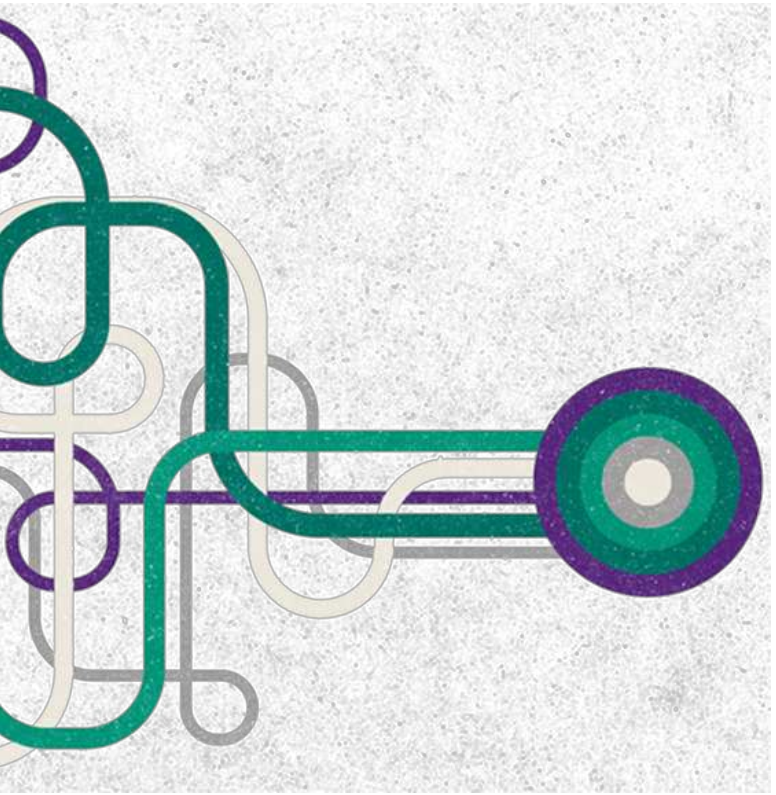
Grant Thornton

An instinct for growth™



Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftaler med kunder pr. 5. november 2019

Epinion P/S

CVR-nr.: 25 63 86 70

Indholdsfortegnelse

Symbol

- Vores gennemgang har ikke ført til bemærkninger.
- Der er konstateret enkelte svagheder.
- Der er fundet væsentlige svagheder eller mangler.

1. Ledelsens udtalelse

Epinion P/S varetager databehandling af personoplysninger for vores kunder, der er dataansvarlige i henhold til EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesforordningen") og "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesloven").

Medfølgende beskrivelse er udarbejdet til brug for dataansvarlige, der har anvendt Epinion P/S' markedsanalyser og meningsmålinger, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen og databeskyttelsesloven er overholdt.

Epinion P/S bekræfter, at:

a) Den medfølgende beskrivelse, side 7-10, giver en retvisende beskrivelse af Epinions ydelse omfattende markedsanalyser og meningsmålinger, hvor der er behandlet personoplysninger for dataansvarlige, som er omfattet af databeskyttelsesforordningen og databeskyttelsesloven d. 5. november 2019. Kriterierne der er anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   i. redegør for, hvordan markedsanalyser og meningsmålinger 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 persondata 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.
      - Kontroller, som vi med henvisning til markedsanalysers og meningsmålingers udformning har forudsat ville være implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen.
      - Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger.

1. Ledelsens udtalelse (fortsat)

ii. indeholder relevante oplysninger om ændringer i databehandlerens ydelse i form af markedsanalyser og meningsmålinger til behandling af personoplysninger foretaget d. 5. november 2019.

iii. ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne markedsanalyser og meningsmålinger til behandling af personoplysninger under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og derfor ikke kan omfatte ethvert aspekt ved Epinions markedsanalyser og meningsmålinger, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt d. 5. november 2019. Kriterierne som er anvendt for at give denne udtalelse var, at:

i. de risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret

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

iii. kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse d. 5. november 2019.

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.

