Erhvervsvej 2
8721 Daugård
CVR-nr.: 30707907
Telefon 7589 6066
info@r-i-d.dk

PeopleTools ApS
Vestergade 14
8660 Skanderborg

CVR-nr.: 31871689

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med People Tools ApS' kunder

27. maj 2020

INDHOLDSFORTEGNELSE

PeopleTools ApS behandler personoplysninger på vegne af vore kunder, der er dataansvarlige, i henhold til de indgåede databehandleraftaler med vore kunder.

Medfølgende systembeskrivelse er udarbejdet til brug for PeopleTools ApS kunder, der har anvendt PeopleTools-systemet og E-stimate-software, som ejes og administreres af databehandleren eller underdatabehandlere, til at indsamle og behandle de nødvendige oplysninger om ansøgere og medarbejdere, for at kunne udarbejde personprofiler, kognitive tests og HR-målinger, og som har en tilstrækkelig forståelse til at vurdere systembeskrivelsen 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") og databeskyttelsesloven er overholdt.

PeopleTools ApS bekræfter, at:

a) Den medfølgende systembeskrivelse på side 7 - 9, giver en retvisende systembeskrivelse af PeopleTools-systemet og E-stimate-software, der pr. den 27. maj 2020 har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende systembeskrivelse:

   i. Redegør for, hvordan ydelserne 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.

- De kontroller, som vi med henvisning til afgrænsningen af ydelsernes udformning har forudsat ville være implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i systembeskrivelsen, er identificeret i systembeskrivelsen.

- Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger.

ii. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne ydelser til behandling af personoplysninger under hensyntagen til, at systembeskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og derfor ikke kan omfatte ethvert aspekt ved vore ydelser, 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 systembeskrivelse, var hensigtsmæssigt udformet pr. den 27. maj 2020. Kriterierne anvendt for at give denne udtalelse var, at:

i. De risici, der truede opnåelsen af de kontrolmål, der er anført i systembeskrivelsen, 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.

c) Der er etableret 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 og databeskyttelsesloven.

Skanderborg, den 29. maj 2020

PeopleTools ApS

Poul Kristian Mouritsen
Direktør

Uafhængig revisors ISAE 3000-erklæring pr. den 27. maj 2020 med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med PeopleTools ApS kunder

Til ledelsen i PeopleTools ApS (databehandleren) og PeopleTools ApS kunder (de dataansvarlige)

Omfang
Vi har fået som opgave at afgive erklæring om PeopleTools ApS systembeskrivelse på side 7-9 af deres ydelser i relation til behandling af personoplysninger på vegne af dataansvarlige i henhold til indgåede databehandleraftaler indgået med de dataansvarlige pr. den 27. maj 2020 samt om udformningen af kontroller, der knytter sig til de kontrolmål, som er anført i systembeskrivelsen.

Vi har ikke udført handlinger rettet mod funktionaliteten af de kontroller, der indgår i systembeskrivelsen, og udtrykker derfor ingen konklusion herom.

Databehandler's ansvar
Databehandler er ansvarlig for udarbejdelsen af systembeskrivelsen og tilhørende udtalelse på side 3-4, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå systembeskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, systembeskrivelsen omfatter, for at anføre kontrolmålene samt for at udforme og implementere kontroller for at opnå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring
Vi har overholdt kravene til uafhængighed og andre etiske krav i FSR – danske revisorers retningslinjer for revisors etiske adfærd (Etiske regler for revisorer), der bygger på de grundlæggende principper om integritet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

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

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

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. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om systembeskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet.

En erklæringsopgave med sikkerhed om at afgive erklæring om systembeskrivelsen og udformningen af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens systembeskrivelse af deres ydelser samt for kontrollernes udformning. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at systembeskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet.

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 på side 3-4.

Som nævnt ovenfor har vi ikke udført handlinger rettet mod funktionaliteten af de kontroller, der indgår i systembeskrivelsen, og vi udtrykker derfor ingen konklusion herom.

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

Begrænsninger i kontroller hos en databehandler
Databehandler's systembeskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved anvendelsen af deres ydelser, 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.

