PeopleTools ApS

Uafhængig ISAE 3000-erklæring om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med PeopleTools ApS' kunder

Pr. 4. april 2019

Indholdsfortegnelse

1. Ledelsens udtalelse

PeopleTools ApS behandler personoplysninger på vegne af dennes kunder i henhold til indgået databehandleraftale.

Medfølgende beskrivelse er udarbejdet til brug for virksomheder, der benytter PeopleTools ApS' ydelser, og som har en tilstrækkelig forståelse til at vurdere 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. PeopleTools ApS bekræfter, at:

a) Den medfølgende beskrivelse, giver en retvisende beskrivelse af den behandling af personoplysninger der foretages ved benyttelse af PeopleTools ApS' ydelser, pr. 26 marts 2019. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan beskrivelsen af behandling af personoplysninger var udformet og implementeret, herunder redegør for:

   - De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger
   - 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
   - De processer, der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige
   - 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
   - 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
   - De processer, der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underrettelse til de registrerede
   - 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

   (ii) Indeholder relevante oplysninger om ændringer ved databehandlerens behandling af personoplysninger foretaget i op til 26. marts 2019.

   (iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne behandling af personoplysninger under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og derfor ikke kan omfatte

ethvert aspekt ved behandlingen, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

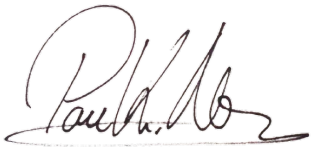
b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet pr. 26 marts 2019. Kriterierne anvendt for at give denne udtalelse var, at:

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

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

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.

D. 4. april 2019



Poul Kristian Mouritsen
Partner

PeopleTools ApS
Vestergade 14
8660 Skanderborg
CVR nr.: 31871689

2. Uafhængig erklæring

Uafhængig ISAE 3000-erklæring om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med dennes kunder.

Til: PeopleTools ApS og dennes kunder

Omfang

Vi har fået som opgave at afgive erklæring om PeopleTools ApS' beskrivelse på af ydelsen i henhold til indgående databehandleraftaler med kunder, pr. 26. marts 2019 og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

PeopleTools ApS' ansvar

PeopleTools ApS er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse på side [aa], herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for at udforme, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

PDS's ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om PeopleTools ApS' beskrivelse samt om udformningen af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet.

En erklæringsopgave om at afgive erklæring om beskrivelsen og udformningen af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af sin behandling af personoplysninger, samt for kontrollernes udformning. De valgte handlinger afhænger af PDS' vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet. Vores handlinger har omfattet test af funktionaliteten 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 databehandleren har specificeret og beskrevet.

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

PeopleTools' beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved ydelsen, som hver enkelt dataansvarlig måtte anse for vigtige efter deres særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden. Herudover er fremskrivningen af enhver vurdering af funktionaliteten 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 ledelsens udtalelse. Det er vores opfattelse,

(a) at beskrivelsen af behandling af personoplysninger, således som denne var udformet og implementeret pr. 26. marts 2019, 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 udformet pr. 26. marts 2019.

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 dataansvarlige, der har anvendt PeopleTools' ydelser, 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.

D. 4. april 2019

_____

Mette Blanner
Partner, DPO, CISA

PersondataSupport ApS
Sverigesvej 10, Horsens

3. Beskrivelse af behandling

Den Dataansvarlige anvender systemet People Tools, PI Software og E-stimate software, som ejes og administreres af Databehandleren eller Underdatabehandlere, til at indsamle og behandle oplysninger om ansøgere og medarbejdere med henblik på udarbejdelse af personprofiler, kognitive tests og HR-målinger.

Karakteren af behandlingen

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om udarbejdelse af personprofiler, kognitive tests og HR-målinger.

Personoplysninger

Almindelige personoplysninger, herunder: Navn, E-mailadresse, uddannelse, erhverv og besvarelsen af spørgsmål i profilerne.

Kategorier af registrerede personer omfattet af databehandleraftalen:

- medarbejdere og ledere hos Dataansvarlig
- kandidater til ledige stillinger hos Dataansvarlig

Praktiske tiltag

Der er implementeret passende tekniske og organisatoriske foranstaltninger til at sikker behandling af personoplysninger. Disse foranstaltninger er implementeret på baggrund af anerkendte branchestandarder herunder IS027001 og retningslinjer fra databeskyttelsesforordningen og tilsynsmyndigheden. Alle medarbejdere er gjort bekendt med de retningslinjer og trænes løbende heri. Diverse underleverandører og samarbejdspartnere er ligeledes gjort bekendt med retningslinjerne. Der bliver løbende ført kontrol med overholdelse af retningslinjerne gennem implementering og anvendelse af GDPR-portalens kontrolmodul.

