F&P Brancheløsninger

ISAE 3000-erklæring omhandlende udvalgte GDPR-kontroller i perioden 1. januar – 31. december 2022 relateret til Autotaks-systemet

Indhold

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

Autotaks er bilforsikringsselskabernes fælles it-skadeopgørelsessystem. Autotaks, der anvendes af selskabernes taksatorer og af danske autoværksteder, indeholder vejledende reparationstider og reservedelspriser for 38 forskellige bilmærker omfattende mere end 750 bilmodeller. Hvert år opgøres ca. 650.000 bilskader i Autotaks til mere end 8 mia. kr. i samlede erstatningsudgifter.

Autotaks har siden indførelsen i 1990 været taksatorernes primære arbejdsredskab og er løbende blevet opdateret og tilpasset de forretningsgange, som vores medlemsselskabers taksatororganisationer ønsker.

Alle interessenter samarbejder igennem forsi.dk, der er tiltænkt som en egentlig portal. Interessenterne omfatter værksteder, taksatorer og selskabernes sagsbehandlere.

Autotaks/Forsi.dk kan primært opdeles i to hovedområder, kalkulationsdelen og "casemanager".

Kalkulationsdelen

Kalkulationsdelen består af et internationalt anerkendt autoskadeopgørelsessystem leveret af det amerikanske firma Solera. Opgørelsessystemet anvendes i dag i ca. 80 lande.

Systemet kendetegnes ved at kunne udføre en beregning af nødvendig arbejdstid, lakering og reservedelsomfang på en given forsikringsskade på henholdsvis person-/varebiler. Systemet arbejder med en homogen arbejdsproces på tværs af alle bilfabrikanter og kan således håndteres af brugere uanset tilhørsforhold til specifik bilfabrikant. Brugeren behøver således ikke at have mærkespecifik baggrund for at kunne foretage den nødvendige beregning.

Systemet beregner reparationen på baggrund af bilfabrikanternes reparationslitteratur og bilimportørens vejledende udsalgspriser på reservedele.

Systemet består af både en frontend og en backend:

- Frontenden er Javascript/HTML, som indeholder en detaljeret sprængskitse af alle bilens komponenter (reservedele) vist i "naturlige" sammenhænge. Det er i dette software brugeren, der angiver skadens omfang og bestemmer de nødvendige reparationsprocesser.
- Backend er en "beregningsmotor", som på basis af det ovennævnte skadesomfang kan finde den nødvendige arbejdstid og beskrivelser samt medgåede reservedele og derved udregne en arbejdstid.
- Systemet indeholder en komplet database med samtlige arbejdsbeskrivelser og reservedele samt modeloptioner for hver bilmodel indeholdt i Autotaks/Forsi.dk-sortimentet (p.t. ca. 750 bilmodeller) og samtlige billeder, som anvendes i forbindelse med takseringen.

