F&P Brancheløsninger

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

Indhold

1 Beskrivelse af F&P Brancheløsningers (F&P) Autotaks-system

Autotaks Autotaks er en elektronisk platform til udveksling af oplysninger om skader og reparationsmuligheder, herunder taksering i forbindelse med forsikringsselskabers behandling af bilskadessager. Der udveksles persondata igennem løsningen. Bag Autotaks står F&P Brancheløsninger P/S, som ejer og drifter løsningen.

1.1 Systembeskrivelse og dataflow

Forsi.dk/Autotaks er det primære værktøj til skadesselskabernes samarbejde omkring autoskader mellem autotaksatorer og autoreparatører i Danmark. Der findes forskellige brugertyper i systemet, som hver især har forskellige rettigheder og pligter for at kunne udføre de nødvendige procedurer/forretningsgange i samarbejdet og derved adgang til data.

Samarbejdet mellem autoreparatør og autotaksator kan ikke stå alene, men kræver også, at der er et forsikringsselskab involveret for at udbetale penge til autoreparatøren. Det betyder, at Forsi.dk/Autotaks "blot" er en kommunikationsplatform med en indbygget autoskade-"beregningsmotor", som kan kvantificere skadestørrelsen i kroner/øre.

Forsi.dk/Autotaks er således blot et anvisningsværktøj til forsikringsselskabet, og den egentlige udbetaling sker igennem forsikringsselskabernes police/kunde/skadesystemer.

Denne "treenighed" (værksted/taksator/forsikringsselskab) giver en høj grad af sikkerhed omkring skadesudbetalingen, da der ud over den af taksator godkendte skadeopgørelsen også skal være en "kunde" i policesystemet og en anmeldt/godkendt skadesanmeldelse i forsikringsselskabets skadesystemer. Arbejdet omkring anmeldelser, policer, erstatningsret og udbetaling foretages af forsikringsselskabernes sags-/skadebehandler. Der er til systemet knyttet et billedarkiv, hvor brugerne af systemet kan uploade billedfiler til brug for skadessagsbehandlingen.

Data udveksles således i systemet mellem skadesforsikringsselskaberne, autoværkstederne og taksatorerne.

Fra systemet udveksles data med følgende partnere, der er at anse for selvstændigt dataansvarlige:

Auto IT

Ved oprettelse af en ny rapport laves der et opslag på registreringsnummer eller stelnummer hos Auto IT. I Autotaks gemmer vi oplysninger om stelnummer, registreringsnummer, fabrikat, model og undertype.

Forsikringsselskaber/Policeopslag

Ved oprettelse af en ny rapport laves der et policeopslag hos forsikringsselskabet, hvis selskabet er konfigureret dette. Resultatet af policeopslaget bliver gemt under rapporten i Autotaks.

Solera

I forbindelse med den reelle skadesopgørelse sender vi informationer om fabrikat, model og undertype til Solera. Disse informationer bruges til at kunne vise de rigtige blueprints af bilen.

Ekstern validering

Hvis et forsikringsselskab har konfigureret ekstern validering af en rapport, så sender vi rapportinformationerne til den eksterne validering.

Tredjeparts integrationer

Der findes et ukendt antal tredjeparts integrationer, der kan hente data på vegne af værksteder og selskaber. Disse integrationer har allesammen fået tildelt en brugerrettighed af værkstedet eller selskabet og agere på vegne af disse.

Selve Autotaks it-systemet er hosted hos Sentia. Billedarkivet i Autotaks-løsningen ligger i skyen på Azure-platformen hos Microsoft.

1.2 Behandlingen af persondata og grundlaget herfor

Data, der udveksles i Autotaks-systemet mellem skadesselskaberne, taksatorerne og autoværkstederne, omfatter persondata.

Data behandles på vegne af skadesselskaberne, der er dataansvarlige, og Autotaks-systemet er databehandler. Der er indgået databehandleraftale mellem de dataansvarlige og Forsikring & Pension, som ejer og drifter Autotaks-systemet. Behandlingen sker på grundlag af denne aftale, der omfatter de dataansvarliges instruks til behandlingen.

