

Partner IT ApS

Uafhængig tredjeparts tilsynsrapport om informationssikkerhed og foranstaltninger i henhold til databehandleraftaler med Partner IT ApS' kunder

Pr. 15. juli 2024

Indholdsfortegnelse

1. Ledelsens udtalelse	3
2. Eksterne auditors udtalelse	4
3. Beskrivelse af behandling	6
4. Kontrolmål, kontrolaktivitet, test og resultat heraf	8

1. Ledelsens udtalelse

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

Nedenstående er udarbejdet til brug for kunder, der benytter Partner IT ApS' ydelser, og skal danne grundlag for at vurdere 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.

Partner IT ApS bekræfter, at:

- a) Den medfølgende beskrivelse af Partner IT ApS' behandling af personoplysninger, giver en retvisende beskrivelse af den behandling af personoplysninger der foretages ved benyttelse af Partner IT ApS' ydelser.
 - (i) Redegør for, hvordan beskrivelsen af behandling af personoplysninger var udformet og implementeret
 - (ii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne behandling af personoplysninger
- b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet pr. 15. juli 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 til databehandlere i henhold til databeskyttelsesforordningen og databeskyttelsesloven.

Herning, den 15. juli 2024

Partner IT ApS

Kim Juul-Henriksen
CEO

2. Eksterne auditors udtalelse

Uafhængig tredjeparts tilsynsrapport om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med Partner IT ApS' kunder

Omfang

Blanner Compliance ApS har fået til opgave at udarbejde en rapport og konklusion på Partner IT ApS' beskrivelse af behandlingen af personoplysninger for deres kunder i henhold til indgåede databehandleraftaler, pr. 15. juli 2024 og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i afsnit 4.

Partner IT ApS' ansvar

Partner IT ApS er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse, 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.

Eksterne auditors ansvar

Blanner Compliance skal på grundlag af audithandlinger udtrykke en konklusion om Partner IT ApS' beskrivelse samt om udformningen og implementeringen af kontroller, der knytter sig til de kontrolmål, der er anført i afsnit 4.

Arbejdet er udført baseret på gældende standarder der kræver, at der planlægges og udføres handlinger for at opnå viden om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og implementeret.

Opgave om at udarbejde en rapport og udtrykke en konklusion om beskrivelsen, udformningen og implementeringen 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 og implementering. De valgte handlinger afhænger af den eksterne auditors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller implementeret. Audithandlinger har omfattet test af implementeringen af sådanne kontroller, som anses for nødvendige for at kunne udtrykke en konklusion om at de kontrolmål, der er anført i beskrivelsen, blev opnået. Opgaven 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 konklusionen.

Begrænsninger i kontroller hos en dataansvarlig

Partner IT ApS' 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

Konklusionen er udformet på grundlag af de forhold, der er redegjort for i denne rapport. De kriterier, der er 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. 15. juli 2024 i alle væsentlige henseender er retvisende, og
- (b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i afsnit 4, i alle væsentlige henseender var hensigtsmæssigt udformet og implementeret pr. 15. juli 2024.

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 rapport og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt dataansvarlige, der har anvendt Partner IT ApS' 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.

Langå, den 15. juli 2024

Mette Blanner

Partner – Blanner Compliance ApS

Cand. Merc. Aud. (Revisor)

Certified Information System Auditor (CISA)

Certificeret Data Protection Officer

ISO 27001 implementation certificeret



3. Beskrivelse af behandling

Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er at databehandler hoster den dataansvarliges platforme og yder support til den dataansvarlige og dennes ansatte i den daglige drift af IT-systemer.

Karakteren af behandlingen

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om at:

- Varetage support til den dataansvarlige, hvor databehandleren kan have adgang til fuldstændige oplysninger hos den dataansvarlige.
- Varetage hosting af platforme, såvel som kontinuerlig driftssupport til den dataansvarlige

Databehandleren er berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal anvendes for at skabe det nødvendige (og aftalte) sikkerhedsniveau omkring oplysningerne.

Databehandleren skal dog – i alle tilfælde og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige (på baggrund af den risikovurdering den dataansvarlige har foretaget):

- Logning af sin dataadgang til dataansvarliges systemer
- Sikre sin dataadgang til dataansvarliges systemer
- Sikre backup af dataansvarliges systemer

Personoplysninger

Typen af personoplysninger, der behandles:

- Almindelige personoplysninger
- Særlige kategorier af personoplysninger,
- Andre personlige oplysninger, herunder oplysninger om strafbare forhold og cpr-numre.

Kategorier af registrerede personer omfattet af databehandleraftalen:

- Dataansvarliges kunder
- Dataansvarliges ansatte
- Dataansvarliges samarbejdspartnere og leverandører

Praktiske tiltag

Der er formuleret og implementeret passende tekniske og organisatoriske foranstaltninger til at sikre behandling af personoplysninger. Disse foranstaltninger er implementeret på baggrund af anerkendte branchestandarder herunder ISO27001 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.