Risikovurdering

For hver behandlingsaktivitet er der foretaget en vurdering af sandsynligheden for at der sker tab af fortrolighed (uvedkommende får adgang til oplysningerne), integritet (oplysningerne er ikke korrekt) eller tilgængelighed (oplysninger mistes). I denne vurdering er der taget udgangspunkt i trusler og i de foranstaltninger der er implementeret for at beskytte oplysningernes fortrolighed, integritet og tilgængelighed.

Dernæst er konsekvensen for de registrerede blevet vurderet. Denne vurdering tager udgangspunkt i hvad konsekvensen for den registrerede er hvis der sker tab af fortrolige, integritet eller tilgængeligheden af oplysningerne. Vurdering er baseret på om oplysningerne er almindelige, fortrolige eller følsomme og de eventuelle indirekte konsekvenser med hensyn til typen af datasættet. Desto større sandsynlighed for at oplysningernes tab af fortrolighed, integritet eller tilgængelighed kan føre til materiel eller immateriel skade for den registreredes, desto større er konsekvensen.

Baseret på vurderingen af sandsynligheden og konsekvensen ved behandlingsaktiviteten er der udregnet en risiko rating. Hvis denne rating vurderes til høj, bliver der udarbejdet en konsekvensanalyse og en handlingsplan for at sænke risikoen. I de tilfælde hvor dette ikke er muligt udarbejdes en konsekvensanalyse

Kontrolforanstaltninger

For at sikre implementeringen af Databeskyttelsesforordningen anvendes GDPR-portalen. Der er udarbejdet:

- fortegnelse over behandlingsaktiviteter
- liste over dataansvarlige

- risikovurderinger på behandlingsaktiviteter
- interne politikker for beskyttelse af persondata og it-sikkerhed
- awarenes træning af medarbejdere i beskyttelse af persondata og it-sikkerhed
- databrugslog og plan for notifikation ved databrud
- årshjul for periodiske kontroller af organisatoriske og tekniske foranstaltninger til overholdelse af Databeskyttelsesforordningen og god it-sikkerhed.

Der henvises i øvrigt til afsnit 4, hvor de konkrete kontrolaktiviteter er beskrevet.

Komplementerende kontroller hos de dataansvarlige

Følgende er en beskrivelse af de kontroller, som forudsættes implementeret af de dataansvarlige, og som er væsentlige for at opnå de kontrolmål, der er anført i afsnit 4.

Den dataansvarlige har følgende forpligtelser:

- at sikre sig, at personoplysningerne er ajourførte
- at sikre sig, at instruksen er lovlig set i forhold til den til enhver tid gældende persondataretlige regulering
- at instruksen er hensigtsmæssig set i forhold til denne databehandleraftale og hovedydelsen.
- at sikre sig, at den dataansvarliges brugere er ajourførte

4. 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 databehandleraftale.**			
Nr.	*Databehandlerens kontrolaktivitet*	*PDS' udførte test*	*Resultat af PDS' 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 foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	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. Den interne persondatapolitik indeholder procedurer om gennemgang af behandlingsaktiviteter og årlig kontrol er udført i kontrolmodulet. Proceduren er opdateret i marts 2019.
A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Inspiceret, at ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks.	Ingen afvigelser konstateret. Behandlingsaktiviteter er gennemgået og det er påset at oplysninger udelukkende benyttes iht. databehandleraftalen. Ledelsen har gennemført kontrol af behandlingsaktiviteter i marts 2019.

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*PDS' udførte test*	*Resultat af PDS' 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.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger. Inspiceret, at procedurer er opdateret. Inspiceret, at der er etableret de aftalte sikringsforanstaltninger.	Ingen afvigelser konstateret. Det er konstateret at databehandler har implementeret alle sikkerhedsforanstaltninger der er aftalt iht. databehandleraftalen.
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 dataansvarlige aftalte sikringsforanstaltninger.	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 databehandler har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen. Inspiceret, at databehandler har implementeret de sikringsforanstaltninger, der er aftalt med de dataansvarlige.	Ingen afvigelser konstateret. Risikovurdering er sidst foretaget i marts 2019 og disse kontrolleres og revurderes minimum en gang årligt. Det er konstateret at databehandler har implementeret alle sikkerhedsforanstaltninger der er aftalt iht. databehandleraftalen.

