

F&P Brancheløsninger

Uafhængig revisors ISAE 3000-
erklæring omhandlende udvalgte GDPR-
kontroller i perioden 1. januar - 31.
december 2024 relateret til Autotaks-
systemet



Indhold

1	Udtalelse fra ledelsen	2
2	Den uafhængige revisors erklæring	4
3	Beskrivelse af Autotaks-systemet i relation til behandling af persondata	7
3.1	Systembeskrivelse og dataflow	7
3.2	Behandlingen af persondata og grundlaget herfor	8
3.3	Revision og kontrol af Autotaks og eventuelle underdatabehandlere	8
3.4	Risikovurdering	8
3.5	Kontrolforanstaltninger	9
3.6	Komplementerende kontroller hos de dataansvarlige	11
4	Tests udført af EY	13
4.1	Formål og omfang	13
4.2	Udførte tests	13
4.3	Kontrolmål, kontrolaktivitet, test og resultat heraf	14

1 Udtalelse fra ledelsen

F&P Brancheløsninger 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 Brancheløsninger anvender Sentia til drift af Autotaks-systemet. Beskrivelsen i sektion 3 medtager de relevante kontrolmål og underliggende kontrolaktiviteter hos Sentia.

Udover Sentia anvender F&P Brancheløsninger en række andre underdatabehandlere som er adresseret i sektion 3. Beskrivelsen i sektion 3 medtager kun kontrolmål og kontrolaktiviteter hos F&P Brancheløsninger og Sentia og medtager således ikke kontrolmål og underliggende kontrolaktiviteter hos andre underdatabehandlere. Visse kontrolmål kan kun nås, hvis underleverandørens kontroller, der forudsættes i designet af vores kontroller, er passende designet og operationelt effektive. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underleverandøren.

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

F&P Brancheløsninger bekræfter, at:

- (a) den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af de generelle it-kontroller med relevans for Autotaks-systemet, der har været anvendt af brugerne af F&P Brancheløsningers Autotaks-system i perioden fra 1. januar - 31. december 2024. 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, informations-system (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 2024.
 - (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 2024, 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 Brancheløsningers kontroller i perioden fra 1. januar - 31. december 2024. 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 2024.
- (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 F&P Brancheløsninger i henhold til databeskyttelsesforordningen.

Hellerup, den 26. marts 2025

Peter Krejberg Nielsen
Direktør F&P brancheløsninger

Peder Herbo
IT-direktør

2 Den uafhængige revisors erklæring

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med dataansvarlige brugere af Autotaks-systemet.

Til: F&P Brancheløsninger og dataansvarlige

Omfang

Vi har fået som opgave at afgive erklæring om F&P Brancheløsninger's beskrivelse i sektion 3 af Autotaks-systemet i henhold til databehandleraftale med medlemmerne, i hele perioden fra 1. januar - 31. december 2024 (beskrivelsen) og om designet og operationel effektivitet af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

F&P anvender Sentia til drift af Autotaks-systemet. Beskrivelsen i sektion 3 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.

Udover Sentia anvender F&P Brancheløsninger en række andre underdatabehandlere som er adresseret i sektion 3. Beskrivelsen i sektion 3 medtager kun kontrolmål og kontrolaktiviteter hos F&P Brancheløsninger og Sentia og medtager således ikke kontrolmål og underliggende kontrolaktiviteter hos andre underdatabehandlere. Visse kontrolmål, der er specificeret i beskrivelsen, kan kun nås, hvis underdatabehandlers kontroller, der forudsættes i designet af F&P Brancheløsninger og Sentia's kontroller, er passende designet og operationelt effektive sammen med de relaterede kontroller. Vores handlinger har ikke omfattet kontrolaktiviteter udført af andre underdatabehandlere og vi har ikke vurderet egnetheden af design eller den operationelle effektivitet af kontrolaktiviteter hos andre underdatabehandlere.

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

F&P Brancheløsninger og Sentia er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i sektion 1, 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.

Revisors 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, ISQM 1, 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 Brancheløsningers beskrivelse samt om designet 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 at afgive erklæring om beskrivelsen, designet og operationel effektivitet af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af Autotaks-systemet samt for kontrollerens design og operationel effektivitet. De valgte handlinger afhænger af 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, egnetheden af de heri anførte mål samt egnetheden af de kriterier, som F&P Brancheløsninger har specificeret og beskrevet i sektion 1.