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 registrerede, 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 er der udarbejdet:

- Fortegnelse over behandlingsaktiviteter
- Liste over dataansvarlige
- Databehandleraftaler med underdatabehandlere
- Kontrol med databehandlere
- Risikovurderinger på behandlingsaktiviteter
- Interne politikker for beskyttelse af persondata og it-sikkerhed
- Awareness 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 best practices indenfor generel it-sikkerhed.

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

Komplementerende kontroller hos de dataansvarlige

Den dataansvarlige har følgende forpligtelser:

- at sikre sig, at personoplysningerne er ajourførte
- at sikre sig, at instruksen er lovlige set i forhold til den til enhver tid gældende persondatarelige regulering
- at instruksen er hensigtsmæssig set i forhold til databehandleraftalen 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.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Auditors udførte test</i>	<i>Resultat af auditors test</i>
A.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks.</p> <p>Inspiceret, at procedurerne indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen.</p> <p>Inspiceret, at procedurer er opdateret.</p>	Ingen afvigelser konstateret
A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Inspiceret at behandlinger af personoplysninger, foregår i overensstemmelse med 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.	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning.</p> <p>Inspiceret, at der er procedurer for underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen.</p>	<p>Ingen afvigelser konstateret</p> <p>Der har ikke været behov for underretning af dataansvarlige kunder.</p>

Kontrolmål A

Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgående databehandleraftale.

<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Auditors udførte test</i>	<i>Resultat af auditors test</i>
		Inspiceret, at den dataansvarlige er underrettet i tilfælde, hvor behandlingen af personoplysninger er vurderet i strid med lovgivningen.	

Kontrolmål B			
Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Auditors udførte test</i>	<i>Resultat af auditor test</i>
B.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger.</p> <p>Inspiceret, at procedurer er opdateret.</p> <p>Inspiceret, at der er etableret sikkerhedsforanstaltninger der, som minimum, lever op til den databehandleraftale, der indeholder de højeste krav til sikkerhed.</p>	Ingen afvigelser konstateret
B.2	<p>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.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandler foretager en risikovurdering for at opnå en passende sikkerhed.</p> <p>Inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger.</p> <p>Inspiceret, at databehandler har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen.</p>	Ingen afvigelser konstateret

Kontrolmål B			
Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Auditors udførte test</i>	<i>Resultat af auditor test</i>
		Inspiceret, at databehandler har implementeret de sikringsforanstaltninger, der er aftalt med de dataansvarlige.	
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
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 passende konfigureret.	Ingen afvigelser konstateret
B.5	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	Ingen afvigelser konstateret Der har ikke været nye ansættelser siden sidste audit og dermed har det ikke været muligt at teste tildeling af adgange.

Kontrolmål B			
Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Auditors udførte test</i>	<i>Resultat af auditor test</i>
		<p>brugernes arbejdsbetingede adgang til personoplysninger.</p> <p>Inspiceret, at adgange til systemer og databaser, er begrænset til medarbejdernes arbejdsbetingede behov.</p> <p>Inspiceret, at nyansatte medarbejdere har fået tildelt de korrekte rettigheder, baseret på deres arbejdsmæssige behov.</p>	
B.6	<p>Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering. Overvågningen omfatter:</p> <ul style="list-style-type: none"> • at servere kører og svarer • at services er kører • ressourceovervågning 	Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning med alarmering.	Ingen afvigelser konstateret
B.7	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at transmission af følsomme og fortrolige oplysninger over internettet er	Ingen afvigelser konstateret

Kontrolmål B			
Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Auditors udførte test</i>	<i>Resultat af auditor test</i>
		<p>beskyttet af stærk kryptering baseret på en anerkendt algoritme.</p> <p>Inspiceret, at teknologiske løsninger til kryptering har været tilgængelige og aktiveret.</p> <p>Inspiceret, at der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet.</p> <p>Forespurgt, om der har været ukrypterede transmissioner af følsomme og fortrolige personoplysninger i det seneste år, samt om de dataansvarlige er behørigt orienteret herom.</p>	
B.8	<p>Der er etableret logning af databehandlerens aktiviteter på dataansvarliges servere:</p> <ul style="list-style-type: none"> • Logon af systemadministratorer • Systemadministrators visning af password • Clearing af log 	<p>Inspiceret, at der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter på dataansvarliges servere.</p> <p>Inspiceret, at logning af brugeraktiviteter på dataansvarliges servere, er konfigureret og aktiveret.</p> <p>Inspiceret, at sletning af logs bliver logget.</p>	Ingen afvigelser konstateret

