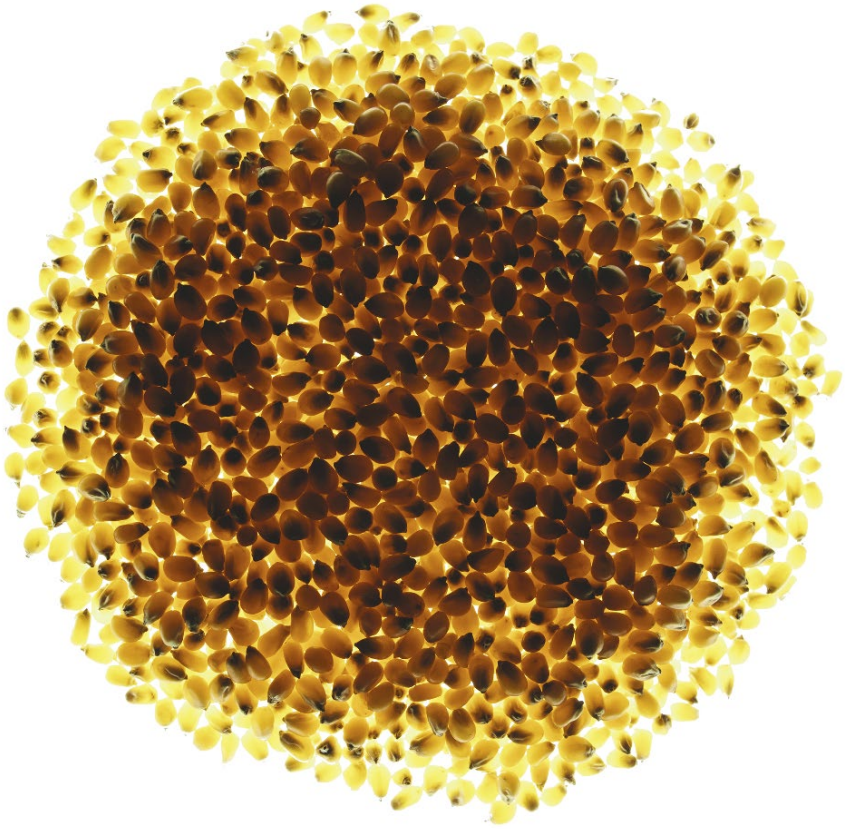
Deloitte
Statsautoriseret
Revisionspartnerselskab
CVR-nr. 33 96 35 56
Weidekampsgade 6
2300 København S

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 Digital Post leveret til Digitaliseringsstyrelsen for perioden 1. januar 2023 til 31. december 2023

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 Digital Post leveret til Digitaliseringsstyrelsen for perioden fra 1. januar 2023 til 31. december 2023.

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' (herefter "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 Digital Post for perioden fra 1. januar 2023 til 31. december 2023 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 2023 til 31. december 2023, dateret den 5. januar 2024.

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 Digital Realty 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 Statsautoriseret Revisionspartnerselskab anvender International Standard on Quality Management 1, ISQM 1, som kræver, at vi designer, implementerer og driver et kvalitetsstyringssystem, herunder politikker eller procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende 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 Digital Post, således som de var udformet og implementeret for perioden fra 1. januar 2023 til 31. december 2023, 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 2023 til 31. december 2023.

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 2023 til 31. december 2023.

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 27. februar 2024

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.

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 2023 til 31. december 2023, dateret den 5. januar 2024. 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 Digital Post-løsningen for perioden fra 1. januar 2023 til 31. december 2023. 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 2023 til 31. december 2023

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 2023 til 31. december 2023. 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 2023 til 31. december 2023

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 Digital Post-løsningen, der behandler personoplysninger, og omfatter således ikke alle Netcompanys forpligtelser i henhold til indgået databehandleraftale.