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 på side 3-4. Det er vores opfattelse,

a) at systembeskrivelsen af ydelsen, således som denne var udformet og implementeret pr. den 27. maj 2020, i alle væsentlige henseender er retvisende, og

b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i systembeskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. den 27. maj 2020

Beskrivelse af test af kontroller
De specifikke kontroller, der blev testet, og resultater af disse tests fremgår på side 10-28.

Tiltænkte brugere og formål
Denne erklæring og beskrivelsen af test af kontroller på side 10-28 er udelukkende tiltænkt dataansvarlige, der har anvendt PeopleTools ydelser, og som har en tilstrækkelig forståelse til at overveje det sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen og databeskyttelsesloven er overholdt.

Daugård, den 29. maj 2020

RID REVISION,
Registreret Revisionsaktieselskab
CVR-nr.: 30 70 79 07

Anette Dam Jacobsen
Statsautoriseret revisor
MNE nr.: mne42894
FSR - danske revisorer

Beskrivelse af behandling
Den Dataansvarlige anvender PeopleTools-systemet og E-stimate-software, som ejes og administreres af Databehandleren eller Underdatabehandlere, til at indsamle og behandle de nødvendige oplysninger om ansøgere og medarbejdere, for at kunne udarbejde personprofiler, kognitive tests og HR-målinger.

Karakteren af behandlingen
Databehandlerens behandling af personoplysninger er nødvendig for at medarbejdere og ansøgere kan modtage invitation til at udfylde test og profiler, ligesom behandlingen skal sikre, at PeopleTools ApS kan registrere de certificerede brugere af værktøjerne.

Personoplysninger
Almindelige personoplysninger i form af:

- Navn
- E-mailadresse
- Køn
- Alder
- Stilling
- Uddannelse
- Erhverv
- Telefonnummer og arbejdsadresse (kun certificerede brugere)

Kategorier af registrerede personer omfattet af databehandleraftalen:

- Medarbejdere og ledere hos Dataansvarlig
- Kandidater til ledige stillinger hos Dataansvarlig

Praktiske tiltag
Der er truffet tekniske og organisatoriske foranstaltninger til sikker behandling af personoplysninger. Heri indgår:

- Sikker teknisk opbevaring af persondata.
- Instrukser omkring it-sikkerhed og korrekt behandling af persondata til medarbejdere og samarbejdspartnere.
- Træning af medarbejder i it-sikkerhed og korrekt behandling af persondata.
- Kontrol af systemer og processer som dokumenteres i GDPR kontrolsystem.

Disse foranstaltninger er implementeret på baggrund af anerkendte branchestandarder herunder IS027001 og retningslinjer fra databeskyttelsesforordningen og tilsynsmyndigheden.

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. Der er i forhold til PeopleTools ApS behandling af personoplysninger i forbindelse med at gennemføre test og anvende vores værktøjer lavet følgende kortlægning af risici og kategorisering af sandsynlighed og konsekvens:

Proces	Sandsynlighed	Konsekvens for den registrerede	Risikovurdering og foranstaltninger
Profiler i PeopleTools system	Mindre sandsynligt	Mindre alvorlig (generende)	Middel risiko Der er unikke brugere med login og personoplysninger pseudonymiseres og automatisk sletning
Test i E-stimate (underdatabehandlers system)	Mindre sandsynligt	Mindre alvorlig (generende)	Middel risiko Der er unikke eller virksomhedsbrugere og personoplysninger slettes uigenkaldeligt efter 6 måneder
Intern og ekstern mailkorrespondance	Mindre sandsynligt	Graverende/ødelæggende (uacceptabelt)	Middel risiko Der anvendes anerkendte leverandører og fysisk sikkerhed. Fortrolige mails slettes i henhold til politikker og der anvendes TLS kryptering
Cookies på hjemmeside	Mindre sandsynligt	Ubetydelig (uvæsentlig)	Lav risiko Der anvendes kun cookies på PeopleTools system til at understøtte brugeroplevelse (sprogvalg)
Backup	Mindre sandsynligt	Graverende/ødelæggende (uacceptabelt)	Middel risiko Der anvendes anerkendt dansk hostingleverandør som leverer ISAE erklæring
Udviklingsmiljø	Mindre sandsynligt	Ubetydelig (uvæsentlig)	Lav risiko Der opbevares ikke personoplysninger permanent og der er fysisk og digital sikkerhed på anerkendt niveau
Brugere i PeopleTools system	Mindre sandsynligt	Mindre alvorlig (generende)	Middel risiko Systemet har sikker login og system til log out ved forsøg på indtrængen (fejlindtastning af kode)