Kontrolmål B			
Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Auditors udførte test</i>	<i>Resultat af auditor test</i>
B.9	Det sikres at relevante opdatering og patches, herunder sikkerhedspatches, bliver installeret.	Inspiceret, at der foreligger formaliserede procedurer for håndtering af patches og sikkerhedspatches.	Ingen afvigelser konstateret
B.10	Adgange til dataansvarliges databaser, hvori der sker behandling af personoplysninger er sikret med passende adgangskrav, herunder sikre passwords og to-faktor autentikation.	Inspiceret, at der foreligger formaliserede procedurer for adgangskrav, herunder sikre passwords og to-faktor autentikation. Inspiceret, at krav til password er passende. Inspiceret, at adgang til dataansvarliges data skal ske gennem VPN med to-faktor når brugeren ikke er på databehandlerens netværk.	Ingen afvigelser konstateret
B.11	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger. Fysisk sikkerhed i datacentre er outsourcet til underdatabehandlere og krav til fysisk sikkerhed er defineret i aftaler. Databehandlerens kontorfaciliteter er sikret med personligt adgangskort og alarmer.	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. Inspiceret, at der er aftaler med datacentre vedrørende fysisk sikkerhed. Inspiceret, at databehandlerens kontorfaciliteter er passende sikret.	Ingen afvigelser konstateret

Kontrolmål B			
Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Auditors udførte test</i>	<i>Resultat af auditor test</i>
B.12	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.13	Det er etableret en beredskabsplan som kan aktiveres i tilfælde af hændelser der tilsigter det, så supporten til dataansvarlige kunder kan opretholdes.	Inspiceret, at der er etableret en operationel beredskabsplan. Inspiceret, at beredskabsplanen er gennemgået indenfor det seneste år.	Ingen afvigelser konstateret
B.14	Der bliver foretaget backup af databaser, samt restoretest hvor det er aftalt med den dataansvarlige. Backuppen gemmes krypteret.	Inspiceret, at der foreligger formaliserede procedurer for backup af databaser. Inspiceret, at backups lavet for dataansvarlige gemmes krypteret. Inspiceret, at der foretages restore test af backup.	Ingen afvigelser konstateret

Kontrolmål C			
Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Auditors udførte test</i>	<i>Resultat af auditors test</i>
C.1	<p>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.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.</p>	<p>Inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år.</p> <p>Inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.</p>	Ingen afvigelser konstateret
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	<p>Inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler.</p> <p>Inspiceret, at kravene i den databehandleraftale der har de højeste krav til sikkerhed, som minimum, er dækket af informationssikkerhedspolitikens krav til sikringsforanstaltninger og behandlingssikkerheden.</p>	Ingen afvigelser konstateret
C.3	<p>Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang:</p> <ul style="list-style-type: none"> • Referencer fra tidligere ansættelser • Eksamensbeviser 	Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.	<p>Ingen afvigelser konstateret</p> <p>Der har ikke været nye ansættelser siden sidste audit og dermed har det ikke været</p>

Kontrolmål C			
Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Auditors udførte test</i>	<i>Resultat af auditors test</i>
		Forespurgt, at efterprøvningen af medarbejdere omfatter: <ul style="list-style-type: none"> • Referencer fra tidligere ansættelser • Eksamensbeviser 	muligt at teste efterprøvning af medarbejdere.
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 medarbejdere har underskrevet en fortrolighedsaftale. Inspiceret, at medarbejdere er blevet introduceret til: <ul style="list-style-type: none"> • Informationssikkerhedspolitikken • Intern persondatapolitik 	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 medarbejders rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages Inspiceret, at fratrådte medarbejders rettigheder er inaktiveret eller ophørt, samt forespurgt på at aktiver er inddraget.	Ingen afvigelser konstateret Der har ikke været fratrædelser siden sidste audit og dermed har det ikke været muligt at teste proceduren.

Kontrolmål C			
Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Auditors udførte test</i>	<i>Resultat af auditors test</i>
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.	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt.</p> <p>Inspiceret, at der er i opsigelsesbrevet, er angivet oplysning om opretholdelse af fortrolighedsaftale og generel tavshedspligt for fratrådte medarbejdere.</p>	<p>Ingen afvigelser konstateret</p> <p>Der har ikke været fratrædelser siden sidste audit og dermed har det ikke været muligt at teste proceduren.</p>
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 udfører awareness-træning af medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger.	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.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Auditors udførte test</i>	<i>Resultat af auditors test</i>
D.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedureerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Inspiceret, at procedureerne er opdateret.</p>	Ingen afvigelser konstateret
D.2	<p>Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner:</p> <p>”Ved ophør af tjenesterne vedrørende behandling forpligtes databehandleren til, efter den dataansvarliges valg, at slette eller tilbagelevere alle personoplysninger til den dataansvarlige, samt at slette eksisterende kopier.”</p>	<p>Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.</p> <p>Inspiceret, at sletning på ophørte aftaler er foretaget efter aftale med kunden.</p> <p>Inspiceret, at der for ophørte databehandlinger er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført.</p>	<p>Ingen afvigelser konstateret</p> <p>Der har ikke været ophør af aftaler siden sidste audit og dermed har det ikke været muligt at teste proceduren.</p>
D.3	<p>Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige:</p> <ul style="list-style-type: none"> • Tilbageleveret til den dataansvarlige og/eller • Slettet, hvor det ikke er i modstrid med anden lovgivning. 	Inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger.	<p>Ingen afvigelser konstateret</p> <p>Der har ikke været ophør af aftaler siden sidste audit og dermed har det ikke været muligt at teste proceduren.</p>