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*PDS' udførte test*	*Resultat af PDS' test*
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirus software. Inspiceret, at antivirus software er opdateret.	Ingen afvigelser konstateret. Antivirus software opdateres automatisk med udbyders opdateringer.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall. Inspiceret, at firewall er konfigureret i henhold til intern politik herfor.	Ingen afvigelser konstateret. Eksterne adgange til systemer og databaser er beskyttet af hostingleverandørens firewalls.
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Forespurgt, om interne netværk er segmenteret med henblik på at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Ingen afvigelser konstateret.
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger. Inspiceret, at der foreligger formaliserede procedurer for opfølgning på, at brugeres adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov.	Ingen afvigelser konstateret. Iht. interne politikker er adgangen til oplysninger begrænset til arbejdsmæssigt behov. Der er etableret årlige ledelseskontroller for gennemgang af brugerrettigheder.

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*PDS' udførte test*	*Resultat af PDS' test*
		Inspiceret, at de aftalte tekniske foranstaltninger understøtter opretholdelsen af begrænsningen i brugernes arbejdsbetingede adgang til personoplysninger.	
B.7	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at transmission af følsomme og fortrolige oplysninger over internettet er beskyttet af stærk kryptering baseret på en anerkendt algoritme. Inspiceret, at teknologiske løsninger til kryptering har været tilgængelige og aktiveret i hele erklæringsperioden. Inspiceret, at der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet eller med e-mail.	Ingen afvigelser konstateret. Der anvendes som minimum TLS kryptering af alle transmissioner af personoplysninger.
B.8	Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af personoplysninger til udvikling, test og lignende, der sikrer, at anvendelsen alene sker i pseudonymiseret eller anonymiseret form.	Ingen afvigelser konstateret.

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*PDS' udførte test*	*Resultat af PDS' test*
		Inspiceret ved en stikprøve på XX udviklings- og testdatabaser, at personoplysninger heri er pseudonymiseret eller anonymiseret. Inspiceret ved en stikprøve på XX udviklings- og testdatabaser, hvor personoplysninger ikke er pseudonymiseret eller anonymiseret, at dette er sket efter aftale med den dataansvarlige og på dennes vegne.	
B.9	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Forespurgt, at der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches.	Ingen afvigelser konstateret.
B.10	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.	Inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Inspiceret at medarbejderes adgange til systemer og databaser, at de tildelte brugeradgange er godkendt, og at der er et arbejdsbetinget behov.	Ingen afvigelser konstateret. Der er fortaget gennemgang af brugerrettigheder i marts 2019. Der foreligger en formel procedure for oprettelse af brugere. Alle fratrådte medarbejdere er deaktiveret i systemet.

Kontrolmål B **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*PDS' udførte test*	*Resultat af PDS' test*
		Inspiceret ved at fratrådte medarbejdere, at disses adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt. Inspiceret, at der foreligger dokumentation for regelmæssig - mindst en gang årligt – vurdering og godkendelse af tildelte brugeradgange.	

Kontrolmål C **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*PDS' udførte test*	*Resultat af PDS' test*
C.1	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik. It-sikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år.	Ingen afvigelser konstateret. Politikken er godkendt d. 31. december 2018.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Inspiceret at databehandleraftaler, at kravene i aftalerne er dækket af informationssikkerhedspolitikkens krav til sikringsforanstaltninger og behandlingssikkerheden.	Ingen afvigelser konstateret.
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: • Referencer fra tidligere ansættelser • Straffeattest • Eksamensbeviser	Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. .	Ingen afvigelser konstateret. Senest godkendt marts 2019.

Kontrolmål C **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*PDS' udførte test*	*Resultat af PDS' 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.	Inspiceret at nyansatte medarbejdere i erklæringsperioden, at de pågældende medarbejdere har underskrevet en fortrolighedsaftale. Inspiceret at nyansatte medarbejdere i erklæringsperioden, at de pågældende medarbejdere er blevet introduceret til: • Informationssikkerhedspolitikken • Procedurer vedrørende databehandling, samt anden relevant information	Ingen afvigelser konstateret. Der har ikke været nyansættelser i perioden. Dog har alle nuværende medarbejdere underskrevet en fortrolighedsaftale og blevet gjort bekendt med politikker vedrørende it sikkerhed og behandling af personoplysninger.
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages Inspiceret at fratrådte medarbejdere i erklæringsperioden, at rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget.	Ingen afvigelser konstateret. Der har ikke været nogle fratrædelser. Det er inspiceret at ingen tidligere medarbejdere har aktive brugere på systemet.
C.6	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt.	Ingen afvigelser konstateret. Det er en del af fortrolighedserklæringen at denne også er gældende efter fratrædelse.