I systemet behandles almindelige persondata som navn, adresse, postnummer, telefonnummer, registreringsnummer, stelnummer, policenummer, kundenummer, skadenummer, selvrisiko samt beskrivelse og billeder af motorkøretøjet (personhenførbare i det omfang, de afslører registreringsnummer samt noget om skadens karakter).

Autotaks' behandling af personoplysninger på vegne skadesforsikringsselskaberne drejer sig primært om udveksling af oplysninger i systemet mellem forsikringsselskabernes taksatorer og autoværkstederne i forbindelse med bilskadesager. I systemet er det også muligt at opbevare oplysninger i et arkiv, der primært bruges til billedmateriale i forhold til skadessager.

De registrerede er forsikringstagere i de tilsluttede selskaber.

1.3 Revision og kontrol af Autotaks og eventuelle underdatabehandlere

Denne erklæring udgør Autotaks' rapportering, som har til formål at give de dataansvarlige indsigt i Autotaks' behandling af personoplysninger. Autotaks 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 Autotaks' 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 Autotaks 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 Autotaks i videst muligt omfang vil gennemføre inspektionen på den dataansvarliges vegne.

Både vedrørende inspektion af Autotaks' 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 Autotaks'/underdatabehandleres fremlæggelse af rapporter, erklæringer eller anden skriftlig dokumentation. Databehandleraftalen fastlægger vilkår for afholdelse af omkostninger i forbindelse med inspektion.

1.4 Risikovurdering

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

Autotaks 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 Autotaks 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 Autotaks efter anmodning bistå de dataansvarlige hermed. Der er ikke for nuværende konstateret en høj risiko ved behandlingen i Autotaks-systemet.

Der er foretaget samlet risikovurdering af systemet og af de enkelte underdatabehandlere. Risikoen for den registrerede ved behandlingen af persondata i Autotaks-systemet vurderes i udgangspunktet som lav – mellem. Den lave risiko skyldes karakteren af persondata, der behandles, som udelukkende omfatter almindelige oplysninger som navn og adresse. Registreringsnummer behandles også, men giver ikke anledning til en særlig risiko. Når risikoen tangerer mellem, skyldes det dels omfanget af transaktioner

og muligheden for at tilføje oplysninger i skadesbeskrivelsen, der kan indikere følsomme forhold for forsikringstager/de registrerede risikoen for overførsel af data til usikre tredjelande, idet dele af systemet er understøttet af Microsoft Azure. Det vil her dog også alene være almindelige persondata – primært registreringsnummer, som har en begrænset identifikationsrisiko grundet registreringssystemet. Samtidig er der truffet forskellige foranstaltninger (organisatoriske og tekniske) for håndtering af risici, så risikoen anses samlet for begrænset. Der er ikke sket ændringer i systemet i 2023 hvor karakteren af behandlingen af personoplysninger og de oplysninger der behandles.

1.5 Kontrolforanstaltninger

Autotaks 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 Autotaks. Procedurerne er ligeledes godkendt i GDPR-styregruppen. Opdatering og kontrol af forretningsgange og procedurer sker en gang årligt og er forankret både i IT, i Autotaks' sekretariat samt i Rammevilkår og EU. Procedurerne er siden aftaleindgåelse med Microsoft blevet opdateret i forhold til kontroller af underdatabehandlere, samt overførsel af data til tredjelande.

Autotask 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 Autotaks' forpligtelser overfor de dataansvarlige, samt kontrol med behandlingen hos underdatabehandleren.

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

Behandlingen af persondata i Autotaks sker udelukkende på grundlag af instruks fra de dataansvarlige, der står inde for, at behandlingen er lovlig. Det påhviler dog Autotaks 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 Autotaks indført politikker og procedurer, der understøtter instruksen fra de dataansvarlige og sikrer, at Autotaks' 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 Autotaks sket behandling i strid med instruksen.

