www.pwc.dk

# *EG A/S*

## ISAE 3000-erklæring, type 2, fra uafhængig revisor vedrørende behandlingssikkerhed for persondata i relation til EG A/S' it-drift og hosting-aktiviteter

*Januar 2018*

# Indhold

# 1. Ledelsens udtalelse

Denne beskrivelse og vurdering vedrører kontroller i relation til EG's overholdelse af persondataloven i forbindelse med EG's rolle som databehandler ved håndtering af personoplysninger i erhvervet som anden aktør. Beskrivelsen knytter sig til kontrollerne, som disse var udformet i perioden 1. januar - 31. december 2017.

EG er som databehandler af personhenførbare informationer bl.a. omfattet af:

- Lov om behandling af personoplysninger (persondataloven)
- Bekendtgørelse nr. 528 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (sikkerhedsbekendtgørelsen).

Herved er EG ansvarlig for, at sikre implementeringen og funktionen af kontroller med henblik på at forebygge og opdage fejl, herunder bevidste fejl, med henblik på overholdelse af lovgivningens krav.

Med baggrund i ovenstående vurderer EG, at vi i relation til persondataloven i alle væsentlige forhold har udformet og implementeret kontroller på et betryggende niveau i perioden 1. januar - 31. december 2017 i relation til EG's it-drift og hosting-aktiviteter, som opbevarer data omfattet af persondataloven og sikkerhedsbekendtgørelsen.

Ballerup, den 31. januar 2018
**EG A/S**

Mikkel Bardram
Adm. direktør, Koncernen

# 2. Uafhængig revisors erklæring med sikkerhed om beskrivelse af kontroller, deres udformning og funktionalitet

Til ledelsen i EG

**Omfang**
Vi har gennemgået den af ledelsen hos EG udarbejdede beskrivelse og vurdering vedrørende kontroller i relation til EG's overholdelse af persondataloven i forbindelse med EG's rolle som databehandler jf. de mellem EG's kunder og EG indgåede databehandlingsaftaler i relation til deres service ydelser.

Vores revision har omfattet relevante sikkerhedskrav for den databehandling, der foretages hos EG i henhold til følgende regler:

- Lov om behandling af personoplysninger (persondataloven, lov nr. 429 af 31. maj 2000, som senest er ændret ved lovbekendtgørelse (LBK) nr. 503 af 12. juni 2009),
- Bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (sikkerhedsbekendtgørelsen), som senest er ændret ved bekendtgørelse nr. 201 af 22. marts 2001,
- Vejledning nr. 37 af 2. februar 2001 om "sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning".

Vores revision omfatter ikke særlige forhold fra kundeaftaler, men omfatter relevante sikkerhedskrav, jf. indgåede databehandleraftaler.

Sikkerhedskravene er oplistet i afsnit 3.

Virksomhedens ledelse har ansvaret for, at sikkerhedskrav i relation til ovenstående regler er overholdt. Vores ansvar er, på grundlag af vores arbejde, at udtrykke en konklusion om, hvorvidt vi er enige i, at de etablerede kontroller er tilstrækkelige til at opfylde de relevante krav i persondataloven.

Vores erklæring dækker perioden 1. januar - 31. december 2017 og er udelukkende udarbejdet til brug for EG og EG's kunder.

**EG's ansvar**
EG's ledelse har ansvaret for, at sikkerhedskrav i relation til behandling af persondata er overholdt. Vores ansvar er på grundlag af vores arbejde at udtrykke en konklusion om, hvorvidt vi er enige i, at de etablerede kontroller er tilstrækkelige til at opfylde de relevante sikkerhedskrav.

**Vores 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.

PricewaterhouseCoopers 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.

**Vores ansvar**
Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om udformningen og funktionen af kontroller, der knytter sig til de sikkerhedskrav, der er anført i afsnit 3.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000 DK, "Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger". Denne standard kræver, at vi plan-

lægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, at kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed, hvor der afgives erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en serviceleverandør, omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anses for nødvendige for at give høj grad af sikkerhed for, at de sikkerhedskrav, der er anført i beskrivelsen, blev nået.

