Deloitte
Statsautoriseret
Revisionspartnerselskab
CVR-nr. 33 96 35 56
Weidekampsgade 6
2300 København S

Telefon: 36102030
www.deloitte.dk

Netcompany A/S

Uafhængig revisors ISAE 3000 type 2-erklæring med sikkerhed om udvalgte kontroller i tilknytning til informationssikkerhed og foranstaltninger mod databeskyttelse af personoplysninger relateret til Netcompanys ydelser på Næste Generations Digital Post leveret til Digitaliseringsstyrelsen for perioden 1. januar 2022 til 31. december 2022

netcompany

Indholdsfortegnelse

Deloitte.

1. Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000 type 2-erklæring med sikkerhed om udvalgte kontroller i tilknytning til informationssikkerhed og foranstaltninger mod databeskyttelse og behandling af personoplysninger relateret til Netcompanys ydelser på Næste Generations Digital Post leveret til Digitaliseringsstyrelsen for perioden fra 1. januar 2022 til 31. december 2022.

Til ledelsen hos Netcompany A/S, Digitaliseringsstyrelsen og deres revisorer

1.1. Omfang

Vi har fået til opgave at afgive erklæring om Netcompany A/S' (Netcompany) beskrivelse i afsnit 3 med sikkerhed om udvalgte kontroller i tilknytning til informationssikkerhed og foranstaltninger mod databeskyttelse og behandling af personoplysninger relateret til Netcompanys ydelser på Næste Generations Digital Post (Løsningen) for perioden fra 1. januar 2022 til 31. december 2022 og om udformningen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen. De omfattede kontroller er udvalgt af Netcompany efter aftale med Digitaliseringsstyrelsen, og denne erklæring skal ses i sammenhæng med ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger mod databeskyttelse samt behandling af personoplysninger for perioden fra 1. januar 2022 til 31. december 2022, dateret den 12. januar 2023.

Vores erklæring er begrænset til de udvalgte kontrolområder, som Netcompany og Digitaliseringsstyrelsen har vurderet at være relevante i forhold til Netcompanys ydelser i forbindelse med Digital Post-løsningen.

Netcompany anvender serviceunderleverandørerne GlobalConnect og InterXion som housing-centre. Netcompanys systembeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos serviceunderleverandørerne. Denne erklæring er udarbejdet efter partielmetoden og omfatter således ikke kontroller hos serviceunderleverandører.

Enkelte af de kontrolmål, der er anført i Netcompanys beskrivelse af Digital post-løsningen, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos Netcompany. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementerende kontroller. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementerende kontroller.

1.2. Netcompanys ansvar

Netcompany er ansvarlig for udarbejdelsen af beskrivelsen og den tilhørende udtalelse i afsnit 2, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret, for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene og for at udforme, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

1.3. Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i IESBA's Etiske regler, som er baseret på grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd.

Deloitte 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.

1.4. Revisors ansvar

Vores ansvar er på grundlag af vores revisionshandlinger at udtrykke en konklusion om Netcompanys beskrivelse samt om udformningen og funktionaliteten af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

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 revisionslovgivning, med henblik på at opnå høj grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er retvisende, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed, hvor der afgives erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en serviceleverandør, omfatter udførelse af revisionshandlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af dens system, samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev nået. En erklæringsopgave med sikkerhed af denne type omfatter desuden vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte mål samt hensigtsmæssigheden af de kriterier, som Netcompany har specificeret og beskrevet i afsnit 2, "Ledelsens udtalelse".

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

1.5. Begrænsninger i kontroller hos en serviceleverandør

Netcompanys beskrivelse er udarbejdet for at opfylde de specifikke behov hos Digitaliseringsstyrelsen, som er aftalt mellem Netcompany og Digitaliseringsstyrelsen, og omfatter derfor ikke nødvendigvis alle aspekter ved behandlingen af personoplysninger. 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.