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

Instruksen omfatter specifikke krav til Autotaks 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 Autotaks. 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.

1.5.3 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 Autotaks-systemet er underlagt it-sikkerhedspolitikken, som gælder for Forsikring organisationernes fællessekretariat 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.

Medarbejdere med adgang til Autotaks-systemet er alle underlagt fortrolighed ved deres ansættelse. Der er endvidere indført procedurer, der sikrer, at medarbejdernes rettigheder inddrages ved fratrædelse.

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. Der er en løbende dialog om GDPR-problemstillinger mellem medarbejderne i Compliance og medarbejderne i F&P Brancheløsninger P/S, herunder Autotaks, som står for hovedparten af behandlingen af persondata i F&P Brancheløsninger P/S.

1.5.4 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 slettes i udgangspunktet efter 5 år + løbende år regnet fra afslutningen af en sag i systemet. Det er muligt for de dataansvarlige at anmode om sletning før dette tidspunkt.

1.5.5 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.

1.5.6 F. Brug af underdatabehandlere (Databeskyttelsesforordningens artikel 32)

Databehandleraftalen regulerer og fastsætter vilkår for Autotaks' 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, og Microsoft Danmark ApS, der via Azure Platformen – som er en cloud-tjeneste –understøtter arkiv-funktionen i løsningen. Softo – Convertio, der leverer en løsning, som kan videokonvertere forskellige formater til et ensartet format i Autotaks, hvor databehandleraftalen blev Informeret og varslet i december 2022 og ibrugtaget 1. april 2023. Auto IT, der leverer en løsning til automatisk at hente stelnummer på baggrund af registreringsnummer frem. Rekor Systems Inc. (OpenALPR) benyttes ved oprettelse af en ny rapport, hvor brugeren uploader et billede som kun indeholder nummerpladen. Autotaks har siden 2014 benyttet OpenALPR som leveres af Rekor Systems Inc. til at analysere billeder af nummerplader med henblik på at finde registreringsnummeret. Rekor Systems Inc. (OpenALPR) fremgår ikke af databehandleraftalen, se udfærdigede risikovurdering

Herudover er der i aftalen givet en generel godkendelse for Autotaks til antagelse af nye underdatabehandlere, efter høring af de dataansvarlige. De interne procedurer for behandlingen af persondata i Autotaks omfatter retningslinjer for høring af de dataansvarlige, der skal have mulighed for at gøre indsigelser mod den valgte underdatabehandler.

Autotaks 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 Autotaks' forpligtelser over for de dataansvarlige samt fører kontrol med behandlingen hos underdatabehandleren.

I forhold til Sentia, der drifter systemet, har Autotaks 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 2023 er modtaget i februar 2024.

Udover Sentia benytter Autotaks følgende underleverandører, der behandler persondata:

- Microsoft Azure, der understøtter arkivsystemet i skyen.

- Softo – Convertio, der leverer en løsning, som kan videokonvertere forskellige formater til et ensartet format i Autotaks.
- Rekor Systems Inc. (OpenALPR), der benyttes ved oprettelse af en ny rapport, hvor brugeren uploader et billede som kun indeholder nummerpladen.

Samt underleverandører, der ikke behandler persondata:

- Auto IT, F&P bruger Auto IT til automatisk at hente stelnummer på baggrund af registreringsnummer.

Der modtages generelle revisionserklæringer for Microsoft (SOC II erklæringer for it-sikkerheden og ISO 27701 for databeskyttelse). Efter aftalen med Microsoft, er der opsat et governance-system for Autotaks, hvor der bl.a. modtages notifikationer ved ændringer i underleverandører og opdatering af kontrolrapporter for systemet, der løbende gennemgås.

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

Efter instruksen i databehandleraftalen med de dataansvarlige er der givet adgang til overførsel af data til tredjelande, hvor dette er nødvendigt for brug af tjenesten. Denne åbning dækker særligt brugen af Microsoft Azure-platformen, der understøtter billedarkivet i Autotaks-løsningen.