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

**Begrænsninger i kontroller hos en serviceleverandør**
Kontroller hos en serviceleverandør vil som følge af deres art muligvis ikke forhindre eller opdage alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en serviceleverandør kan blive utilstrækkelige eller svigte.

**Konklusion**
Det er vores opfattelse, at ledelsens beskrivelse og vurdering af kontrollerne i relation til deres serviceydelser, som EG har implementeret med henblik på at opnå en passende behandlingssikkerhed i relation til persondata, er retvisende, og at kontrollerne i perioden 1. januar - 31. december 2017 har været opretholdt på et betryggende niveau i overensstemmelse med aftale herom. I afsnit 3 har vi identificeret de sikkerhedskrav, som vores revision har omfattet.

Aarhus, den 31. januar 2018
**PricewaterhouseCoopers**
Statsautoriseret Revisionspartnerselskab

Jesper Parsberg Madsen
statsautoriseret revisor

Iraj Bastar
senior manager

# 3. Sikkerhedskrav, kontrolaktivitet, test og resultat heraf

| *Sikkerhedskrav jf. persondataloven og sikkerhedsbekendtgørelsen* | *EG's kontrolaktiviteter* | *Udførte test* | *Resultat af test* |
|---|---|---|---|
| **1. Behandlingssikkerhed** | | | |
| 1.1. Virksomheder der udfører arbejde under den dataansvarlige eller databehandleren, og som får adgang til oplysninger, må kun behandle disse efter instruks fra den dataansvarlige.<br><br>(*Persondataloven § 41, stk. 1*). | EG har tilrettelagt formaliserede processer til sikring af, at data behandles i overensstemmelse med kontrakt/tillæg fra dataansvarlig.<br><br>Instruktion fra dataansvarlig er indarbejdet i EG's formaliserede forretningsgange (it-sikkerhedshåndbog). | Vi har påset, at EG har tilrettelagt formaliserede processer til sikring af, at data behandles i overensstemmelse med kontrakt/tillæg fra dataansvarlig.<br><br>Vi har påset, at it-sikkerhedshåndbogen indeholder alle relevante instruktioner fra en dataansvarlig. | Området er gennemgået uden væsentlige bemærkninger. |
| 1.2. Databehandlere skal træffe tekniske og organisatoriske sikkerhedsforanstaltninger, som sikrer mod, at oplysningerne hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med lov om behandling af personoplysninger.<br><br>(*Persondataloven § 41, stk. 3, og sikkerhedsbekendtgørelsen § 3, stk. 1*). | EG har tilrettelagt formaliserede processer til sikring mod, at oplysningerne hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med lov om behandling af personoplysninger.<br><br>Disse kontroller omfatter:<br>• Retningslinjer for bortskaffelse af medier og udstyr,<br>• Retningslinjer for sikkerhedskopiering,<br>• Lagrede kopier gemmes på en anden fysisk lokalitet, som sikrer fortrolige eller følsomme personoplysninger mod uvedkommendes kendskab, misbrug eller øvrig behandling i strid med loven,<br>• Datamedier, der har indeholdt fortrolige eller følsomme personoplysnin- | Vi har påset, at EG har tilrettelagt formaliserede procedurer, der sikrer mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven om behandling af personoplysninger.<br><br>Vi har stikprøvevist efterprøvet, at kontrollerne vedrørende lagring, ulovlig destruktion samt uautoriseret adgang er effektive. | Området er gennemgået uden væsentlige bemærkninger. |