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 Brancheløsningers beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved Autotaks-systemet, som hver enkelt dataansvarlig måtte anse for vigtige efter deres særlige forhold. Endvidere vil kontroller hos en databehandler vil som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden. Herudover er fremskrivningen af enhver vurdering af den operationelle effektivitet til fremtidige perioder undergivet risikoen for, at kontroller hos en databehandler, 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 1 er det vores opfattelse, at:

- A) at beskrivelsen af Autotaks-systemet, således som denne var designet og implementeret i hele perioden fra 1. januar - 31. december 2024, i alle væsentlige henseender er retvisende, og
- B) at 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 2024, hvis kontroller hos underleverandører var hensigtsmæssigt designet og hvis dataansvarlige har designet og implementeret de komplementerende kontroller, der forudsættes i designet af F&P Brancheløsningers kontroller i hele perioden fra 1. januar - 31. december 2024, og
- C) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har været operationelt effektive i hele perioden fra 1. januar - 31. december 2024, hvis kontroller hos underleverandører var operationelt effektive og hvis de komplementerende kontroller hos de dataansvarlige, der forudsættes i designet af F&P Brancheløsningers kontroller har været operationelt effektive i hele perioden fra 1. januar - 31. december 2024.

Beskrivelse af test af kontroller

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



Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i sektion 4 er udelukkende tiltænkt dataansvarlige, der har anvendt Autotaks-systemet, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen er overholdt.

København, den 26. marts 2025
EY Godkendt Revisionspartnerselskab
CVR-nr.: 30 70 02 28

Jesper Due Sørensen
Partner

Nils B. Christiansen
statsaut. revisor
mne34106

3 Beskrivelse af Autotaks-systemet i relation til behandling af persondata

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 (herefter Brancheløsninger), som ejer og driver løsningen.

3.1 Systembeskrivelse og data flow

Forsi.dk/Autotaks er det primære værktøj til skadeselskabernes 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/forretningssange 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-plattformen hos Microsoft.

3.2 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, kundennummer, 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 skadesager.

De registrerede er forsikringstagere i de tilsluttede selskaber.

3.3 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 underdatabehandlers 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'/underdatabehandlers fremlæggelse af rapporter, erklæringer eller anden skriftlig dokumentation. Databehandleraftalen fastlægger vilkår for afholdelse af omkostninger i forbindelse med inspektion.

3.4 Risikovurdering

Det er de dataansvarliges ansvar at vurdere 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.

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.

3.5 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.

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 overfor de dataansvarlige, samt kontrol med behandlingen hos underdatabehandleren.

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 instruks er i strid med lovgivningen. Instruks er indeholdt i databehandleraftalen.

Der er for Autotaks indført politikker og procedurer, der understøtter instruks 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 instruks.

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 instruks.

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.

C. Organisatoriske sikkerhedsforanstaltninger (Artikel 25 og 32)

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

Medarbejdere med adgang til Autotaks-systemet er underlagt it-sikkerhedspolitikken og denne er godkendt af bestyrelsen. 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.

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.

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.

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. 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.

Udover Sentia benytter Autotaks følgende godkendte underdatabehandlere:

Navn	Beskrivelse af behandling
Microsoft Danmark Aps	Understøttelse af arkiv i Autotaks-løsningen. Arkiv hostes på Microsoft Azure Platformen, som er en cloud-tjeneste. Behandlingen af data består udelukkende i opbevaring. Microsoft har ingen mulighed for at tilgå data og Jf. databehandleraftale med Microsoft sker der ingen 3. landsoverførelse af data og data vil altid være placeret i Europa.
Adaptive Recognition Nordic A/S	Systemet analyserer et billede af en nummerplade for at finde registreringsnummeret, som bruges ved oprettelse af en ny rapport i Autotaks.
Softo - Convertio	Softo - Convertio leverer en løsning, der kan konvertere videoer. Der er tale om videoer, hvor der fremgår registreringsnumre.