Der er foretaget generel risikovurdering af brugen af Microsoft, herunder også en vurdering af beskyttelsesniveauet i tilfælde af eventuelle tredjelands overførsler. Her er der taget udgangspunkt i at Autotaks' brug af funktionerne på Azure-platformen er begrænset og følgeligt også risikoen for overførsel til tredjelande. Endvidere er der lagt vægt på Microsofts begrænsede adgang til data i systemet, der ligeledes minimerer risikoen for overførsler. Overførsel vil følgelig umiddelbart alene komme på tale i forbindelse med support og/eller server-bouncing ved kapacitetsudfordringer. På baggrund heraf, er der sikret overførselsgrundlag i form af Kommissionens standardkontrakter, som Microsoft har forpligtet sig til at bruge, samt truffet supplerende foranstaltninger i form af yderligere adgangsbegrænsninger til data i systemet, herunder ved kryptering, der administreres af Sentia.

Der har ikke været anmodet om samtykke til overførsel i relation til support-opgaver i 2023.

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

Autotaks 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 Autotaks' forpligtelser overfor de dataansvarlige.

Når Autotaks modtager en henvendelse relateret til selskabernes forpligtelser over for den registrerede, informerer Autotaks den registrerede person om, at Autotaks alene er databehandler, og at personen skal rette henvendelse til den dataansvarlige. Autotaks 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. Autotaks har ikke i 2023 modtaget anmodninger fra registrerede eller de dataansvarlige om bistand.

1.5.9 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 (Databeskyttelsesforordningens artikel 33 og 34)

Databehandleraftalen indeholder instruks om og regulerer Autotaks' forpligtelse overfor de dataansvarlige ved mistanke om eller konstatering af brud på persondatasikkerheden hos Autotaks eller hos en underleverandør.

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

I forbindelse med GDPR-revisionen af Autotaks for 2022 er F&P blevet opmærksomme på, at oversigten over underdatabehandlere i databehandleraftalen ikke var fyldestgørende. Derfor har vi foretaget en anmeldelse til Datatilsynet af det databrud, som består i, at "instruksen" om databehandling er udført ved brug af underdatabehandlere, som de dataansvarlige ikke har været tilstrækkeligt informerede om.

Der er blevet sendt en information ud, hvor F&P beklager den manglende information, men samtidig understreger, at databehandlingen i Autotaks har fundet sted som aftalt, men desværre som nævnt i nogle tilfælde af virksomheder, der ikke fremgik af oversigten af underdatabehandlere. I samme information blev der vedhæftet en Risikovurdering af Microsoft, Softo – Convertio og Rekor Systems Inc. (OpenALPR).

1.6 Komplementerende kontroller hos de dataansvarlige

Kontroller hos Autotaks 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 Autotaks og brugerne af systemet i forhold til brugeradministration, passwordpolitik, periodisk gennemgang af brugernes adgangsrettigheder, beredskab og helt enkelt, hvilke data der lægges i systemet. I forhold til sidstnævnte er det vigtigt at understrege, at adgangen for brugerne af Autotaks-systemet til at lægge data i arkivløsningen p.t. er begrænset til håndtering af billedmateriale i forbindelse med skadessager.

Brugeradministration (oprettelse, ændring og sletning)	**Autotaks**	**Brugere af Autotaks**
Medarbejdere hos brugere af Autotaks		X
Medarbejdere hos Forsikring & Pension	x	
Passwordpolitik	Autotaks	Brugere af Autotaks
Medarbejdere hos brugere af Autotaks		X
Medarbejdere hos Forsikring & Pension	x	
Regelmæssig gennemgang af adgangsrettigheder	Autotaks	Brugere af Autotaks
Medarbejdere hos brugere af Autotaks		X
Regelmæssig gennemgang af adgangsrettigheder	Autotaks	Brugere af Autotaks
Medarbejdere hos Forsikring & Pension	x	
Kontrol af data, der lægges i systemet	Autotaks	Brugere af Autotaks
Medarbejdere hos brugere af Autotaks		X

2 Udtalelse fra ledelsen

Forsikring og Pension (F&P) behandler personoplysninger på vegne af de dataansvarlige, der anvender Autotaks-systemet, i henhold til databehandleraftalen.

