F&P Brancheløsninger

Uafhængig revisors ISAE 3000-erklæring omhandlende udvalgte GDPR-kontroller i perioden 1. januar – 31. december 2023 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

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

WebEDI-systemet er et elektronisk system til udveksling af oplysninger forsikrings- og pensionsselskaberne imellem og mellem selskaberne og deres forskellige samarbejdspartnere, herunder banker, praktiserende læger, speciallæger og tandlæger. WebEDI-systemet omfatter 9 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 F&P Brancheløsninger.

1.1 Systembeskrivelse og dataflow

Udveksling af oplysninger i WebEDI-systemet er baseret på, at de deltagende parter kan udveksle dokumenter via Webblanketter, EDIFACT, XML og JSON. 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 forsikringsselskaber, pensionsselskaber 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 ni ordninger via WebEDI-serveren, der har en daglig volumen på knap 15.000 dokumenter svarende til godt 10 dokumenter i minuttet.

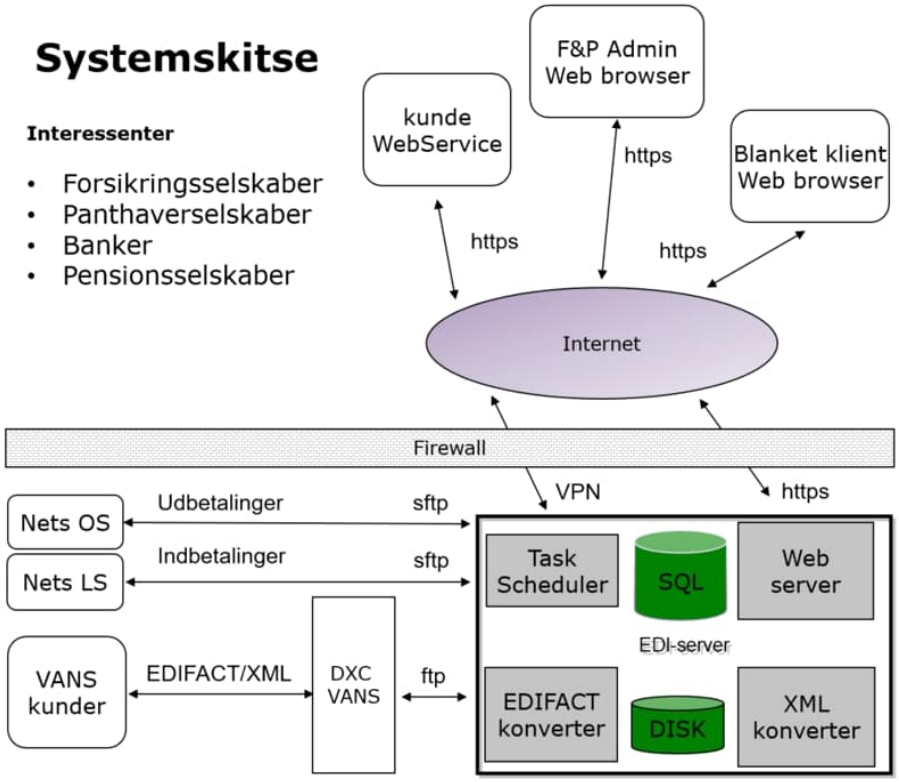
Bag WebEDI står som nævnt F&P Brancheløsninger, som står for drift, udvikling og support af løsningen.

De ansatte, der bistår WebEDI, er alle ansat i F&P Brancheløsninger.

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

WebEDI-it-systemet er hosted hos Sentia, der ligger Lyskær 3A, 2730 Herlev.

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	8 %	92 %		
Regres	3 %	97 %		
Panthaverdeklaration	47 %	53 %		
Pensionsoverførsler – PGF41	18 %		82 %	
Pensionsoverførsler – UPB	67 %		33 %	
LD-flytning	34 %		66 %	
FP-attester	100 %			
TL-attester	100 %			
Skadehistorik				100 %

(*) baseret på tal for 2022.

