Energinet DataHub A/S

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til Energinet DataHub A/S' standarddatabehandleraftale med de dataansvarlige, der har anvendt DataHub

ENERGINET
DataHub

Indhold

1 Ledelsens udtalelse

Energinet DataHub A/S (Energinet) 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").

Energinet behandler personoplysninger på vegne af vores kunder i henhold til indgået databehandleraftaler.

Medfølgende beskrivelse er udarbejdet til brug for dataansvarlige, der har anvendt DataHub nævnt i sektion 3, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som underleverandører og de dataansvarlige selv har udført ved vurdering af, om kravene i EU's databeskyttelsesforordning er overholdt.

Energinet anvender CGI til driftsunderstøttelse af DataHub. Beskrivelsen i sektion 3 medtager kun kontrolmål og kontrolaktiviteter hos Energinet og medtager således ikke kontrolmål og underliggende kontrolaktiviteter hos CGI. Beskrivelsen angiver også, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan nås, hvis underleverandørers kontroller, der forudsættes i designet af vores kontroller, er passende designet og er operationelt effektive. Beskrivelsen omfatter ikke kontrolaktiviteter udført af CGI.

Beskrivelsen angiver, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan opnås, hvis komplementerende kontroller hos de dataansvarlige, der forudsættes i designet af Energinets kontroller, er passende designet og operationelt effektive. Beskrivelsen omfatter ikke kontrolaktiviteter udført af de dataansvarlige.

Energinet bekræfter, at:

a) Den medfølgende beskrivelse, sektion 3, giver en retvisende beskrivelse af DataHub, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen i hele perioden fra 1. januar til 31. december 2022. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) redegør for, hvordan DataHub var designet og implementeret, herunder redegør for:

   - De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger.
   - De processer i både it-systemer 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.
   - Ydelser udført af underleverandører, hvis relevant, herunder om de er medtaget efter helhedsmetoden eller udeladt efter partielmetoden.

- Kontroller, som vi med henvisning til DataHubs afgrænsning 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.

(ii) indeholder relevante oplysninger om ændringer i databehandlerens DataHub til behandling af personoplysninger foretaget i perioden fra 1. januar til 31. december 2022.

(iii) ikke udelader eller forvansker oplysninger, der er relevante for omfanget af beskrivelsen af DataHub 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 DataHub, 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 designet og operationelt effektive i hele perioden fra 1. januar til 31. december 2022, hvis relevante kontroller hos CGI var operationelt effektive, og kunder har udført de komplementerende kontroller, som forudsættes i designet af Energinets kontroller i hele perioden fra 1. januar til 31. december 2022. Kriterierne anvendt for at give denne udtalelse var, at:

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

(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 designet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. januar til 31. december 2022.

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.

Erritsø, den 10. februar 2023
Energinet DataHub A/S

Martin Lervad Lundø
Administrerende Direktør

2 Uafhængig revisors erklæring

2.1 Uafhængig revisors ISAE 3000-erklæring med sikkerhed om beskrivelsen af kontroller rettet mod databeskyttelse og behandling af personoplysninger

Til: Energinet og Energinets kunder, der har anvendt DataHub

Omfang

Vi har fået som opgave at afgive erklæring om Energinet DataHub A/S' (Energinet) beskrivelse i sektion 3 af DataHub til behandling af personoplysninger i henhold til Energinets standarddatabehandleraftale i hele perioden fra 1. januar til 31. december 2022 (beskrivelsen) og om designet og operationel effektivitet af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Beskrivelsen angiver, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan opnås, hvis komplementerende kontroller hos de dataansvarlige, der forudsættes i designet af Energinets kontroller, er passende designet og er operationelt effektive sammen med relaterede kontroller hos Energinet. Beskrivelsen omfatter ikke kontrolaktiviteter udført af dataansvarlige. Vi har ikke udført handlinger vedrørende operationel effektivitet af de komplementerende kontroller hos dataansvarlige, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

Energinet anvender CGI til driftsunderstøttelse af DataHub. Beskrivelsen i sektion 3 medtager kun kontrolmål og relaterede kontroller hos Energinet, og medtager således ikke kontrolmål og relaterede kontroller hos CGI. Visse kontrolmål i beskrivelsen kan kun nås, hvis CGI's kontroller, der forudsættes i designet af Energinets kontroller, er passende designet og operationelt effektive sammen med de relaterede kontroller hos Energinet. Vores handlinger har ikke omfattet kontrolaktiviteter udført af CGI, og vi har ikke vurderet egnetheden af design eller den operationelle effektivitet af kontrolaktiviteter hos CGI.

Energinets ansvar

Energinet er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i sektion 1, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter; for at anføre kontrolmålene; identifikation af de risici, der påvirker opnåelsen af kontrolmålene; udvælgelsen af de kriterier, der er præsenteret i ledelsens udtalelse; samt for at designe, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i International Ethics Standards Board for Accountants' internationale retningslinjer for revisorers etiske adfærd (IESBA Code), der bygger på de grundlæggende principper om integritet, objektivitet, professionel kompetence og fornøden omhu, fortrolighed og professionel adfærd, samt etiske krav gældende i Danmark.