Casemanager

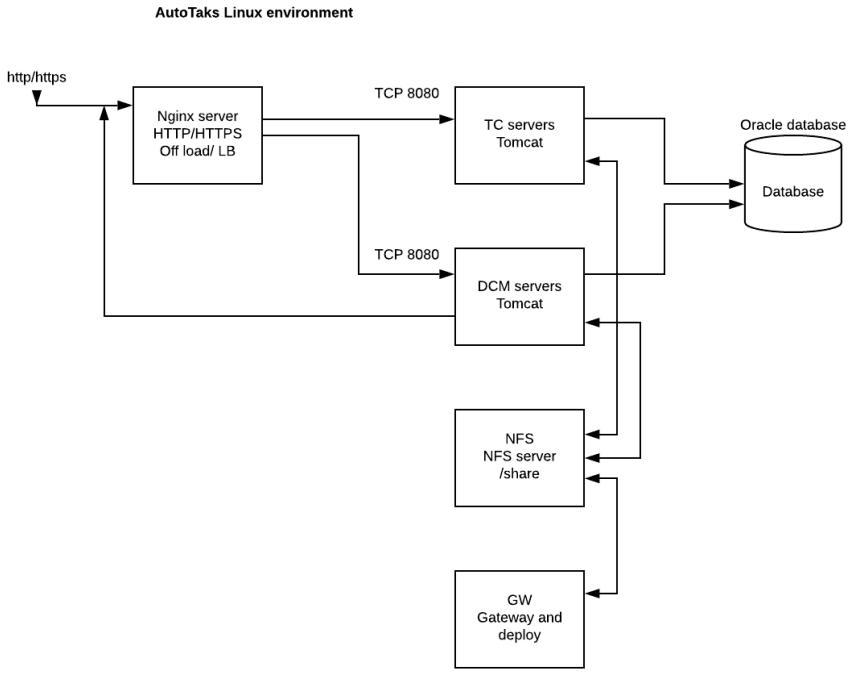
Casemanager består af en Javascript/HTML-frontend og en Java-baseret backend, som binder alle brugere i autoskadeopgørelsesprocessen sammen i en arbejdsplatform. De primære brugere er her forsikringsselskabets taksatorer og Danmarks autoskadereparatører. Samarbejdsformen er typisk den, at reparatøren beregner et reparationstilbud til forsikringsselskabets autotaksator i www.forsi.dk, og reparationstilbuddet overføres automatisk til den forudbestemte autotaksator i selskabet. Det er muligt for det enkelte forsikringsselskab at tilpasse denne relation mellem reparatør og taksator alt efter samarbejdsformen i selskabet. Nogle autotaksatorer arbejder som enkeltpersoner, og andre arbejder i teams – eller i kombination af begge former.

Når taksator har godkendt (og måske ændret) værkstedstilbuddet, bliver tilbuddet til en gældende taksatorrapport, og selskabets sagsbehandler kan behandle og udbetale erstatningsbeløbet. Taksatorrapporten bliver samtidig synlig for reparatøren og står til rådighed for yderligere processer, såsom arbejdskort, planlægning og lagerstyring.

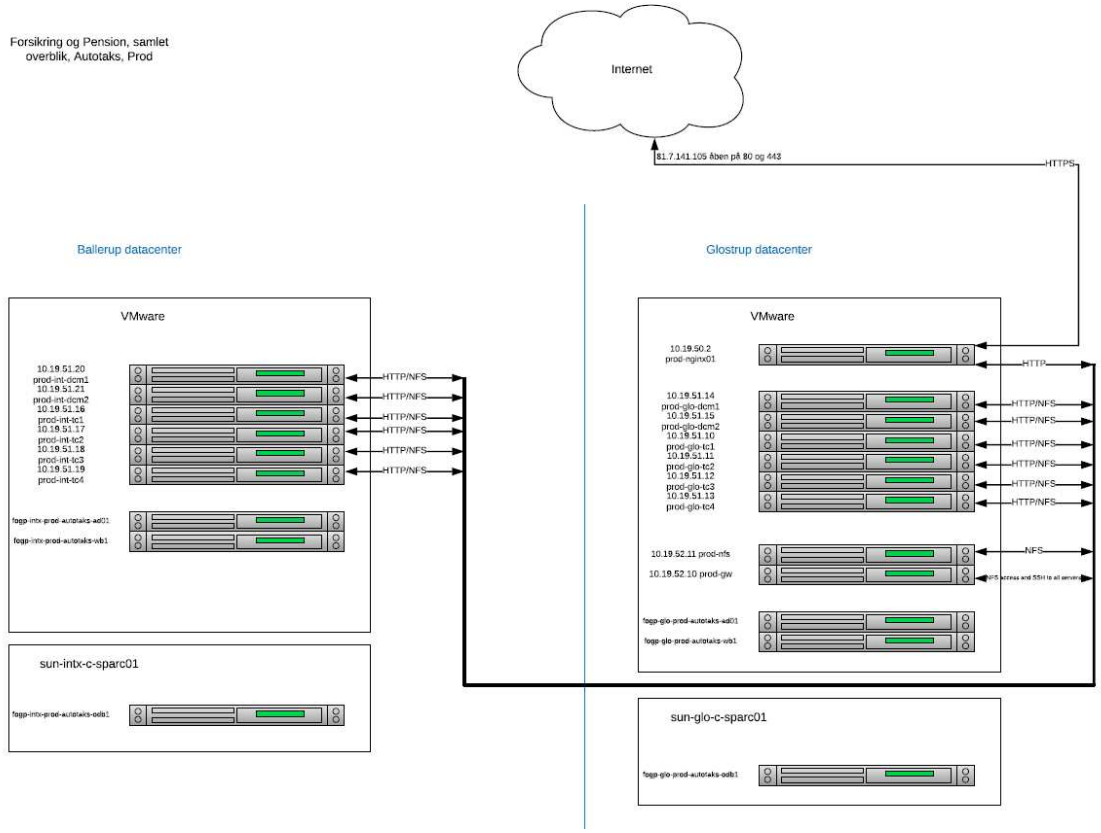
Forsi.dk er som tidligere omtalt autotaksatorernes primære værktøj og understøtter alle de processer, forsikringsselskaberne og lovgivningen forlanger.