København, 3 december 2019
Ryesgade 3 F, 3. sal,
2200 København N
CVR-nr: 25 63 86 70

Berit Hoelgaard Didriksen
Adm. Direktør

2. Uafhængig revisors ISAE 3000-erklæring

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftaler med Epinion P/S' kunder.

Til: Epinion P/S og deres kunder

Omfang

Vi har fået som opgave at afgive erklæring om Epinion P/S' beskrivelse på side 7-10 af sin ydelse i form af markedsanalyser og meningsmålinger til behandling af personoplysninger på vegne af dataansvarlige omfattet af EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesforordningen") og "Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesloven") d. 5. november 2019 (beskrivelsen) og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Epinion P/S' ansvar

Epinion P/S er ansvarlig for udarbejdelsen af udtalelsen på side 3-4 samt den tilhørende beskrivelsen på side 7-10, 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 og implementere 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.

Grant Thornton 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 Epinion P/S' beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000, Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger og yderligere krav ifølge dansk revisorlovgivning. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af sin ydelse vedr. markedsanalyser og meningsmålinger samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af 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 anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte mål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet på side 7-10.

2. Uafhængig revisors ISAE 3000-erklæring (fortsat)

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

Begrænsninger i kontroller hos en dataansvarlig

Epinion P/S' beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved markedsanalyser og meningsmålinger, som hver enkelt dataansvarlig måtte anse for vigtige efter deres særlige forhold. Endvidere vil kontroller hos en databehandler som følge af deres art muligvis ikke forhindre eller opdage alle brud på persondatasikkerheden. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en databehandler kan blive utilstrækkelige eller svigte.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i ledelsens udtalelse. Det er vores opfattelse,

a) at beskrivelsen af ydelse vedr. markedsanalyser og meningsmålinger således som denne var udformet og implementeret d. 5. november 2019, i alle væsentlige henseender er retvisende, og

b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet d. 5. november 2019 og

c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt d. 5. november 2019.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultater af disse tests fremgår på side 12-38.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller på side 12-38 er udelukkende tiltænkt dataansvarlige, der har anvendt Epinion P/S' markedsanalyser og meningsmålinger, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen er overholdt.

København, 3 december 2019

Grant Thornton
Statsautoriserede revisionspartnerselskab
CVR-nr. 34 20 99 36

Jacob Helly Juell-Hansen
Statsautoriseret revisor

Anders Grønning-Kjærgaard
Director, Head of IT Audit & Advisory

3. Systembeskrivelse

3.1 Beskrivelse Epinion

Epinion er etableret i 1999 med det hovedformål at levere værdiskabende strategisk beslutningsinformation ved brug af nyeste teknologi gennem kombineret kvalitativ- og kvantitativ metode. Sidenhen har virksomheden vokset sig stor, og er i dag en ledende spiller indenfor management insights og markeds research. Epinion er internationalt funderet og beskæftiger i dag ca. 170 fastansatte og 500 deltidsansatte, og har afdelinger i København, Århus, Stavanger og seks øvrige lokationer rundt omkring i verden.

Epinion leverer *sense-making* i form af rådgivning gennem forretningsindsigter til institutioner og private virksomheder. I den forbindelse opbevarer og behandler Epinion persondata, og i nogle tilfælde følsomme personoplysninger på kunder. Oplysningerne kan tilkomme Epinion ad flere forskellige kanaler såsom paneler, e-mail, e-Boks, telefonsamtale ved callcentre eller almindelig post. Oplysningerne bliver efterbehandlet i virksomhedens forretningsenheder (Business Units/BU) af konsulenter, der er tildelt relevante systemadgange efter leders godkendelse. Epinion har etableret en række forretningsgangsbeskrivelser, instrukser, samtykker samt databehandleraftaler, som skal sikre, at kundernes data behandles med en høj grad af fortrolighed og integritet.