København, den 27. februar 2024

Netcompany A/S

Torben Arent
partner

3. Systembeskrivelse

Denne beskrivelse er udfærdiget med henblik på at levere information om efterlevelse af databeskyttelsesforordningen i forbindelse med leverance af DigitalPost.dk for Digitaliseringsstyrelsen (herefter DIGST).

Erklæringen er organiseret i overensstemmelse med ISAE 3000-rammeværket, opsat efter de kontroller, som Foreningen for statsautoriserede revisorer anbefaler. Erklæringen er dækkende for perioden fra 1. januar 2023 frem til 31. december 2023.

Nærværende sektion indeholder beskrivelse af de artikler i databeskyttelsesforordningen, som er relevante for Netcompanys leverancer på DigitalPost.dk, og som Netcompany har ansvar for at efterleve. Netcompany er databehandler og ikke dataansvarlig vedrørende leverancen og efterlever de krav, som kunden som dataansvarlig, har fremsat på baggrund af aftalegrundlag samt databehandleraftalen.

Netcompany som databehandler ifalder et selvstændigt ansvar for, at leverancerne leveres sikkert i forhold til beskyttelse af persondata og processer, som sikrer, at behandling af persondata efterlever databeskyttelsesforordningen.

3.1 Løsningsbeskrivelse

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.

Digital Post-løsningen består af følgende 8 kernekomponenter:

- Distributionskomponenten: Når en offentlig myndighed ønsker at sende meddelelser til en borger eller en virksomhed, sker dette ved, at myndigheden via dennes afsendersystem sender postmeddelelsen eller postmeddelelserne til NgDPs komponent Distribution. Det vil ske via snitflader, der er forkortet: REST m. HTTPS, SMTP med S/MIME og SFTP.
- Kontaktregister: Digital Post har et såkaldt Kontaktregister, der indeholder oplysninger om tilmeldte og fritagne borgere og virksomheder samt deres kontaktoplysninger (telefonnummer og/eller almindelig e-mail) og person- eller CVR-nummer.
- Opbevaringskomponenten: Modtagelse og efterfølgende opbevaring af borgeres og virksomheders postmeddelelser vil ske i komponenten Opbevaring, som fungerer som den enkeltes postkasse. Meddelelserne vil herfra blive udstillet på de kommercielle og offentlige visningsklienter, f.eks. for borgere på borger.dk og for virksomheder på Virk. Tilsvarende vil de af borgerne og virksomhederne afsendte meddelelser blive opbevaret i opbevaringskomponenten.
- Systemregister: Myndigheder registreres i Digital Posts Systemregister, der har til formål at registrere, hvilke myndigheder der må sende og kan modtage postmeddelelser via Digital Post, og sikre, at meddelelserne afleveres i de korrekte systemer hos myndighederne
- Hændelseslogs: Digital Post indeholder desuden Hændelseslogs, hvis funktion er at registrere og udstille f.eks. information om, hvornår en forsendelse er foretaget, hvem der er afsender og modtager og lign. Alle borgere og virksomheder har adgang til en hændelseslog, der vedrører dem selv.
- Administrativ Adgang: Det er en forudsætning for, at myndigheder kan sende postmeddelelser via Digital Post-løsningen, at deres afsender- og modtagersystemer er tilsluttet Digital Post. Dette sker via komponenten Administrativ Adgang, som er en portal, hvor myndigheder og virksomheder kan tilslutte og administrere deres anvendelse af løsningen.
- Identitetsregister: Identitetsregistret har til formål at opbevare alle identiteter, som bruger eller er en del af Digital Post-løsningen. Dette inkluderer systembrugere, eksterne systemer, medarbejdere, virksomheder og borgere samt deres rettigheder i Digital Post-løsningen.
- Proceskomponent: Proceskomponenten sørger for at håndtere asynkrone handlinger i Digital Post-løsningen ved at kommunikere hændelser og handlinger på tværs af komponenter, f.eks. når en kontakt skal opdateres i kontaktregistret, eller en status skal ændres i en komponent.

- Transformationskomponent: Transformationskomponenten har til formål at understøtte transformationen fra det tidligere Digital Post-format til det nye format, kaldet MeMo.