Af hensyn til Autotaks-systemets driftsstabilitet er drifts- og produktionsmiljøerne adskilte. Løsningen kører både i test og produktion i et dubleret setup på to forskellige geografiske lokationer. Hvis det ene datacenter lukker ned, vil det andet datacenter tage over. De to datacentre er begge aktive under normal drift, og de er begge dimensioneret, så de kan overtage den samlede belastning og stadig give gode svar tider i forhold til brugerne.

Autotaks-miljøet kan skitseres således:



Følgende diagram viser antallet af de forskellige servere, samt opdelingen i de to datacentre. Dette diagram er specifikt for PROD. Der er en tilsvarende, men mindre opbygning til TEST-miljøet.



1.1 Risikostyring

F&P har i 2022 gennemført en it-risikovurdering for Autotaks.

Med risikovurderingen har vi været interesserede i at forstå og besvare følgende spørgsmål:

- Hvad er det samlede risikoniveau for Autotaks?
- Hvordan er risikoniveauet sammenholdt med risikoappetitten?
- Hvad kan vi og medlemmerne risikere at miste i forbindelse med dette system?
- Hvordan ser et typisk tab for Autotaks ud?
- Hvordan er sikkerhedsniveauet for Autotaks?
- Hvordan rangerer de forskellige typer af it-risici i forhold til hinanden?
- Hvilke risikoreducerende foranstaltninger kan vi med fordel implementere for at nedbringe risikoniveauet?

Den anvendte metode i risikovurderingen er den samme som i 2021. Risikovurderingen redegør for trusselsbilledet i sandsynlig frekvens sat op imod størrelsen af tab i kroner og ører. I forbindelse med risikovurderingen er risikoniveauet også sat i forhold til F&P's risikoappetit for systemet, og det ligger generelt meget tæt på eller under appetitten for de forskellige trusselsområder.

Estimater afgivet af personale fra F&P og fra udvalgte medlemmer, kombineret med hændelser fra 2022, ligger til grund for de resultater og nøgletal, som risikovurderingen præsenterer.

Fortsat opsamling af data fra hændelser, opfølgning på effekten af implementerede sikringsforanstaltninger og iagttagelse af relevant ekstern statistik i de kommende 12 måneder skal medvirke til at forbedre de estimater, der ligger til grund for næste års vurdering. Denne kontinuerlige optimering skal løbende modne F&P's it-risikostyring frem mod at blive blandt de bedste på it-risikostyringsområdet.

1.2 Organisering af sikkerheden i it-miljøerne

Informationssikkerhedspolitik

Tilrettelæggelse og implementering af generelle it-kontroller vedrørende Autotaks-systemet sker med udgangspunkt i F&P's informationssikkerhedspolitik, som er baseret på den internationale it-sikkerhedsstandard ISO27002:2013. Standarden omfatter nedenstående hovedområder.

A.5	Informationssikkerhedspolitikker	A.12	Driftssikkerhed
A.6	Organisering af informationssikkerhed	A.13	Kommunikationssikkerhed
A.7	Personalesikkerhed	A.14	Anskaffelse, udvikling og vedligeholdelse af systemer
A.8	Styring af aktiver	A.15	Leverandørforhold
A.9	Adgangsstyring	A.16	Styring af informationssikkerhedsbrud
A.10	Kryptografi	A.17	Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring
A.11	Fysisk sikring og miljøsikring	A.18	Overensstemmelse

F&P har med udgangspunkt i hovedområderne udvalgt kontrolmål for styringen af informationssikkerheden og relaterede kontroller, der er implementeret. Kontrolmålene og kontrollerne fremgår af oversigten i afsnit 4.3.

