Revisorerklæring

Docpoint A/S

ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftaler med kunder for perioden fra 1. januar 2022 til 31. december 2022

Grant Thornton | www.grantthornton.dk
Højbro Plads 10, 1200 København K
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

Maj 2023

Indholdsfortegnelse

Afsnit 1: Docpoint A/S' beskrivelse af behandlingsaktivitet for leverancen af docDirect og docPost løsningerne

I dette afsnit gives en overordnet beskrivelse af produkterne docDirect og docPost set ud fra den kontekst, som disse er tiltænkt at fungere i. Beskrivelsen danner grundlag for de efterfølgende afsnit.

Funktionalitet

docDirect

docDirect er udviklet med det formål, at det skal være let for kunder at få sendt post i e-Boks/Digital Post. Produktet benyttes af både private kunder og offentlige kunder derfor sondringen mellem e-Boks og Digital Post.

docDirect tilbydes kunderne på 2 forskellige måder:

1. Via 2 stykker software - Lasernet Meta og Lasernet Client, som installeres hos kunden. Dette software gør det muligt at sende sikker post i e-Boks eller til Digital Post fra alle Windows baserede programmer f.eks. Word eller et lønsystem.

2. Via en grænseflade sådan kunden kan opnå en grad af systemintegration, uden at skulle ændre nævneværdigt i egne systemer. Her er 3 varianter:
    a. Læsning af data fra en Windows folder hos kunden. Dette kræver at kunden installerer et stykke software fra Docpoint.
    b. Via en SFTP-server
    c. Via et API/en WEB-service

Løsningen er baseret på Lasernet Output Management server (LOM) og Lasernet Meta /- Client PC-software, kombineret med egenudviklet kode.

Ud over at kunne sende post i e-Boks/Digital Post, så kan løsningen også bruges til digital underskrift, som er baseret på enten en e-Boks service eller Nets eSignering, som løsningen også integrerer med.

Løsningen kan også sende fysisk post til personer, som har valgt at være fritaget for offentlig digital post eller hvis afsender ønsker dette.

docDirect markedsføres som et standardprodukt, som de fleste kunder anvender, og med mulighed for kundeindividuelle tilpasninger, hvilket blandt andet omfatter integration til Nets eArkiv.

Der er mulighed for at lave et opslag i CPR-registeret til brug for visuel kontrol af navneoplysninger knyttet til en forsendelse, inden denne effektueres.

Data lagres kun i det omfang, det er nødvendigt for at kunne gennemføre en stabil og fejlfri drift samt for at kunne give en tilfredsstillende og brugbar support. docDirect løsningen tilbyder ikke et arkiv, men en temporær lagring af data i et begrænset tidsrum, hvorefter data slettes.

docPost

docPost er en batchoverførsels service af post fra kunden til e-Boks, hvor Docpoint optræder som mellemmand. Kunden afleverer den post, der skal sendes, i et defineret XML-format på en SFTP-server anvist af Docpoint. Når disse XML-data er modtaget, sendes videre fra Docpoint til e-Boks*. Kvitteringer etc. modtages retur fra e-Boks og afleveres på Docpoints SFTP-server, hvorfra kunden kan hente disse data.

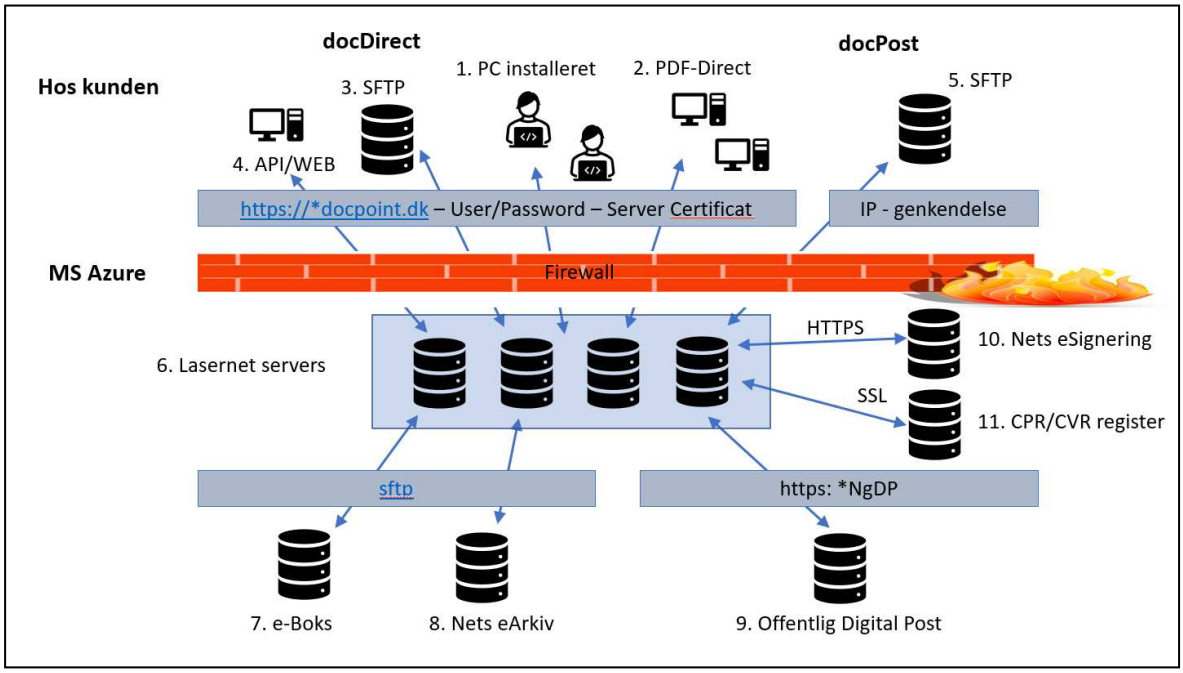
Kunden kan selv slette data efter de er læst og ellers sørger oprydningskørsler for, at ingen data ligger i mere end 31 dage.