3.2 Underdatabehandlere

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

3.3 Karakteren af behandlingen

Netcompany behandler persondata som databehandler, og karakteren af behandlingen sker på vegne af instruks fra dataejeren. 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 underleverandør 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.

3.4 Personoplysninger

Digital Post behandler en lang række forskellige typer persondata som led i de aftaler, som er indgået. Det drejer sig om personoplysninger og de særlige kategorier af personoplysninger, jf. databeskyttelsesforordningens artikel 4.

De enkelte leverancer har gennem anvendelse af Netcompanys Metode beskrevet, hvilke kategorier af persondata som behandles og tilhørende risici.

Netcompany oppebærer som leverandør og databehandler et selvstændigt ansvar for at føre *fortegnelse* over behandlingsaktiviteter på Digitalpost, jf. databeskyttelsesforordningens artikel 30. Netcompany efterlever dette krav ved at anvende Netcompany Metoden, som i forbindelse med dokumentation for behandlingsaktiviteten sikrer, at selve *fortegnelsen* over behandlingsaktiviteten dokumenteres. I *fortegnelsen* registreres bl.a. de kategorier af behandling af persondata, som findes på løsningen. Derudover udarbejdes en beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger, som er implementeret på baggrund af en konkret risikovurdering. Disse informationer indgår som element i leverancebeskrivelserne, som er godkendt af Digitaliseringsstyrelsen.

På Digital Post er de behandlede personoplysninger oplistet i Databehandleraftalen, stk. 18.1.d.

3.5 Risikovurdering

Netcompany udfører regelmæssigt en vurdering af, om organisationens generelle informationssikkerhedspolitik er i overensstemmelse med formelle politikker, lovgivning og anerkendte standarder samt en vurdering af det aktuelle risikobillede.

I overensstemmelse med kravene i GDPR-lovgivningen og ISO 27001-rammeværket identificerer, dokumenterer og implementerer Netcompany desuden procedurer og kontroller for at sikre den nødvendige informationssikkerhed specifikt på de enkelte løsninger. Løsningerne er mangeartede, hvorfor de specifikke risikovurderinger vil fremstå ligeså - men i vurderingerne tager Netcompany bl.a. stilling til behandlingsformål, personoplysningernes karakter, slettefrister og konsekvenser for den registrerede og kunden.

I risikovurderingerne inddrages officielle risikovurderinger fra eksempelvis Center for Cybersikkerhed og Forsvarets Efterretningstjeneste, men også andre anerkendte kilder såsom Microsoft.

Hermed foretages en faglig, velfunderet vurdering af risikobilledet generelt på organisationsniveau og specifikt på løsningerne samt en afvejning af disse risici i forhold til de forholdsregler, der bliver truffet for at beskytte de registreredes rettigheder.

3.6 Kontrolforanstaltninger

Netcompany har implementeret kontroller vedr. behandling af personoplysninger inden for følgende områder:

Netcompany har implementeret kontrolforanstaltninger, som sikrer, at behandling af persondata sker under hensyntagen til de risici, som er identificeret. Dette betyder desuden, at der er implementeret mitigerende tiltag for at sikre, at risici håndteres korrekt.

Herunder findes kortfattede beskrivelser af Netcompanys kontroller og foranstaltninger indenfor de områder, som er omfattet af nærværende erklæring: I afsnit 4 er de kontrolforanstaltninger, Netcompany anser for relevante for behandlingen af persondata, beskrevet. Nedenfor findes en uddybende beskrivelse af et udvalg af relevante kontrolforanstaltninger.

3.6.1 Tekniske sikringsforanstaltninger (kontrolmål B)

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

Anvendte procedurer og kontroller
Netcompany har, baseret på en risikovurdering, implementeret passende tekniske sikringsforanstaltninger, i henhold til de indgåede databehandleraftaler. Sikringsforanstaltninger omfatter anvendelse af antivirus, firewalls, segmentering af netværk, adgangsstyring til data, overvågning og alarmering, logning, patchning samt fysisk adgangssikkerhed (listen er ikke udtømmende).