Kontrolmål C **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*PDS' udførte test*	*Resultat af PDS' test*
	behandling af personoplysninger, databehandleren udfører for de dataansvarlige.		
C.7	Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Inspiceret, at databehandleren 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. Det er påset at medarbejderne løbende awareness trænes i it-sikkerhed og behandling af personoplysninger.

Kontrolmål D **Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres såfremt der indgås aftale herom med den dataansvarlige.**			
Nr.	*Databehandlerens kontrolaktivitet*	*PDS' udførte test*	*Resultat af PDS' 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.	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. Proceduren er opdateret i marts 2019.
D.2	Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: • Alle persondata slettes automatisk. • Brugere forbliver registreret da certificeringen er personlig og PeopleTools skal kunne konstatere om brugeren er uddannet.	Inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger.	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.	*Databehandlerens kontrolaktivitet*	*PDS' udførte test*	*Resultat af PDS'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.	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. Der foretages én gang årligt gennemgang af behandlingsaktiviteter.
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder. Inspiceret at databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen, herunder opbevaring af personoplysninger, alene foretages på de lokaliteter, der fremgår af databehandleraftalen – eller i øvrigt er godkendt af den dataansvarlige.	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.	*Databehandlerens kontrolaktivitet*	*PDS' udførte test*	*Resultat af PDS' test*
F.1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	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.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere. Inspiceret at underdatabehandlere fra databehandlerens oversigt over underdatabehandlere, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige.	Ingen afvigelser konstateret. Iht. databehandleraftaler er alle underdatabehandlere godkendt af den dataansvarlige.
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underretters 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.	Inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere.	Ingen afvigelser konstateret. Der har ikke været ændring i underdatabehandlere.

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.	*Databehandlerens kontrolaktivitet*	*PDS' udførte test*	*Resultat af PDS' test*
		Inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændring i anvendelse af underdatabehandlerne i erklæringsperioden.	
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Inspiceret, at der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af databehandlerens oversigt. Inspiceret at underdatabehandleraftaler, indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Ingen afvigelser konstateret. Der foreligger databehandleraftaler med alle underdatabehandlere og disse indeholder samme eller stærkere krav.
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: • Navn • CVR-nr. • Adresse • Beskrivelse af behandlingen	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.

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.	*Databehandlerens kontrolaktivitet*	*PDS' udførte test*	*Resultat af PDS' test*
F.6	Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.	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, behandlingssikkerheden hos de anvendte underdatabehandlere, tredjelands overførselsgrundlag og lignende.	Ingen afvigelser konstateret. Databehandlere er risikovurderet og der er ført kontrol med samtlige databehandlere ved indhentelse af gennemgang af revisorerklæringer vedrørende it-sikkerhed.

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.	*Databehandlerens kontrolaktivitet*	*PDS' udførte test*	*Resultat af PDS' test*
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 foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	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. Der bliver ikke overført data til usikre tredjelande.

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.	*Databehandlerens kontrolaktivitet*	*PDS' udførte test*	*Resultat af PDS' test*
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	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. Intern persondatapolitik er opdateret i marts 2019.
H.2	Databehandleren 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.	Inspiceret, at de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for: • Udlevering af oplysninger • Rettelse af oplysninger • Sletning af oplysninger • Begrænsning af behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede. Inspiceret dokumentation for, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer.	Ingen afvigelser konstateret. Intern persondatapolitik er opdateret i marts 2019. Alle IT-systemer er gennemgået med det formål at sikre de registreredes rettigheder kan imødekommes.

Kontrolmål I **Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.**			
Nr.	*Databehandlerens kontrolaktivitet*	*PDS' udførte test*	*Resultat af PDS' 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.	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. Intern persondatapolitik er opdateret i marts 2019.
I.2	Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: • Awareness hos medarbejdere	Inspiceret, at databehandler udbyder awareness-træning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden.	Ingen afvigelser konstateret.
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Inspiceret, at samtlige registrerede brud på persondatasikkerheden hos databehandleren eller underdatabehandlerne er meddelt de berørte dataansvarlige uden unødig forsinkelse efter, at databehandleren er blevet opmærksom på brud på persondatasikkerheden.	Ingen afvigelser konstateret. Der holdes en databrudslog. Der har ikke været nogle hændelser i perioden.

Kontrolmål I **Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.**			
Nr.	*Databehandlerens kontrolaktivitet*	*PDS' udførte test*	*Resultat af PDS' test*
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.	Inspiceret, at de foreliggende procedurer for underretning af 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. De relevante punkter er indeholdt i databrudsloggen.