Solera Technology Centre GmbH c/o Audatex GmbH	Der sendes stelnummer til Solera for at hente fabriksoplysninger om køretøj der bruges ved beregning af skade. Derudover afsendes rapportnummer, reparationsoplysninger, billeder og video af skadede dele på køretøj.
AutoIT	Brugere af Autotaks sender registreringsnummer via et API hos AutoIT for at hente stelnummer samt oplysninger om køretøjet i Motorregistret.

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-plattformen, 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 tredjelandsoverførsler. Her er der taget udgangspunkt i at Autotaks' brug af funktionerne på Azure-plattformen er begrænset og derfor 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 derfor 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 adgangsbeskrænkninger til data i systemet, herunder ved kryptering, der administreres af Sentia.

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 forpligtet 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 henvende sig 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.

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.

3.6 Komplementerende kontroller hos de dataansvarlige

Kontroller hos Brancheløsninger er udformet således, at nogle af kontrollerne nævnt i denne erklæring skal suppleres med kontroller hos medlemmerne.

Foruden Brancheløsningers og Sentias kontrolforanstaltninger, er det medlemmernes ansvar at:

- sikre kontroller for oprettelse, ændring og sletning af medarbejdere hos medlemmerne, herunder at der foretages regelmæssig gennemgang af adgangsrettigheder af de respektive medarbejdere.
- at der er implementeret en tilstrækkelig passwordpolitik og konfiguration i forhold til de medarbejdere hos medlemmerne, som logger på Autotaks-systemet.
- iværksættelse af medlemmernes egne beredskabsplaner baseret på information fra Brancheløsninger om hændelserne.
- sikre, at givne instrukser er lovlige, set i forhold til den til enhver tid gældende persondatarelige lovgivning
- sikre, at personoplysninger i Autotaks-systemet holdes ajourførte
- vurdere 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.



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 sektion 4. Eventuelle andre kontrolmål, tilknyttede kontroller og kontroller hos Brancheløsninger og Sentia, der anvender løsningen, beskrevet i sektion 3, er ikke omfattet af vores test.

Test af design 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 2024.

For den del af it-miljøerne, der i perioden 1. januar - 31. december 2024 har været outsourcet til Sentia, har vi foretaget test af design, implementering og operationel effektivitet af kontrollerne hos Sentia.

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 og effektive i hele perioden fra 1. januar - 31. december 2024.
Forespørgsler	Forespørgsel af passende personale hos Brancheløsninger. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Vi har observeret kontrollens udførelse.

4.3 Kontrolmål, kontrolaktivitet, test og resultat heraf

Kontrolmål A			
Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgående databehandlersaftale.			
Nr.	Brancheløsninger's kontrolaktivitet	EY's udførte test	Resultat af EY's test
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.	Brancheløsninger: Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Inspiceret, at procedurer er opdateret.	Ingen afvigelser konstateret.
A.2	Brancheløsninger udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Brancheløsninger: Inspiceret, at ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks.	Ingen afvigelser konstateret.
A.3	Brancheløsninger 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.	Brancheløsninger: Inspiceret, at der er procedurer for underretning til den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. Forespurgt, om der har været tilfælde af behandling i strid med databeskyttelsesforordningen.	Brancheløsninger har oplyst, at der har ikke været handlet i strid med databeskyttelsesforordningen i erklæringsperioden. Ingen afvigelser konstateret.

Kontrolmål B

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	Brancheløsninger's kontrolaktivitet	EY's udførte test	Resultat af EY's test
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 foretages løbende - og mindst en gang årligt - vurdering af, om procedurerne skal opdateres.	Brancheløsninger: Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger. Inspiceret, at procedurer er opdateret. Stikprøvevist inspiceret, at der er etableret de sikringsforanstaltninger, der fremgår af databehandleraftalerne.	Ingen afvigelser konstateret.
B.2	Brancheløsninger 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 dataansvarlige aftalte sikringsforanstaltninger.	Brancheløsninger: Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at Brancheløsninger 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 Brancheløsninger har identificeret tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen.	Ingen afvigelser konstateret.
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Sentia: Inspiceret proceduren for sikring mod malware. Stikprøvevist inspiceret, at servere har opdateret antivirus program.	Ingen afvigelser konstateret.