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
- 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 de specifikke kontroller, der blev testet, og resultater af disse tests, som fremgår på side 10-28.

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, og at der alene opbevares oplysninger, som er relevante i forhold til formålet med at opbevare oplysningerne,
- at systemmail der beskriver sammenhæng imellem respondenten og profilnummeret slettes i henhold til virksomhedens politik,
- at overholde sin oplysningspligt i forhold til respondenten omkring hvordan data anvendes og slettes,
- 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 og at PeopleTools gives besked når brugeres adgang skal deaktiveres.

KONTROLMÅL, KONTROLLER, TEST OG RESULTAT AF TEST

I testskemaet på de næste sider er præsenteret relevante kontrolmål, kontroller, test og resultat af test. Eventuelle andre kontrolmål, kontroller og test, herunder kontroller udført hos PeopleTools ApS kunder (de datasvarlige) er ikke omfattet af vor erklæring. Ligeledes er der ikke inkluderet kontroller hos underleverandører, da disse delvist dækkes ved modtagelse af revisionserklæringer fra underleverandørerne.

De udførte test, som er beskrevet, omfatter de test, som er vurderet som nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål er opnået, og de tilhørende kontroller er hensigtsmæssigt udformet.

Test af kontroller hos PeopleTools ApS pr. den 27. maj 2020 er udført ved følgende handlinger:

- Forespørgsel, som omfatter forespørgsel af passende ansatte hos PeopleTools ApS i forhold til at opnå viden om indførte politikker, procedurer, retningslinjer samt kontroller, herunder hvordan kontroller udføres.

- Observation, som omfatter, at eksistensen, implementeringen eller/samt anvendelsen og udførelsen af relevante kontroller observeres.

- Inspektion, som omfatter, at der foretages gennemgang og stillingtagen til politikker, procedurer, retningslinjer mv. for udførelse af kontroller i forhold til at vurdere udformningens hensigtsmæssighed og om kontroller overvåges tilstrækkeligt og med passende intervaller.

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*	*Revisors udførte test*	*Resultat af revisors 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
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
A.3	Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning. Inspiceret, at der er procedurer for underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen.	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*	*Revisors udførte test*	*Resultat af revisors 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 ved en stikprøve på 4 databehandleraftaler, at der er etableret de aftalte sikringsforanstaltninger.	Ingen afvigelser konstateret
B.2	Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de med 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
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende	Inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger,	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*	*Revisors udførte test*	*Resultat af revisors test*
	opdateres.	er installeret antivirus software. Inspiceret, at antivirus software er opdateret.	
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.	Ingen afvigelser konstateret
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.	Interne netværk er ikke segmenteret.
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. Inspiceret, at de aftalte tekniske foranstaltninger understøtter opretholdelsen af begrænsningen i brugernes arbejdsbetingede adgang til personoplysninger. Inspiceret ved oversigt over brugeres adgange til systemer og databaser, at de er begrænset til medarbejdernes arbejdsbetingede behov.	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*	*Revisors udførte test*	*Resultat af revisors test*
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering. Overvågningen omfatter: • Adgang til systemer	Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering.	Ingen afvigelser konstateret
B.8	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 kryptering. Forespurgt, om der har været ukrypterede transmissioner af følsomme og fortrolige personoplysninger, samt om de dataansvarlige er behørigt orienteret herom.	Ingen afvigelser konstateret
B.9	Der er etableret logning i systemer, databaser og netværk	Inspiceret, at der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, herunder gennemgang og opfølgning på logs.	Der er ikke etableret logning i systemer, databaser og netværk. Logning bliver mulig med ny release af systemer over sommeren 2020.
B.10	Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af personoplysninger til udvikling, test og lignende, der sikrer, at anvendelsen alene sker	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*	*Revisors udførte test*	*Resultat af revisors test*
	ansvarliges formål i henhold til aftale og på dennes vegne.	i pseudonymiseret eller anonymiseret form.	
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	Vi har forespurgt til formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder gennemførsel af sårbarhedsscanninger og penetrationstests.	Der testes ikke med sårbarhedsscanninger og penetrationstests. Men der anvendes ekstern hostingleverandør, som mindst halvårligt foretager en sikkerhedsscanning af driftssystemerne.
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Inspiceret, 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.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Inspiceret ved en oversigt over medarbejderes adgange til systemer og databaser, at de tildelte brugeradgange er godkendt, og at der er et arbejdsbetinget behov. Inspiceret ved en oversigt over medarbejderes adgange at	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*	*Revisors udførte test*	*Resultat af revisors test*
		fratrådte medarbejderes 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.	
B.14	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører højrisiko for de registrerede, sker som minimum ved anvendelse af to-faktor autentifikation.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at to-faktor autentifikation anvendes ved behandling af personoplysninger, der medfører højrisiko for de registrerede.	Der sker ikke behandling af personoplysninger der medfører højrisiko for de registrerede. Anvendte adgangskontroller er i overensstemmelse med databehandleraftaler.
B.15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Ingen afvigelser konstateret