*I efteråret 2022 er der foretaget et skifte i relation til leverancer til e-Boks, sådan at data nu leveres direkte til e-Boks i stedet for at disse sendes gennem Nets. Post der skal sendes til fysisk print og forsendelse med Post Danmark, vil blive sendt til en underdatabehandler hos e-Boks, som vil stå for denne opgave.

Teknisk beskrivelse

docDirect og docPost

Følgende tegning illustrerer de tekniske komponenter og netværksmæssige forbindelser, som docDirect og docPost løsningerne er baseret på.



Teknisk overblik der viser implementering af den basale sikkerhed i relation til dataudveksling med kunder og samarbejdspartnere.

docDirect

1. Der installeres 2 klienter på brugerens PC. Lasernet Meta, som simulerer en printer og Lasernet Client, som er en administrativ klient, som bruges til godkendelse af forsendelser af dokumenter samt håndtering af post, som kommer fra e-Boks/Digital Post til kunden herunder status på aktive digitale underskrifter.
   Begge klienter får forbindelse til server via Brugerident og Password, som indsættes ved installation af klienterne. Der skal ikke foretages logon efterfølgende.
   Der etableres hermed en forbindelse mellem brugerens PC og serverinstallationen via en HTTPS med et serverbaseret certifikat. Data/dokumenter transporteres via denne krypterede forbindelse til server. Der benyttes port 443.
   Klienterne kan også installeres på Terminalserver/Citrix.
2. Der kan også installeres et program, som lytter efter post hos afsender og automatisk sender posten, når den lander i den pågældende folder – PDF Direct.
3. Posten sendes via en SFTP-server
4. Posten sendes via HTTPS baseret WEB-service/API

docPost

5. Der kommunikeres via en SFTP-server, hvor IP-adressen som kunden kalder fra, er registreret på en positivliste.

MS Azure

6. LOM er installeret på servere hos Microsoft Azure i deres Europe setup.
   Tegningen viser 4 servere, men der er aktuelt 7 servere. Dette tal vil variere i forhold til, hvilke kunder vi har og opgaver der skal løses.

e-Boks, Nets og andre samarbejdspartnere

7. Der etableres en SFTP-forbindelse fra Lasernet Servere til e-Boks suppleret af et certifikat, som sikrer at modtager (e-Boks) kender afsender (Docpoint). Data/dokumenter afleveres via denne krypterede forbindelse.

8. Der etableres på samme måde en forbindelse til Nets eArkiv, når der afleveres data hertil.

9. Der benyttes en https-og REST protokol til at sende til og hente data fra Offentlig Digital Post.
   Da der sendes på vegne af kunder, skal der udveksles en API-key med kunden, som kunden får fra NgDP administrationssystemet. Denne API-key registreres i Docpoints kunde-DB.

10. Nets eSignering kaldes via https og med et certifikat udstedt af Nets.

11. Ved opslag i CPR-registeret efter navn benyttes SSL og et certifikat udstedt af CPR-registeret.

Sikkerhedsimplementering i docDirect

Der arbejdes med krav til sikkerhedsimplementering under følgende overskrifter:

1. Sikkerhed i relation til medarbejdere
2. Sikkerhed i infrastrukturen
3. Sikkerhed i applikationen
4. Klient software til installation hos kunden (afsender)

Sikkerheden er implementeret ud fra det mål, at løsningerne skal efterleve markedsmæssige krav, sådan vi fra Docpoints side kan indgå databehandleraftaler med kunder fra det offentlige, finans og det private.

Sikkerheden er implementeret baseret på et ISM (Information Security Management) program for Docpoint generelt og docDirect/docPost specifikt. Denne implementering har bl.a. forholdt sig til følgende.

Sikkerhed i relation til medarbejdere

Sikkerhed i relation til medarbejdere skal sikre, at medarbejdere ikke har adgang til infrastruktur, funktioner og data, som ikke er nødvendige for deres arbejde. Desuden skal sikkerhedsimplementeringen håndtere, at hvis medarbejdere får adgang til data, som er personlige/personfølsomme, at medarbejderen så ved, hvordan denne skal håndtere dette.

Samtidig skal sikkerhedsimplementeringen give plads til, at der kan ydes den nødvendige support.

Opgaver i relation til ændringer i systemet er styret af change management processer og understøttet af backup/restore, sådanne ændringer er dokumenteret og det er muligt at lave systemmæssig fallback, hvis en fejlbehæftet ændring kræver det.

Sikkerhed i infrastrukturen

Opsætningen af server infrastrukturen, som leveres af MS Azure, skal sikre, at der ikke tabes data, at data er krypteret i nødvendigt omfang ved lagring og transporteres samt at driften er stabil.

Sikkerhed i applikationen og i driften af applikationen

Applikationen er bygget sådan, at data ikke kan mistes under transport, at persondata kun lagres temporært og nødvendigt i det omfang der skal til, for at kunne levere support og fejlfri transport.
Data der lagres permanent, indeholder ikke persondata og kun nødvendige data for at kunne dokumentere forsendelser, afregne opgaver og supportere løsningen.

Sikkerhedsimplementering i klientsoftware

Løsningen kræver, at der installeres 2 programmer hos kunden (afsender) pr. bruger, der benytter løsningen. Installationen kan foretages direkte på PC eller via Citrix eller Terminal Server.

Disse programmer installeres under brugerens Windows logon, hvorfor det kun er den/de brugere, som har fået programmerne installeret, som kan benytte disse. Det vil sige, at rettighedsstyringen til programmerne ligger hos kunden (afsender) selv.

I forbindelse med installation skal der benyttes bruger-ID og Password, som er nødvendige for at kunne skabe en sikker krypteret forbindelse mellem kunden (afsender) og Docpoints server.