Selskaberne er opdelt i følgende typer:

Selskabstype	Udveksler	Bemærkninger
Forsikringsselskab	Opsigelser Regres Panthaverdeklarationer FP-attester TL-attester Skadehistorik	
Panthaverselskab	Panthaverdeklarationer	
Pensionsselskab	Pensionsoverførsler (PGF41, pension-pension) Pensionsoverførsler (UPB, pension-bank) LD-flytning FP-attester TL-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 F&P Brancheløsninger, som ejer og drifter 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 F&P Brancheløsninger 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 Forsikring & Pension, 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 Forsikring & Pension.

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 revisorerklæringer 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.

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 erklæringer mellem selskaberne og de praktiserende læger tilknyttet løsningen.
- Mailgun, der anvendes til at udsende adviseringsmail til de brugere og selskaber, der anvender systemet.
- F&P Brancheløsninger anvendes i forbindelse med registrering af supporthenvendelser fra de selskaber, der anvender systemerne.

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.

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 F&P Brancheløsningers rapportering, som har til formål at give de dataansvarlige indsigt i WebEDI's kontroller i relation til behandling af personoplysninger. F&P Brancheløsninger 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.

F&P Brancheløsninger 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.

1.6 Kontrolforanstaltninger

WebEDI er underlagt den overordnede persondatapolitik for Forsikring & Pension. Politikken er godkendt af bestyrelsen i F&P. Persondatapolitikken revideres efter behov og mindst én gang årligt. I tillæg til politikken hører en række forretningsgange, der tilsammen sikrer overholdelse af persondataretlige lovgivning.

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 F&P Brancheløsningers 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 F&P Brancheløsninger 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 F&P Brancheløsninger.

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. WebEDI'skontrol af Sentia sker ved fremsendelse af GDPR-revisorerklæring én gang årligt. Der afholdes yderligere månedlige møder med Sentia omkring projekter, patches, Disaster Recovery, adgang og rettigheder, drift og oppetider 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 & Pension og er godkendt af Forsikring & 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 er senest sket i december 2023.

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. Medarbejderstaben i relation til WeEDI er udvidet med en ny medarbejder i maj 2023.

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 awareness-træning, der afholdes for alle medarbejdere.

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.

På TEST systemet slettes alt data efter 6 mdr. Dette sker via et job, der kører hver måned, så det er løbende måned + 6 mdr.

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 pensionsselskaber	Afsluttede overførsler og forespørgsler slettes efter 10 år. Afviste overførsler, ubesvarede anmodninger eller forespørgsler slettes efter 2 år.
Pensionsoverførsler mellem pensionsselskaber 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.

EDI-løsning	Opbevarings-/sletteregler
	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	Svar fra tandlægen gemmes ikke i EDI-systemet, men hentes online fra Nasure, der er centrale dataleverandører for tandlægerne, via SYNLAB. Sletteproceduren er sat op til at slette data og adgang til data efter forskellige tidsfrister. Tidsfristerne er: 14 dage: Selskabets adgang til helbredsoplysningerne, som tandlægen har videregivet, bliver slettet 14 dage efter, at selskabet har hentet helbredsoplysningerne. 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. 6 måneder: Oplysninger om kundens helbred, som selskabet har indtastet i anmodningen, fx skadestidspunkt, bliver slettet efter 6 måneder. 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.

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 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 2022 er modtaget i januar 2023. Erklæringen er givet uden anmærkninger.

Udover Sentia benytter WebEDI følgende underleverandører, der behandler persondata:

- DXC, der står for forbindelsen til VANS-netværket
- SYNLAB, der står for løsningen ud til de praktiserende læger.
- Mailgun, der står for adviseringsmails
- F&P Brancheløsninger, der står for registrering af supporthenvendelser

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

Nasure er taget ud af listen af underdatabehandlere, da Nasure ikke er underleverandør for WebEDI, men er dataleverandører for tandlægerne.

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 2023 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 F&P Brancheløsningers 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.

1.8 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 F&P Brancheløsninger	x	
Passwordpolitik	WebEDI	Brugere af WebEDI
Medarbejdere hos brugere af WebEDI		x
Medarbejdere hos F&P Brancheløsninger	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 F&P Brancheløsninger	x	
Kontrol af data, der lægges i systemet	WebEDI	Brugere af WebEDI
Medarbejdere hos brugerne af WebEDI		x

2 Udtalelse fra ledelsen

Forsikring og Pension (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 sektion 1 medtager de relevante kontrolmål og underliggende kontrolaktiviteter hos Sentia.