Organisering af it-sikkerhed i it-miljøerne sker gennem nedenstående hovedprocesser, der er baseret på standarden ISO27002:2013 og følger den overordnede struktur. De følgende beskrivelser refererer til afsnittene i standarden.

5 Informationssikkerhedspolitikker

It-sikkerhedspolitikken udarbejdes af direktionen og godkendes af bestyrelsen. It-sikkerhedspolitikken er gældende, uanset om it-anvendelsen finder sted internt i F&P, hos en samarbejdspartner eller i forbindelse med outsourcing.

6 Organisering af informationssikkerhed

Arbejdet med it-sikkerhed indgår i de daglige arbejdsrutiner, så det ønskede it-sikkerhedsniveau opnås med færrest mulige administrative og organisatoriske ressourcer. Alle medarbejdere i F&P er fortrolige med it-sikkerhedspolitikken og forretningsgange, der er relevante for den enkeltes funktion og arbejdsopgaver.

7 Personalesikkerhed

Medarbejdersikkerhed stiller krav om tiltag for at reducere risici ved menneskelige fejl samt misbrug, bedrageri og lignende. Alle har pligt til at rapportere brud på sikkerheden til deres leder og/eller F&P's sikkerhedschef.

8 Styring af aktiver

It-sikkerhedspolitikken omfatter alle aktiver, som understøtter F&P's forretningsområder og organisation. Disse består af data, systemer, fysiske aktiver samt tekniske forsyninger, der understøtter it-anvendelsen.

9 Adgangsstyring

Adgangsstyring stiller krav til sikring af adgang til systemer og data. Systemer og data, herunder teknisk basissoftware, er sikret mod uberettiget eller utilsigtet adgang. Adgangen til anvendelse af terminaler, pc-arbejdspladser og servere er beskyttet ved logisk adgangskontrol. Tildeling af adgangsrettigheder m.v. sker ud fra et arbejdsbetinget behov og under hensyntagen til en effektiv funktionsadskillelse.

10 Kryptografi

F&P anvender forskellige krypteringsteknikker afhængig af, hvorledes systemerne risikovurderes.

11 Fysisk sikring og miljøsikring

Fysisk sikkerhed stiller krav til sikring af bygninger, forsyninger og tekniske installationer, der er relevante for F&P.

12 Driftssikkerhed

Styring af kommunikation og drift stiller krav til stabilitet, overvågning og sikkerhed i forbindelse med afvikling af den daglige produktion samt i de anvendte netværksløsninger. Der er etableret dokumentation af driftsprocesser, driftsafvikling, udstyr, systemer og datakommunikationsforbindelser i et sådant omfang, at det muliggør en effektiv vedligeholdelse samt hurtig og korrekt indgriben ved nødsituationer.

13 Kommunikationssikkerhed

Herunder stilles krav til stabilt netværk, hvor datatransmissionen mellem F&P og kunder/samarbejdspartnere er beskyttet mod uautoriseret adgang, forvanskning samt utilgængelighed.

14 Anskaffelse, udvikling og vedligeholdelse af systemer

Anskaffelse, udvikling og vedligeholdelse af systemer stiller krav til F&P's kontroller til sikring af kvalitet, sikkerhed og dokumentation af brugersystemer og basissoftware. De godkendte udviklingsmetoder sikrer systemudvikling med standardiseret brugergrænseflade, høj kvalitet og lav fejlrate. Desuden sikrer udviklingsmodellen, at der tidligt i udviklingsforløbet tages stilling til det ønskede sikkerhedsniveau, herunder at relevante sektor- og lovkrav overholdes. Alle produktionssystemer er dokumenterede, testede og godkendte forud for idriftsættelse.

15 Leverandørforhold

Omfatter informationssikkerhedskravene til at styre risici forbundet med leverandører og outsourcing-partners adgang til F&P's aktiver. Der skal foreligge dokumenterede aftaler med de relevante leverandører.