Organisering af persondatasikkerhed

Epinion etablerede et persondataudvalg i starten af 2018 med den administrerende direktør som primær ansvarlig for etablering af GDPR-fokus og compliance til det nye regelsæt. Fokus har været på at sikre en professionel og rettidig behandling af det, som udgør Epinions eksistensgrundlag - nemlig persondata. I første halvår af 2018 var fokus på at rydde op i persondata, samt at undervise forretningen i GDPR og nye arbejdsgange. Nye systemer og procedurer blev defineret og kommunikeret for effektivt og på systemunderstøttet vis, at kunne håndtere de nye krav i EU's 'General Data Protection Regulation' (EU GDPR) forordning, der trådte i kraft 25. maj 2018.

Epinion har udpeget en dedikeret DPO (databeskyttelsesrådgiver), som ligeledes er single-point-of-contact for alle eksterne GDPR-henvendelser. Det overordnede ansvar for compliance til GDPR-forordningen ligger ved driftsdirektøren (Operations Director), som er en del af ledelsen i Epinion - også kaldet General Management Team (GMT).

Det var således udvalgets opgave at udarbejde, implementere og kontrollere interne procedurer og databeskyttende politikker. Epinions nøgledokumenter, som er produkter af udvalgets arbejde, består bl.a. i informationssikkerhedspolitikken og informationssikkerhedshåndbogen.

3. Systembeskrivelse

3.2 IT og infrastruktur

Epinion anvender en hosted cloud infrastruktur til opbevaring og drift af sine systemer. Epinion anvender den cloud baserede løsning til lagring og udveksling af data, der bl.a. sikrer løbende backup, så filer og data kan genskabes i tilfælde af nedbrud. Tilsvarende gemmes logfiler, så der er transparens i forhold til hvem der arbejder med data, f.eks. i tilfælde af databrud. Løsningen giver også mulighed for at anvende 2-faktor validering i udvekslingen af data med eksterne, herunder kunder, således at det sikres, at kun navngivne parter får adgang til data.

Adgangsrettigheder til IT-systemer, databaser, netværk mv. tildeles ud fra et arbejdsbetinget behov, samt under hensyntagen til lovgivningsmæssige og kontraktlige forpligtelser. Epinion har begrænset brugen af administrative konti, og der anvendes alene individuelle bruger-id'er og adgangskoder. For at begrænse adgangen til persondata og faciliteter, der behandler persondata, skal alle anmodninger om adgang til den dataansvarliges data godkendes af den dataansvarlige. Effektuering (oprettelse) af korrekt adgang sker hos Epinions IT-afdeling. Når en medarbejder med tildelt adgang fratræder eller ikke længere har et arbejdsbetinget behov for adgangen slettes denne.

Hvis Epinion har behov for at foretage transmission af persondata, skal det foregå krypteret, herunder hvis data transmitteres på fysiske harddiske, FTP-servere eller tilsvarende, eller sendes som e-mail. Epinion har en løsning til at sende persondata via e-mail med sikker post, hvorunder det ligeledes er muligt at sende e-mail via e-Boks. Der er dertil implementeret krav om, at flytbare enheder som udgangspunkt ikke skal benyttes til transmission af data. Evt. ekstraordinær brug af USB til datatransmission skal gå via IT, der sikrer kryptering, hvis data skal forlade Epinions lokaler.

I efteråret 2018 gennemførte Epinion anden bølge PC-standardisering, hvor alle Epinions ansatte fik nye PC'er. Det har givet mulighed for at designe et image (tilladte programmer, rettigheder) centralt fra IT i et sikkerhedsmæssigt GDPR-perspektiv med fokus på at skabe endnu mere ensartede brugerprofiler og systemer på tværs af Epinion, herunder sikring af PC'er i tilfælde af tab via kryptering. Adgang til kunders data må nu kun ske fra det arbejdsgiverudleveret udstyr, og eventuelle ønsker om brug af særligt hard- eller software skal godkendes af IT forud for installation.

