret.
B	B.10	<p>Personoplysninger, der anvendes til udvikling, test eller lignede, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål.</p>	<p>F&P:</p> <p>Forespurgt om proceduren for sikring af testdata. Inspiceret informationssikkerhedspolitikken for sikring af testdata.</p> <p>Inspiceret, at testdata er pseudonymiseret.</p>	Ingen afvigelser konstateret.
B	B.11	<p>De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.</p>	<p>F&P:</p> <p>Forespurgt om tekniske foranstaltninger og løbende test, herunder sårbarhedsscanninger og penetrationstests.</p> <p>Sentia:</p> <p>Forespurgt, om der løbende laves sårbarhedsscanninger i deres netværk.</p>	<p>Vi har konstateret, at der ikke er udført test på tekniske foranstaltninger i rapporteringsperioden.</p> <p>Ingen yderligere afvigelser konstateret.</p>

Pkt.	Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
B	B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer 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. Stikprøvevist inspiceret, at der afholdes periodiske driftsstatusmøder, hvor ændringer gennemgås. Stikprøvevist inspiceret, at ændringer testes, inden de bliver lagt i produktion, samt at de er afsluttet.	Ingen afvigelser konstateret.
B	B.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugerens 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.
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. Inspiceret, at datacenteret er 27001-certificeret.	Ingen afvigelser konstateret.

Pkt.	Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
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 informationsikkerhedspolitik, 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 informationsikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Inspiceret dokumentation for, at informationsikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.	Vi har konstateret, at der indenfor rapporteringsperioden ikke har været formel godkendelse af informationsikkerhedspolitikken, grundet organisationsændringer. Vi er blevet informeret om, at dette er gennemført på bestyrelsesmøde 2. februar 2022. Ingen yderligere afvigelser konstateret.
C	C.2	Databehandlerens ledelse har sikret, at informationsikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	F&P: Inspiceret dokumentation for ledelsens vurdering af, at Informationsikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Stikprøvevist inspiceret, at kravene i databehandleraftalerne er dækket af informationsikkerhedspolitikens 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: <ul style="list-style-type: none"> - Referencer fra tidligere ansættelser. - Straffeattest. - M.m. 	F&P: Forespurgt, hvordan der foretages efterprøvning af medarbejdere i forbindelse med ansættelse.	Ingen afvigelser konstateret.

Pkt.	Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
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: Forespurgt til proceduren for fortrolighedsaftale ved ansættelse. Inspiceret liste af til- og fratrådte i 2021. Inspiceret, at standardkontraktformularen indeholder et punkt vedrørende fortrolighedsaftale og tavshedspligt. Stikprøvevist inspiceret, at nyansatte medarbejdere har underskrevet en ansættelseskontrakt. Inspiceret, at informationssikkerhedspolitikken er tilgængelig for medarbejdere.	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 nedlæggelse af brugerkonti i forbindelse med fratrædelse eller behandlingsophør. Inspiceret liste af til- og fratrådte i 2021. Inspiceret, at der er procedurer for at gøre brugerkonti inaktive ved fratrædelse eller behandlingsophør.	Ingen afvigelser konstateret.
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 2021.	Vi har konstateret, at Forsikring & Pension ikke har afholdt GDPR-awareness-kurser. Ingen yderligere afvigelser konstateret.

Pkt.	Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
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 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.
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.