1.6. 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 i afsnit 2. Det er vores opfattelse

a) at beskrivelsen med sikkerhed om udvalgte kontroller i tilknytning til informationssikkerhed og foranstaltninger mod databeskyttelse og behandling af personoplysninger relateret til Netcompanys ydelser på Næste Generations Digital Post, således som de var udformet og implementeret for perioden fra 1. januar 2022 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 udformet for perioden fra 1. januar 2022 til 31. december 2022.

c) 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 i hele perioden fra 1. januar 2022 til 31. december 2022.

1.7. Beskrivelse af test af kontroller

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

Deloitte.

1.8. Tiltænkte brugere og formål med erklæringen

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt Digitaliseringsstyrelsen samt deres revisorer, som har en tilstrækkelig forståelse til at overveje disse sammen med anden information, herunder information om egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer.

København, den 23. marts 2023

Deloitte
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 96 35 56

Thomas Kühn
partner, statsautoriseret revisor

Dan Leitner
partner

2. Ledelsens udtalelse

Netcompany A/S fungerer som databehandler for Digitaliseringsstyrelsen i forbindelse med leverance af ydelser til Digitaliseringsstyrelsen i relation til Digital Post-løsningen.

Den medfølgende beskrivelse er udarbejdet til brug for Digitaliseringsstyrelsen, der har anvendt Netcompanys services til udvikling, vedligeholdelse og support af Digital Post-løsningen, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført. Beskrivelsen i afsnit 3 og de tilhørende kontroller i afsnit 4 omfatter, efter aftale mellem Netcompany og Digitaliseringsstyrelsen, kun en delmængde af de kontroller, der er relevante i forhold til Netcompanys leverancer vedrørende Digital Post til Digitaliseringsstyrelsen. Beskrivelsen og kontrollerne skal således ses i sammenhæng med ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger mod databeskyttelse samt behandling af personoplysninger for perioden fra 1. januar 2022 til 31. december 2022, dateret den 12. januar 2023. Netcompany bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en retvisende beskrivelse af de udvalgte kontroller, som Netcompany og Digitaliseringsstyrelsen har vurderet er relevante, i tilknytning til informationssikkerhed og foranstaltninger mod databeskyttelse og behandling af personoplysninger i relation til ydelser på Næste Generations Digital Post for perioden fra 1. januar 2022 til 31. december 2022. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

   i. redegør for, hvordan den generelle informationssikkerhed og de generelle foranstaltninger til databeskyttelse 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, som omfatter de udvalgte kontroller i relation til Digital Post-løsningen
      - De processer, der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige, henset til de udvalgte kontroller i relation til Digital Post-løsningen
      - De processer, der sikrer, at de personer, som 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 og underretning af de registrerede
      - De processer, der sikrer passende tekniske og organisatoriske sikringsforanstaltninger for behandling af personoplysninger under hensyntagen til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet, henset til de udvalgte kontroller i relation til Digital Post-løsningen
      - Kontroller, som vi med henvisning til afgrænsning af Netcompanys generelle informationssikkerhed og de generelle foranstaltninger til databeskyttelse 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 tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger, henset til henset til de udvalgte kontroller i relation Digital Post-løsningen.

   ii. Indeholder relevante oplysninger om ændringer ved databehandlerens applikationer til behandling af personoplysninger foretaget i perioden fra 1. januar 2022 til 31. december 2022

   iii. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne udvalgte kontroller i tilknytning til informationssikkerhed og foranstaltninger mod databeskyttelse og behandling af personoplysninger i

relation til databehandleraftale med Digitaliseringsstyrelsen om behandling af personoplysninger, under hensyntagen til at beskrivelsen er udarbejdet for at afdække de udvalgte kontroller, som Netcompany og Digitaliseringsstyrelsen har vurderet relevante i relation til Digital Post-løsningen og derfor ikke kan omfatte ethvert aspekt ved Netcompanys virke.

b) De udvalgte kontroller i relation til Digital Post-løsningen, der er aftalt mellem Netcompany og Digitaliseringsstyrelsen, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 1. januar 2022 til 31. december 2022. De kriterier, der blev anvendt for at give denne udtalelse, var, at:

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

   ii. de identificerede udvalgte kontroller ville, hvis anvendt som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrer opnåelsen af de anførte kontrolmål.