Medfølgende beskrivelse er udarbejdet til brug for de dataansvarlige, der har anvendt Autotaks, 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 Autotaks-systemet. Beskrivelsen i sektion 1 medtager de relevante kontrolmål og underliggende kontrolaktiviteter hos Sentia.

F&P anvender Microsoft Azure til arkivering af billeder og andre dokumenter, Softo – Convertio, der leverer en løsning, som kan videokonvertere forskellige formater til et ensartet format i Autotaks. Rekor Systems Inc. (OpenALPR), der benyttes ved oprettelse af en ny rapport, hvor brugeren uploader et billede som kun indeholder nummerpladen. Beskrivelsen i sektion 1 medtager kun kontrolmål og kontrolaktiviteter hos F&P og medtager således ikke kontrolmål og underliggende kontrolaktiviteter hos Microsoft Azure, Softo – Convertio og Rekor Systems Inc. Beskrivelsen angiver også, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan nås, hvis underleverandørels kontroller, der forudsættes i designet af vores kontroller, er passende designet og er operationelt effektive. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underleverandører.

Beskrivelsen angiver, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan opnås, hvis komplementerende kontroller hos kunderne, der forudsættes i designet af F&Ps kontroller, er passende designet og er operationelt effektive sammen med relaterede kontroller hos F&P. Beskrivelsen omfatter ikke kontrolaktiviteter udført af kunder.

F&P bekræfter, at:

(a) den medfølgende beskrivelse i sektion 1 giver en retvisende beskrivelse af de generelle it-kontroller med relevans for Autotaks-systemet, der har været anvendt af brugerne af F&P's Autotaks-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 Autotaks' 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 dataansvarlige 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.

(c) Der er etableret og opretholdt passende tekniske og organisatoriske foranstaltninger med henblik på at opfylde aftalerne med de dataansvarlige, god databehandlerskik og relevante krav til databehandlere i henhold til databeskyttelsesforordningen.

Hellerup, den 23. februar 2024

Thomas Brenøe
Direktør

Peder Herbo
it-direktør

3 Den uafhængige revisors erklæring

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

Til: F&P Brancheløsninger (F&P) og brugere af Autotaks-systemet

Omfang
Vi har fået som opgave at afgive erklæring om F&P's beskrivelse i sektion 1 af udvalgte GDPR-kontroller relateret til Autotaks-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.

Beskrivelsen angiver, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan opnås, hvis komplementerende kontroller hos kunderne, 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 kunderne, og vi har ikke vurderet egnetheden af design eller den operationelle effektivitet af kontrolaktiviteter hos kunderne.

F&P anvender Sentia til drift af Autotaks-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 Microsoft Azure til arkivering af billeder og andre dokumenter, Softo – Convertio, der leverer en løsning, som kan videokonvertere forskellige formater til et ensartet format i Autotaks. Rekor Systems Inc. (OpenALPR), der benyttes ved oprettelse af en ny rapport, hvor brugeren uploader et billede som kun indeholder nummerpladen. Beskrivelsen i sektion 1 medtager kun kontrolmål og relaterede kontroller hos F&P og medtager således ikke kontrolmål og relaterede kontroller hos Microsoft Azure, Softo – Convertio og Rekor Systems Inc. Visse kontrolmål, der er specificeret i beskrivelsen, kun kan 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 Microsoft Azure, Softo – Convertio og Rekor Systems Inc., og vi har ikke vurderet egnetheden af design eller den operationelle effektivitet af kontrolaktiviteter hos underleverandører.

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 ISAE 3000, Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger, som er udstedt af IAASB 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 dataansvarlig

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 Autotaks, 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 afsnit 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt medlemmer af F&P, der har anvendt Autotaks, og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om medlemmernes egne kontroller.

København, den 23. 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 operationelle 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 F&P, 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 hele perioden fra 1. januar – 31. december 2023.