Kontrolmål B

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	Brancheløsninger's kontrolaktivitet	EY's udførte test	Resultat af EY's test
		Inspiceret at antivirus program ikke kan slås fra. Stikprøvevist inspiceret, at klienter er registreret i Intune og dermed overvåget for antimalware.	
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Sentia: Inspiceret, at sikkerhedsmekanismer, serviceniveauer og styringskrav til netværkstjenester indgår i kontrakten.	Ingen afvigelser konstateret.
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til Autotaks.	Sentia: Forespurgt om procedure for netværksstyring. Observeret, at der anvendes MPLS og VLAN til beskyttelse af kundenetværk. Inspiceret, at der anvendes MPLS og VLAN til opdeling af kundenetværk. Inspiceret netværksdiagram samt opdeling af brugere og informationssystemer. Inspiceret oversigt over brugere med adgang til netværket.	Ingen afvigelser konstateret.
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Brancheløsninger: Inspiceret, at informationssikkerhedspolitikken indeholder styring af privilegerede adgangsrettigheder. Inspiceret listen over brugere med adgangsrettigheder og fået bekræftet, at disse har et arbejdsbetinget behov for adgangen.	Ingen afvigelser konstateret.



Kontrolmål B

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	Brancheløsninger's kontrolaktivitet	EY's udførte test	Resultat af EY's test
		Sentia: Forespurgt om proceduren for styring af privilegerede adgangsrettigheder. Inspiceret listen over brugere med adgange samt forespurgt, hvorvidt disse brugere har et arbejdsbetinget behov for adgangen.	
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	Sentia: Forespurgt om procedure for hændelseslogging. Stikprøvevis inspiceret, at der er opsat hændelseslogging på servere. Stikprøvevis inspiceret, at der er opsat logging af aktiviteter udført af systemadministratorer m.v. på servere. Stikprøvevist inspiceret, at klienter er registreret i Intune og dermed overvåget for antimalware. Inspiceret dokumentation for at der foretages månedlige sårbarhedsscanninger.	Ingen afvigelser konstateret.
B.8	Der er udarbejdet og implementeret en politik for anvendelse af kryptografi til beskyttelse af information.	Brancheløsninger: Inspiceret proceduren for kryptografi. Inspiceret dokumentation for opsætningen af offentlig web trafik er beskyttet med SSL, herunder at der foreligger et validt certifikat.	Ingen afvigelser konstateret.

Kontrolmål B

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	Brancheløsninger's kontrolaktivitet	EY's udførte test	Resultat af EY's test
B.9	Hændelseslogging til registrering af brugeraktivitet, undtagelser, fejl og informationssikkerhedshændelser udføres og opbevares. Aktiviteter udført af systemadministrator og systemoperatør logges, og loggene beskyttes.	Sentia: Forespurgt om proceduren for beskyttelse af logging. Stikprøvevis inspiceret, at der er opsat hændelseslogging på servere. Inspiceret, om opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod manipulation og sletning.	Logs opbevares ikke på separate servere, der er utilgængelige for personer, hvis handlinger bliver logget. Loggen kan dermed manipuleres eller slettes af alle administratorer. Ingen yderligere afvigelser konstateret.
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	Sentia: Forespurgt om der foreligger formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder gennemførsel af sårbarhedsscanninger og penetrationstests. Inspiceret dokumentation for at der foretages månedlige sårbarhedsscanninger.	Sentia har oplyst, at de ikke udfører penetrationstest i henhold til kontrakten med Brancheløsninger. 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.	Brancheløsninger og Sentia: Inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches. Inspiceret ved udtræk af tekniske sikkerhedsparametre og -opsætninger, at systemer, databaser og netværk er opdateret med aftalte ændringer	Ingen afvigelser konstateret.

Kontrolmål B

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	Brancheløsninger's kontrolaktivitet	EY's udførte test	Resultat af EY's test
		og relevante opdateringer, patches og sikkerhedspatches.	
B.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugerens adgang revideres regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Brancheløsninger og Sentia: Inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Stikprøvevist inspiceret på medarbejderes adgang til Autotaks, at de tildelte brugeradgange er godkendt, og at der er et arbejdsbetinget behov. Stikprøvevist inspiceret på fratrådte medarbejdere, at disses adgang til Autotaks er rettidigt deaktiveret eller nedlagt. Inspiceret, at der foreligger dokumentation for regelmæssig - mindst en gang årligt - vurdering og godkendelse af tildelte brugeradgange.	Ingen afvigelser konstateret.