   iii. de udvalgte kontroller var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. januar 2022 til 31. december 2022

c) Der er etableret og opretholdt passende tekniske og organisatoriske foranstaltninger med henblik på at opfylde aftalen med Digitaliseringsstyrelsen, god databehandlerskik og relevante krav til databehandlere i henhold til databeskyttelsesforordningen. De tekniske og organisatoriske foranstaltninger, der er anført i medfølgende beskrivelse, er begrænset til udvalgte kontrolområder, som Netcompany og Digitaliseringsstyrelsen har vurderet relevante i forhold til Netcompanys ydelser på Næste Generations Digital Post-løsningen, der behandler personoplysninger, og omfatter således ikke alle Netcompanys forpligtelser i henhold til indgået databehandleraftale.

København, den 23. marts 2023

Netcompany A/S

Torben Arent
partner

3. Systembeskrivelse

3.1 Indledning

Denne beskrivelse er udfærdiget med henblik på at levere information omkring informationssikkerhed og foranstaltninger rettet mod databeskyttelse og behandling af personoplysninger i forbindelse med leverance af løsningen "Næste Generations Digital Post" til Digitaliseringsstyrelsen.

Nærværende systembeskrivelse indeholder beskrivelse af kontrolforanstaltninger i tilknytning til databeskyttelsesforordningen, som er relevante for Netcompanys ydelser på Næste Generations Digital Post-løsningen, og som Netcompany har ansvar for at efterleve. Netcompany er databehandler, og ikke dataejer, i leverancer og efterlever de krav, som kunder som dataejere har fremsat igennem aftalegrundlag samt databehandleraftaler.

Netcompany har som leverandør et selvstændigt ansvar for, at leverancerne leveres sikkert i forhold til beskyttelse af persondata samt at etablere processer, som sikrer, at behandling af persondata efterlever databeskyttelsesforordningen.

3.2 Beskrivelse af løsningen

Digital Post-løsningen og dens formål kan overordnet beskrives ved:

- Systemets hovedformål er distribution af Digital Post mellem offentlige afsendere (myndigheder) og borgere, virksomheder og myndigheder. For at understøtte dette, varetager systemet også information om hvem, hvor og hvordan, der kan kommunikeres
- Systemet indeholder både offentligt tilgængelige data, og almindelige persondata. Meddelelserne, der distribueres og opbevares i systemet, kan også indeholde både følsomme persondata og fortrolige eller følsomme data (i teorien om alle danske borgere)
- Antallet af brugere af systemet omfatter 5 mio.+ (borgere, myndigheder, virksomheder, drift, forvaltning og udvikling)
- Systemet integreres med SMS gateway, printservice, mobilvask, Danmarks Statistik, eID, NemLog-in, Datafordeleren og ERST CVR-register.

3.3 Organisation og risikostyring

Netcompany har etableret et informationssikkerhedssystem i overensstemmelse med ISO/IEC27001 rammeværket. Dette vedligeholdes løbende af Netcompanys Chief Information Security Officer (CISO) og sikkerhedsansvarlige for forretningsområderne, således at leverancer lever op til krav i Netcompanys sikkerhedspolitik, lovgivning og indgåede kontrakter.

Netcompany har etableret en sikkerhedsstyringsmodel, som omfatter, at Netcompanys ledelse gennem godkendelse af sikkerhedspolitikken sikrer, at Netcompanys risikoniveau er forankret i og accepteret af ledelsen. Sikkerhedspolitikken opdateres og godkendes minimum årligt og kommunikeres til alle medarbejdere.

Netcompany har ligeledes udarbejdet sikkerhedsprocedurer, som fastsætter kontrolkrav i forhold til sikkerhedspolitikken, og som dermed udmønter specifikke kontrolkrav, som fremgår af ISO/IEC27002 i konkret kontekst i forhold til Netcompanys løsninger.