Docpoint oplyser bruger-ID og Password i forbindelse med installationen. Som bruger-ID benyttes kundens CVR-nr. evt. med et suffiks. Nye password er som standard minimum 8 karakterer med en blanding af små og store tal og bogstaver. Har kunden (afsender) specielle krav til password, vil disse blive imødekommet så vidt det er muligt. Password er max. 10 karakter langt.

Password fremsendes af anden kanal til kunden end oplysning om bruger-ID f.eks. SMS.

Den krypterede dialog mellem klienten og Docpoint LOM server sker krypteret baseret på serverinstalleret certifikat, hvorfor der ikke skal vedligeholdes certifikat på klienterne.

Password er statisk og ændres ikke. Password kan oplyses/ændres på kundens anfordring, hvis dette ønskes. Som udgangspunkt installeres alle klienter med samme, bruger ID og password hos en kunde medmindre andet aftales, hvorfor alle installationer skal opdateres, såfremt password ændres.

Drift og support

Driftsmål

LOM har samme oppetidsmål, som den platform denne afvikles på hos MS Azure, som arbejder med en SLA med en oppetid på 99,9% målt over døgnets 24 timer, 365 dage om året. Der rapporteres ikke en faktisk leveret oppetid og der er ingen bod, hvis der skulle opstå en situation, hvor der ikke bliver leveret den målsatte oppetid.

Docpoint har reserveret et servicevindue alle søndage mellem kl. 09.00 og 11.00, hvor det er tilladt at gennemføre ændringer, hvor nedetid er nødvendigt.

På Docpoint.dk er der link til driftsstatus hos e-Boks og Nets.

Er der problemer med LOM-server eller andet, som Docpoint er ansvarlig for, vil de berørte kunder blive informeret direkte via kontaktperson (se denne).

Kontakt vedrørende drift

Kunden oplyser Docpoint følgende:

1. e-mailadresse evt. flere til brug for modtagelse af distributionsrapport
2. Kontaktinformation – Navn, telefonnr. og e-mail tilhørende person, som Docpoint kan kontakte, hvis der er driftsmæssige problemer eller evt. et databrud. Det er kundens pligt at holde Docpoint informeret, hvis kontaktinformation ændres.
3. e-mailadresse evt. flere tilknyttet den enkelte forsendelse. Denne information bruges til at holde afsender person informeret om den specifikke forsendelse/transaktion, hvilket kan være i en fejlsituation eller f.eks. hvis en kontrakt er blevet digital underskrevet.

Support

Docpoint er support level 1 og e-Boks/Nets support level 2, hvorfor kunden altid skal kontakte Docpoint, sådan der sikres den rigtige behandling af en given problemstilling

Fejl/problemer som vedr. kundernes aflevering af data/dokumenter via de klienter, der er installeret hos kunden, håndteres af Docpoint, hvilket også gælder evt. forsendelse af digitalt underskrevne dokumenter til kundens elektroniske arkiv.

Docpoint yder support i kontortiden 08.30 – 16.00 alle hverdage på telefon/mail. Ved fejlsituationer udenfor kontortid ydes der kun support ved generelle driftsfejl.

Docpoint anvender TeamViewer eller Microsoft Teams i forbindelse med supportopgaver.

Support vil blive ydet, når Docpoint kontaktes og i den rækkefølge som henvendelserne indløber. Docpoint kan ikke give en tidsmæssig garanti for problemløsning, men vil altid bestræbe sig på at løse et problem hurtigst muligt.

Support vedr. driftsfejl-/problemer, som skyldes fejl i LOM setup eller dennes tekniske relationer til e-Boks, Nets eSignering, offentlig Digital Post, netværk etc., ydes uden beregning.

Support vedr. driftsfejl-/problemstillinger, som skyldes forkert brug af systemet eller på anden måde skyldes forhold hos kunden, afregnes som en supportydelse med den medgåede tid.
Supportkald, som skyldes fejl/problemer, som Docpoint ikke er skyld i, vil blive håndteret med servicemæssig konduite, sådanne misforståelser eller småproblemer løses uden fakturering.

Docpoint yder support i forbindelse med opstart og evt. senere udvidelse/vedligeholdelse af klienter hos en kunde.

Backup

Der tages en daglig backup af de aktive data i LOM, hvilket omhandler følgende:

- Data der definerer opsætningen pr kunde
- Procesdata vedr. forsendelser/digitale underskrifter som endnu ikke er afsluttet
- Dokumenter der er lagt op i LOM, men afventer kundens godkendelse til forsendelse

Backup gemmes i 14 dage, hvilket vil sige, at der i backup ikke er lagret evt. kundedokumenter i mere end 14 dage, hvorefter de vil blive slettet. Backup kan kun bruges til genetablering af serverinstallation og ikke til fremfinding af tidligere fremsendte dokumenter.

Logning

Applikationen (LOM) logger de data, der er nødvendige for at kunne afregne forsendelser og følge udviklingen i den driftsmæssige leverance. Der er ingen personfølsomme data i loggen ud over modtagers CPR-nr. på en konkret forsendelse. Af systemmæssige årsager lagres data vedr. forsendelser mellem 30 og 60 dage afhængig af typen, hvorefter de slettes.

Reetablering

LOM kan reetableres ved at følge procedure for reetablering af LOM på Azure. Reetableringen er baseret på seneste etablerede driftsversion og kundeopsætning etableret på seneste backup tidspunkt.

Klient opdateringer / nye versioner

Klient software, som installeres hos kunden, holdes ajour på 2 niveauer:

1. Ændringer til applikationens funktionalitet f.eks. udvidelse med et nyt felt, vil ikke kræve reinstallation men blot en genstart af klientprogrammet, hvormed ændringerne vil slå igennem.