Kontrolmål C

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	Brancheløsninger's kontrolaktivitet	EY's udførte test	Resultat af EY's test
C.1	Brancheløsninger's ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder Brancheløsninger's medarbejdere. It-sikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende - og mindst en gang årligt - vurdering af, om it-sikkerhedspolitikken skal opdateres.	Brancheløsninger: 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.
C.2	Brancheløsninger's ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Brancheløsninger: Inspiceret dokumentation for ledelsens vurdering af, at Informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Stikprøvevist inspiceret, om kravene i databehandleraftalerne er dækket af informationssikkerhedspolitikens 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.	Brancheløsninger: Inspiceret informationssikkerhedspolitikken for screeningsproces for personer, der vil få adgang til it-kritiske data. Forespurgt om der ansat medarbejdere i erklæringsperioden, som har fået adgang til Autotaks.	Brancheløsninger har oplyst, at der ikke er ansat nogle medarbejdere i erklæringsperioden, som har fået adgang til Autotaks. Ingen afvigelser konstateret.



Kontrolmål C

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	Brancheløsninger's kontrolaktivitet	EY's udførte test	Resultat af EY's test
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.	Brancheløsninger: Inspiceret procedure for ansættelser og de sikkerhedsopgaver, der skal udføres i den forbindelse. Inspiceret, at standardkontraktformularen indeholder et punkt vedrørende ansvar for informationssikkerhed. Forespurgt om der ansat medarbejdere i erklæringsperioden, som har fået adgang til Autotaks. Sentia: Forespurgt om procedure for udarbejdelse af kontrakter til medarbejdere og kontrahenter. Inspiceret, at en standardansættelseskontrakt indeholder pågældendes og virksomhedens ansvar for informationssikkerhed. Inspiceret, at medarbejdere under alle tidspunkter er underlagt informationssikkerhedspolitikken, jf. personalehåndbogen. Stikprøvevis inspiceret, at nyansatte får tilsendt relevante procedurer og politikker.	Brancheløsninger: Brancheløsninger har oplyst, at der ikke er ansat nogle medarbejdere i erklæringsperioden, som har fået adgang til Autotaks. Ingen afvigelser konstateret.



Kontrolmål C

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	Brancheløsninger's kontrolaktivitet	EY's udførte test	Resultat af EY's test
C.5	Ved fratrædelse er der implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Brancheløsninger: Inspiceret informationssikkerhedspolitikken for fratrædelsespolitik. Stikprøvevist inspiceret, at fratrådte medarbejdere i erklæringsperioden, har fået frataget sine adgange til Autotaks, herunder at aktiver er inddraget. Sentia: Forespurgt om proceduren for inddragelse og justering af adgangsrettigheder. Stikprøvevis inspiceret, at fratrådte medarbejderes adgange lukkes ved fratrædelse.	Ingen afvigelser konstateret.
C.6	Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Brancheløsninger: Inspiceret, at Brancheløsninger udbyder awareness-træning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger. Inspiceret dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awareness-træning.	Ingen afvigelser konstateret.

Kontrolmål D

Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres såfremt der indgås aftale herom med den dataansvarlige.

Nr.	Brancheløsninger's kontrolaktivitet	EY's udførte test	Resultat af EY's test
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 foretages løbende - og mindst en gang årligt - vurdering af, om procedurerne skal opdateres.	Brancheløsninger: 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 Brancheløsningers opbevaringsperioder og sletterutiner for Autotaks: ▶ Data slettes, såfremt en kontrakt ophører. ▶ Data slettes automatisk efter gældende regler i databehandleraftalen.	Brancheløsninger: Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlers opbevaringsperioder og sletterutiner. Stikprøvevist inspiceret, at der er dokumentation for, at personoplysninger er slettet i overensstemmelse med de aftalte sletterutiner.	Ingen afvigelser konstateret.
D.3	Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: ▶ Tilbageleveret til den dataansvarlige og/eller ▶ Slettet, hvor det ikke er i modstrid med anden lovgivning.	Brancheløsninger: Inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger. Stikprøvevist inspiceret ved ophørte databehandlinger i erklæringsperioden, at der er dokumentation for, at den aftalte sletning af data er udført.	Ingen afvigelser konstateret.