Kontrolmål C **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
C.1	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. It-sikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der 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. Inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.	Ingen afvigelser konstateret
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 ved en stikprøve på 4 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 • Certificering	Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.	Ingen afvigelser konstateret

Kontrolmål C **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
	• Eksamensbeviser		
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 ved en stikprøve på 2 medarbejdere, at de pågældende medarbejdere har underskrevet en fortrolighedsaftale. Inspiceret ved en stikprøve på 2 medarbejdere, at de pågældende medarbejdere er blevet introduceret til: • Informationssikkerhedspolitikken • Procedurer vedrørende databehandling, samt anden relevant information	Ingen afvigelser konstateret
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 pc etc. inddrages	Ingen afvigelser konstateret
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 behandling af personoplysninger, databehandleren udfører for de dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt.	Ingen afvigelser konstateret

Kontrolmål C **Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
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

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*	*Revisors udførte test*	*Resultat af revisors 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
D.2	Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner: o IQ-potentials anonymisering – brugere slettes efter 6 måneder o Alle persondata i PeopleTools-systemet slettes automatisk	Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.	Ingen afvigelser konstateret
D.3	Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: o Alle persondata slettes automatisk. o 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*	*Revisors udførte test*	*Resultat af revisors 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
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.	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*	*Revisors udførte test*	*Resultat af revisors 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 ved en stikprøve på 3 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
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	Inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af 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*	*Revisors udførte test*	*Resultat af revisors test*
	databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.		
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 ved en stikprøve, at disse underdatabehandleraftaler indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Ingen afvigelser konstateret
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: • Navn • CVR-nr. • Adresse • Behandlingsbeskrivelse	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.	Ingen afvigelser konstateret
F.6	Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved	Inspiceret, at der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af	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*	*Revisors udførte test*	*Resultat af revisors test*
	møder, inspektioner, gennemgang af revisionserklæring eller lignende.	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.	

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*	*Revisors udførte test*	*Resultat af revisors 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.	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 tredje-lande.
G.2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over overførsler af personoplysninger til tredjelande eller internationale organisationer.	N/A
G.3	Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	Inspiceret, at der foreligger formaliserede procedurer for sikring af et gyldigt overførselsgrundlag.	N/A

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*	*Revisors udførte test*	*Resultat af revisors 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.
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.	Ingen afvigelser konstateret.

Kontrolmål I **Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors 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.
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. Forespurgt underdatabehandlerne, om de har konstateret nogen brud på persondatasikkerheden i erklæringsperioden	Ingen afvigelser konstateret.
I.4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet	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	Ingen afvigelser konstateret.

Kontrolmål I **Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.**			
Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
	på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere 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.	