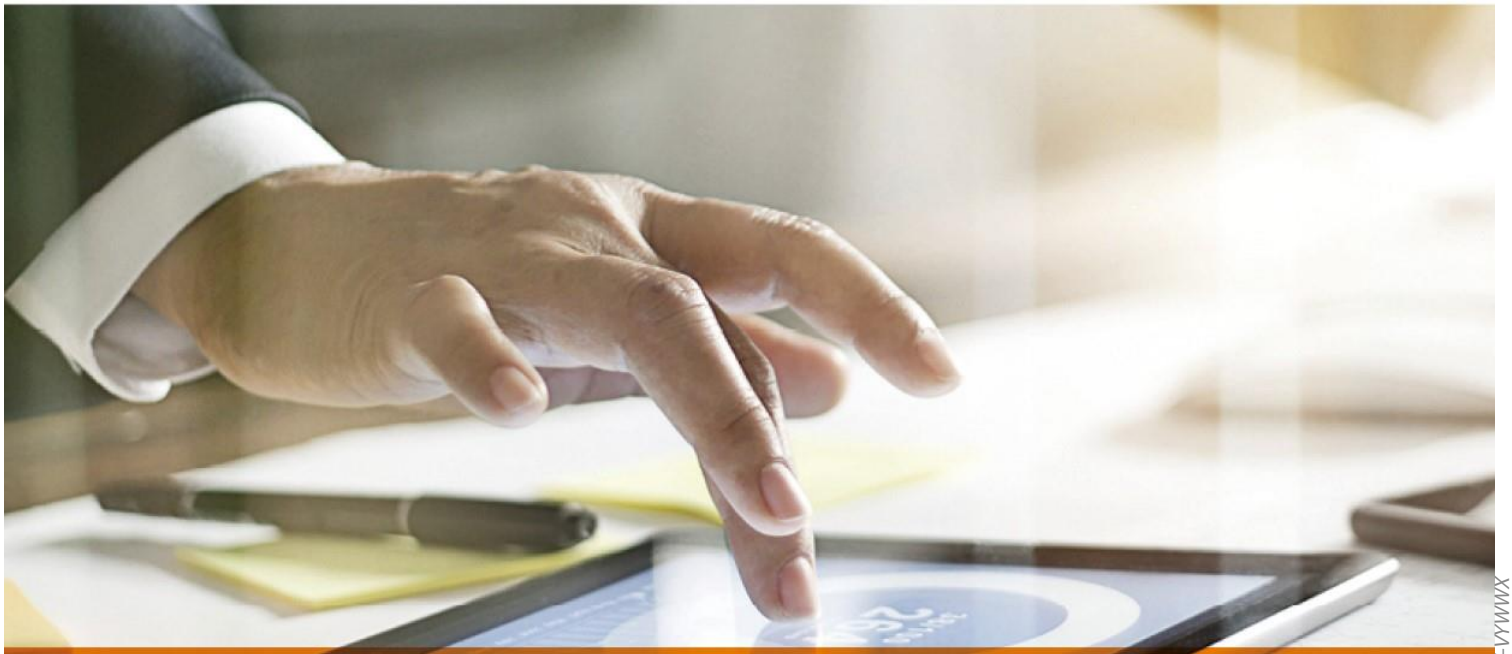
BEIERHOLM
VI SKABER BALANCE



*April 2024*

# Docpoint A/S

## ISAE 3000 TYPE 2 ERKLÆRING

CVR 35641807

Uafhængig revisors ISAE 3000 erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med dataansvarlige.



**Beierholm**
**Statsautoriseret Revisionspartnerselskab**
Knud Højgaards Vej 9
2860 Søborg
CVR 32 89 54 68
Tlf +45 39 16 76 00

www.beierholm.dk

# Erklæringsopbygning

Kapitel 1:
Ledelsens udtalelse.

Kapitel 2:
Uafhængig revisors erklæring.

Kapitel 3:
Beskrivelse af behandling.

Kapitel 4:
Kontrolmål, kontrolaktivitet, test og resultat heraf.

KAPITEL 1:

# Ledelseserklæring

Docpoint A/S behandler personoplysninger på vegne af sine kunder i henhold til databehandleraftalen.