I forbindelse med den enkelte leverance, hvori der behandles persondata, sikres det gennem anvendelse af Netcompanys Metode, at trussels- og konsekvensvurdering leveres som en fast del af leverancen. I den forbindelse sikres det gennem struktureret gennemgang, at trusler afvejes i forhold til konsekvens og sandsynlighed, og at passende tekniske og organisatoriske tiltag beskrives og implementeres. I den forbindelse sikres det, at krav, som indgår i de konkrete databehandleraftaler, medtages således, at det sikres, at den dataansvarliges sikkerhedsmæssige krav indgår i leverancen.

Kunder hos Netcompany bliver tilknyttet et team af medarbejdere, der arbejder med kunders leverance. Dette sikrer, at kunder har adgang til dedikerede, kompetente og dygtige medarbejdere med dyb viden om konkrete løsninger – både forretningsmæssigt og teknisk.

Ved fastsættelse af Netcompanys leveranceteam, tages der højde for den anvendte teknologi, så leverancerne varetages af teams med indgående kendskab til den teknologiske platform.

Hvert team består typisk af op til 20 medarbejdere med spidskompetence inden for en primær teknologi eller kunderelation. Der vil altid være minimum to personer tilknyttet den enkelte kundes løsning, således at Netcompany kan servicere kunder optimalt.

3.4 Karakteren af behandlingen

Netcompany behandler persondata som databehandler, og karakteren af behandlingen sker på vegne af instruks fra dataansvarlig. Netcompany leverer en række forskellige leverancer til kunder, og karakteren af behandlingen er derfor meget forskellig.

Netcompanys leverancer sikrer fortrolighed, integritet samt tilgængelighed gennem det design, der ligger til grund for leverancerne, samt den generelle sikkerhed, som Netcompany leverer via intern sikkerhedsstyring. Netcompany leverer ydelser sikkerhedsmæssigt professionelt, som overordnet er styret gennem processer og kontroller beskrevet og påkrævet i Netcompanys informationssikkerhedspolitik, som efterlever ISO27001-rammeværket.

Netcompany har som databehandler implementeret generelle principper for behandling af persondata. I forhold til leverancerne fungerer kunder som dataejere og har igennem kravspecifikation samt databehandleraftale opstillet principper eller krav til behandling af persondata. Netcompany implementerer disse krav i løsningsdesign, som godkendes af kunder.

Netcompany har en række generelle procedurer, som er bestemmende for Netcompanys adgang til leverancer, herunder persondata. Disse procedurer vurderes løbende i forhold til generelt risikobillede samt lovmæssige krav.

3.5 Personoplysninger

Der behandles en lang række forskellige typer persondata i Digital Post-løsningen som led i de indgåede aftaler. Det drejer sig om personoplysninger, som indgår både i kategorien almindelige personoplysninger samt i den særlige kategori, hvor beskyttelse af informationer er essentiel for det enkelte fysiske individ.

Der er for de enkelte leverancer gennem anvendelse af Netcompanys Metode beskrevet hvilke kategorier af persondata, som behandles, og tilhørende risici.

Digital Post omfatter følgende typer af personoplysninger:

- Almindelige personoplysninger (herunder navn, adresse, telefonnummer og personhenførbare ID'er)
- CPR-nummer (herunder tilhørende registeroplysninger)

Borgernes postkasser indeholder borgernes meddelelser og dermed fritekst, der kan indeholde følsomme oplysninger, herunder racemæssig og etnisk baggrund, politisk/religiøs/filosofisk overbevisning, fagforeningsmæssige forhold, helbredsoplysninger og seksuelle forhold.

Netcompany har som databehandler et selvstændigt krav om at føre en fortegnelse over behandlingsaktiviteter. Netcompany efterlever dette krav ved anvendelse af Netcompanys Metode, som sikrer, at behandlingsaktiviteter dokumenteres i fortegnelsen over behandlingsaktiviteter. I fortegnelsen registreres de kategorier af behandling af persondata, som foretages samt beskrivelser af eventuelle overførelser til tredjelande. Derudover ligger der ligeledes en beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger, som er implementeret. Disse informationer indgår som element i leverancebeskrivelserne, som er godkendt af kunder.