| *Sikkerhedskrav jf. persondataloven og sikkerhedsbekendtgørelsen* | *EG's kontrolaktiviteter* | *Udførte test* | *Resultat af test* |
|---|---|---|---|
| | ger, afleveres til destruktion<br>• Sikkerhedskopi af lokale data (midlertidige arbejdskopier), hvor dette omfatter fortrolige eller følsomme personoplysninger, opbevares på en forsvarlig måde, og sådanne backup medier destrueres. | | |
| 1.3. Databehandlere skal træffe de fornødne tekniske og organisatoriske foranstaltninger mod, at personoplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med lov om behandling af personoplysninger.<br>*(Sikkerhedsbekendtgørelsen § 3 stk. 1)* | EG har tilrettelagt formaliserede processer til sikring af sikkerhedskopiering og restore af produktionsmiljøer som EG har driftsansvaret for. EG anvender ikke dedicerede testsystemer og har ikke adgang til testdata. | Vi har påset, at EG har tilrettelagt formaliserede processer for, gennemgang af backup samt restore.<br>Vi har stikprøvevist efterprøvet, at kontrollerne vedrørende lagring, restore samt uautoriseret adgang fungerer som beskrevet. | Området er gennemgået uden væsentlige bemærkninger. |
| 1.4. For personoplysninger som er af særlig interesse for fremmede magter skal de dataansvarlige træffe foranstaltninger, der muliggør bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold.<br>*(Persondataloven § 41, stk. 4, og sikkerhedsbekendtgørelsen § 3, stk. 2).* | EG har tilrettelagt formaliserede processer til sikring af bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold. | Vi har påset, at EG har tilrettelagt formaliserede processer til sikring af bortskaffelse eller tilintetgørelse i tilfælde af krig eller lignende forhold. | Området er gennemgået uden væsentlige bemærkninger. |
| 1.5. Gennemførelse af en behandling ved en databehandler skal ske i henhold til en skriftlig aftale parterne imellem. Af aftalen skal det fremgå, at databehandleren alene handler efter instruks fra den dataansvarlige.<br>*(Persondataloven § 42, stk. 2).* | EG har tilrettelagt formaliserede processer for aftaleindgåelser, til sikring af, at enhver databehandling, modtagelse og videregivelse af data sker i henhold til instruks fra en dataansvarlig i henhold til indgåede databehandlingsaftaler. | Vi har påset, at EG har tilrettelagt formaliserede processer for aftaleindgåelser, som sikrer, at EG alene handler efter instruks fra en dataansvarlig.<br>Vi har stikprøvevist efterprøvet, at der foreligger databehandleraftaler for EG's kunder. | Området er gennemgået uden væsentlige bemærkninger. |

| *Sikkerhedskrav jf. persondataloven og sikkerhedsbekendtgørelsen* | *EG's kontrolaktiviteter* | *Udførte test* | *Resultat af test* |
|---|---|---|---|
| 1.6. Den dataansvarlige skal give den fornødne instruktion til de medarbejdere, som behandler personoplysningerne.<br><br>*(Sikkerhedsbekendtgørelsen § 5).* | EG har tilrettelagt formaliserede processer, som sikrer, at de organisatoriske forhold under-støtter sikkerhedsforanstaltningerne i persondataloven.<br><br>Alle medarbejdere underskriver hvert år en sikkerhedserklæring, hvori der gøres opmærksom på såvel politik som sikkerhedshåndbog med de gældende retningslinjer.<br><br>Ved indgåelse af aftaler med eksterne parter sikres den fornødne information om it-sikkerhedsmæssige krav, indgåelser af tavshedserklæringer o. lign. | Vi har påset at EG har tilrettelagt de organisatoriske forhold så sikkerhedsforanstaltningerne i persondataloven understøttes.<br><br>Vi har stikprøvevis testet, at medarbejderne hvert år underskriver en sikkerhedserklæring, hvori der gøres opmærksom på såvel politik som sikkerhedshåndbog med de gældende retningslinjer.<br><br>Vi har desuden påset, at der er indhentet en revisionserklæring fra en underleverandør, som sikrer, at tilsvarende krav overholdes på områder, hvor der er foretaget outsourcing. Vi har herudover drøftet underleverandørens setup i forhold til adgang til EG's data. | Området er gennemgået uden væsentlige bemærkninger. |
| 1.7. Databehandlere skal fastlægge retningslinjer til sikring af fysisk sikkerhed.<br><br>*(Sikkerhedsbekendtgørelsen §§ 5, 8 og 10).* | EG har tilrettelagt kontroller til sikring af fysisk sikkerhed.<br><br>Disse kontroller omfatter en række adgangskontroller i bygninger, hvor der behandles personoplysninger (adgangskort og adgangskode).<br><br>Ved indgåelse af aftaler med eksterne parter sikres det, at den eksterne part modtager den fornødne information om de it-sikkerhedsmæssige krav. | Vi har påset at EG har tilrettelagt kontroller til sikring af den fysiske sikkerhed.<br><br>Vi har stikprøvevis testet, at de fysiske adgangskontroller fungerer som beskrevet.<br><br>Vi har desuden påset, at der er indhentet en revisionserklæring fra en underleverandør som sikrer, at tilsvarende krav overholdes på områder, hvor der er foretaget outsourcing. Vi har herudover drøftet underleverandørens setup i forhold til adgang til EG's data. | Området er gennemgået uden væsentlige bemærkninger. |
| 1.8. Databehandlere skal fastlægge retningslinjer for sikkerhedsorganisa- | EG har tilrettelagt arbejdsgange for sikkerhedsorganisationen. | Vi har påset at EG har tilrettelagt arbejdsgange for sikkerhedsorganisatio- | Området er gennemgået uden væsentlige bemærknin- |