4.2 Udførte tests

De udførte tests i forbindelse med fastlæggelsen af kontrollers design og operationelle 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 fungeret effektivt i perioden fra 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.

For den del af it-miljøerne, der i perioden 1. januar – 31. december 2023 har været outsourcet til Sentia, har vi foretaget test af design, implementering og operationel effektivitet af kontrollerne hos Sentia.

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 indgåede 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 anvendt to 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.	Ingen afvigelser konstateret.

Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
		Inspiceret, at der er procedurer for underretning til den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen.	
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. Stikprøvevist 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 brugere med adgang til personoplysninger. Inspiceret, at der hver anden måned afholdes statusmøder, hvor der foretages gennemgang af brugernes adgang.	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, i henhold til aftale og på dennes vegne.	**F&P:** Forespurgt om proceduren for sikring af testdata. Inspiceret informationssikkerhedspolitikken for sikring af testdata.	Ingen afvigelser konstateret.
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	**F&P:** Forespurgt, hvordan der foretages opfølgning med underleverandøren. Inspiceret, at F&P har modtaget og gennemgået ISAE 3402-erklæring samt ISAE 3000 GDPR-erklæring fra underleverandøren.	Ingen afvigelser konstateret.
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.	Ingen afvigelser konstateret.

Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
		Inspiceret, at Sentias wiki site indeholder procedure for ændringshåndtering. Stikprøvevis inspiceret, at der afholdes periodiske drifts-statusmøder, hvor ændringer gennemgås. **Sentia:** Forespurgt om proceduren for ændringer af organisationen, forretningsprocesser, informationsbehandlingsfaciliteter og -systemer, som påvirker informationssikkerheden.	
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. Der er krav om løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	**F&P:** Inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.	Ingen afvigelser konstateret.

Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
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.
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.	Ingen afvigelser konstateret.

Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
		Stikprøvevis inspiceret, at fratrådte medarbejderes systemadgange lukkes, samt at eventuelle aktiver tilbageleveres.	
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.
D.2	Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner: - Data slettes, såfremt en kontrakt ophører. - Data slettes automatisk efter gældende regler i databehandleraftalen.	**F&P:** Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner. Observeret, at sletterutiner er opsat i systemet og følger databehandleraftalen. Stikprøvevist inspiceret, at persondata slettes.	Ingen afvigelser konstateret.

Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
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.	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.
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. 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.	F&P har anvendt to underdatabehandlere, som ikke fremgår af databehandleraftalerne med de dataansvarlige. Ingen yderligere afvigelser konstateret.

Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
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. 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.	F&P har anvendt to underdatabehandlere, som ikke fremgår af databehandleraftalerne med de dataansvarlige. Ingen yderligere afvigelser konstateret.
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.

Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
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 3 ud af 5 underdatabehandlere, er der ikke de samme eller tilsvarende 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.

Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
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. 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.
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 databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. 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.

Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
G.2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	**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.	Ingen afvigelser konstateret.
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.	Ingen 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.

Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
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. Stikprøvevist inspiceret, at der er aftalte foranstaltninger i databehandleraftaler.	Ingen afvigelser konstateret.
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 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.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.	Ingen afvigelser konstateret.

Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
		Stikprøvevis inspiceret, at der er afholdt awareness-træning for nyansatte som en del af deres onboarding.	
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 liste af incidents.	Ingen afvigelser konstateret.
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.	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."

Peder Herbo
F&P Brancheløsninger P/S CVR: 42855588
It-direktør
På vegne af: F&P Brancheløsninger
Serienummer: a7ebdab7-0425-4b51-92da-a0f81b43d65c
IP: 188.244.xxx.xxx
2024-02-23 11:39:53 UTC

Thomas Brenøe
Direktion
På vegne af: F&P Brancheløsninger
Serienummer: d811ad1d-89fe-4adb-805c-98b50180b8ba
IP: 188.244.xxx.xxx
2024-02-23 11:43:37 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
2024-02-23 11:53:50 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
2024-02-23 12:52:04 UTC