3.6 Praktiske tiltag

Netcompanys leverancer til kunder har passende tekniske og organisatoriske sikkerhedsforanstaltninger. Foranstaltningerne vurderes løbende ud fra en risikomæssig betragtning, og såfremt der er ændringer i det risikomæssige billede, tilpasses leverancerne til det ændrede risikobillede.

Netcompany har fået udarbejdet en ekstern revisionserklæring ISAE 3402-erklæring relateret til generelle IT-kontroller, "Uafhængig revisors erklæring angående generelle IT-kontroller relateret til drifts- og hostingydelser samt udvikling for perioden fra 1. januar til 31. december 2022", som indeholder test af en lang række kontroller relateret til IT-sikkerhed, som også er relevante i forbindelse med beskyttelse og behandling af personoplysninger.

Netcompany har foretaget vurdering af, om der er yderligere tekniske eller organisatoriske foranstaltninger, som er relevante i forbindelse med behandlingen og beskyttelsen af personoplysninger i forbindelse med Netcompanys rolle som databehandler. Leverancerne leveres efter kravspecifikation og godkendelse af kunder, herunder databeskyttelseskrav. Netcompany sikrer gennem processer, at krav til behandling af persondata reflekteres i de processer, som Netcompany arbejder efter. Som en del af leverancen til kunder beskrives sikkerhedsdesign i leverancedokumenterne, som godkendes af kunder.

Netcompany har implementeret en proces, som sikrer, at brud på persondatasikkehed formelt håndteres samt rapporteres til Digitaliseringsstyrelsen. Det er Digitaliseringsstyrelsen, der som dataansvarlig, afgør behov for samt varetager eventuel rapportering til relevant tilsynsmyndighed og registrerede.

Netcompanys ITSM-system anvendes til formel registrering af brud på persondatasikkerheden. Derved sikres det, at brud dokumenteres, og at der sker sporbarhed i håndtering af brud.

Netcompany er fungerende databehandler for kunder, og det er dermed Netcompanys ansvar at notificere kunder om et brud på persondatasikkerheden uden unødigt ophold. Netcompany vil desuden løbende medvirke til, at omstændigheder omkring brud belyses og mulige konsekvenser for de registrerede analyseres, således at kunder i videst muligt omfang modtager relevante informationer, som kan benyttes til en faglig vurdering af persondatasikkerhedsbruddet og mulige konsekvenser for de registrerede.

3.7 Kontrolforanstaltninger

Netcompany har implementeret kontrolforanstaltninger som sikrer, at behandling af persondata sker på baggrund af de risici som er identificeret. Dette betyder, at der er implementeret mitigerende tiltag for at sikre, at de risici som er identificeret i risikovurderingen håndteres korrekt for at håndtere risici.

Herunder findes kortfattede beskrivelser af Netcompanys kontroller og foranstaltninger indenfor de områder, som er omfattet af nærværende erklæring:

Tekniske sikringsforanstaltninger (kontrolmål B)

Netcompany har, baseret på en risikovurdering, implementeret passende tekniske sikringsforanstaltninger, i henhold til de indgåede databehandleraftaler. Sikringsforanstaltninger omfatter blandt andet følgende tiltag, som ikke er udtømmende: Anti-virus/anti-malware, firewalls, segmentering af netværk, brugerstyring, overvågning og alarmering, logning og logopsamling, patchning og sårbarhedsstyring, overvåget backup og restore, kryptering, samt fysisk adgangssikkerhed.

Sletning og tilbagelevering (kontrolmål D)

Netcompany har formaliserede procedurer, der beskriver, hvorledes persondata skal behandles efter aftale med dataansvarlige, herunder hvordan persondata skal slettes og tilbageleveres.

Opbevaring af data (kontrolmål E)

Netcompany har en samlet og opdateret oversigt over behandlingsaktiviteterne. Netcompany har formaliserede procedurer, der sikrer at der alene foretages opbevaring og behandling af persondata i henhold til de indgåede databehandleraftaler.