Endeligt har Epinion implementeret firewalls, som overvåges af en ekstern udbyder af IT-sikkerhed, og beskytter data fra udefrakommende. Klienter og servere er herudover beskyttet med anti-virus. Epinion bruger desuden optimeringssoftware til at installere og opdatere alle computere på netværket fra centralt hold. Dette sikrer, at alle computere er opdaterede, samt at alt software er i samme version. Der er opsat krav til stærke adgangskoder, og alle systemejere og medarbejdere er gjort bekendt med dette.

3. Systembeskrivelse

3.3 Medarbejdere og projekter

Alle udførende konsulenter har kompetencer inden for de områder, de beskæftiger sig med. Dette er dokumenteret ved hjælp af uddannelsespapirer, kursusbeviser, certificeringer o. lign. Baggrunds- eller verifikationskontrol udføres på personale (medarbejdere), når det er relevant og tilladt i henhold til lokale love.

Personale er forpligtet til at læse og acceptere adfærdskodeks og fortrolighedserklæring under on-boarding processen. Træning i GDPR-processer og procedurer udføres ved ansættelse for alt personale, og der laves obligatorisk GDPR-refresh træning halvårligt på kvartalsmøder, samt årlig gennemførsel af en beredskabsøvelse med fokus på bl.a. informationssikkerhed.

Alle konsulenter er instrueret i at gøre sig løbende overvejelser om databeskyttelse gennem dataminimering, pseudonymisering og anonymisering så vidt muligt. De er ligeledes instrueret i, hvordan man sikrer korrekt udveksling af data via cloudløsningen, samt at minimere brugen af flytbare enheder til datatransmission.

Alt personale (både konsulenter og interviewere) er forpligtet til at holde al viden om kunder og kunders forhold fortrolige; både under og efter projektets afslutning. Dette fremgår både af Epinions personalehåndbog og af de enkelte medarbejderes ansættelseskontrakter. Tavshedspligten gælder for alt materiale og viden, som er kommet Epinion i hænde i projektforløbet, med mindre andet aftales eksplicit med kunden; f.eks. at Epinion har lov til at anvende kunden som reference.

For de forretningsområder hvor det giver mening, er det muligt at opsætte adgangsbegrænsning på mappe-niveau, så der alene er adgang til persondata for kundeansvarlige og konsulenter, der arbejder på det konkrete projekt. Det er projektlederens pligt at sikre, at kun relevante personer internt og evt. eksternt har adgang til data. Adgangsbegrænsningen ophæves tidligst, når projektet er overleveret til kunden og data er anonymiseret eller slettet.

Epinion har implementeret en række procedurer for opbevaring af data, herunder sletning/anonymisering eller tilbagelevering ved afslutning af projekt. Der gennemføres kontinuerligt kontrol af at data slettes inden for de fastsatte tidsfrister samt sikres, at der følges op på projekter, som har overskredet tidsfristen.

3.4 Fysisk sikkerhed

Der er alene adgang til Epinions fysiske kontorer via en bemandet reception. Gæster må kun forlade receptionsområdet under ledsagelse af en ansat fra Epinion. Alle medarbejdere er instrueret i at stoppe eventuelle uledsagede gæster, og hjælpe dem med at finde den rette kontaktperson eller forlade Epinions lokaler. Den sidste Epinion medarbejder, der forlader kontoret om aftenen, skal sikre sig, at alle vinduer er lukkede, og at alarmen aktiveres.

3.5 Styring af informationssikkerhedshændelser og brud

Der er udarbejdet procedurebeskrivelser for forskellige typer af hændelser, der kan have indflydelse på sikkerheden. Alle medarbejdere er orienteret om, at hændelser hurtigst muligt skal indrapporteres til ledelsen, samt hvordan dette skal gøres. Det er ledelsens ansvar at definere og koordinere processen, som skal sikre en passende reaktion.

3.6 Brug af underleverandører

Epinion sikrer, at der foreligger en databehandleraftale og lovligt grundlag for databehandling med relevant(e) underdatabehandler(e), og at disse kan dokumentere et passende teknisk og organisatorisk sikkerhedsniveau, herunder, at der er implementeret passende procedurer og kontroller, for således at overholde de i aftalerne stillede krav til informationssikkerhed.