2. Ændringer i selve klientsoftwaren vil kræve en reinstallation af denne, hvilket f.eks. kunne være en ny version, som er nødvendig for at kunne tilvejebringe ny og ønsket funktionalitet i den applikation, som afvikles på klienten. Der kan foretages opgraderinger og ændringer på LOM Server uden det har indflydelse på klient software.

Datasikkerhed

Lagring og sletning af data

I forhold til den brugsmæssige anvendelse af docDirect lagres data/dokumenter kun i det omfang, det er nødvendigt af hensyn til en fejlfri og stabil leverance fra kunden til e-Boks/Digital Post samt mulighed for at give en brugbar support. Der foreligger en oversigt over datagrupper, hvor bl.a. slettekriterier er angivet. Ingen data lagres længere end 60 dage efter en transaktion er gennemført.

Eneste undtagelse er den driftsmæssige log, hvor data gemmes op til et år.

I docPost er det kundens (afsenders) egen opgave at sikre, at data slettes. En oprydningskørsel udført af Docpoint sørger dog for, at ingen data lagres i mere end 31 dage.

Adgang til data

Der kan som sådan ikke gives adgang til kundens data, da data/dokumenter kun lagres temporært i LOM.
En medarbejder, der har driftsmæssige opgaver f.eks. i forbindelse med support, vil kunne få adgang til enkeltdokumenter eller en batch af dokumenter, som er aktuelle i forbindelse med supportopgaven, men ellers er der ikke mulighed for at få adgang til dokumenter/data fremsendt af kunden.

Tredjelandsoverførsler

Der overføres ikke data til tredjeland. Skal der overføres data til andre end de underdatabehandlere, der fremgår af indgået databehandleraftale, skal der være en udførlig instruks om dette udarbejdet af den dataansvarlige.

Tavshedspligt

Alle medarbejdere, evt. eksterne konsulenter og partnere i Docpoint, som vil kunne komme i berøring med persondata i forbindelse med support evt. anden aktivitet, underskriver en fortrolighedserklæring, af hvilken det fremgår, at det vil være strafbart at videregive personoplysninger til 3.-mand.

Væsentlige ændringer

Der har ikke været væsentlige ændringer i perioden.

Komplementerende kontroller – som anbefales udført af den dataansvarlige

Den dataansvarlige (afsender) anbefales at arbejde med følgende typer komplementerende kontroller:

docDirect

1. Adgang til løsningen docDirect hos dataansvarlig. Det er sådan, at de personer, der har adgang til docDirect løsningen hos den dataansvarlige, vil kunne sende post på vegne af denne. Da sikker digital post er en kanal, som overvejende benyttes til fortrolig post af en vis betydning for modtager og evt. afsender, så kan et misbrug af denne kanal være skadelig for den dataansvarlige (afsender). Dataansvarlig bør derfor sikre, at det kun er de medarbejdere, som faktisk skal have denne mulighed for at sende post i e-Boks, også er dem, som kun har det.
2. At post ikke fejlforsendes, hvilket kan ske, hvis et forkert CPR-nr. knyttes til et brev på samme måde, som hvis et brev kom i en kuvert anført en forkert modtageradresse. docDirect indeholder mulighed for visuel kontrol først i Lasernet Meta og efterfølgende i Lasernet Client. I Lasernet Meta kan et CPR-nr. kontrolleres ved at lave et opslag i CPR-registeret og i Lasernet Client kan en forsendelse f.eks. en samlet forsendelse, som er resultatet af en brevfletning i Word, kontrolleres med hensyn til antal, modtagere og indhold i brev, inden posten frigives. Det anbefales derfor, at dataansvarlig sikrer, at medarbejdere, der har adgang til docDirect, er uddannet og oplært i at benytte løsningen, sådan risikoen for fejlforsendelser minimeres.
3. Arkivering af modtagne kvitteringer (Distributionsrapporter evt. digital signerede dokumenter). Den dataansvarlige vil dagligt modtage en kvitteringsrapport, som sendes til en aftalt mailadresse evt., henter dataansvarlig distributionsrapporten i Lasernet Client (Postklienten).
   Denne rapport indeholder en kvittering for den leverede digitale post, hvorfor der anbefales, at den dataansvarlige har indført en instruks, af hvilken det fremgår, hvordan disse rapporter skal arkiveres. Dette gælder også, hvis dataansvarlig benytter docDirect til at få dokumenter digitalt underskrevet, så bør der også være en instruks, som sikrer, at dokumenter påført den digitale underskrift arkiveres.

docPost

docPost er en mere teknisk løsning, hvorfor de komplementerende kontroller bør fokusere på henholdsvis input og output til løsningen.

1. Der være procedurer for test, når der ændres i de systemer, der danner input til forsendelser, sådan det sikres, at der ikke opstår fejl i det materiale der sendes. Fejl kan være i relation til indhold i breve, f.eks. at der knyttes et forkert CPR-nr. til data eller at indhold simpelthen er fejlbehæftet.
   Fejl kan også ligge i det visuelle/det grafiske, som kunne vise sig at se anderledes ud, når det når frem til modtager end forventet. Størrelsen på brevet målt i kB kan også have en betydning, idet post der sendes af privat virksomhed i e-Boks afregnes efter størrelse.
2. At det output der kommer fra e-Boks f.eks. kvitteringer for leverancer – både dem der er gået godt og dem, som er gået skidt, bliver gemt på en måde, sådan disse kan fremfindes igen. Dette kan have stor betydning, hvis det skal kunne bevises, at en forsendelse faktisk er sendt til en modtager eller hvis der skal vælges en anden forsendelsesform, hvis levering af digital post fejler.

Afsnit 2: Docpoint A/S' udtalelse

Medfølgende beskrivelse er udarbejdet til brug for Docpoint A/S' kunder, som har indgået en databehandleraftale med Docpoint A/S, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført ved vurdering af, om kravene i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesforordningen") er overholdt.