Anvendelse af underdatabehandlere (kontrolmål F)

Netcompany vedligeholder løbende en oversigt over anvendte underdatabehandler, som er godkendt af dataansvarlige. Netcompany sikrer, at der er indgået underdatabehandleraftaler med underdatabehandlere, og at der løbende udføres kontrol af underdatabehandlere. Gennemgangen af databehandleraftaler og underdatabehandlere udføres mindst én gang årligt.

I forbindelse med leverance af Digital Post-løsningen til DIGST anvender Netcompany ikke underdatabehandlere.

Sikkerhedsbrud (kontrolmål I)

Netcompany har etableret procedurer der sikrer registrering af sikkerhedshændelser samt underretning af dataansvarlige, ifm. et eventuelt sikkerhedsbrud. Netcompany sikrer gennem overvågning, logning og awareness hos medarbejdere, at der identificeres eventuelle brud på persondatasikkerheden.

3.8 Komplementerende kontroller hos den dataansvarlige

Netcompany leverer ydelser på baggrund af databehandleraftale, og derfor er der en række kontroller, som den dataansvarlige har ansvar for efterleves. Herunder sikre at:

- personoplysninger er ajourførte
- databehandleraftalen er lovlig i forhold til gældende persondataretlig regulering
- databehandleraftalen er retvisende i forhold til leverancens omfang
- der er udarbejdet risikovurdering af behandling af persondata, herunder en konsekvensvurdering af behandling af persondata

4. Kontrolmål, kontrolaktivitet, test og resultat heraf

4.1 Introduktion

Denne erklæring er udformet med henblik på at informere Digitaliseringsstyrelsen om Netcompanys udvalgte kontroller, som kan påvirke behandlingen af personoplysninger, og samtidig informere den dataansvarlige, for hvem Netcompany behandler personoplysninger, om funktionaliteten af de udvalgte kontroller, der blev efterprøvet. Afsnittet, når det kombineres med en forståelse og vurdering af kontrollerne i kundernes forretningsprocesser, har til hensigt at hjælpe kundernes revisor med at vurdere risici for fejl, som muligvis påvirkes af kontroller hos Netcompany.

Vores test af Netcompanys kontroller er begrænset til de kontrolmål og tilknyttede kontroller, som er nævnt i nedenstående kontrolmatrix i denne del af rapporten, og er ikke udvidet til at omfatte alle de kontroller, som er beskrevet i systembeskrivelsen, eller til de generelle it-kontroller, som skal være implementeret i brugerorganisationerne for at opfylde kontrolmålene.

Det er de dataansvarliges ansvar at evaluere denne information i forhold til de kontroller, som eksisterer i hver brugerorganisation. Hvis bestemte supplerende kontroller ikke er til stede i brugerorganisationerne, kan Netcompanys kontroller muligvis ikke kompensere for sådanne svagheder.

4.2 Test af kontroller

De test, der udføres i forbindelse med fastlæggelsen af kontrollers funktionalitet, består af en eller flere af følgende metoder:

Metode	Beskrivelse
Forespørgsel	Forespørgsel hos udvalgt personale hos Netcompany
Observation	Observation af kontrollens udførelse
Inspektion	Inspektion af dokumenter og rapporter, som indeholder angivelse af udførelse af kontroller. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er udformet, så de kan forventes at blive effektive, hvis de implementeres. Endvidere vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Genudførelse af kontrollen	Gentagelse af den relevante kontrol med henblik på at verificere, at kontrollen fungerer som forudsat

4.3 Test af udformning og implementering

I nedenstående skema er de testede udvalgte kontrolmål og udvalgte kontroller anført, ligesom vi har beskrevet, hvilke revisionshandlinger der er udført og resultatet af disse handlinger. I det omfang vi har konstateret væsentlige kontrolsvagheder, har vi anført dette.

4.4 Kontrolmål, kontroller og resultater af test

I nedenstående skema er de testede kontrolmål og kontroller anført, ligesom vi har beskrevet, hvilke revisionshandlinger der er udført og resultatet af disse handlinger. I det omfang vi har konstateret væsentlige kontrolsvagheder, har vi anført dette.