EY Godkendt Revisionspartnerselskab er underlagt international standard om kvalitetsstyring, ISQC 1, og anvender således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende krav i lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Energinets beskrivelse samt om designet og operationel effektivitet 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, 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 designet og operationelt effektive.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, designet og operationel effektivitet af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af DataHub samt for kontrollernes design og operationel effektivitet. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt designet eller ikke er operationelt effektive. Vores handlinger har omfattet test af den operationelle effektivitet 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 i sektion 3.

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

Energinets beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved DataHub, 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 den operationelle effektivitet 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 ledelsesudtalelse. Det er vores opfattelse:

a) at beskrivelsen af DataHub, således som denne var designet og implementeret i hele perioden fra 1. januar til 31. december 2022, 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 designet i hele perioden fra 1. januar til 31. december 2022, hvis kontroller hos CGI var hensigtsmæssigt designet, og hvis dataansvarlige har designet og implementeret de komplementerende kontroller, der forudsættes i designet af Energinets kontroller i hele perioden fra 1. januar til 31. december 2022, 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 været operationelt effektive i hele perioden fra 1. januar til 31. december 2022, hvis kontroller hos CGI var operationelt effektive, og hvis de komplementerende kontroller hos dataansvarlige, der forudsættes i designet af Energinets kontroller, har været operationelt effektive i hele perioden fra 1. januar til 31. december 2022.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultater af disse test fremgår i sektion 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i sektion 4 er udelukkende tiltænkt dataansvarlige, der har anvendt Energinet, 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, den 10. februar 2023
EY Godkendt Revisionspartnerselskab
CVR-nr.: 30 70 02 28

Jesper Due Sørensen
Partner

Nils B Christiansen
statsaut. Revisor
mne34106

3 Systembeskrivelse

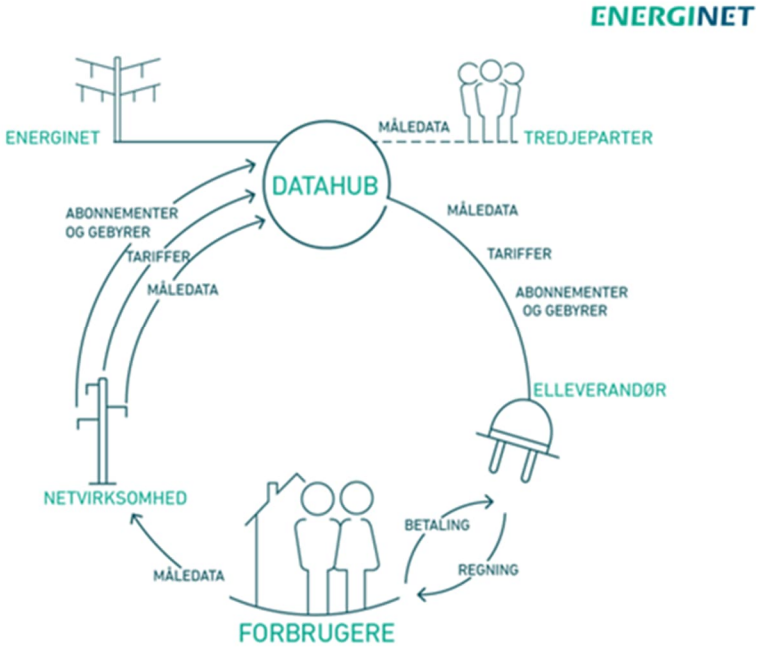
Beskrivelse af databehandling i DataHub.

3.1 Indledning og omfang

Energinet DataHub A/S ejer og driver DataHub-systemet (herefter DataHub). Behandling af data i DataHub sker som udgangspunkt for at understøtte efterlevelsen af el-forsyningsloven samt kravene udformet i Energinet DataHub A/S' databehandleraftale, der er indgået med elleverandørerne og netvirksomhederne. Energinet DataHub A/S' databehandleraftale-skabelon indgår som bilag 1 i aftalen "Vilkår for adgang til og brug af DataHub".

3.1.1 Beskrivelse af aktørernes ansvar og typer af data

Alle aktører, som kommunikerer med DataHub, har ansvar for, at de data, de sender til DataHub, er korrekte og opdaterede.



Elleverandørerne har ansvaret for de kunderelaterede stamdata; eksempelvis kundernes navne og kontaktadresser.

Netvirksomhederne har ansvaret for de målepunktsrelaterede stamdata, som f.eks. målepunkts-id og netområdenummer, samt for at den samlede indsendelse af måledata er komplet.