| *Sikkerhedskrav jf. persondataloven og sikkerhedsbekendtgørelsen* | *EG's kontrolaktiviteter* | *Udførte test* | *Resultat af test* |
|---|---|---|---|
| tionen.<br><br>(*Sikkerhedsbekendtgørelsen § 5*). | | nen. | ger. |
| 1.9. Databehandlere skal fastlægge interne retningslinjer for administration af og kontrol med autorisationer.<br><br>*(Sikkerhedsbekendtgørelsen § 5).* | EG har tilrettelagt processer for administration af, og kontrol med, autorisationer.<br><br>Alle autorisationer godkendes af medarbejdernes nærmeste chef og autorisationen af medarbejderen fremsendes til EG's kunder. | Vi har påset at EG har tilrettelagt processer for administration af, og kontrol med, autorisationer.<br><br>Vi har stikprøvevis testet, at der foreligger godkendelse fra nærmeste chef og fra EG's kunder med adgang til løsningen. | Området er gennemgået uden væsentlige bemærkninger. |
| 1.10. Databehandlere skal fastlægge interne retningslinjer for logisk sikkerhed, herunder logning og kontrol af afviste adgangsforsøg.<br><br>(*Sikkerhedsbekendtgørelsen §§ 5, 12 og 18*). | EG har tilrettelagt foranstaltninger for logisk sikkerhed, herunder logning og kontrol af afviste adgangsforsøg.<br><br>Disse kontroller omfatter:<br>• Kvalitetskrav til password<br>• Kontrol af afviste adgangsforsøg<br>• Log og opfølgning over afviste adgangsforsøg. | Vi har påset at EG har tilrettelagt foranstaltninger for logisk sikkerhed, herunder logning og kontrol af afviste adgangsforsøg.<br><br>Vi har stikprøvevis testet opsætningen af Windows domænekontroller og påset, at<br>• Kvalitetskravene til password lever op til kravene i Datatilsynets anbefalinger til god skik<br>• Der foretages lockout af brugere efter tre afviste adgangsforsøg ved forkert password.<br><br>Vi har desuden påset, at der foretages opfølgning på eventuelle afviste adgangsforsøg. | Området er gennemgået uden væsentlige bemærkninger. |
| 1.11. Databehandleren skal sikre, at kun autoriserede brugere har adgang til personfølsomme data, og at de tildelte brugeradgange er i overensstemmelse med arbejdsmæssigt betin- | EG har tilrettelagt formaliserede processer som sikrer, at tildelte brugeradgange er i overensstemmelse med arbejdsmæssigt betingede behov. | Vi har påset, at EG har tilrettelagt formaliserede processer for brugeradministration og rettighedsstyring.<br><br>Vi har stikprøvevis testet, at der for | Området er gennemgået uden væsentlige bemærkninger. |