Docpoint A/S anvender underleverandørerne og underdatabehandlerne Microsoft Azure A/S, e-Boks og NETS A/S. Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos Docpoint A/S' underleverandører og underdatabehandlere. Visse kontrolmål i beskrivelsen kan kun nås, hvis underleverandørens kontroller, der forudsættes i designet af vores kontroller, er passende designet og er operationelt effektive. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underleverandører.

Enkelte af de kontrolmål, der er anført i Docpoint A/S' beskrivelse i afsnit 1 af docDirect og docPost løsningerne, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos Docpoint A/S. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disses komplementerende kontroller.

Docpoint A/S bekræfter, at:

a) Den medfølgende beskrivelse, afsnit 1, giver en retvisende beskrivelse af, hvordan Docpoint A/S har behandlet personoplysninger på vegne af dataansvarlige i perioden fra 1. januar 2022 til 31. december 2022. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan Docpoint A/S' processer og kontroller relateret 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
   - 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 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
   - Kontroller, som vi med henvisning til docDirect og docPost løsningernes 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 ved databehandlerens docDirect og docPost løsningerne 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 den beskrevne docDirect og docPost løsningerne 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 docDirect og docPost løsningerne, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i perioden fra 1. januar 2022 til 31. december 2022, hvis relevante kontroller hos underleverandører var operationelt effektive, og dataansvarlige har udført de komplementerende kontroller, som forudsættes i designet af Docpoint A/S i perioden fra 1. januar 2022 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 identificeret

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

(iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i 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 aftalerne med de dataansvarlige, god databehandlerskik og relevante krav til databehandlere i henhold til databeskyttelsesforordningen.

Brøndby, den 12. maj 2023
Docpoint A/S

Søren Kvorning
Adm. direktør

Afsnit 3: Uafhængig revisors erklæring med høj grad af sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftaler med kunder i perioden fra 1. januar 2022 til 31. december 2022

Til Docpoint A/S og Docpoint A/S' kunder i rollen som dataansvarlige.

Omfang

Vi har fået til opgave at afgive erklæring med høj grad af sikkerhed om Docpoint A/S' beskrivelse i "Afsnit 1" af docDirect og docPost løsningerne i henhold til databehandleraftaler med deres kunder, i rollen som dataansvarlig i perioden fra 1. januar 2022 til 31. december 2022 og b+c om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Docpoint A/S anvender underleverandørerne og underdatabehandlerne Microsoft Azure A/S, e-Boks og NETS A/S. Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos Docpoint A/S' underleverandører og underdatabehandlere. Visse kontrolmål i beskrivelsen kan kun nås, hvis underdatabehandlernes kontroller, der forudsættes i designet af Docpoint A/S´ kontroller, er passende designet og fungerer effektivt sammen med de relaterede kontroller hos Docpoint A/S.

Enkelte af de kontrolmål, der er anført i Docpoint A/S' beskrivelse i afsnit 1 af docDirect og docPost løsningerne, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos Docpoint A/S. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disses komplementerende kontroller.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Docpoint A/S' ansvar

Docpoint A/S er ansvarlig for udarbejdelsen af beskrivelsen og 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 samt for at udforme, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Grant Thorntons 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.

Grant Thornton anvender international standard om kvalitetsstyring, ISQC 1[1] , og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder og gældende krav ifølge lovgivning og øvrig regulering.

[1] ISQC 1, Kvalitetsstyring i firmaer, som udfører revision og review af regnskaber, Andre erklæringsopgaver med sikkerhed og beslægtede opgaver.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Docpoint A/S' beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

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

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af docDirect og docPost løsningerne samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte mål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i "Afsnit 2".

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

Begrænsninger i kontroller hos en databehandler

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

Konklusion

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

(a) at beskrivelsen af docDirect og docPost løsningerne, således som denne var udformet og implementeret i 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 i perioden fra 1. januar 2022 til 31. december 2022, for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, ville blive opnået, hvis kontroller hos underleverandører var operationelt effektive, og hvis dataansvarlige har designet og implementeret de komplementerende kontroller, der forudsættes i designet af Docpoint A/S' kontroller i perioden fra 1. januar 2022 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 fungeret effektivt i perioden fra 1. januar 2022 til 31. december 2022.

Beskrivelse af test af kontroller

De specifikke kontroller, der er testet, samt arten og resultater af disse tests, fremgår i afsnit 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i det efterfølgende afsnit, Afsnit 4, er udelukkende tiltænkt dataansvarlige, der har anvendt Docpoint A/S' docDirect og docPost løsningerne, 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 12. maj 2023

Grant Thornton
Statsautoriseret Revisionspartnerselskab

Jacob Helly Juell-Hansen
Statsautoriseret revisor

Basel Rimon Obari
Executive director, CISA, CISM

Afsnit 4: Kontrolmål, udførte kontroller, test og resultater heraf

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

Vores test af funktionaliteten har omfattet de kontrolmål og tilknyttede kontroller, der er udvalgt af ledelsen, og som fremgår af kontrolmålene A-I nedenfor. Vores test har omfattet de kontroller, som blev vurderet nødvendige for at kunne opnå en høj grad af sikkerhed for, at de anførte kontrolmål blev nået i perioden fra 1. januar 2022 til 31. december 2022.

Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos Docpoint A/S' underleverandører og underdatabehandlere.

Kontroller udført hos de dataansvarlige er ikke omfattet af vores erklæring.

Vi har udført vores tests af kontroller hos Docpoint A/S via følgende handlinger:

Metode	Overordnet beskrivelse
Forespørgsel	Forespørgsel af passende personale hos Docpoint A/S. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Observation af, hvordan kontroller udføres
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.
Genudførelse af kontrol	Vi har gentaget udførelse af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

Kortlægning af kontrolområder op mod GDPR-artikler, ISO 27701 og ISO 27001/2

I tabellen nedenfor er kontrolaktiviteterne i den følgende oversigt kortlagt op mod artiklerne i GDPR, samt mod ISO 27701 og ISO 27001/2.