Energinet og aktørerne har et delt ansvar for de engrosrelaterede stamdata:

- Netvirksomheden er ansvarlig for oprettelse og tilknytning til egne priselementer, som f.eks. distributionstarif og abonnement,
- Energinet er ansvarlig for opdatering af prisen på egne tariffer samt elafgift,
- Elleverandøren er ansvarlig for korrekt tilknytning af Energinets priselementer, jf. Forskrift H3 – herunder korrekt tilknytning til elafgift. Energinet har indført supplerende kontroller herfor.

Det er de danske markedsaktører – elleverandører og netvirksomheder – der er ansvarlige for korrektheden af de personoplysninger, der er i DataHub. Dette indebærer således, at elleverandøren er ansvarlig for kundestamdata, dvs. kundernes navne og kontaktadresser, mens netvirksomheden er ansvarlig for målepunktsstamdata, som i forbindelse med nogle af markedsprocesserne formidles mellem markedets aktører gennem DataHub.

Generelt er Energinet DataHub A/S selvstændig dataansvarlig i forhold til DataHub, men i forbindelse med processer på specifikke områder er Energinet databehandler på vegne af den dataansvarlige aktør.

3.2 Hvornår er Energinet DataHub A/S databehandler i DataHub?

Energinet DataHub A/S formidler data i henhold til processer beskrevet i forskrifter udstedt af Energinet ved den dataansvarliges anmeldelse af:

- BRS-002: Leveranceophør, undtaget er dog RSM-021 i relation til BRS-002, hvor Energinet Datahub A/S i enkelte tilfælde er dataansvarlig.
- BRS-016: Fremsend forventet årsforbrug - elleverandør.
- BRS-039: Anmodning om serviceydelse hos netvirksomhed.
- BRS-044: Tvunget leverandørskifte på målepunkt, når den dataansvarlige instruerer databehandleren i at gøre brug af BRS-044 ved fusion af 2 af den dataansvarliges GLN-numre.
- BRS-046: Fremsendelse af kontaktadresse fra netvirksomhed.

Energinet DataHub A/S agerer ligeledes databehandler i forbindelse med webforms sendt fra den dataansvarlige gennem DataHub til en anden bruger af DataHub, samt i forbindelse med rettelser af oplysninger i DataHub efter indsendelse fra aktøren (HTX) – dog udelukkende efter aftale med den dataansvarlige og på dennes foranledning.

3.3 Hvordan behandler Energinet DataHub A/S data?

Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, herunder for så vidt angår overførsel (overladelse, videregivelse samt intern anvendelse) af personoplysninger til tredjelande eller internationale organisationer, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt, jf. aktørdatabehandleraftalen; i så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

Behandling af de i aftalen omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end de følgende:

- Energinet DataHub A/S, lokation Danmark, CVR-nr. 39 31 50 41
- CGI Danmark A/S, lokation Danmark, CVR-nr. DK-28980671
- CGI Holland, lokation Holland, CVR-nr. NL001620952B01
- CGI Norge, lokation Norge, NO919562390CGI Sverige, SE556337219101
- Sentia A/S, lokation Danmark, CVR-nr. DK-10008123 (Underleverandør til CGI – Sentia A/S er ikke omfattet af nærværende erklæring).

Energinet DataHub A/S 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.

Energinet DataHub A/S sikrer, at kun de personer, der, på baggrund af et arbejdsbetinget behov, aktuelt er autoriseret hertil, har adgang til de personoplysninger, der behandles på vegne af den dataansvarlige. Adgangen til oplysningerne lukkes derfor straks ned, hvis autorisationen fratages eller udløber.

Der må således alene autoriseres personer, for hvem det er nødvendigt at have adgang til personoplysningerne for at kunne opfylde databehandlerens forpligtelser over for den dataansvarlige.

Energinet DataHub A/S sikrer, at de personer, der er autoriseret til at behandle personoplysninger på vegne af den dataansvarlige, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt, jf. bl.a. forvaltningslovens § 27.

Energinet DataHub A/S kan efter anmodning fra den dataansvarlige påvise, at de relevante medarbejdere er underlagt ovennævnte tavshedspligt.

Energinet DataHub A/S iværksætter alle de relevante tekniske og organisatoriske kontrolforanstaltninger, som kræves i henhold til databeskyttelsesforordningen. Der henvises i øvrigt til kontrolmål B og C i nærværende erklæring afsnit 4, hvor de konkrete kontrolaktiviteter er beskrevet, og hvoraf det bl.a. fremgår, at der under hensyntagen til det aktuelle niveau, implementeringsomkostningerne og den pågældende behandlingskarakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder skal gennemføres passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.

Ovenstående forpligtelse indebærer, at Energinet DataHub A/S skal foretage en risikovurdering, og herefter gennemføre foranstaltninger for at imødegå og dermed nedbringe de identificerede risici.