| *Sikkerhedskrav jf. persondataloven og sikkerhedsbekendtgørelsen* | *EG's kontrolaktiviteter* | *Udførte test* | *Resultat af test* |
|---|---|---|---|
| gede behov.<br>(*Sikkerhedsbekendtgørelsen §§ 11 og 16, autorisation og adgangskontrol*). | Alle autorisationer godkendes af medarbejdernes nærmeste chef og indeholder begrundelse for det ønskede adgang til Løsningen. | tildelte autorisationer foreligger begrundelse for den ønskede adgang og godkendelse fra nærmeste chef. | |
| 1.12. Tildelte brugeradgange revurderes mindst en gang hvert halve år for at sikre, at de autoriserede personer fortsat opfylder betingelserne.<br>(*Sikkerhedsbekendtgørelsen § 17*). | EG har tilrettelagt formaliserede processer, som sikrer at egne autorisationer revurderes mindst én gang hvert halve år.<br>For så vidt angår autorisationer til testmiljøet udstedes disse for en begrænset periode på seks måneder, og der kræves nye autorisationer ved forlængelse. | Vi har påset, at der er tilrettelagt formaliserede processer for brugeradministration og rettighedsstyring.<br>Vi har stikprøvevis testet, at brugeradgange revurderes mindst én gang hvert halve år. | Området er gennemgået uden væsentlige bemærkninger. |
| 1.13 Databehandlere skal fastlægge interne retningslinjer for om behandling og destruktion af ind- og uddatamateriale.<br>(*Sikkerhedsbekendtgørelsen § 5*). | EG har tilrettelagt formaliserede processer for behandling og destruktion af ind- og uddatamateriale.<br>Disse kontroller omfatter:<br>• Valideringskontroller for inddatamateriale<br>• Retningslinjer for sikker destruktion af uddatamateriale. | Vi har påset, at EG har tilrettelagt formaliserede processer for behandling og destruktion af ind- og uddatamateriale.<br>Vi har stikprøvevis testet, at kontrollerne vedrørende valideringskontroller for inddatamateriale samt retningslinjer for sikker destruktion af uddatamateriale udføres. | Området er gennemgået uden væsentlige bemærkninger. |
| 1.14 Databehandlere skal fastlægge interne retningslinjer for anvendelsen af edb-udstyr.<br>(*Sikkerhedsbekendtgørelsen § 5*). | EG har udarbejdet retningslinjer, som beskriver anvendelsen af it-udstyr. | Vi har påset, at EG's retningslinjer for anvendelse af it-udstyr indeholder alle relevante kontroller, og vi har påset at de indeholder alle, for sikkerhedsbekendtgørelsens § 5, relevante retningslinjer. Vi har desuden påset, at disse retningslinjer omtales i den årlige sikkerhedserklæring som underskrives af medarbejderne. | Området er gennemgået uden væsentlige bemærkninger. |
| 1.15 Databehandlere skal give den fornødne instruktion til de medarbejdere, som behandler personoplysningerne. | EG har fastsat regler for uddannelse, træning og oplysninger om informationssikkerhed. | Vi har gennemgået EG's regler for kurser om informationssikkerhed.<br>Vi har påset, at undervisningsmateria- | Området er gennemgået uden væsentlige bemærkninger. |