Kontrolmål B Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	**Netcompanys kontrolmål og kontroller**	**Udførte test**	**Resultat af test**
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.	Vi har foretaget forespørgsel hos den ansvarlige for kontrollen. Vi har inspiceret datasikkerhedsplanen og observeret, at der forligger procedure for årlig risikovurdering. Vi har inspiceret risikovurdering for Løsningen og observeret, at roller og ansvar er klart defineret, at relevante risici rettet mod databeskyttelse er identificeret og vurderet, samt at restrisiko kan accepteres. Vi har inspiceret den mellem Netcompany og Digitaliseringsstyrelsen indgåede databehandleraftale, og observeret, at der er beskrevet krav til tekniske og organisatoriske sikkerhedsforanstaltninger.	Ingen afvigelser konstateret.
B.6	Adgang til personoplysninger er begrænset til brugere med et arbejdsbetinget behov herfor.	Vi har foretaget forespørgsel hos den ansvarlige for kontrollen. Vi har inspiceret informationssikkerhedspolitik og observeret, at der er beskrevet formelle procedurer for tildeling af adgang til systemer og data. Vi har inspiceret datasikkerhedsplanen og observeret, at der foreligger procedure for periodisk gennemgang af brugere og rettigheder, herunder adgang til produktionsdata mv. Vi har stikprøvevis inspiceret oversigt over brugeradgange til systemer i relation til Løsningen. Vi har fået observeret, at brugeres adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov. Vi har inspiceret 2 månedlige driftsrapport til Digitaliseringsstyrelsen, og observeret, at der fremgår en liste over aktive brugere og deres adgange/rettigheder til systemer og data.	Ingen afvigelser konstateret.

Kontrolmål C Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.			
Nr.	**Netcompanys kontrolmål og kontroller**	**Udførte test**	**Resultat af 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.	Vi har foretaget forespørgsel hos den ansvarlige for kontrollen. Vi har inspiceret datasikkerhedsplanen og observeret, at der fremgår procedure for behandling af personoplysninger. Vi har for udvalgte stikprøver inspiceret underskrevet ansættelseskontrakt og observeret, at fortrolighedsaftale i relation til databeskyttelse og behandling af personoplysninger fremgår af ansættelseskontrakten. Vi har fået oplyst, at medarbejdere i forbindelse med ansættelse har kvitteret for, at vedkommende bl.a. har læst og forstået følgende interne dokumenter: • Informationssikkerhedspolitik • Databeskyttelsespolitik • Code of Conduct.	Ingen afvigelser konstateret.
C.6	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, som databehandleren udfører for de dataansvarlige.	Vi har foretaget forespørgsel hos den ansvarlige for kontrollen. Vi har inspiceret sikkerhedsproceduren og observeret, at der er beskrevet procedure for medarbejdernes fratrædelse. Vi har for udvalgte stikprøver inspiceret underskrevet ansættelseskontrakt og observeret, at medarbejderen har underskrevet fortrolighedserklæring, som er en del af ansættelsesforholdet og som er gældende efter ansættelsesforholdets ophør. Vi har fået oplyst, at man ved fratrædelse bliver gjort opmærksom på, at alle fortrolighedskrav stadig gælder efter endt ansættelse.	Ingen afvigelser konstateret.

Kontrolmål D Der efterleves procedurer og kontroller, som medfører, at personoplysninger kan slettes eller tilbageleveres, såfremt der indgås aftale herom med den dataansvarlige.			
Nr.	**Netcompanys kontrolmål og kontroller**	**Udførte test**	**Resultat af 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.	Vi har foretaget forespørgsel hos den ansvarlige for kontrollen. Vi har inspiceret databeskyttelsespolitikken og observeret, at der er beskrevet krav vedrørende opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Vi har inspiceret datasikkerhedsplanen og observeret, at det er beskrevet, at der skal foretages løbende – og mindst en gang årligt – vurdering af, om de relevante procedurer skal opdateres.	Ingen afvigelser konstateret.
D.2	Der er aftalt specifikke krav til Netcompanys opbevaringsperioder og sletterutiner.	Vi har foretaget forespørgsel hos den ansvarlige for kontrollen. Vi har inspiceret databeskyttelsespolitikken og observeret, at der er beskrevet krav vedrørende opbevaring og sletning af data. Vi har inspiceret databehandleraftalen mellem Digitaliseringsstyrelsen og Netcompany og observeret, at der fremgår krav vedrørende tilbagelevering og sletning af persondata ved ophør. Vi har inspiceret procedure for opbevaringsperioder og sletterutiner og observeret, at den omfatter specifikke krav i relation til Digital Post-løsningen. Vi har forespurgt om ophørte databehandlinger i erklæringsperioden, og om der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført, og har her fået oplyst, at der ikke er sket sletning af data i erklæringsperioden, hvorfor der ikke udført yderligere handlinger	Ingen afvigelser konstateret.