3.4 Hvilke krav er gældende ved brug af underdatabehandlere?

Energinet DataHub A/S har den dataansvarliges generelle godkendelse til at gøre brug af underdatabehandlere. Energinet DataHub A/S skal dog indhente godkendelse hos den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre underdatabehandlere, og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer. En sådan underretning skal være den dataansvarlige i hænde minimum én måned før anvendelsen eller ændringen skal træde i kraft. Såfremt den dataansvarlige har indsigelser mod ændringerne, skal den dataansvarlige give meddelelse herom til Energinet DataHub A/S inden 14 kalenderdage efter modtagelsen af underretningen. Den dataansvarlige kan alene gøre indsigelse, såfremt den dataansvarlige har rimelige, konkrete årsager hertil.

3.5 Hvordan bruger Energinet DataHub A/S underleverandører?

Energinet DataHub A/S har outsourcet udvikling og vedligehold af DataHub-applikationen til CGI. Der foreligger kontrakter og operationelt framework, som er grundlaget for samarbejdet mellem Energinet DataHub A/S og CGI. Det er reguleret via hovedkontrakten pkt. 5.8, i hvilket omfang og under hvilke betingelser CGI kan anvende underleverandører. *"Leverandøren kan ikke uden Kundens skriftlige samtykke overlade Kontraktens opfyldelse til underleverandører i videre udstrækning end angivet i Kontrakten. Kunden kan ikke nægte et sådant samtykke uden rimelig grund."*

Aftalegrundlaget for applikationsudvikling og -vedligehold er funktionelle designs og User Stories, som beskriver funktionaliteten i DataHub med udgangspunkt i BRS- og RSM-guiderne (tekniske beskrivelser af forretningsprocesserne i DataHub). Der er formelle udvalg/arbejdsgrupper i Energinet DataHub A/S, som regulerer og styrer samarbejder, bl.a. styregruppe, planning board og operational meeting.

Hosting af DataHub var i perioden fra 1. januar 2022 til 31. december 2022 outsourcet til CGI, som derved havde ansvaret for rapportering og driftsvedligehold.

CGI A/S anvender Sentia A/S som underleverandør. Sentia A/S er ikke omfattet af nærværende erklæring.

3.6 Hvilke krav om revisionserklæring er der til Energinet DataHub A/S' underleverandører?

Underleverandøren skal hvert år indhente en erklæring fra et godkendt revisionsselskab angående underleverandørens implementering af egne retningslinjer samt tilstrækkeligheden heraf, i forhold til at sikre fortrolighed, integritet og tilgængelighed om de behandlede personoplysninger. Erklæringen skal udarbejdes på grundlag af en anerkendt standard for sådanne erklæringer. Erklæringen skal sendes til Energinet DataHub A/S senest den 31. januar for det foregående år. Erklæringen skal altid bilægges en liste med observationer og væsentlighed, samt underleverandørens kommentarer og tidsfrist for udbedring. Såfremt der ingen observationer har været, skal dette fremgå eksplicit af erklæringen.

3.7 Persondatacompliance

Det er de enkelte selskaber i Energinet, der har ansvaret for at overholde reglerne om beskyttelse af personoplysninger. Dokumentationen består blandt andet af en samlet datafortegnelse over alle de databehandlinger, der foretages i Energinet. Derudover skal der udarbejdes risikovurdering på alle behandlingerne, inden de påbegyndes.

Al dokumentation skal opdateres løbende, således det altid er ajourført og klar til fremvisning for Datatilsynet. Der opsættes kontroller til sikring heraf både på afdelingsniveau og koncernniveau.

3.8 Hvordan håndteres brud på persondatasikkerheden?

Denne procedure skal følges ved brud, uanset arten af bruddet.

Brud på persondatasikkerheden håndteres lokalt i Energinet DataHub A/S i samarbejde med Energinet koncernens persondatajurist. Energinet DataHub A/S sikrer efterfølgende relevant kommunikation vedrørende sikkerhedsbrud til den dataansvarlige. Ansvaret for håndteringen af interessenter og efterfølgende information til de registrerede ligger hos Energinets persondatajurist.

3.9 Hvordan bistår Energinet DataHub A/S de dataansvarlige, og hvordan håndterer Energinet DataHub A/S henvendelser vedrørende GDPR

Teamet DataHub Support i Energinet DataHub A/S er kontaktpunkt for henvendelserne, som enten behandler henvendelsen eller videreformidler den til Energinets persondatajurist. Sagerne håndteres i det interne sagshåndteringssystem.

A) Der er fokus på, at der ikke sker en ulovlig behandling af personoplysninger. Dette vil fremgå af den enkelte sag i Energinet DataHub A/S' sagssystem.

B) Hvis en instruks fra aktøren (dataansvarlige) vurderes at være i strid med GDPR, vil Energinet DataHub A/S' support sende en underretning til aktøren (dataansvarlig) med henblik på at få afklaret dette. Alternativt vil sagen blive lukket, herefter informeres aktøren, som har henvendt sig, dette sker i selve sagen.

C) Når sagen er løst, informeres aktøren, som har henvendt sig, dette sker i selve sagen.

- Under forudsætning af punkt B er overholdt.