16 Styring af informationssikkerhedsbrud

Styring af sikkerhedsbrud stiller krav til kontroller for at sikre overblik over indtrufne sikkerhedshændelser samt en hurtig, effektiv og metodisk håndtering af sikkerhedsbrud.

17 Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Omfatter F&P's krav til beredskabsstyring, herunder beredskabsplaner, afprøvning og reetablering i tilfælde af større driftshændelser.

18 Overensstemmelse

Overensstemmelse med lovbestemte og kontraktlige krav stiller krav til kontroller for at forhindre brud på relevante sikkerhedskrav samt indgåede kontraktlige forpligtelser. F&P overvåger og tilpasser løbende sikkerheden til gældende sektor- og lovgivningskrav.

F&P har outsourcet it-drift vedrørende Autotaks-systemet til Sentia. Det er derfor væsentligt, at F&P's informationssikkerhedspolitik også implementeres og efterleves i forbindelse med drift af Autotaks-systemet hos Sentia. Med henblik på at sikre dette, har F&P indgået en aftale med Sentia, som indeholder en række sikkerhedsmæssige krav, der skal overholdes af Sentia.

F&P følger løbende op på Sentias overholdelse af kravene ved gennemgang af driftsrapportering, deltagelse i driftsstyregruppemøder med Sentia m.v. samt ved gennemgang og vurdering af resultatet af årlig revisionsmæssig gennemgang af it-sikkerheden hos Sentia.

Der hentes og gennemgås generelle revisionserklæringer for Microsoft (SOC II-erklæringer for it-sikkerheden og ISO 27701 for databeskyttelse). De til enhver tid nyeste erklæringer er tilgængelige på Microsofts hjemmeside.

1.3 Væsentlige ændringer i it-miljøerne

Der har ikke været nogen væsentlige ændringer i miljøerne i 2022.

1.4 Komplementerende kontroller hos brugerne

Kontroller hos F&P er udformet sådan, at nogle af kontrollerne nævnt i denne erklæring skal suppleres med kontroller hos brugerne.

Oversigten nedenfor beskriver overordnet fordelingen af kontroller mellem F&P og brugerne af Autotaks-systemet i forhold til brugeradministration, password-politik, periodisk gennemgang af brugernes adgangsrettigheder og beredskab.

Brugeradministration (oprettelse, ændring, sletning)	F&P	Brugere af Autotaks-systemet
Medarbejdere hos brugere af F&P		x
Medarbejdere hos F&P	x	
Passwordpolitik	**F&P**	**Brugere af Autotaks-systemet**
Medarbejdere hos brugere af F&P		x
Medarbejdere hos F&P	x	
Regelmæssig gennemgang af adgangsrettigheder	**F&P**	**Brugere af Autotaks-systemet**
Medarbejdere hos brugere af F&P		x
Regelmæssig gennemgang af adgangsrettigheder	**F&P**	**Brugere af Autotaks-systemet**
Medarbejdere hos F&P	x [1]	

[1] De applikationsspecifikke kontroller med adgangsrettigheder og funktionsadskillelse i Autotaks-systemet indgår ikke i denne ISAE 3000 om generelle it-kontroller.

Beredskab	F&P	Brugere af Autotaks-systemet
Iværksættelse af beredskabsplaner ved større hændelser og information om hændelsen til brugerne	x	
Iværksættelse af brugernes egne beredskabsplaner baseret på information fra F&P om hændelserne		x
Netværk	**F&P**	**Brugere af Autotaks-systemet**
Sikkerheden i management-netværk hos Sentia	x	
Sikkerheden i netværksforbindelser mellem Sentia og brugerne		x

2 Udtalelse fra ledelsen

Medfølgende beskrivelse er udarbejdet til brug for de dataansvarlige, der har anvendt F&P Brancheløsningers (F&P) Autotaks-system, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som underleverandører og 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 afsnit 1 medtager de relevante kontrolmål og underliggende kontrolaktiviteter hos Sentia.