Netcompany opdaterer løbende sin sårbarhedsvurdering ift. vurdering af, om der er implementeret et passende niveau af tekniske foranstaltninger. Disse foranstaltninger dækker over blandt andet antivirus, kryptering/VPN, logmonitorering, driftsovervågning, løbende sikkerhedsuddannelse af medarbejdere samt multifactor-autorisering og optagelse af adgang til servermiljøet.

3.6.2 Organisatoriske foranstaltninger (kontrolmål C)

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

Anvendte procedurer og kontroller
Netcompany har implementeret og etableret organisatoriske foranstaltninger, baseret på en vurdering af risiko. Dette indbefatter, at der er en opdateret sikkerhedspolitik samt procedurer, der sikrer, at sikkerhedspolitikken kommunikeres til medarbejdere. Løbende uddannelse af medarbejderne hos Netcompany foretages blandt andet via Netcompany Academy-portalen, hvor det kontrolleres, at medarbejderne har gennemgået relevant sikkerhedspolitisk uddannelse samt jævnlige opdateringer fra Netcompanys centrale sikkerhedsafdeling på mere overordnede områder.

Ansættelse og onboarding:
Netcompanys onboarding-procedure er omfattende og designet til at sikre, at alle nye medarbejdere er godt rustet til at udføre deres roller og samtidig overholde Netcompanys sikkerheds- og privatlivspolitikker. Alle nye medarbejdere modtager Netcompanys medarbejderhåndbog, som giver en detaljeret forståelse af Netcompany som arbejdsplads. Håndbogen indeholder både globale politikker og standarder, der gælder for alle Netcompanys medarbejdere, og et lokalt bilag med information om lokale politikker og lovkrav. Det er obligatorisk for alle medarbejdere at læse denne håndbog.

Alle medarbejdere er desuden forpligtet til at læse og bekræfte Netcompanys sikkerhedspolitik, procedurer og privatlivspolitikker. Dette omfatter retningslinjer for brug af elektroniske enheder, håndtering af sikkerhedshændelser og behandling af personoplysninger i overensstemmelse med gældende GDPR-lovgivning.

Ved ansættelse underskriver medarbejdere i Netcompany i kraft af deres ansættelseskontrakt en fortrolighedsaftale, og ved fratrædelse påmindes medarbejdere om denne fortrolighedsaftale, ligesom der lukkes ned for medarbejdernes adgang til personoplysninger.

3.6.3 Sletning og tilbagelevering (kontrolmål D)

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

Anvendte procedurer og kontroller
Netcompany har beskrevne procedurer, der beskriver, hvorledes persondata skal behandles. I disse procedurer er det beskrevet overordnet, hvorledes Netcompany på anvisning fra kunder sletter og tilbageleverer data. Således er det til enhver tid muligt at få slettet eller tilbageleveret data, såfremt dette ikke er i strid med anden lovgivning.

3.6.4 Opbevaring af data (kontrolmål E)

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

Anvendte procedurer og kontroller
Netcompany har udarbejdet en vejledning i, hvordan persondata skal behandles og opbevares. Denne vejledning er kommunikeret til alle relevante medarbejdere i Netcompany og opdateres løbende.

3.6.5 Anvendelse af underdatabehandlere (kontrolmål F)

Formål
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.

Anvendte procedurer og kontroller
Der anvendes ikke underdatabehandlere på løsningen.

I forbindelse med leverance af Digital Post-løsningen anvender Netcompany udelukkende GlobalConnect og Digital Realty som housing-centre. Både den logiske og fysiske sikkerhed vedrørende adgangen til servere, der indeholder persondata, er således under Netcompanys direkte kontrol. Der foretages således ikke databehandling hos GlobalConnect og Digital Realty.

3.6.6 Bistand til dataansvarlige (kontrolmål H)

Formål
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.