3.10 Risikovurdering

Energinet DataHub A/S har foretaget en risikovurdering af de konkrete databehandlinger i relation til de registreredes rettigheder, herunder en afvejning af disse risici i forhold til de forholdsregler, der er truffet for at beskytte disse rettigheder. Selve risikovurderingen består af flere dele, herunder:

- Risikovurdering i Energinet DataHub A/S' datafortegnelser.
- Risikovurdering i Energinet DataHub A/S' centrale register.
- Risikovurdering i Energinet DataHub/S' decentrale register.

I Energinet DataHub A/S' egne risikovurderinger er det vurderet, at der i forbindelse med de konkrete databehandlinger ikke er høj risiko for de registrerede på tværs af alle typer af registrerede og kategorier af personoplysninger.

3.11 Grundlag for udarbejdelse af erklæring

Nærværende erklæring dækker Energinet DataHub A/S' kontrolmål og kontroller, der er etableret for som udgangspunkt at understøtte efterlevelse af Energinet DataHub A/S' standarddatabehandleraftale.

Energinet er forpligtet til at drive DataHub, jf. elforsyningsloven § 28, stk. 2, nr. 7, og netvirksomhederne er forpligtede til at indberette til DataHub, jf. elforsyningsloven § 22, stk. 3. Aktører i DataHub er forpligtet til at overholde de til enhver tid gældende markedsforskrifter og vilkår, jf. elforsyningsloven § 28, stk. 2, nr. 12 og 13. Markedsforskrifterne er tilgængelige på www.energinet.dk.

De etablerede foranstaltninger og kontroller omfatter følgende kontrolmål:

- **Kontrolmål A**

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

- **Kontrolmål B**

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.

- **Kontrolmål C**

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.

- **Kontrolmål D**

Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres, såfremt der indgås aftale herom med den dataansvarlige.

- **Kontrolmål E**

Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.

- **Kontrolmål F**

Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.

- **Kontrolmål H**

Der efterleves procedurer og kontroller, som sikrer, at databehandleren kan bistå den dataansvarlige med udlevering, rettelse, sletning eller begrænsning af oplysninger om behandling af personoplysninger til den registrerede.

- **Kontrolmål I**

Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.

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

3.12 Komplementerende kontroller hos de dataansvarlige

Som et led i levering af ydelserne er der kontroller, som forudsættes implementeret af de dataansvarlige, og som er væsentlige for at opnå de kontrolmål, der er anført i beskrivelsen. Dette omfatter bl.a.:

- Stillingtagen til konsekvenser i relation til persondatabeskyttelse ved fremsættelse af ændringsønsker.
- Sikring af, at følsomme eller fortrolige personoplysninger ikke medsendes i supportsager eller i fritekstfelter i DataHub-systemet.
- Dataansvarlige er selv ansvarlige for at kontrollere sletteregler, inden bestillingen af kundesletning foretages.

- Dataansvarlige er selv ansvarlige for administration og overvågning af Dataansvarliges medarbejderes adgang til og anvendelse af personoplysninger.
- Dataansvarlige er selv ansvarlige for, at personoplysningerne er ajourførte.
- Dataansvarlige er selv ansvarlige for at sikre, at instruksen til Energinet DataHub A/S er lovlig set i forhold til den til enhver tid gældende persondataretlige regulering og hensigtsmæssig set i forhold til databehandleraftalen.
- Dataansvarlige er selv ansvarlige for håndtering af henvendelser fra den registrerede selv, myndigheder og evt. tredjemand samt for anmodning til Energinet DataHub A/S om rettidig assistance med denne håndtering.

Dataansvarlige er selv ansvarlige for håndtering af fysisk sikkerhed ved behandling af personoplysninger.

4 Tests udført af EY

I dette afsnit beskrives de af Energinet definerede kontrolmål og tilknyttede kontroller, som sikrer opnåelse af de enkelte kontrolmål. Herudover beskrives de af EY udførte faktiske tests af Energinets kontroller samt resultaterne af de udførte tests.

4.1 Formål og omfang

Vores arbejde blev gennemført i overensstemmelse med ISAE 3000, Andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger.

Vores test af kontrollers design og operationelle effektivitet har omfattet de kontrolmål og tilknyttede kontroller, der er udvalgt af ledelsen, og som fremgår nedenfor. Eventuelle andre kontrolmål, tilknyttede kontroller og kontroller hos Energinets kunder, der anvender løsningen, beskrevet i afsnit 1, er ikke omfattet af vores test.

Vores test af design og operationel effektivitet har omfattet de kontroller, som blev vurderet nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev nået i perioden 1. januar til 31. december 2022.

4.2 Udførte tests

De udførte tests i forbindelse med fastlæggelsen af kontrollers udformning og effektivitet er beskrevet nedenfor:

Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at blive effektive, hvis de implementeres. Endvidere vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Forespørgsler	Forespørgsel af passende personale hos Energinet. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Vi har observeret kontrollens udførelse.