Artikler og punkter markeret med fed angiver primære områder.

Kontrolaktivitet	GDPR-artikler	ISO 27701	ISO 27001/2
A.1	5, 26, **28**, 29, 30, 32, 40, 41, 42, 48	8.5.5, 5.2.1, 6.12.1.2, 6.15.1.1, 8.2.1, **8.2.2**	*Nyt område ift. ISO 27001/2*
A.2	**28**, 29, 48	8.5.5, 6.15.2.2, **6.15.2.2**	18.2.2
A.3	**28**	**8.2.4, 6.15.2.2**	18.2.2
B.1	31, **32**, 35, 36	**5.2.2**	4.2
B.2	**32,** 35, 36	**7.2.5, 5.4.1.2, 5.6.2**	6.1.2, 5.1, 8.2
B.3	**32**	**6.9.2.1**	**12.2.1**
B.4	28 stk. 3; litra e, **32; stk. 1**	**6.10.1.1, 6.10.1.2, 6.10.1.3**, 6.11.1.3	**13.1.2**, 13.1.3, 14.1.3, 14.2.1
B.5	32	6.6.1.2, 6.10.1.3	9.1.2, 13.1.3, 14.2.1
B.6	**32**	**6.6**	9.1.1, 9.2.5
B.7	**32**	**6.9.4**	12.4
B.8	**32**	**6.15.1.5**	18.1.5
B.9	**32**	**6.9.4**	12.4
B.10	**32**	**6.11.3**	14.3.1
B.11	**32**	**6.9.6.1**	12.6.1
B.12	28, **32**	**6.9.1.2, 8.4**	12.1.2
B.13	**32**	**6.6**	9.1.1
B.14	**32**	**7.4.9**	*Nyt område ift. ISO 27001/2*
B.15	**32**	**6.8**	11.1.1-6
C.1	**24**	**6.2**	5.1.1, 5.1.2
C.2	**32, 39**	**6.4.2.2, 6.15.2.1, 6.15.2.2**	7.2.2, 18.2.1,18.2.2
C.3	**39**	**6.4.1.1-2**	7.1.1-2
C.4	28, 30, **32, 39**	**6.10.2.3**, 6.15.1.1, 6.4.1.2	7.1.2, 13.2.3
C.5	**32**	**6.4.3.1, 6.8.2.5, 6.6.2.1**	7.3.1, 11.2.5, 8.3.1
C.6	**28,** 38	**6.4.3.1, 6.10.2.4**	7,3.1, 13.2.4
C.7	**32**	**5.5.3, 6.4.2.2**	7.2.2, 7.3
C.8	**38**	**6.3.1.1, 7.3.2**	6.1.1
C.9	6, 8, 9, 10, 15, 17, 18, 21, 28, **30**, 32, 44, 45, 46, 47, 48, 49	6.12.1.2, 6.15.1.1, 7.2.2, **7.2.8**, 7.5.1, 7.5.2, 7.5.3, 7.5.4, **8.2.6**, 8.4.2, 8.5.2, 8.5.6	*Nyt område ift. ISO 27001/2*
D.1	6, 11, **13, 14,** 32	**7.4.5**, **7.4.7**, 7.4.4	*Nyt område ift. ISO 27001/2*
D.2	6, 11, 13, 14, **32**	**7.4.5**, **7.4.7**, 7.4.4	*Nyt område ift. ISO 27001/2*
D.3	13, **14**	**7.4.7**, 7.4.4	*Nyt område ift. ISO 27001/2*
E.1	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*Nyt område ift. ISO 27001/2*
E.2	13, 14, **28,** 30	**8.4.2, 7.4.7, 7.4.8**	*Nyt område ift. ISO 27001/2*
F.1	6, 8, 9, 10, 17, 18, 22, 24, 25, 28, **32,** 35, 40, 41, 42	5.2.1, **7.2.2**, **7.2.6**, 8.2.1, 8.2.4, 8.2.5, 8.4.2, 8.5.6, 8.5.7	15
F.2	**28**	**8.5.7**	15
F.3	**28**	**8.5.8**, 8.5.7	15
F.4	**33, 34**	**6.12.1.2**	15
F.5	**28**	**8.5.7**	15
F.6	**33, 34**	**6.12.2**	15.2.1-2
G.1	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, **8.5.1**, 8.5.2, 8.5.3	13.2.1, 13.2.2
G.2	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1,** 7.5.2, 7.5.3, 7.5.4, **8.4.2,** 8.5.2, 8.5.3	13.2.1
G.3	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, 8.5.3	13.2.1
H.1	12, **13, 14,** 15, 20, 21	**7.3.5, 7.3.8, 7.3.9**	*Nyt område ift. ISO 27001/2*
H.2	12, **13, 14,** 15, 20, 21	**7.3.5, 7.3.8, 7.3.9**	*Nyt område ift. ISO 27001/2*
I.1	**33, 34**	**6.13.1.1**	16.1.1-5
I.2	**33, 34**, 39	6.4.2.2, **6.13.1.5, 6.13.1.6**	16.1.5-6
I.3	**33, 34**	**6.13.1.4**	16.1.5
I.4	**33, 34**	**6.13.1.4,** 6.13.1.6	16.1.7

Kontrolmål A – Instruks vedrørende behandling af personoplysninger

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

Nr.	*Docpoint A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af 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.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.
A.2	Databehandleren udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Vi har stikprøvevis inspiceret, at behandlinger af personoplysninger foregår i overensstemmelse med instruks.	Ingen afvigelser konstateret.
A.3	Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Vi har inspiceret, at der er en proces, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning. Vi har forespurgt, om databehandleren har modtaget instrukser, som efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Vi er blevet informeret om, at databehandleren ikke har modtaget instrukser, som efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret, hvorfor vi ikke har testet effektiviteten af relevante processer. Ingen afvigelser konstateret.