Anvendte procedurer og kontroller
Netcompany har etableret procedurer for bistand til de dataansvarlige med udlevering, rettelse og sletning, i det omfang der rettes henvendelse herom.

3.6.7 Sikkerhedsbrud (kontrolmål I)

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

Anvendte procedurer og kontroller
Netcompany har etableret procedurer, der beskriver den proces, der skal følges ifm. et eventuelt sikkerhedsbrud.

3.7 Komplementerende kontroller hos de dataansvarlige

Netcompany leverer ydelser på baggrund af databehandleraftale, og derfor er der en række kontroller, som den dataansvarlige har ansvar for efterleves, herunder;

- At sikre, at personoplysninger er ajourført.
- At databehandleraftalen er lovlig i forhold til gældende persondataretlig regulering.
- At databehandleraftalen er retvisende i forhold til leverancens omfang.
- At der er udarbejdet risikovurdering af behandling af persondata, herunder en konsekvensvurdering samt vurdering af øvrige relevante forhold ved behandling af persondata.
- At udføre en risikovurdering og udarbejde instruks til Netcompany, hvis der er behov for særlige sikringstiltag i forbindelse med overførsler til tredjelande.
- At de etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger. Således udføres penetrationstest kun efter anmodning fra kunden.
- At kontrollere egne medarbejderes adgang til data, således at adgang til data minimeres og kun tildeles medarbejdere, som har behov for sådan adgang til at udføre deres arbejde.

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 udformning og 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, at risikovurderingen er opdateret og godkendt i perioden. 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 stikprøvevist inspiceret månedlige driftsrapporter til Digitaliseringsstyrelsen, og observeret, at der fremgår en liste over aktive brugere og deres adgange/rettigheder til systemer og data. Vi har baseret på forespørgsler fået bekræftet, at adgang til personoplysninger er begrænset til brugere med et arbejdsbetinget behov.	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 ved interview forespurgt en ansvarlig til kontrollen. Vi har stikprøvevist inspiceret dokumentation for, at medarbejdere underskriver, at de har læst og forstået Netcompanys informationssikkerhedspolitik. Vi har stikprøvevist inspiceret dokumentation for, at medarbejdere underskriver fortrolighedserklæring som en del af ansættelsesforholdet.	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 ved interview forespurgt en ansvarlig til kontrollen. Vi har stikprøvevist inspiceret, at medarbejdere underskriver en fortrolighedserklæring som en del af ansættelsesforholdet. Vi har på baggrund af forespørgsler fået oplyst, at medarbejdere 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, samt at denne blev opdateret og godkendt medio 2023 Vi har inspiceret dokumentet Sensitive data in the solution, hvoraf instruks relateret til sensitive data er indeholdt. 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 proceduren for bistand til den dataansvarlige og observeret, at denne indeholder krav til sletning af persondata.	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 "Procedurer for bistand til den dataansvarlige" og "Sensitive data in the solution" for opbevaringsperioder og sletterutiner og observeret, at de omfatter specifikke krav til Digital Post-løsningen. Vi har inspiceret dokumentation for konfigurationen af slettejob og observeret, at det automatiske job bliver kørt.	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. Vi har fået oplyst, at de eksakte adresser er udeladt af sikkerhedshensyn.	Vi har konstateret, at der ikke er indhentet godkendelse fra DIGST efter opdatering af servicelokationer. Ingen yderligere afvigelser konstateret.

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 observeret, at datasikkerhedsplanen er opdateret og godkendt i juni 2023.	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 formaliserede procedurer 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 stikprøvevist inspiceret dokumentation for udført bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af personoplysninger til den registrerede i erklæringsperioden.	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 formaliserede procedurer med henblik på at identificere krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Vi har observeret, at proceduren er opdateret. Vi har stikprøvevist inspiceret dokumentation for håndtering af persondatasikkerhedshændelser med henblik på at verificere, at proceduren efterleves, og DIGST er underrettet.	Ingen afvigelser konstateret.