F&P anvender Microsoft Azure til arkivløsning til billeder. Beskrivelsen i afsnit 1 medtager kun kontrolmål og kontrolaktiviteter hos F&P og medtager således ikke kontrolmål og underliggende kontrolaktiviteter hos Microsoft Azure. Visse kontrolmål, der er specificeret i beskrivelsen, 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 underleverandører.

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

F&P bekræfter, at:

(a) den medfølgende beskrivelse i afsnit 1 giver en retvisende beskrivelse af F&P's Autotaks-system, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen i hele perioden fra 1. januar – 31. december 2022. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

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

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

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

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

    iv. De processer, der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt

    v. De processer, der ved ophør af databehandling sikrer, at der efter den dataansvarliges valg sker sletning eller tilbagelevering af alle personoplysninger til den dataansvarlige, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne

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

    vii. De processer, der sikrer passende tekniske og organisatoriske sikringsforanstaltninger for behandlingen af personoplysninger under hensyntagen til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet

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

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

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 ved databehandlerens Autotaks-system til behandling af personoplysninger foretaget i perioden fra 1. januar – 31. december 2022.

(iii) ikke udelader eller forvansker oplysninger, der er relevante for omfanget af det beskrevne system under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af brugere af Autotaks-systemet og deres revisorer og derfor ikke kan omfatte ethvert aspekt ved kontrollerne, som den enkelte bruger af Autotaks-systemet måtte anse for vigtigt efter deres særlige forhold.

(b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt designet og operationelt effektive i hele perioden fra 1. januar – 31. december 2022, hvis relevante kontroller hos underleverandører var operationelt effektive, og brugere af Autotaks-systemet har udført de komplementerende kontroller, som forudsættes i designet af F&P's kontroller i hele perioden fra 1. januar – 31. december 2022. Kriterierne anvendt for at give denne udtalelse var, at:

(i) de risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret,

(ii) de identificerede kontroller ville, hvis anvendt som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål, og

(iii) kontrollerne var anvendt konsistent som designet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. januar – 31. december 2022.

(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 24. februar 2023

Thomas Brenøe
Direktør

Julie Greve Nonboe
DPO

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 afsnit 1 af udvalgte GDPR-relaterede kontroller i relation til Autotaks-systemet, i henhold til databehandleraftale med de dataansvarlige, i hele perioden fra 1. januar – 31. december 2022 (beskrivelsen) og om designet og den operationelle effektivitet af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

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

F&P anvender Microsoft Azure til arkivløsning til billeder. Beskrivelsen i afsnit 1 medtager kun kontrolmål og relaterede kontroller hos F&P og medtager således ikke kontrolmål og relaterede kontroller hos Microsoft Azure. Visse kontrolmål, der er specificeret i beskrivelsen, kan kun nås, hvis underleverandørens 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, 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 afsnit 2, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter; for at anføre kontrolmålene, identifikation af de risici, der påvirker opnåelsen af kontrolmålene; udvælgelsen af de kriterier, der er præsenteret i ledelsens udtalelse, samt for at designe, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Vores uafhængighed og kvalitetsstyring

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

Vores ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om F&P's beskrivelse samt om design og operationel 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 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 operationel 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 afsnit 2.

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

Begrænsninger i kontroller hos en dataansvarlig

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

(a) beskrivelsen af de udvalgte GDPR-relaterede kontroller hos F&P med relevans for Autotaks, således som de var designet og implementeret i hele perioden 1. januar – 31. december 2022, i alle væsentlige henseender er retvisende,

(b) kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt designet i hele perioden fra 1. januar – 31. december 2022, hvis kontroller hos underleverandører var hensigtsmæssigt designet, og hvis dataansvarlige har designet og implementeret de komplementerende kontroller, der forudsættes i designet af F&P's kontroller i hele perioden fra 1. januar – 31. december 2022, og

(c) de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har været operationelt effektive i hele perioden fra 1. januar – 31. december 2022, hvis kontroller hos underleverandører var operationelt effektive, og hvis de komplementerende kontroller hos de dataansvarlige, der forudsættes i designet af F&P's kontroller, har været operationelt effektive i hele perioden fra 1. januar – 31. december 2022.

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 24. februar 2023
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 2022.