Pkt.	Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
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.	Ingen afvigelser konstateret.
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. Stikprøvevist 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. Stikprøvevist inspiceret, at der er dokumentation for, at underdatabehandlere fra databehandlerens oversigt over underdatabehandlere fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige.	Ingen 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. Stikprøvevist 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: <ul style="list-style-type: none"> - 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.	Ingen 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 underdatabehandlere 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 detaljerede 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 dataansvarlige 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 2021. Inspiceret dokumentation for gennemført awareness-træning i 2021.	Vi har konstateret, at Forsikring & Pension ikke har afholdt GDPR-awareness-kurser. Ingen yderligere afvigelser konstateret.
I	I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødigt 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 har været brud på persondatasikkerheden i erklæringsperioden. Inspiceret sagsforløb på sikkerhedshændelsen.	Vi har konstateret, at der har været en situation, hvor F&P på baggrund af henvendelse fra en dataansvarlig har konstateret, at persondata fejlagtigt var sendt til forkert modtager pga. en systemfejl. F&P undersøgte forholdet og underrettede 16 dage senere de berørte dataansvarlige om databrudet, efter at F&P havde fået klarlagt forholdet, og hvilke dataansvarlige der kunne være berørt af fejlen. Ingen yderligere 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: <ul style="list-style-type: none"> - 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: <ul style="list-style-type: none"> - 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.

5 Supplerende information

Revisor har givet anmærkning vedrørende it-sikkerhedspolitikken, der ikke i overensstemmelse med de interne procedurer forelå i opdateret og endeligt godkendt version på tidspunktet for revisors afslutning af kontroller. Dette skyldes sen forelæggelse for Forsikring & Pensions bestyrelse som følge af de igangværende organisationsændringer. En ny version af it-sikkerhedspolitikken blev godkendt af bestyrelsen på et møde den 3. februar 2022.

For så vidt angår tekniske og organisatoriske sikkerhedsforanstaltninger for WebEDI, er der af revisor givet bemærkning i relation til GDPR-awareness-træning, som ikke har fundet sted i 2022. Almindeligvis afholdes der løbende kurser for medarbejdere med henblik på både generel GDPR-awareness og specifikt i relation til WebEDI. Der har i 2021 ikke været gennemført GDPR-awareness-træning for medarbejdere i relation til behandlingen af persondata i WebEDI, hvilket bl.a. skyldes corona-pandemien.

PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registreret, og informationerne er listet herunder.

“Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument.”

Thomas Brenøe

Vicedirektør

På vegne af: Forsikring & Pension

Serienummer: CVR:42855588-RID:17257469

IP: 188.244.xxx.xxx

2022-02-11 15:16:51 UTC

NEM ID 

Torben Weiss Garne

Underdirektør

På vegne af: Forsikring & Pension

Serienummer: PID:9208-2002-2-964724568677

IP: 188.244.xxx.xxx

2022-02-11 15:48:54 UTC

NEM ID 

Nils Bonde Christiansen

Statsautoriseret revisor

På vegne af: EY Godkendt Revisionspartnerselskab

Serienummer: PID:9208-2002-2-243192639174

IP: 213.32.xxx.xxx

2022-02-11 17:19:11 UTC

NEM ID 

Jesper Due Sørensen

Partner

På vegne af: EY Godkendt Revisionspartnerselskab

Serienummer: PID:9208-2002-2-421950499915

IP: 87.49.xxx.xxx

2022-02-12 12:53:24 UTC

NEM ID 

Penneo dokumentnøgle: 64NPP-4DTBY-WOZJJ-KV5WE-QSIOF-XGY1B

Dette dokument er underskrevet digitalt via **Penneo.com**. Signeringsbeviserne i dokumentet er sikret og valideret ved anvendelse af den matematiske hashværdi af det originale dokument. Dokumentet er låst for ændringer og tidsstemplet med et certifikat fra en betroet tredjepart. Alle kryptografiske signeringsbeviser er indlejret i denne PDF, i tilfælde af de skal anvendes til validering i fremtiden.

Sådan kan du sikre, at dokumentet er originalt

Dette dokument er beskyttet med et Adobe CDS certifikat. Når du åbner dokumentet

i Adobe Reader, kan du se, at dokumentet er certificeret af **Penneo e-signature service** <penneo@penneo.com>. Dette er din garanti for, at indholdet af dokumentet er uændret.

Du har mulighed for at efterprøve de kryptografiske signeringsbeviser indlejret i dokumentet ved at anvende Penneos validator på følgende websted: <https://penneo.com/validate>