Kontrolmål B – Tekniske foranstaltninger

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

Nr.	*Docpoint A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der er formelle driftsprocedurer, som sikrer løbende overensstemmelse. Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.
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 inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger.	Ingen afvigelser konstateret.
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Vi har stikprøvevis inspiceret aktiver, som har adgang til personoplysninger, og påset, at disse er udstyret med malwarebeskyttelse. Vi har inspiceret, at antivirus software er opdateret.	Ingen afvigelser konstateret.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Vi har inspiceret informationssikkerhedspolitikken, og påset, at der er krav til firewall. Vi har stikprøvevis inspiceret firewall, og stikprøvevis påset, at denne er konfigureret i overensstemmelse med politikken.	Ingen afvigelser konstateret.
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Vi har inspiceret netværksdokumentation for at sikre behørig segmentering.	Ingen afvigelser konstateret.

Kontrolmål B – Tekniske foranstaltninger

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

Nr.	*Docpoint A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Vi har inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugernes adgang til personoplysninger. Vi har forespurgt til, om der har været ansættelser eller fratrædelser i perioden.	Vi er blevet informeret om, at der ikke har været ansættelser eller fratrædelser i perioden, hvorfor vi ikke har kunnet teste effektiviteten af databehandlerens procedurer. Ingen afvigelser konstateret.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	Vi har stikprøvevis inspiceret overvågning af systemer og servere, og stikprøvevis påset, at der er etableret overvågning med alarmering.	Ingen afvigelser konstateret.
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Vi har stikprøvevis inspiceret transmission af personoplysninger over nettet, og stikprøvevis påset, at dette sker krypteret.	Vi har observeret, at der for én ud af to stikprøver, understøttes en forældet protokol. Ingen yderligere afvigelser konstateret.
B.9	Der er etableret logning i systemer, databaser og netværk.	Vi har stikprøvevis inspiceret logopsætning, og stikprøvevis påset, at denne er konfigureret i henhold til intern politik.	Ingen afvigelser konstateret.
B.10	Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.	Vi har forespurgt til, om der anvendes personoplysninger i forbindelse med test. Vi har stikprøvevis inspiceret dokumentation for anvendelse af anonymiseret eller pseudonymiseret data i test.	Ingen afvigelser konstateret.
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	Vi har stikprøvevis påset, at der er blevet udført sårbarhedsskanninger i perioden.	Ingen afvigelser konstateret.

Kontrolmål B – Tekniske foranstaltninger

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

Nr.	*Docpoint A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Vi har inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches. Vi har stikprøvevis inspiceret ændringer i perioden, og stikprøvevis påset, at disse følger den interne procedure.	Ingen afvigelser konstateret.
B.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Vi har inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Vi har forespurgt til, om der har været ansættelser eller fratrædelser i perioden. Vi har inspiceret, at der foreligger dokumentation for regelmæssig – og mindst en gang årligt – vurdering og godkendelse af tildelte brugeradgange.	Vi er blevet informeret om, at der ikke har været ansættelser eller fratrædelser i perioden, hvorfor vi ikke har kunnet teste effektiviteten af databehandlerens procedurer. Ingen afvigelser konstateret.
B.14	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører højrisiko for de registrerede, sker som minimum ved anvendelse af to-faktor autentifikation.	Vi har forespurgt til anvendelse af to-faktor login til servermiljøet. Vi har inspiceret, at der er implementeret kompenserende kontroller i stedet for to-faktor autentificering.	Ingen afvigelser konstateret.
B.15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Vi har inspiceret, at databehandleren har oversigt over nøgler til kontor.	Ingen afvigelser konstateret.

Kontrolmål C – Organisatoriske foranstaltninger

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

Nr.	*Docpoint A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
C.1	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. It-sikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Vi har inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Vi har forespurgt om informationssikkerhedspolitikken er tilgængelig for relevante medarbejdere.	Ingen afvigelser konstateret.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Vi har stikprøvevis inspiceret at kravene i databehandleraftalerne 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.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Vi har forespurgt til ansættelser i erklæringsperioden.	Vi er blevet informeret om, at der ikke har været ansættelser i perioden, hvorfor vi ikke har kunnet teste effektiviteten af databehandlerens procedurer. Ingen afvigelser konstateret.
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 inspiceret, at der foreligger formaliserede procedurer, som sikrer, at nyansatte medarbejdere underskriver en fortrolighedsaftale og bliver introduceret til relevante politikker og procedurer. Vi har forespurgt til ansættelser i erklæringsperioden.	Vi er blevet informeret om, at der ikke har været ansættelser i perioden, hvorfor vi ikke har kunne teste effektiviteten af databehandlerens procedurer. Ingen afvigelser konstateret.
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Vi har inspiceret procedurer der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages. Vi har forespurgt til fratrædelser i erklæringsperioden.	Vi er blevet informeret om, at der ikke har været fratrædelser i erklæringsperioden, hvorfor vi ikke har kunnet teste effektiviteten af relevante procedurer. Ingen afvigelser konstateret.

Kontrolmål C – Organisatoriske foranstaltninger

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

Nr.	*Docpoint A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
C.6	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, databehandleren udfører for de dataansvarlige.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt Vi har forespurgt til fratrædelser i erklæringsperioden.	Vi er blevet informeret om, at der ikke har været fratrædelser i erklæringsperioden, hvorfor vi ikke har testet effektiviteten af relevante procedurer. Ingen afvigelser konstateret.
C.7	Der gennemføres løbende awarenesstræning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Vi har inspiceret, at databehandleren udbyder awareness-træning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger.	Ingen afvigelser konstateret.
C.8	Databehandleren har vurderet behovet for en DPO, og har sikret, at DPO'en har tilstrækkelig faglighed til at udføre sine opgaver, samt at DPO'en bliver inddraget i relevante områder.	Vi har inspiceret dokumentation for, at databehandleren har vurderet behov for en databeskyttelsesrådgiver i perioden.	Ingen afvigelser konstateret.
C.9	Der foreligger hos databehandleren en fortegnelse over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige.	Vi har inspiceret, at der foreligger fortegnelser, som ledelsen har behandlet og godkendt inden for det seneste år.	Ingen afvigelser konstateret.