Kontrolmål A

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

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Inspiceret, at procedurerne indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen. Inspiceret dokumentation for, at der er foretaget årlig vurdering af behov for opdatering af procedure.	Ingen afvigelser konstateret.
A.2	Energinet udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Inspiceret, at der er etableret procedurer for registrering af henvendelser fra kunderne til sikring af, at behandling af personoplysninger alene foregår i henhold til instruks.	Ingen afvigelser konstateret.
A.3	Energinet 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. Forespurgt, om den dataansvarlige er underrettet i tilfælde, hvor behandlingen af personoplysninger er vurderet i strid med lovgivningen.	Energinet har oplyst, at der ikke har været tilfælde, hvor behandlingen af personoplysninger er vurderet i strid med lovgivningen i perioden. Ingen afvigelser konstateret.

Kontrolmål B

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.1	Energinet sikrer, at kun de personer, der aktuelt er autoriseret hertil, har adgang til de personoplysninger, der behandles på vegne af den dataansvarlige.	Forespurgt til procedurer, der sikrer kvartalsvis gennemgang af adgange til DataHub. Stikprøvevist inspiceret, at der fortages kvartalsvis kontrol af, at adgange er begrundet i et arbejdsbetinget behov.	Ingen afvigelser konstateret.
B.2	Adgang til personoplysninger bliver kvartalsvist overvåget.	Forespurgt til procedurer vedrørende overvågning af brugere. Stikprøvevist inspiceret, at der foretages kvartalsvis kontrol af Energinets og Energistyrelsens brugeres adgangsrettigheder i DataHub.	Ingen afvigelser konstateret.
B.3	Der må alene autoriseres personer, for hvem det er nødvendigt at have adgang til personoplysningerne for at kunne opfylde Energinets forpligtelser over for den dataansvarlige.	Forespurgt til procedurer for gennemgang af adgangsrettigheder i DataHub. Stikprøvevist inspiceret, at der fortages kvartalsvis kontrol af adgangene, som er defineret i DataHub, og at disse er autoriserede.	Ingen afvigelser konstateret.
B.4	Energinet kontrollerer månedligt, at personoplysninger er anonymiseret i de non-prod DataHub-miljøer, som it-leverandører og elmarkedets aktører har adgang til.	Stikprøvevist inspiceret, at der fortages månedlig kontrol af, at personoplysninger bliver anonymiseret i DataHubs testmiljø.	Ingen afvigelser konstateret.
B.5	Energinet krypterer personoplysninger på både DataHubs produktions- og non-produktionsmiljøer.	Inspiceret, at der er anvendt kryptering på DataHubs produktions- og non-produktionsmiljøer.	Ingen afvigelser konstateret.
B.6	Energinet kontrollerer månedligt ændringer af IP-adresser i DataHubs firewalls.	Forespurgt til processen for etableret validering af dataafsender. Stikprøvevist inspiceret, at Energinet månedligt gennemgår ændringer af IP-adresser i DataHubs firewalls.	Ingen afvigelser konstateret.

Kontrolmål B

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
B.7	Energinet gennemgår månedligt driftsrapport fra underdatabehandlere vedrørende patchning af servere, firewalls og opdatering af antivirus.	Forespurgt til processen for behandlingen af driftsrapporten fra underleverandøren. Stikprøvevist inspiceret, at der er fortages månedlig kontrol af opfølgning på leverancer fra underdatabehandlere i relation til patchning af servere, firewalls og opdatering af antivirus.	Ingen afvigelser konstateret.
B.8	Energinet kontrollerer månedligt, at processer for adgangsgodkendelse til DataHub overholdes ved underdatabehandlere.	Forespurgt til processen for adgangsgodkendelse til DataHub. Stikprøvevist inspiceret, at der er fortages månedlig kontrol af gennemgang af underdatabehandleres adgang til DataHub.	Ingen afvigelser konstateret.
B.9	Energinet gennemgår månedligt driftsrapporter fra underdatabehandlere vedrørende overholdelse af SLA i forhold til kapacitetsstyring.	Forespurgt til processen for behandlingen af driftsrapporten fra underleverandøren. Stikprøvevist inspiceret, at der foretages månedlig kontrol af at SLA er overholdt i forhold til kapacitetsstyring.	Ingen afvigelser konstateret.
B.10	Energinet gennemgår kvartalsvis rapportering i forhold til udstyr, som skal sikres mod strømsvigt og andre driftsforstyrrelser.	Forespurgt til processen for styring af driftsforstyrrelser. Stikprøvevist inspiceret, at der fortages kvartalsvis kontrol af gennemgang af udstyr i DataHubs infrastruktur.	Ingen afvigelser konstateret.
B.11	Energinet afholder månedlige CAB-møder, hvor tekniske ændringer i infrastrukturen gennemgås.	Stikprøvevist inspiceret, at der afholdes månedlige CAB-møder med underleverandøren, hvor tekniske ændringer gennemgås.	Ingen afvigelser konstateret.
B.12	Energinet kontroller kvartalsvist, at applikationsændringer i DataHub-applikationen er autoriseret, testet og godkendt inden de idriftsættes i produktion.	Forespurgt til processen for, at der fortages test og godkendelse, inden idriftsættelse i produktionen. Stikprøvevist inspiceret, at der fortages kvartalsvis kontrol af gennemgang af de releases, der har	Ingen afvigelser konstateret.