| *Sikkerhedskrav jf. persondataloven og sikkerhedsbekendtgørelsen* | *EG's kontrolaktiviteter* | *Udførte test* | *Resultat af test* |
|---|---|---|---|
| *(Sikkerhedsbekendtgørelsen § 6).* | Den enkelte medarbejder underskriver en sikkerhedserklæring hvert år. | let er tilstrækkeligt til, at afdække sikkerhedskravene.<br><br>Vi har testet, at der foreligger underskrevne sikkerhedserklæringer fra alle medarbejdere. | |
| 1.16 Hvis behandling af personoplysninger foretages af en databehandler på den dataansvarliges vegne, skal der foreligge en skriftlig aftale, hvoraf det fremgår, at reglerne i denne bekendtgørelse ligeledes gælder for behandlingen ved databehandleren.<br><br>*(Sikkerhedsbekendtgørelsen § 7, stk. 1).* | Der foreligger en skriftlig aftale med den dataansvarlige, hvori det fremgår, at behandling af personoplysninger skal foregå i overensstemmelse med reglerne i sikkerhedsbekendtgørelsen. | Vi har påset, at der foreligger en skriftlig aftale mellem EG's kunder og EG, som henviser til reglerne i sikkerhedsbekendtgørelsen. | Området er gennemgået uden væsentlige bemærkninger. |
| 1.17 Databehandlere skal fastlægge interne retningslinjer for sikkerhedsreglerne i forbindelse med anvendelse af hjemmearbejdspladser.<br><br>(*Sikkerhedsbekendtgørelsen § 7, stk. 2).* | EG har udarbejdet retningslinjer for overholdelse af sikkerhedsreglerne i forbindelse med anvendelse af hjemmearbejdspladser.<br><br>Disse kontroller omfatter:<br>• Krav til opkobling via en sikker VPN-forbindelse<br>• Forbud mod at etablere andre kommunikationsforbindelser på pc'en<br>• Retningslinjer for behandling af data, herunder forbud mod at gemme data lokalt<br>• Den enkelte medarbejder bekræfter i den årlige sikkerhedserklæring, at ovenstående retningslinjer overholdes. | Vi har påset, at der foreligger retningslinjer for overholdelse af sikkerhedsreglerne i forbindelse med anvendelse af hjemmearbejdspladser<br><br>Vi har stikprøvevis testet EG's adgangskontroller via VPN og vurderet, at disse overholder de sikkerhedsmæssige krav i persondataloven.<br><br>Vi har desuden påset, at de årlige sikkerhedserklæringer, som underskrives af medarbejderne, indeholder omtale af retningslinjerne for brug af hjemmearbejdspladser, herunder forbud mod at downloade personfølsomme oplysninger på pc'er som anvendes ved hjemmearbejdspladser. | Området er gennemgået uden væsentlige bemærkninger. |

| *Sikkerhedskrav jf. persondataloven og sikkerhedsbekendtgørelsen* | *EG's kontrolaktiviteter* | *Udførte test* | *Resultat af test* |
|---|---|---|---|
| 1.18 Databehandlere skal fastlægge interne retningslinjer for bortskaffelse, salg, kassation, reparation og service af it- udstyr med persondata.<br>(*Sikkerhedsbekendtgørelsen § 9*). | EG har udarbejdet retningslinjer for bortskaffelse, salg, kassation, reparation og service af it- udstyr indeholdende persondata. | Vi har påset at EG har udarbejdet retningslinjer for bortskaffelse, salg, kassation, reparation og service af it-udstyr indeholdende persondata.<br>Vi har stikprøvevis testet at udstyr med persondata bortskaffes i henhold til retningslinjerne. | Området er gennemgået uden væsentlige bemærkninger. |
| 1.19 Databehandlere skal fastlægge interne retningslinjer for behandling af inddata.<br>*(Sikkerhedsbekendtgørelsen § 10).* | EG har udarbejdet retningslinjer for behandling af inddata.<br>Den enkelte medarbejder underskriver en sikkerhedserklæring hvert år, hvor der kvitteres for, at retningslinjerne for behandling af inddata overholdes. | Vi har påset, at EG har udarbejdet retningslinjer for behandling af inddata.<br>Vi har stikprøvevis testet, at de årlige sikkerhedserklæringer, indeholder omtale af retningslinjerne for inddata, og underskrives hvert år af medarbejderne. | Området er gennemgået uden væsentlige bemærkninger. |
| 1.20. Databehandlere skal fastlægge interne retningslinjer for behandling af uddatamaterialer.<br>(*Sikkerhedsbekendtgørelsen § 13).* | EG har udarbejdet retningslinjer for behandling af uddatamaterialer.<br>Den enkelte medarbejder underskriver en sikkerhedserklæring hvert år, hvor der kvitteres for, at retningslinjerne for behandling af uddata overholdes. | Vi har påset at EG har udarbejdet retningslinjer for behandling af uddatamaterialer.<br>Vi har stikprøvevis testet, at de årlige sikkerhedserklæringer, indeholder omtale af retningslinjerne for uddata, og underskrives hvert år af medarbejderne. | Området er gennemgået uden væsentlige bemærkninger. |
| 1.21. Databehandlerens skal udarbejde retningslinjer for sikring af eksterne kommunikationslinjer og træffe foranstaltninger, der sikrer, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.<br>(*Sikkerhedsbekendtgørelsen § 14*). | EG har udarbejdet retningslinjer for sikring af eksterne kommunikationslinjer, og EG har tilrettelagt formaliserede processer som sikrer, at uvedkommende ikke gennem disse forbindelser kan få adgang til personoplysninger.<br>Disse kontroller omfatter: | Vi har påset at EG har udarbejdet retningslinjer for sikring af eksterne kommunikationslinjer.<br>Vi har foretaget gennemgang af netværksopsætningen og testet, at kommunikationslinjerne er stærkt krypteret. | Området er gennemgået uden væsentlige bemærkninger. |