F&P anvender DXC, Synlab, og Mailgun til henholdsvis VANS-netværk, udveksling af data mellem praktiserende læger og adviseringsmails. Beskrivelsen i sektion 1 medtager kun kontrolmål og kontrolaktiviteter hos F&P og medtager således ikke kontrolmål og underliggende kontrolaktiviteter hos DXC, Synlab og MailGun. Visse kontrolmål kan kun nås, hvis underleverandørens kontroller, der forudsættes i designet af vores kontroller, er passende designet og operationelt effektive. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underleverandøren.

Beskrivelsen angiver, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan opnås, hvis komplementerende kontroller hos medlemmer, 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 medlemmer.

F&P bekræfter, at:

(a) den medfølgende beskrivelse i sektion 1 giver en retvisende beskrivelse af de generelle it-kontroller med relevans for WebEDI-systemet, der har været anvendt af brugerne af F&P's WebEDI-system i perioden fra 1. januar - 31. december 2023. Kriterierne for 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 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. Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger

(ii) indeholder relevante oplysninger om ændringer i serviceleverandørens system foretaget i perioden fra 1. januar - 31. december 2023.

(iii) ikke udelader eller forvansker information, der er relevant for omfanget af det beskrevne system, under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og derfor ikke kan omfatte ethvert aspekt ved systemet, som den enkelte kunde 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 perioden fra 1. januar - 31. december 2023, hvis relevante kontroller hos underleverandører var hensigtsmæssigt designet og operationelt effektive, og de danatasvarlige har udført de komplementerende kontroller, som forudsættes i designet af F&P's kontroller i perioden fra 1. januar – 31. december 2023. Kriterierne for 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 udført konsistent som designet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i perioden fra 1. januar – 31. december 2023.

Hellerup, den 19. februar 2024

Thomas Brenøe
Direktør F&P brancheløsninger

Michael Rasch
underdirektør, Infrastruktur og helbredsdata

3 Uafhængige revisors erklæring

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

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

Omfang

Vi har fået som opgave at afgive erklæring om F&P's beskrivelse i sektion 1 af udvalgte GDPR-kontroller relateret til WebEDI-systemet i perioden 1. januar – 31. december 2023 (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 sektion 1 medtager de relevante kontrolmål og underliggende kontrolaktiviteter hos Sentia. Vores handlinger har omfattet vurdering af beskrivelsen samt designet og operationel effektivitet af kontrolmål og relaterede kontroller hos Sentia.

F&P anvender DXC, Synlab, og Mailgun til henholdsvis VANS-netværk, udveksling af data mellem praktiserende læger og adviseringsmails. Beskrivelsen i sektion 1 medtager kun kontrolmål og kontrolaktiviteter hos F&P og medtager således ikke kontrolmål og underliggende kontrolaktiviteter hos DXC, Synlab og MailGun. 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 Mailgun, 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 sektion 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

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.

EY Godkendt Revisionspartnerselskab anvender International Standard on Quality Management 1, ISQM1, som kræver, at vi designer, implementerer og driver et kvalitetsstyringssystem, herunder politikker eller procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende lov og øvrig regulering.

Vores ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om F&P's 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 serviceleverandørens 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 F&P har specificeret og beskrevet i sektion 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

F&P's 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.

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 sektion 2, 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 perioden 1. januar – 31. december 2023, i alle væsentlige henseender er retvisende,

(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt designet i perioden 1. januar – 31. december 2023, hvis kontroller hos underleverandører og komplementerende kontroller hos dataansvarlige var hensigtsmæssigt designet og implementeret i perioden fra 1. januar – 31. december 2023, som forudsat i designet af F&P's kontroller, 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 perioden fra 1. januar – 31. december 2023, 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 perioden fra 1. januar – 31. december 2023.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i sektion 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 19. februar 2024
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 sektion 1. Eventuelle andre kontrolmål, tilknyttede kontroller og kontroller hos de medlemmer af F&P, der anvender løsningen, beskrevet i sektion 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 2023.