Underleverandører er underlagt tavshedsforpligtelser tilsvarende den Epinions medarbejdere selv er underlagt.

3. Systembeskrivelse

3.7 Compliance og kontrol setup

Epinions informationssikkerheds-setup er beskrevet i privatlivspolitikken samt i informationssikkerhedspolitik og -håndbog med tilhørende procedurer, vejledninger og kontroller. Heri er fastlagt roller og ansvar i forhold til informationssikkerhed for alle i Epinions organisation.

Al dokumentation er systemunderstøttet for på bedste vis at organisere, registrere og analysere vores IT-sikkerhedsframework og compliance, herunder i forhold til efterlevelse af relevant dansk og international lovgivning.

Der gennemføres månedlige, kvartalsvise og årlige kontroller af vores compliance med informationssikkerhedsframeworket og som er vurderet relevante for at imødekomme kontrolmålene i persondataforordningen og databeskyttelsesloven. Kontrollerne er opdelt i 4 hovedområder; (1) den overordnede GDPR-compliance, (2) informationssikkerheds compliance, (3) data processering i projekter og endeligt (4) specifik test af IT-sikkerheden. Resultatet af kontrollerne forelægges Epinions ledelse.

Epinions DPO varetager løbende kvalitetssikring og kontrollerer Epinions interne procedurer, samt sikrer datasubjekternes rettigheder.

3.8 Risikostyring

Det er Epinions politik, at der mindst en gang årligt skal gennemføres en risikovurdering af de arbejdsprocesser, systemer og underdatabehandlere, som anvendes i behandling af personoplysninger. Ligeledes sker der årlig opdatering af privatlivspolitikken på Epinions eksterne hjemmeside, samt af det interne nøgledokument; personalehåndbogen.

Der er indarbejdet faste procedurer, som skal sikre et acceptabelt niveau, og det er driftsdirektørens ansvar i samråd med den øvrige ledelse (GMT), at sikre dette.

3.9 Komplementerende kontroller hos de dataansvarlige

Den dataansvarlige har ansvar for følgende komplementerende kontroller:

- 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 databehandleraftale og hovedydelse

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Den følgende oversigt er udformet for at skabe en forståelse for effektiviteten af de kontroller, som Epinion har implementeret. Vores test af funktionaliteten har omfattet de kontroller, som vi har vurderet nødvendige for at kunne opnå en høj grad af sikkerhed for, at de anførte kontrolmål har været nået d. 5. november 2019.

Vi har således ikke nødvendigvis testet alle de kontroller, som Epinion har nævnt i sin beskrivelse på side 7-10. Kontroller udført hos Epinions kunder er herudover ikke omfattet af vores erklæring, idet kundernes egne revisorer må foretage denne gennemgang og vurdering.

Beskrivelse og resultat af vores tests ud fra de testede kontroller fremgår af de efterfølgende skemaer. I det omfang vi har konstateret væsentlige svagheder i kontrolmiljøet eller afvigelser herfra, har vi anført dette.

Vi har udført vores tests af kontroller hos Epinion ud fra nedenstående metoder:

Metode	Overordnet beskrivelse
Forespørgelse	Interview af udvalgte medarbejdere angående kontroller
Observation	Observation af hvordan kontroller udførelse (Design)
Inspektion	Gennemgang af politikker, procedurer og dokumentation af kontrollernes udførelse (Implementering)
Test af kontrol	Gennemførelse af kontrolhandlinger, som vi selv har udført eller som har observeret gennemført af ansvarlige medarbejdere (Udførelse)

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Efterlevelse af instruks (kontrolmål A)

Kontrolmål:

Der efterleves procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger efterleves i overensstemmelse med den indgåede 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.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
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. Inspiceret ved en stikprøve på seks behandlinger af personoplysninger, at disse foregår i overensstemmelse med instruks.	Der er fundet enkelte svagheder, se D.2.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Efterlevelse af instruks (kontrolmål A) - fortsat

Kontrolmål:

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

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
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. Inspiceret, at den dataansvarlige er underrettet i tilfælde, hvor behandlingen af personoplysninger er vurderet i strid med lovgivningen.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Tekniske foranstaltninger (kontrolmål B)

Kontrolmål:

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 seks databehandler-aftaler, at der er etableret de aftalte sikringsforanstaltninger.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
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.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Tekniske foranstaltninger (kontrolmål B) – fortsat

Kontrolmål:

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.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.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall. Inspiceret, at firewall er konfigureret i henhold til intern politik herfor.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
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. Inspiceret netværksdiagrammer og anden net-værksdokumentation for at sikre behørig segmentering.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Tekniske foranstaltninger (kontrolmål B) – fortsat

Kontrolmål:

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.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. Vi har inspiceret brugeradgang til tre forskellige projekter samt gennemgået 44 brugere med adgang til SharePoint sider for to Business Units, og set at disse er begrænset til medarbejdere med et arbejdsbetingede behov.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
B.7	Der er for de systemer og databaser, der anvendes til at sende personoplysninger, er etableret systemovervågning.	Inspiceret, at der for systemer og databaser, der anvendes til at sende personoplysning, er etableret systemovervågning.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Tekniske foranstaltninger (kontrolmål B) – fortsat

Kontrolmål:

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.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 stærk kryptering baseret på en anerkendt algoritme. Inspiceret, at teknologiske løsninger til kryptering er tilgængelige og aktiveret på erklæringstidspunktet. Inspiceret, at der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet eller med e-mail. Forespurgt, om der har været ukrypterede transmissioner af følsomme og fortrolige personoplysninger på erklæringstidspunktet, samt om de dataansvarlige er behørigt orienteret herom.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Tekniske foranstaltninger (kontrolmål B) – fortsat

Kontrolmål:

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.9	Der er etableret logning i systemer, databaser og netværk af følende forhold: • Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder • Sikkerhedshændelser omfattende: o Ændringer i logopsætninger, herunder deaktivering af logning. o Ændringer i systemrettigheder til brugere. o Fejlede forsøg på log-on til systemer, databaser og netværk. Logoplysninger er beskyttet mod manipulation og tekniske fejl.	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. Inspiceret, at logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, er konfigureret og aktiveret. Inspiceret, at opsamlede oplysninger om bruger-aktivitet i logs er beskyttet mod manipulation og sletning. Inspiceret at logfiler har det forventede indhold i forhold til opsætning, og at der er dokumentation for den foretagne opfølgning og håndtering af evt. sikkerhedshændelser. Inspiceret at der er dokumentation for den foretagne opfølgning på aktiviteter udført af systemadministratorer og andre med særlige rettigheder.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Tekniske foranstaltninger (kontrolmål B) – fortsat

Kontrolmål: **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.10	Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af personoplysninger til udvikling, test og lignende, der sikrer, at anvendelsen alene sker i pseudonymiseret eller anonymiseret form. Inspiceret ved en stikprøve på to projekter, at data anonymiseres inden aflevering til kunde og ved overførsel til 'Knowledge Bank'. Inspiceret at der laves løbende kontrol på sletning i SPSSD og i 'Knowledge Bank.'	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Tekniske foranstaltninger (kontrolmål B) – fortsat

Kontrolmål: **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.11	De etablerede tekniske foranstaltninger evalueres løbende.	Inspiceret, at der foretages løbende evaluering af tekniske foranstaltninger ifm. risikovurdering. Inspiceret at der er dokumentation for løbende tests af de etablerede tekniske foranstaltninger. Inspiceret, at evt. afvigelser og svagheder i de tekniske foranstaltninger er rettidigt og betryggende håndteret samt meddelt de dataansvarlige i behørigt omfang.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
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 sikkerheds-patches.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Tekniske foranstaltninger (kontrolmål B) – fortsat

Kontrolmål: **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.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 brugeradgang til tre forskellige projekter samt gennemgået 44 brugere med adgang til SharePoint sider for to Business Units, og set at disse er begrænset til medarbejdere med et arbejdsbetingede behov. Inspiceret liste over fratrådte medarbejdere, at disses adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt. Inspiceret, at der er løbende vurdering og godkendelse af tildelte brugeradgange.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
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 det er muligt at implementere to-faktor autentifikation anvendes ved behandling af personoplysninger, der medfører højrisiko for de registrerede.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Tekniske foranstaltninger (kontrolmål B) – fortsat