Kontrolmål E

Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.

Nr.	Brancheløsninger's kontrolaktivitet	EY's udførte test	Resultat af EY's test
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 foretages løbende - og mindst en gang årligt - vurdering af, om procedurerne skal opdateres.	Brancheløsninger: 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	Brancheløsninger's databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller lande områder.	Brancheløsninger: Forespurgt om Brancheløsninger har en samlet oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller lande områder. Stikprøvevist inspiceret, om der er dokumentation for, at opbevaring af personoplysninger, alene foretages på de lokaliteter, der fremgår af databehandleraftalen.	Ingen afvigelser konstateret.

Kontrolmål F

Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.

Nr.	Brancheløsninger's kontrolaktivitet	EY's udførte test	Resultat af EY's test
F.1	Der foreligger skriftlige procedurer, som indeholder krav til Brancheløsninger 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.	Brancheløsninger: 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	Brancheløsninger anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Brancheløsninger: Inspiceret, om Brancheløsninger har en samlet og opdateret oversigt over anvendte underdatabehandlere. Stikprøvevist inspiceret, at der er dokumentation for, at underdatabehandlere fra Brancheløsningers 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.	Brancheløsninger: Inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Inspiceret dokumentation for, at de dataansvarlige er underrettet ved ændring i anvendelse af underdatabehandlerne i erklæringsperioden.	Ingen afvigelser konstateret.

Kontrolmål F

Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.

Nr.	Brancheløsninger's kontrolaktivitet	EY's udførte test	Resultat af EY's test
F.4	Brancheløsninger har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Brancheløsninger: Inspiceret, at Brancheløsninger har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Ingen afvigelser konstateret.
F.5	Brancheløsninger har en oversigt over godkendte underdatabehandlere med angivelse af: ▶ Navn ▶ CVR-nr. ▶ Adresse ▶ Beskrivelse af behandlingen	Brancheløsninger: Inspiceret, at Brancheløsninger 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	Brancheløsninger foretager på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandlere.	Brancheløsninger: Forespurgt dokumentation for, at der er foretaget en risikovurdering af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne. Forespurgt dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger og behandlingssikkerheden hos de anvendte underdatabehandlere.	Brancheløsninger har ikke foretaget en risikovurdering af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne, samt foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger og behandlingssikkerheden hos 4 ud af 5 af de anvendte underdatabehandlere. Ingen yderligere afvigelser konstateret.



Kontrolmål G

Der efterleves 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.

Nr.	Brancheløsninger's kontrolaktivitet	EY's udførte test	Resultat af EY's test
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at Brancheløsninger alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Der foretages løbende - og mindst en gang årligt - vurdering af, om procedurerne skal opdateres.	Brancheløsninger: Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at personoplysninger alene overføres til tredjelande eller internationale organisationer i henhold til aftale med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
G.2	Brancheløsninger må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	Brancheløsninger: Inspiceret, at Brancheløsninger har en oversigt over overførsler af personoplysninger til tredjelande eller internationale organisationer. Inspiceret at lokationen for Microsofts behandling af data er Amsterdam.	Ingen afvigelser konstateret.
G.3	Brancheløsninger har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	Brancheløsninger: Inspiceret at der er dokumentation at Brancheløsninger har vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag i forbindelse med overførsel af personoplysninger til tredjelande.	Ingen afvigelser konstateret.

Kontrolmål H

Der efterleves 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.

Nr.	Brancheløsninger's kontrolaktivitet	EY's udførte test	Resultat af EY's test
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at Brancheløsninger skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende - og mindst en gang årligt - vurdering af, om procedurerne skal opdateres.	Brancheløsninger: Inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
H.2	Brancheløsninger har etableret procedurer, som i det omfang, dette 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.	Brancheløsninger: 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. Forespurgt om Brancheløsninger har ydet bistand til den dataansvarlige i erklæringsperioden i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	Brancheløsninger har oplyst, at de ikke har modtaget anmodninger om bistand i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede i erklæringsperioden. Ingen afvigelser konstateret.