| *Sikkerhedskrav jf. persondataloven og sikkerhedsbekendtgørelsen* | *EG's kontrolaktiviteter* | *Udførte test* | *Resultat af test* |
|---|---|---|---|
| | • Retningslinjer for netværksadgang,<br>• Stærk kryptering af kommunikationslinjer. | | |
| 1.22 Databehandleren skal sikre, at der foretages maskinel registrering (logning) af alle anvendelser af personoplysninger. Registreringen skal mindst indeholde oplysning om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium. Loggen skal opbevares i 6 måneder, hvorefter den skal slettes.<br>*(Sikkerhedsbekendtgørelsen § 19).* | EG har tilrettelagt en række formaliserede processer til logning og håndtering af log-oplysninger. Loggen opbevares i henhold til aftale med EG's kunder i fem år, hvorefter den destrueres.<br>EG's procedurer omfatter:<br>• Alle medarbejderes adgang til systemerne logges med de nødvendige oplysninger om, hvilken bruger der har tilgået systemet, samt hvilke personer der er tilgået.<br>• Stikprøvekontrol af brugernes systemanvendelse. | Vi har påset at EG har tilrettelagt formaliserede processer for logning og håndtering af log-oplysninger.<br>Vi har ydermere foretaget inspektion af EG's egenkontrol af brugernes adgange til,- og anvendelse af systemerne. | Området er gennemgået uden væsentlige bemærkninger. |
| 1.23. De interne bestemmelser skal gennemgås mindst én gang hvert år med henblik på at sikre, at de er fyldestgørende og afspejler de faktiske forhold hos databehandleren.<br>(*Sikkerhedsbekendtgørelsen § 5, stk. 2).* | EG har tilrettelagt formaliserede processer, som sikrer at alle retningslinjer gennemgås mindst én gang årligt, og at ændringer til retningslinjerne dokumenteres i en log. | Vi har påset at der foreligger dokumentation for EG's it-sikkerhedspolitik, og vi har testet, at håndbogen revurderes og opdateres mindst én gang årligt. | Området er gennemgået uden væsentlige bemærkninger. |

# 4. Andre oplysninger

Det er kundernes ansvar at skabe sammenhæng mellem kravene i persondataloven og kundernes egne processer, herunder:

- At administrere egne medarbejderes adgang til de forskellige funktioner (roller),
- At tilrettelægge de kontroller omkring annullering af uddelte certifikater til fratrådte medarbejdere,
- At tilrettelægge de kontroller omkring håndtering af produktionsmiljøet hos driftsleverandøren der er nødvendige i forhold til overholdelse af persondataloven og sikkerhedsbekendtgørelsens krav.