Kontrolmål D -Tilbagelevering og sletning af personoplysninger

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

Nr.	*Docpoint A/S' kontrolaktivitet*	*Grant Thorntons 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 inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.

Kontrolmål D -Tilbagelevering og sletning af personoplysninger

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

Nr.	*Docpoint A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
D.2	Der er aftalt specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.	Vi har stikprøvevis inspiceret ophørte databehandleraftaler, og stikprøvevis påset, at der er aftalt opbevaring og sletterutiner.	Ingen afvigelser konstateret.
D.3	Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: • Tilbageleveret til den dataansvarlige og/eller • Slettet, hvor det ikke er i modstrid med anden lovgivning.	Vi har stikprøvevis inspiceret, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført for ophørte databehandlinger i erklæringsperioden.	Ingen afvigelser konstateret.

Kontrolmål E – Opbevaring af personoplysninger

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

Nr.	*Docpoint A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af 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.	Vi har inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Vi har inspiceret, at procedurerne er opdateret i perioden.	Ingen afvigelser konstateret.
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Vi har stikprøvevis inspiceret, at der er dokumentation for, at databehandlingen, herunder opbevaring af personoplysninger, alene foretages på de lokaliteter, der fremgår af databehandleraftalen – eller i øvrigt er godkendt af den dataansvarlige.	Vi har observeret, at der for én stikprøve ud af elleve ikke er indgået en databehandleraftale. Ingen yderligere afvigelser konstateret.

Kontrolmål F – Anvendelse af underdatabehandlere

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.	*Docpoint A/S' kontrolaktivitet*	*Grant Thorntons 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 inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Vi har stikprøvevis inspiceret, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige.	Ingen afvigelser konstateret.
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underretters den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Vi har forespurgt til ændringer af underdatabehandlere i perioden.	Vi er blevet informeret om, at der ikke har været ændringer i anvendelse af underdatabehandlere i perioden, hvorfor vi ikke har testet effektiviteten af databehandlerens processer. Ingen afvigelser konstateret.
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Vi har stikprøvevis inspiceret databehandleraftaler og underdatabehandleraftaler, og stikprøvevis påset, at disse er i overensstemmelse.	Ingen afvigelser konstateret.
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere.	Vi har stikprøvevis inspiceret dokumentation for, at underdatabehandlere fremgår af databehandlerens aftaler med dataansvarlige.	Ingen afvigelser konstateret.

Kontrolmål F – Anvendelse af underdatabehandlere

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.	*Docpoint A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
F.6	Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende.	Vi har inspiceret dokumentation for, at databehandleren har ført tilsyn med underdatabehandlere i perioden.	Ingen afvigelser konstateret

Kontrolmål G – Overførsel af personoplysninger til tredjelande

Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.

Nr.	*Docpoint A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at databehandleren har formelle procedurer for overførsler til tredjelande. Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.
G.2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	Vi har stikprøvevis inspiceret databehandleraftaler, og stikprøvevis påset, at der er taget stilling til tredjelandsoverførsler. Vi har stikprøvevis inspiceret lokation for opbevaring af data. Vi har forespurgt, om databehandleren har overført personoplysninger til tredjelande eller internationale organisationer.	Vi er blevet informeret om, at personoplysninger ikke overføres til tredjelande eller internationale organisationer, og vi finder dette sandsynliggjort på baggrund af vores testhandlinger. Ingen afvigelser konstateret.

Kontrolmål G – Overførsel af personoplysninger til tredjelande

Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.

Nr.	*Docpoint A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
G.3	Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	Vi har stikprøvevis inspiceret databehandleraftaler, og stikprøvevis påset, at der er taget stilling til tredjelandsoverførsler. Vi har stikprøvevis inspiceret lokation for opbevaring af data. Vi har forespurgt, om databehandleren har overført personoplysninger til tredjelande eller internationale organisationer	Vi er blevet informeret om, at personoplysninger ikke overføres til tredjelande eller internationale organisationer, og vi finder dette sandsynliggjort på baggrund af vores testhandlinger. Ingen afvigelser konstateret.

Kontrolmål H – De registreredes rettigheder

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.	*Docpoint A/S' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder. Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.
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 inspiceret procedurer, som sikrer mulig rettidig bistand til den dataansvarlige i forbindelse med GDPR-anmodninger. Vi har forespurgt til, om der har været GDPR-anmodninger i perioden fra dataansvarlige.	Vi er blevet informeret om, at databehandleren ikke har modtaget anmodninger fra den dataansvarlige i relation til de registreredes rettigheder, hvorfor vi ikke har testet effektiviteten af databehandlerens procedurer. Ingen afvigelser konstateret.

Kontrolmål I – Håndtering af persondatasikkerhedsbrud

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

Nr.	*Docpoint A/S' kontrolaktivitet*	*Grant Thorntons udførte 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 inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Vi har inspiceret, at proceduren er opdateret.	Ingen afvigelser konstateret.
I.2	Databehandleren har etableret kontroller for identifikation af eventuelle brud på persondatasikkerheden.	Vi har inspiceret, at databehandler udbyder awarenesstræning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden.	Ingen afvigelser konstateret.
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Vi har inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Vi har forespurgt, om der har været persondatassikkerhedsbrud i perioden.	Vi er blevet informeret om, at der ikke har været nogle persondatasikkerhedsbrud i erklæringsperioden, hvorfor vi ikke har testet effektiviteten af databehandlerens procedurer. Ingen afvigelser konstateret.
I.4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	Vi har inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden.	Ingen afvigelser konstateret.