Kontrolmål I			
Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandlaftale.			
Nr.	Brancheløsninger's kontrolaktivitet	EY's udførte test	Resultat af EY's test
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende - og mindst en gang årligt - vurdering af, om procedurerne skal opdateres.	Brancheløsninger: Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Inspiceret, at proceduren er opdateret.	Ingen afvigelser konstateret.
I.2	Brancheløsninger har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: ▶ Awareness hos medarbejdere	Brancheløsninger: Forespurgt, hvordan der gennemføres awareness-træning i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger. Inspiceret dokumentation for afholdt awareness-træning. Stikprøvevis inspiceret, at der er afholdt awareness-træning for nyansatte som en del af deres onboarding.	Ingen afvigelser konstateret.
I.3	Brancheløsninger har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødigt forsinkelse efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos Brancheløsninger eller en underdatabehandler.	Brancheløsninger: Forespurgt Brancheløsninger og deres underdatabehandlere, om de har konstateret nogen brud på persondatasikkerheden i erklæringsperioden. Inspiceret liste af sikkerhedshændelser og potentielle persondatabrud.	Brancheløsninger har oplyst, at der ikke er registreret nogen brud på persondatasikkerheden i erklæringsperioden som relaterer sig til Autotaks. Ingen afvigelser konstateret.

Kontrolmål I

Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.

Nr.	Brancheløsninger's kontrolaktivitet	EY's udførte test	Resultat af EY's test
I.4	Brancheløsninger 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.	Brancheløsninger: Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden. Forespurgt om Brancheløsninger har konstateret nogen brud på persondatasikkerheden i erklæringsperioden.	Brancheløsninger har oplyst, at der ikke er registreret nogen brud på persondatasikkerheden i erklæringsperioden, hvorpå man er blevet bedt om at assistere i forhold til anmeldelse til Datatilsynet. Ingen afvigelser konstateret.

PENNEO

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

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

Peter Krejberg Nielsen

Direktør F&P brancheløsninger

På vegne af: F&P Brancheløsninger

Serienummer: e4e309df-7bc5-4802-9062-01f503490bd8

IP: 188.244.xxx.xxx

2025-03-26 13:19:35 UTC



Peder Herbo

F&P Brancheløsninger P/S CVR: 42855588

IT-direktør

På vegne af: F&P (Forsikring og Pension)

Serienummer: a7ebdab7-0425-4b51-92da-a0f81b43d65c

IP: 188.244.xxx.xxx

2025-03-26 14:19:05 UTC



Nils Bonde Christiansen

EY Godkendt Revisionspartnerselskab CVR: 30700228

Statsaut. revisor

På vegne af: EY Godkendt Revisionspartnerselskab

Serienummer: a4c7bea3-5a9f-4f35-bb2c-9ca1124e41f1

IP: 147.161.xxx.xxx

2025-03-26 14:33:50 UTC



Jesper Due Sørensen

EY Godkendt Revisionspartnerselskab CVR: 30700228

Partner

På vegne af: EY Godkendt Revisionspartnerselskab

Serienummer: a6d834d7-442d-428e-ade9-c250dca23ab3

IP: 37.96.xxx.xxx

2025-03-26 14:37:12 UTC



Dette dokument er underskrevet digitalt via **Penneo.com**. De underskrevne data er valideret vha. den matematiske hashværdi af det originale dokument. Alle kryptografiske beviser er indlejret i denne PDF for validering i fremtiden.

Dette dokument er forseglet med et kvalificeret elektronisk segl med brug af certifikat og tidsstempel fra en kvalificeret tillidstjenesteudbyder.

Sådan kan du verificere, at dokumentet er originalt

Når du åbner dokumentet i Adobe Reader, kan du se, at det er certificeret af **Penneo A/S**. Dette beviser, at indholdet af dokumentet er uændret siden underskriftstidspunktet. Bevis for de individuelle underskrivers digitale underskrifter er vedhæftet dokumentet.

Du kan verificere de kryptografiske beviser vha. Penneos validator, <https://penneo.com/validator>, eller andre valideringstjenester for digitale underskrifter