Kontrolmål: **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.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. Inspiceret dokumentation for, at kun autoriserede personer har haft fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Organisatoriske foranstaltninger (kontrolmål C)

Kontrolmål:

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.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
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 6 databehandler-aftaler, at kravene i aftalerne er dækket af informationssikkerhedspolitikkens krav til sikringsforanstaltninger og behandlingssikkerheden.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Organisatoriske foranstaltninger (kontrolmål C) - fortsat

Kontrolmål: **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.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: • Straffeattest	Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Inspiceret ved en stikprøve på 6 databehandleraftaler, at kravene til efterprøvning af medarbejdere i aftalerne er dækket af databehandlerens procedurer for efterprøvning. Inspiceret at der er dokumentation for, at efterprøvningen har omfattet straffeattest.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Organisatoriske foranstaltninger (kontrolmål C) - fortsat

Kontrolmål:

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.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 der indgår tavshedspligt i standard medarbejderkontrakter. Inspiceret at medarbejdere er blevet introduceret til: - Informationssikkerhedspolitikken -Procedurer vedrørende databehandling, samt anden relevant information.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages Inspiceret ved en stikprøve på 2 fratrådte medarbejdere, at rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget.	Vores gennemgang har ikke først til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Organisatoriske foranstaltninger (kontrolmål C) - fortsat

Kontrolmål:

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.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. Inspiceret ved en stikprøve på en fratrådte i erklæringsperioden samt tjekliste over fratrædelser, at der er dokumentation for opretholdelse af fortrolighedsaftale og generel tavshedspligt.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
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.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Sletning eller tilbagelevering af personoplysninger (kontrolmål D)

Kontrolmål:

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.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
D.2	Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner: Databehandleren har opsat specifikke krav for hvor længe personhenførbare oplysninger gemmes uagtet kundens ønsker. • Udgangspunkt for alle projekter er, at data slettes / anonymiseres efter 3 måneder. • For kunder, der ønsker længere opbevaring, anføres dette i databehandleraftalen eller hovedaftalen.	Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner. Inspiceret ved en stikprøve på 3 databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder. Inspiceret behandlingsaktiviteter i SPSSD, at der er dokumentation for, at personoplysninger er slettet i overensstemmelse med de aftalte sletterutiner.	Vi har observeret, at der på erklæringstidspunktet var 29 projekter, hvor data ikke er slettet i SPSSD tre måneder efter projektafslutning. Vores gennemgang har ikke ført til yderligere væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Sletning eller tilbagelevering af personoplysninger (kontrolmål D) - fortsat

Kontrolmål:

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.3	Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: • Tilbageleveret til den dataansvarlige og/eller • Slettet, hvor det ikke er i modstrid med anden lovgivning.	Inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger. Inspiceret ved en stikprøve på 5 ophørte databehandlinger, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Opbevaring af personoplysninger (kontrolmål E)

Kontrolmål:

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. Inspiceret ved en stikprøve på 6 databehandlinger, at der er dokumentation for, at databehandlingen sker i henhold til databehandleraftalen.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder. Inspiceret ved en stikprøve på 6 databehandlinger, 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.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Brug af underdatabehandlere (kontrolmål F)

Kontrolmål:

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.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
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 6 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.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underretters den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Inspiceret dokumentation for, at den dataansvarlige er underrettet ved ændring i anvendelse af underdatabehandlerne.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Brug af underdatabehandlere (kontrolmål F) - fortsat

Kontrolmål:

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.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i data-behandleraftalen el.lign. med den dataansvarlige.	Inspiceret, at der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af databehandlerens oversigt. Inspiceret ved en stikprøve på 3 underdatabehandleraftaler, at disse indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
F.5	Databehandleren har en oversigt over godkendte underdata-behandlere med angivelse af: • Navn • CVR-nr. • Adresse • Beskrivelse af behandlingen	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Brug af underdatabehandlere (kontrolmål F) - fortsat