Kontrolmål E Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer og behandler personoplysninger i overensstemmelse med aftalen med den dataansvarlige.			
Nr.	**Netcompanys kontrolmål og kontroller**	**Udførte test**	**Resultat af test**
E.2	Databehandlerens databehandling, inklusive opbevaring, må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Vi har foretaget forespørgsel hos den ansvarlige for kontrollen. Vi har inspiceret datasikkerhedsplanen og observeret, at der foreligger procedure og retningslinjer for behandling og opbevaring af data på lokationer i Danmark. Vi har inspiceret databehandleraftalen mellem Digitaliseringsstyrelsen og Netcompany og observeret, at der fremgår godkendte leverandører og lokationer.	Ingen afvigelser konstateret.

Kontrolmål E Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer og behandler personoplysninger i overensstemmelse med aftalen med den dataansvarlige.			
Nr.	**Netcompanys kontrolmål og kontroller**	**Udførte test**	**Resultat af test**
		Vi har endvidere inspiceret Netcompanys lokationsgaranti og observeret, at den er underskrevet.	

Kontrolmål F Der efterleves procedurer og kontroller, som sikrer, at der alene anvendes godkendte underdatabehandlere, og 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.	**Netcompanys kontrolmål og kontroller**	**Udførte test**	**Resultat af 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	Vi har foretaget forespørgsel hos den ansvarlige for kontrollen. Vi har inspiceret datasikkerhedsplanen og observeret, at der ikke anvendes underdatabehandlere i forbindelse med drift og vedligeholdelse af Løsningen. Vi har endvidere observeret, at datasikkerhedsplanen er opdateret og godkendt i oktober 2022.	Ingen afvigelser konstateret.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Vi har foretaget forespørgsel hos den ansvarlige for kontrollen. Vi har forespurgt til, hvorvidt der anvendes underdatabehandlere i forbindelse med Netcompanys leverancer. Vi har konstateret, at der ikke anvendes underdatabehandlere i forbindelse med løsningen dækket af denne erklæring, hvorfor der ikke er udført yderligere handlinger.	Ingen afvigelser konstateret.

Kontrolmål H Der efterleves procedurer og kontroller, som sikrer, at databehandleren kan bistå den dataansvarlige med udlevering af personoplysninger til den registrerede, rettelse eller sletning af personoplysninger, begrænsning af behandling af personoplysninger og oplysning om behandling af personoplysninger til den registrerede.			
Nr.	**Netcompanys kontrolmål og kontroller**	**Udførte test**	**Resultat af test**
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.	Vi har foretaget forespørgsel hos den ansvarlige for kontrollen. Vi har inspiceret procedure for bistand til den dataansvarlige i forhold til de registreredes rettigheder og observeret, at det er defineret, hvordan bistand skal finde sted i forbindelse med udlevering, sletning og korrektion af registreres personoplysninger. Vi har inspiceret dokumentet 'Sensitive data in the solution' og observeret, at der er beskrevet type af data, der indgår i Løsningen, databehandlingsflow samt en beskrivelse af behandlingsaktiviteter.	Ingen afvigelser konstateret.

Kontrolmål I **Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.**			
Nr.	**Netcompanys kontrolaktivitet**	**Deloittes test**	**Resultat af 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.	Vi har ved interview forespurgt en ansvarlig til kontrollen. Vi har inspiceret, om der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden, samt om proceduren er opdateret.	Ingen bemærkninger.