Kontrolmål D			
Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres såfremt der indgås aftale herom med den dataansvarlige.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Auditors udførte test</i>	<i>Resultat af auditors test</i>
		Inspiceret, at der for ophørte databehandlinger er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført.	

Kontrolmål E			
Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Auditors udførte test</i>	<i>Resultat af auditors test</i>
E.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne.</p> <p>Inspiceret, at procedurerne er opdateret.</p> <p>Inspiceret, at der er dokumentation for, at databehandlingen sker i henhold til databehandleraftalen.</p>	Ingen afvigelser konstateret
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	<p>Inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder.</p> <p>Inspiceret, 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.</p>	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.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Auditors udførte test</i>	<i>Resultat af auditors test</i>
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 der er dokumentation for, at databehandlerens 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 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.	Inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændring 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.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Auditors udførte test</i>	<i>Resultat af auditors test</i>
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
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: <ul style="list-style-type: none"> • 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
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	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.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Auditors udførte test</i>	<i>Resultat af auditors test</i>
		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.	

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.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Auditors udførte test</i>	<i>Resultat af auditors test</i>
G.1	<p>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.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at personoplysninger alene overføres til tredjelande eller internationale organisationer i henhold til aftale med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.</p> <p>Inspiceret, at procedurerne er opdateret.</p>	<p>Ingen afvigelser konstateret</p> <p>Der overføres ikke data til usikre tredjelande.</p>
G.2	<p>Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.</p>	<p>Inspiceret, at databehandleren har en samlet og opdateret oversigt over overførsler af personoplysninger til tredjelande eller internationale organisationer.</p>	<p>Ingen afvigelser konstateret</p> <p>Der overføres ikke data til usikre tredjelande.</p>

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.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Auditors udførte test</i>	<i>Resultat af auditors test</i>
H.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder.</p> <p>Inspiceret, at procedurerne er opdateret.</p>	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.	<p>Inspiceret, at de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for:</p> <ul style="list-style-type: none"> • Udlevering af oplysninger • Rettelse af oplysninger • Sletning af oplysninger • Begrænsning af behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede. <p>Inspiceret dokumentation for, at de anvendte systemer og databaser understøtter gennemførelsen af de nævnte detaljerede procedurer.</p>	Ingen afvigelser konstateret

Kontrolmål I			
Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Auditors udførte test</i>	<i>Resultat af auditors test</i>
I.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden.</p> <p>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden.</p> <p>Inspiceret, at proceduren er opdateret.</p>	Ingen afvigelser konstateret
I.2	<p>Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden:</p> <ul style="list-style-type: none"> • Awareness hos medarbejdere • Overvågning af servere • Logning af brugeraktivitet 	<p>Inspiceret, at databehandle awareness- træner medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden.</p> <p>Inspiceret dokumentation for, at servere overvåges, samt at der sker opfølgning på overvågningsalarmer.</p> <p>Inspiceret at der sker logning af brugeraktiviteter.</p>	Ingen afvigelser konstateret
I.3	<p>Databehandleren 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 databehandleren eller en underdatabehandler.</p>	<p>Inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden.</p> <p>Inspiceret, at databehandleren har medtaget eventuelle brud på persondatasikkerheden hos underdatabehandlere i databehandlerens oversigt over sikkerhedshændelser.</p>	<p>Ingen afvigelser konstateret</p> <p>Der har ikke været brud på sikkerheden siden sidste audit, som har påvirket tilgængelig, fortrolighed eller integritet af kunde-data.</p>

Kontrolmål I			
Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.			
<i>Nr.</i>	<i>Databehandlerens kontrolaktivitet</i>	<i>Auditors udførte test</i>	<i>Resultat af auditors test</i>
		Inspiceret, at samtlige registrerede brud på persondatasikkerheden hos databehandleren eller underdatabehandlerne er meddelt de berørte dataansvarlige uden unødigt forsinkelse.	
I.4	<p>Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet:</p> <ul style="list-style-type: none"> • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. 	<p>Inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede procedurer for:</p> <ul style="list-style-type: none"> • 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. <p>Inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden.</p>	Ingen afvigelser konstateret