Kontrolmål:

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.6	Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.	Inspiceret, at der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne. Inspiceret dokumentation for, at der er foretaget en risikovurdering af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne. Inspiceret dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerheden hos de anvendte underdatabehandlere, tredjelands overførselsgrundlag og lignende. Inspiceret dokumentation for, at information om opfølgning hos underdatabehandlere meddeles den dataansvarlige, således at denne kan tilrettelægge eventuelt tilsyn.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Overførsel til tredjelande (kontrolmål G)

Kontrolmål:

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. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at personoplysninger alene overføres til tredjelande eller internationale organisationer i henhold til aftale med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Inspiceret, at procedurerne er opdateret.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
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. Inspiceret ved en stikprøve på 6 dataoverførsler, at der er dokumentation for, at overførslen er aftalt med den dataansvarlige i databehandleraftalen eller senere godkendt.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Overførsel til tredjelande (kontrolmål G) - fortsat

Kontrolmål:

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.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. Inspiceret, at procedurerne er opdateret. Inspiceret at der er dokumentation for et gyldigt overførselsgrundlag i databehandleraftalen med den dataansvarlige, samt at der kun er sket overførsler, i det omfang dette er aftalt med den dataansvarlige.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Udlevering, rettelse, sletning og begrænsning af personoplysninger (kontrolmål H)

Kontrolmål:

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.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
H.2	Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	Inspiceret, at de foreliggende procedurer for bistand til den dataansvarlige indeholder detaljerede procedurer for: • Udlevering af oplysninger • Rettelse af oplysninger • Sletning af oplysninger • Begrænsning af behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede. Inspiceret, at dokumentation for anmodninger om bistand fra den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede er korrekt og rettidigt gennemført.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Håndtering af sikkerhedsbrud (kontrolmål I)

Kontrolmål:

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.	Vores gennemgang har ikke ført til væsentlige bemærkninger.
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. Inspiceret dokumentation for, at der er taget stilling til overvågning af netværkstrafik. Inspiceret dokumentation for, at der er taget stilling til opfølgning på logning af tilgang til personoplysninger.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Håndtering af sikkerhedsbrud (kontrolmål I) - fortsat

Kontrolmål: **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.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. Inspiceret, at databehandleren har medtaget eventuelle brud på persondatasikkerheden hos underdatabehandlere i databehandlerens oversigt over sikkerhedshændelser. Inspiceret, at samtlige registrerede brud på persondatasikkerheden hos databehandleren eller underdatabehandlerne er meddelt de berørte dataansvarlige uden unødig forsinkelse efter, at databehandleren er blevet opmærksom på brud på persondatasikkerheden.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

Håndtering af sikkerhedsbrud (kontrolmål I) - fortsat

Kontrolmål:

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.4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	Inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede procedurer for: • Beskrivelse af karakteren af bruddet på persondatasikkerheden • Beskrivelse af sandsynlige konsekvenser af bruddet på persondatasikkerheden • Beskrivelse af foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. Inspiceret dokumentation for, at der ved brud på persondatasikkerheden er truffet foranstaltninger, som har håndteret bruddet på persondata-sikkerheden.	Vores gennemgang har ikke ført til væsentlige bemærkninger.

PENNEO

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

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

Jacob Helly Juell-Hansen
Statsautoriseret revisor
Serienummer: CVR:34209936-RID:50904197
IP: 62.243.xxx.xxx
2019-12-03 11:47:31Z
NEM ID

Berit Hoelgaard Didriksen
Underskriver
Serienummer: PID:9208-2002-2-330610175516
IP: 213.32.xxx.xxx
2019-12-03 20:09:04Z
NEM ID

Anders Grønning Kjærgaard
Revisor
Serienummer: PID:9208-2002-2-822661869402
IP: 213.32.xxx.xxx
2019-12-07 08:07:04Z
NEM ID