4.2 Udførte tests

De udførte tests i forbindelse med fastlæggelsen af kontrollers design og operationel effektivitet 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 operationelt effektive i perioden 1. januar – 31. december 2023.
Forespørgsler	Forespørgsel af passende personale hos F&P. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Vi har observeret kontrollens udførelse.

4.3 Resultater af tests

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.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.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.	F&P har I 2023 anvendt 1 underdatabehandlere, som ikke fremgår af databehandleraftalerne med de dataansvarlige. Ingen yderligere afvigelser konstateret.
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.	F&P har oplyst, at der har ikke været handlet i strid med databeskyttelsesforordningen i erklæringsperioden. Ingen afvigelser konstateret.

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.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.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.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
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.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.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 opdeling af kundenetværk. Inspiceret opsætning i det virtuelle miljø samt netværksdiagram for adskillelse mellem udviklings-, test- og driftsmiljøer.	Ingen afvigelser konstateret.

Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
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 liste af personer med adgang til personoplysninger.	Ingen afvigelser konstateret.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering. Overvågningen omfatter kapacitetsovervågning.	**F&P og Sentia:** Inspiceret Sentias wiki site for procedure vedrørende kapacitetsstyring. Inspiceret, at der er etableret overvågning og rapportering af kapacitetsudnyttelse.	Ingen afvigelser konstateret.
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.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
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. Logningsfaciliteter og log-oplysninger er beskyttet mod manipulation og uautoriseret adgang.	**Sentia:** Forespurgt om procedure for hændelseslogning. Stikprøvevis 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.	Hændelseslogning er ikke konfigureret, jf. leverandørens anbefalinger, på 2 parameter, for 2 ud af 2 Windows-servere. Ingen yderligere afvigelser konstateret.
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 og brugen af testdata. Inspiceret informationssikkerhedspolitikken for sikring af testdata.	F&P har oplyst, at medlemsselskaberne er ansvarlige for testdata i systemet. Ingen afvigelser konstateret.
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	**F&P:** Forespurgt om tekniske foranstaltninger og løbende test, herunder sårbarhedsscanninger og penetrationstests. **Sentia:** Forespurgt, om der løbende laves sårbarhedsscanninger i deres netværk.	Ingen afvigelser konstateret.

Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
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. Stikprøvevis inspiceret, at der afholdes periodiske driftsstatusmøder, hvor ændringer gennemgås. **Sentia:** Inspiceret liste af ændringer. Stikprøvevis inspiceret, at ændringer til systemer, databaser og netværk følger proceduren. Inspiceret, at systemer er opdaterede.	Ingen afvigelser konstateret.
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.
B.14	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler hvori der opbevares og behandles personoplysninger.	**F&P:** Observeret, at adgang til lokaler hvori der opbevares og behandles personoplysninger, er begrænset til autoriserede personer.	Ingen afvigelser konstateret.
C	**Kontrolmål: Der er procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.**		
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.	**F&P:** Inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år.	Ingen afvigelser konstateret.

Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
	Der er krav om løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.	
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.3	Der udføres en efterprøvning af medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: - Referencer fra tidligere ansættelser. - Straffeattest.	**F&P:** Forespurgt, hvordan der foretages efterprøvning af medarbejdere i forbindelse med ansættelse. Stikprøvevis inspiceret, at screening er foregået i forbindelse med ansættelser.	Ingen afvigelser konstateret.
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, at standardkontraktformularen indeholder et punkt vedrørende fortrolighedsaftale og tavshedspligt. Stikprøvevis inspiceret, at nyansatte medarbejdere har underskrevet en ansættelseskontrakt. Inspiceret, at informationssikkerhedspolitikken er tilgængelig for medarbejdere.	Ingen afvigelser konstateret.

Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
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, at der er procedurer for at gøre brugerkonti inaktive ved fratrædelse eller behandlingsophør, samt tilbagelevering af aktiver. Stikprøvevis inspiceret, at fratrådte medarbejderes systemadgange lukkes, samt at eventuelle aktiver tilbageleveres.	Ingen afvigelser konstateret.
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. Stikprøvevis inspiceret, at der er afholdt awareness-træning for nyansatte som en del af deres onboarding.	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.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.

Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
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. Inspiceret, at slette jobs afvikles efter gældende regler og procedurer. Stikprøvevis inspiceret, at data slettes efter gældende regler.	Ingen afvigelser konstateret.
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. Stikprøvevis 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.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.

Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	**F&P:** Inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder. 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.	F&P har i 2023 anvendt 1 underdatabehandler, som ikke fremgår af databehandleraftalerne med de dataansvarlige. Ingen yderligere 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.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.
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.	F&P har i 2023 anvendt 1 underdatabehandler, som ikke fremgår af databehandleraftalerne med de dataansvarlige. Ingen yderligere afvigelser konstateret.

Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
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.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.	For 1 ud af 4 underdatabehandlere, er der ikke de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen med de dataansvarlige. Ingen yderligere afvigelser konstateret.
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.	Ingen afvigelser konstateret.
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, statusrapporter eller lignende.	**F&P:** Inspiceret, at der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne.	F&P har ikke dokumenteret opfølgning på 2 ud af 4 underdatabehandlere. Ingen yderligere afvigelser konstateret.

Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
		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.	
G	**Kontrolmål: Der er procedurer og kontroller, som sikrer, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.**		
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at da-tabehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførsels-grundlag. 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 personoplysninger alene overføres til tredjelande eller internationale organisationer i henhold til aftale med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
G.2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den data-ansvarlige.	**F&P:** Inspiceret, at databehandleren har en samlet og opdateret oversigt over overførsler af personoplysninger til tredjelande eller internationale organisationer. Forespurgt, om der sker overførsler til tredjelande.	F&P har overført persondata til tredjeland uden instruks fra den dataansvarlige. Ingen yderligere afvigelser konstateret.

Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
G.3	Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	**F&P:** Inspiceret, at der foreligger formaliserede procedurer for sikring af et gyldigt overførselsgrundlag. Inspiceret, at procedurerne er opdateret. Forespurgt, om der sker overførsler til tredjelande.	F&P har overført persondata til tredjeland uden instruks fra den dataansvarlige. Ingen yderligere afvigelser konstateret.
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.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.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.	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.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.2	Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: - Awareness hos medarbejdere.	**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. Stikprøvevis inspiceret, at der er afholdt awareness-træning for nyansatte som en del af deres onboarding.	Ingen afvigelser konstateret.
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 har været brud på persondatasikkerheden i erklæringsperioden. Inspiceret handlinger udført i relation til brud persondatasikkerheden. Herunder at dataansvarlige er underrettet.	Ingen afvigelser konstateret.

Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
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. Forespurgt, om der har været henvendelser vedr. bistand, fra de dataansvarlige i erklæringsperioden.	F&P har oplyst, at der ikke har været brud på persondatasikkerheden i erklæringsperioden. Ingen afvigelser konstateret.

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

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

Thomas Brenøe
Direktør F&P Brancheløsninger
På vegne af: F&P
Serienummer: d811ad1d-89fe-4adb-805c-98b50180b8ba
IP: 104.28.xxx.xxx
2024-02-19 18:01:42 UTC

Michael Rasch
F&P Brancheløsninger P/S CVR: 42855588
Underdirektør Infrastruktur og helbredsdata
På vegne af: F&P
Serienummer: 1e639566-a27f-499a-bfe2-5c3c7c43398e
IP: 188.244.xxx.xxx
2024-02-20 06:55:45 UTC

Jesper Due Sørensen
EY Godkendt Revisionspartnerselskab CVR: 30700228
Partner
På vegne af: EY Godkendt Revisionspartnerselskab
Serienummer: a6d834d7-442d-428e-ade9-c250dca23ab3
IP: 80.208.xxx.xxx
2024-02-20 06:59:26 UTC

Nils Bonde Christiansen
EY Godkendt Revisionspartnerselskab CVR: 30700228
Statsautoriseret revisor
På vegne af: EY Godkendt Revisionspartnerselskab
Serienummer: a4c7bea3-5a9f-4f35-bb2c-9ca1124e41f1
IP: 165.225.xxx.xxx
2024-02-20 09:42:38 UTC