Kontrolmål B

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
		været i kvartalet til sikring af, at processen omkring autorisation, test og godkendelse har været fulgt.	
B.13	Energinet afholder møder med underdatabehandler for større releases, hvor prioriteter og indhold til kommende releases gennemgås.	Inspiceret, at der afholdes møder med underleverandøren vedrørende større releases.	Ingen afvigelser konstateret.
B.14	Energinet afholder månedlige møder med underdatabehandler, hvor risici gennemgås i forhold til drift og udvikling i forhold til DataHub.	Stikprøvevist inspiceret, at der afholdes månedlige møder med underleverandøren.	Ingen afvigelser konstateret.
B.15	Energinet afholder årligt et møde med underdatabehandler for at sikre, at it-kapacitet, -availability, -kontinuitet og -sikkerhed i it-systemet er afstemt med Energinet.	Forespurgt til processen for behandlingen af driftsrapporten fra underleverandøren. Inspiceret, at der årligt afholdes et møde om SLA med underleverandøren. Inspiceret, at der fortages opfølgning på, at de aftalte KPI'er og SLA'er fortsat er aktuelle.	Ingen afvigelser konstateret.
B.16	Energinet gennemgår månedligt driftsrapporter vedrørende backup.	Forespurgt til processen for behandlingen af driftsrapporten fra underleverandøren. Stikprøvevist inspiceret, at der månedligt fortages gennemgang af backup.	Ingen afvigelser konstateret.
B.17	Energinet sikrer, at der årligt gennemføres en disaster recovery-øvelse med underdatabehandler i forhold til DataHub-systemet.	Inspiceret, at der er fortaget en årlig disaster recovery-øvelse med underdatabehandler.	Ingen afvigelser konstateret.
B.18	Energinet sikrer årligt, at beredskabsplaner er gennemgået og opdateret.	Inspiceret, at der foreligger en beredskabsplan. Inspiceret dokumentation for, at beredskabsplanen er opdateret og godkendt i erklæringsperioden.	Ingen afvigelser konstateret.

Kontrolmål C

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
C.1	Energinets 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. Inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere. Inspiceret at it-sikkerhedspolitikken er opdateret og godkendt af Energinets ledelse.	Ingen afvigelser konstateret.
C.2	Energinets ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Inspiceret, at kravene i databehandleraftalen er dækket af informationssikkerhedspolitikkens krav til sikringsforanstaltninger og behandlingssikkerheden.	Ingen afvigelser konstateret.
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: ► Eksamensbeviser	Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Stikprøvevist inspiceret, at der er indhentet eksamensbevis i forbindelse med ansættelse.	Ingen afvigelser konstateret.

Kontrolmål C

Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
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.	Stikprøvevist inspiceret, at nyansatte medarbejdere har underskrevet en fortrolighedsaftale. Stikprøvevist inspiceret, at nyansatte medarbejdere er blevet introduceret til: ► Informationssikkerhedspolitikken. ► Procedurer vedrørende databehandling samt anden relevant information.	Ingen afvigelser konstateret.
C.5	Energinet-koncernen gennemfører løbende awareness-træning af alle ansatte 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 medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awareness-træning.	Ingen afvigelser konstateret.

Kontrolmål D

Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres, såfremt der indgås aftale herom med den dataansvarlige.

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
D.1	Energinet har skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
D.2	I henhold til Energinets procedurer for opbevaringsperioder og sletterutiner skal personoplysninger opbevares i otte år, hvorefter de slettes hos Energinet.	Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner. Forespurgt til regler for opbevaringsperioder og sletterutiner implementeret i systemet.	Der er ikke data i DataHub, som har eksisteret i otte år, hvorfor der ikke har været krav om sletning endnu . Ingen afvigelser konstateret.

Kontrolmål E

Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
E.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Forespurgt, om der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.
E.2	Energinets databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder. Inspiceret, at skabelon for databehandleraftale indeholder information om opbevaring af personoplysninger, samt at dette alene foretages på de lokaliteter, der fremgår af databehandleraftalen, som er godkendt af den dataansvarlige.	Ingen afvigelser konstateret.