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 2022.
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 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.	Ingen 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 ikke har været handlet i strid med databeskyttelsesforordningen i erklæringsperioden, hvorfor effektiviteten ikke kan testes. 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. 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 antivirus-systemer. Observeret, at det ikke er muligt for brugeren at ændre indstillinger og derved stoppe de implementerede kontroller mod malware.	Ingen afvigelser konstateret.
B.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.	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 beskyttelse af kundenetværk. Inspiceret netværkstegning for sikkerhed i netværket samt opdeling af brugere og informationssystemer.	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.	**Sentia** Inspiceret Sentias wiki site for procedure vedrørende kapacitetsstyring. Inspiceret, at der er etableret systemovervågning med alarmering og rapportering af kapacitetsudnyttelse.	Ingen afvigelser konstateret.
B.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. 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. Stikprøvevist inspiceret, at der er opsat hændelseslogning på servere. Stikprøvevist inspiceret, at der er opsat logning af aktiviteter udført af systemadministratorer m.v. på servere.	Ingen 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.	Vi har konstateret, at der ikke er udført en penetrationstest i erklæringsperioden, men at denne efterfølgende er udført i januar 2023. Ingen yderligere 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. Inspiceret, at Sentias wiki site indeholder procedure for ændringshåndtering.	Ingen afvigelser konstateret.

Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
		Stikprøvevist 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. Stikprøvevist 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 - M.m.	**F&P** Forespurgt, hvordan der foretages efterprøvning af medarbejdere i forbindelse med ansættelse. Stikprøvevist 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 liste af til- og fratrådte i 2022. Inspiceret, at standardkontraktformularen indeholder et punkt vedrørende fortrolighedsaftale og tavshedspligt. Stikprøvevist inspiceret, at nyansatte medarbejdere har underskrevet en ansættelseskontrakt. Inspiceret, at informationssikkerhedspolitikken er tilgængelig for medarbejdere.	Ingen afvigelser konstateret.
C.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
		Stikprøvevist 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 i 2022. Stikprøvevist 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.	Ingen 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.	Ingen 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. Stikprøvevist inspiceret, at underdatabehandleraftaler indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Vi har konstateret, at 1 ud af 2 underdatabehandlere ikke er pålagt de samme databeskyttelsesforpligtelser som F&P. 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. 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.	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.		

Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
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. Forespurgt, om der sker overførsler til tredjelande.	Ingen afvigelser konstateret.
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.	F&P har oplyst, at der ikke har været anmodninger om bistand i erklæringsperioden. 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 i 2022. Stikprøvevist inspiceret, at der er afholdt awareness-træning for nyansatte som en del af deres onboarding.	Ingen afvigelser konstateret.

Pkt.	Kontrolmål og tilknyttede kontroller	Udførte tests	Resultater af tests
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	**F&P** Inspiceret beredskabsplanen for håndtering af brud på persondatasikkerheden. Forespurgt, om der er konstateret nogen brud på persondatasikkerheden i erklæringsperioden. Inspiceret liste af incidents.	F&P har oplyst, at der ikke har været brud på persondatasikkerheden i erklæringsperioden, hvorfor effektiviteten ikke kan testes. 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.	Ingen afvigelser konstateret.

PENNEO

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
På vegne af: Forsikring og Pension
Serienummer: d811ad1d-89fe-4adb-805c-98b50180b8ba
IP: 188.244.xxx.xxx
2023-02-24 15:34:11 UTC
MitID

Julie Greve Nonboe
DPO
På vegne af: Forsikring og Pension
Serienummer: 46885a8b-a429-471e-9b9d-737499063a69
IP: 188.244.xxx.xxx
2023-02-26 13:02:51 UTC
MitID

Jesper Due Sørensen
Partner
På vegne af: EY Godkendt Revisionspartnerselskab
Serienummer: c706566b-5a2d-44b8-8f41-5133e988cd9f
IP: 80.208.xxx.xxx
2023-02-26 18:55:22 UTC
MitID

Nils Bonde Christiansen
Statsautoriseret revisor
På vegne af: EY Godkendt Revisionspartnerselskab
Serienummer: PID:9208-2002-2-243192639174
IP: 145.62.xxx.xxx
2023-02-27 07:17:56 UTC
NEM ID