Kontrolmål F

Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
F.1	Der foreligger skriftlige procedurer, som indeholder krav til Energinet ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
F.2	Energinet 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. Stikprøvevist inspiceret dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige.	Ingen afvigelser konstateret.
F.3	Energinet har den dataansvarliges generelle godkendelse til at gøre brug af underdatabehandlere. Energinet skal dog underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre databehandlere og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer.	Inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Forespurgt, om den dataansvarlige er underrettet ved ændring i anvendelse af underdatabehandlerne i erklæringsperioden.	Vi har fået oplyst af Energinet, at der ikke har været ændringer til underdatabehandlere i erklæringsperioden. Ingen afvigelser konstateret.
F.4	Energinet har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Inspiceret, at der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af databehandlerens oversigt. Inspiceret, at underdatabehandleraftaler indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Ingen afvigelser konstateret.

Kontrolmål F

Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, samt at databehandleren ved opfølgning på disses tekniske og organisatoriske foranstaltninger til beskyttelse af de registreredes rettigheder og behandlingen af personoplysninger sikrer en betryggende behandlingssikkerhed.

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
F.5	Energinet har en oversigt over godkendte underdatabehandlere, med angivelse af: ► Navn ► CVR-nr. ► Land ► Beskrivelse af behandlingen	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Stikprøvevis inspiceret, at oversigten over godkendte underdatabehandlere som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.	Ingen afvigelser konstateret.
F.6	Energinet 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.	Inspiceret, at der foreligger procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne. Stikprøvevis inspiceret dokumentation for, at der løbende er foretaget opfølgning og risikovurdering på 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 og lignende. Inspiceret dokumentation for, at information om opfølgning hos underdatabehandlere meddeles den dataansvarlige, således at denne kan tilrettelægge eventuelt tilsyn.	Ingen afvigelser konstateret.

Kontrolmål H

Der efterleves procedurer og kontroller, som sikrer, at databehandleren kan bistå den dataansvarlige med udlevering, rettelse, sletning eller begrænsning af oplysninger om behandling af personoplysninger til den registrerede.

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at Energinet skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
H.2	Energinet har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til følgende: ► Oplysningspligten ved indsamling af personoplysninger hos den registrerede. ► Oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede. ► Den registreredes indsigtsret. ► Retten til berigtigelse. ► Retten til sletning. ► Retten til begrænsning af behandling. ► Underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling. ► Retten til dataportabilitet. ► Retten til indsigelse. ► Retten til at gøre indsigelse mod resultatet af automatiske individuelle afgørelser, herunder profilering.	Inspiceret, at de foreliggende formaliserede procedurer 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. Inspiceret dokumentation for at Energinet har bistået til dataansvarlig vedrørende indsigt i oplysninger.	Ingen afvigelser konstateret.

Kontrolmål I

Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlig ved brud på persondatasikkerheden. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Inspiceret, at proceduren er opdateret.	Ingen afvigelser konstateret.
I.3	Energinet har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: ► Overvågning af netværkstrafik.	Stikprøvevist inspiceret, at Energinet månedligt foretager opfølgning på CGI-leverancer vedrørende overvågning af netværkstrafik.	Ingen afvigelser konstateret.
I.4	Energinet har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: ► Månedlig opfølgning på logning af tilgang til fortrolige personoplysninger.	Stikprøvevist inspiceret, at der foretages månedlig opfølgning på logning af adgang til personoplysninger.	Ingen afvigelser konstateret.
I.5	Energinet har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse og om muligt senest 72 timer efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos Energinet eller en underdatabehandler.	Inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Inspiceret, at databehandleren har medtaget eventuelle brud på persondatasikkerheden hos underdatabehandlere i databehandlerens oversigt over sikkerhedshændelser.	Energinet har oplyst, at der ikke har været nogen brud i erklæringsperioden, hvor Energinet har været databehandler. Ingen afvigelser konstateret.

Kontrolmål I

Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.

Nr.	*Databehandlerens kontrolaktivitet*	*Revisors udførte test*	*Resultat af revisors test*
I.6	Energinet har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet, som inkluderer: ► Karakteren af bruddet på persondatasikkerheden. ► Sandsynlige konsekvenser af bruddet på persondatasikkerheden. ► Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	Inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede procedurer for: ► Beskrivelse af karakteren af bruddet på persondatasikkerheden. ► Beskrivelse af sandsynlige konsekvenser af bruddet på persondatasikkerheden. ► Beskrivelse af foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. Inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden.	Ingen afvigelser konstateret.

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."

Martin Lervad Lundø
Administrerende direktør
På vegne af: Energinet DataHub A/S
Serienummer: PID:9208-2002-2-198569507588
IP: 87.56.xxx.xxx
2023-02-10 13:07:44 UTC
NEM ID

Jesper Due Sørensen
Partner
På vegne af: EY Godkendt Revisionspartnerselskab
Serienummer: c706566b-5a2d-44b8-8f41-5133e988cd9f
IP: 217.116.xxx.xxx
2023-02-10 13:54:22 UTC
MitID

Nils Bonde Christiansen
Statsautoriseret revisor
På vegne af: EY Godkendt Revisionspartnerselskab
Serienummer: PID:9208-2002-2-243192639174
IP: 145.62.xxx.xxx
2023-02-10 14:25:45 UTC
NEM ID