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt Docpoint A/S' IT-løsninger, docDirect og docPost, 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 bekræfter, at:

(A) Den medfølgende beskrivelse, kapitel 3, giver en retvisende beskrivelse af Docpoint A/S' IT-løsninger, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen i hele perioden fra 1. januar 2023 til 31. december 2023. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

(i) Redegør for, hvordan kontrollerne 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 kunden dvs. 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 underretning 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 systemets 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 anvendte forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger

(ii) Indeholder relevante oplysninger om ændringer ved Docpoint A/S' IT-løsninger i behandlingen af personoplysninger foretaget i hele perioden fra 1. januar 2023 til 31. december 2023.

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne kontroller under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov

hos en bred kreds af kunder og deres revisorer og derfor ikke kan omfatte ethvert aspekt ved kontroller, som den enkelte kunde måtte anse som 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 hele perioden fra den 1. januar 2023 til 31. december 2023. Kriterierne for dette udsagn er, at:

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

(ii) De identificerede kontroller ville, hvis anvendt som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrer 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 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 aftalerne med de dataansvarlige, god databehandlerskik og relevante krav til databehandlere i henhold til databeskyttelsesforordningen.

Brøndby, den 26. april 2024

**Direktør, Søren Kvorning**
Docpoint A/S, Kildebjerg Parkvej 12, DK-2605 Brøndby, CVR-nummer: 35641807

KAPITEL 2:

# Uafhængig revisors ISAE 3000 erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med Docpoints kunder

Til Docpoint og relevante dataansvarlige

## Omfang

Vi har fået som opgave at afgive erklæring om Docpoint A/S' beskrivelse af IT-løsningerne, docDirect og docPost, jf. kapitel 3 i henhold til databehandleraftale med Docpoint A/S' kunder i hele perioden fra 1. januar 2023 til 31. december 2023 (beskrivelsen) og om udformningen og funktionen af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

## Docpoints ansvar

Docpoint A/S er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse jf. kapitel 3, 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.

## Beierholms uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i FSR – danske revisorers retningslinjer for revisors etiske adfærd (Etiske regler for revisorer), der bygger på de grundlæggende principper om integritet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

Beierholm er underlagt international standard om kvalitetsstyring, ISQM 1, og anvender og opretholder således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og krav ifølge lov og øvrig regulering.

## Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om 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. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af sit system 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 fungeret 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 jf. kapitel 3.

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

## Begrænsninger i kontroller hos Docpoint A/S

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 systemet, 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 Docpoint A/S' IT-løsninger, således som de var udformet og implementeret i hele perioden fra 1. januar 2023 til 31. december 2023, i alle væsentlige henseender er retvisende, og

b) at kontrollerne, som knyttede sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 1. januar 2023 til 31. december 2023, 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 hele perioden fra 1. januar 2023 til 31. december 2023

## Beskrivelse af test kontroller

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

## Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller under kapital 3 er udelukkende tiltænkt Docpoint A/S' kunder og deres revisorer, som har en tilstrækkelig forståelse til at overveje dem sammen med anden information, herunder information om kunders egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i deres regnskaber.

Søborg, den 26. april 2024

**Beierholm**
Statsautoriseret Revisionspartnerselskab

Kim Larsen
Statsautoriseret revisor

Allan Nielsen
Seniorkonsulent, IT-revision

KAPITEL 3:

# Indledning

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.

# Beskrivelse af docDirect og docPost

**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.

## 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 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 vedr. 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 service-mæssig 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 opdatering / 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 re-installation 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.

## Komplementerende kontroller – som anbefales udført af den dataansvarlige

**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

KAPITEL 4:

# Revisors beskrivelse af kontrolmål, sikkerhedstiltag, test og resultater heraf

KONTROLMÅL A:

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

| Docpoints kontroller | Revisors test af kontroller | Resultat af test |
|---|---|---|
| Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks.<br><br>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres. | Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks.<br><br>Inspiceret, at procedurerne indeholder krav om minimum årlig vurdering af behov for opdatering, herunder ved ændringer i dataansvarliges instruks eller ændringer i databehandlingen.<br><br>Inspiceret, at procedurer er opdateret. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |
| Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig. | Inspiceret, at ledelsen sikrer, at behandling af personoplysninger alene foregår i henhold til instruks.<br><br>Inspiceret ved en stikprøve på behandlinger af personoplysninger, at disse foregår i overensstemmelse med instruks. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |
| Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandleren mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret. | Inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning.<br><br>Inspiceret, at der er procedurer for underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen.<br><br>Vi har forespurgt databehandleren, om der har været anledning til underretning af den dataansvarlige.<br><br>Vi har fået bekræftet, at der ikke har været anledning til underretning af den dataansvarlige. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |

KONTROLMÅL B:

| Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed. | | |
|---|---|---|
| Docpoints kontroller | Revisors test af kontroller | Resultat af test |
| Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.<br><br>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres. | Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger.<br><br>Inspiceret, at procedurer er opdateret.<br><br>Inspiceret ved en stikprøve på databehandleraftaler, at der er etableret de aftalte sikringsforanstaltninger. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |
| Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de med dataansvarlige aftalte sikringsforanstaltninger. | Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandler foretager en risikovurdering for at opnå en passende sikkerhed.<br><br>Inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger.<br><br>Inspiceret, at databehandler har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen.<br><br>Inspiceret, at databehandler har implementeret de sikringsforanstaltninger, der er aftalt med de dataansvarlige. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |
| Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres. | Inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirus software og at denne er opdateret.<br><br>Inspiceret, at antivirus software er opdateret. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |
| Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall. | Inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |

KONTROLMÅL B:

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

| Docpoints kontroller | Revisors test af kontroller | Resultat af test |
|---|---|---|
| Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger. | Forespurgt, om interne netværk er segmenteret med henblik på at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.<br><br>Inspiceret netværksdokumentation for behørig segmentering. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |
| Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor. | Inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger.<br><br>Inspiceret, at der foreligger formaliserede procedurer for opfølgning på, at brugeres adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov.<br><br>Inspiceret, at de aftalte tekniske foranstaltninger understøtter opretholdelsen af begrænsningen i brugernes arbejdsbetingede adgang til personoplysninger.<br><br>Inspiceret, at der er sket opfølgning på brugeres adgange til systemer og databaser, at de er begrænset til medarbejdernes arbejdsbetingede behov. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |
| Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering. | Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret systemovervågning. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |

KONTROLMÅL B:

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

| Docpoints kontroller | Revisors test af kontroller | Resultat af test |
|---|---|---|
| Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail. | Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at transmission af følsomme og fortrolige oplysninger over internettet er beskyttet af stærk kryptering baseret på en anerkendt algoritme.<br><br>Inspiceret, at teknologiske løsninger til kryptering har været tilgængelige og aktiveret på erklæringstidspunktet.<br><br>Inspiceret, at der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet eller med e-mail.<br><br>Vi har fået bekræftet, at der ikke er sket ukrypterede transmissioner af personoplysninger i kontrolperioden. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |
| Der er etableret logning i systemer, databaser og netværk af følende forhold:<br>• Sikkerhedshændelser omfattende:<br>○ Ændringer i systemrettigheder til brugere<br><br>Logoplysninger er beskyttet mod manipulation og tekniske fejl og gennemgås løbende. | Inspiceret, at der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger herunder gennemgang og opfølgning.<br><br>Inspiceret, at logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, er konfigureret og aktiveret.<br><br>Inspiceret, at opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod manipulation og sletning.<br><br>Inspiceret ved en stikprøve på logfiler har det forventede indhold i forhold til opsætning. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |
| Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne. | Inspiceret, at der foreligger formaliserede procedurer for anvendelse af personoplysninger til udvikling, test og lignende, der sikrer, at anvendelsen alene sker i pseudonymiseret eller anonymiseret form.<br><br>Vi har fået bekræftet, at der ikke har været anvendt persondata i forbindelse med test og udvikling, og at testdata udelukkende er fiktive data. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |

KONTROLMÅL B:

| Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed. | | |
|---|---|---|
| Docpoints kontroller | Revisors test af kontroller | Resultat af test |
| De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests. | Inspiceret, at der foreligger formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder gennemførsel af sårbarhedsscanninger og penetrationstests.<br>Inspiceret ved stikprøver, at der er dokumentation for løbende tests af de etablerede tekniske foranstaltninger. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |
| Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches. | Inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches.<br>Inspiceret ved stikprøver, at der er dokumentation for løbende opdatering og patching. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |
| Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov. | Inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger.<br>Inspiceret ved en stikprøve på medarbejderes adgange til systemer og databaser, at de tildelte brugeradgange er godkendt, og at der er et arbejdsbetinget behov.<br>Inspiceret ved en stikprøve på fratrådte medarbejdere, at disses adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt.<br>Inspiceret, at der foreligger dokumentation for regelmæssig - mindst en gang årligt – vurdering og godkendelse af tildelte brugeradgange. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |
| Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører højrisiko for de registrerede, sker som minimum ved anvendelse af to-faktor autentifikation. | Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at to-faktor autentifikation anvendes ved behandling af personoplysninger, der medfører højrisiko for de registrerede.<br>Inspiceret, at brugernes adgang til at udføre behandling af personoplysninger, der medfører høj-risiko for de registrerede, alene kan ske ved anvendelse af to-faktor autentifikation. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |

KONTROLMÅL B:

| Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed. | | |
|---|---|---|
| Docpoints kontroller | Revisors test af kontroller | Resultat af test |
| Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger. | Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |

KONTROLMÅL C:

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

| Docpoints kontroller | Revisors test af kontroller | Resultat af test |
|---|---|---|
| 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.<br><br>Der foretages løbende – og mindst en gang årligt – vurdering af, om IT-sikkerhedspolitikken skal opdateres. | Inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år.<br><br>Inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |
| Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler. | Inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler.<br><br>Inspiceret ved en stikprøve på databehandleraftaler, at kravene i aftalerne er dækket af informationssikkerhedspolitikkens krav til sikringsforanstaltninger og behandlingssikkerheden. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |
| Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. | Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.<br><br>Vi har forespurgt på nyansættelser i kontrolperioden.<br><br>Vi har fået bekræftet, at der ikke er sket nyansættelser i kontrolperioden. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |

KONTROLMÅL C:

| Der efterleves procedurer og kontroller, som sikrer, at databehandleren har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed. | | |
|---|---|---|
| Docpoints kontroller | Revisors test af kontroller | Resultat af test |
| Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger. | Inspiceret, at der foreligger formaliserede procedurer, der sikrer at medarbejdere underskriver en fortrolighedsaftale ved ansættelse og bliver introduceret til informationssikkerhedspolitikken såvel som procedurerne vedrørende databehandling samt anden relevant information. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |
| Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages. | Inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver inddrages.<br>Vi har forespurgt på fratrådte medarbejdere i kontrolperioden.<br>Vi har fået bekræftet, at der ikke er sket fratrædelser i kontrolperioden. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |
| Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, databehandleren udfører for de dataansvarlige. | Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |
| Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til IT-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger. | Inspiceret, at databehandleren udbyder awareness-træning til medarbejderne omfattende generel IT-sikkerhed og behandlingssikkerhed i relation til personoplysninger.<br>Inspiceret ved interview, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført intern awareness-træning. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |

KONTROLMÅL D:

| Der efterleves procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres såfremt der indgås aftale herom med den dataansvarlige. | | |
|---|---|---|
| Docpoints kontroller | Revisors test af kontroller | Resultat af test |
| Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.<br><br>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres. | Inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.<br><br>Inspiceret, at procedurerne er opdateret. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |
| Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner:<br>• Aftalens ophør. | Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.<br><br>Inspiceret ved en stikprøve på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder.<br><br>Inspiceret ved en stikprøve på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger er slettet i overensstemmelse med de aftalte sletterutiner. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |
| Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige:<br>• Tilbageleveret til den dataansvarlige og/eller<br>• Slettet, hvor det ikke er i modstrid med anden lovgivning | Inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger.<br><br>Inspiceret ved en stikprøve på ophørte databehandlinger i erklæringsperioden, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |

KONTROLMÅL E:

| Der efterleves procedurer og kontroller, som sikrer, at databehandleren alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige. | | |
|---|---|---|
| Docpoints kontroller | Revisors test af kontroller | Resultat af test |
| Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.<br><br>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres. | Inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne.<br><br>Inspiceret, at procedurerne er opdateret.<br><br>Inspiceret ved en stikprøve på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen sker i henhold til databehandleraftalen. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |
| Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder. | Inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder.<br><br>Inspiceret ved en stikprøve på databehandlinger fra databehandlerens oversigt over behandlingsaktiviteter, 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 ikke ved vores test konstateret væsentlige afvigelser. |

KONTROLMÅL F:

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

| Docpoints kontroller | Revisors test af kontroller | Resultat af test |
|---|---|---|
| Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks.<br><br>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres. | Inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks.<br><br>Inspiceret, at procedurerne er opdateret. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |
| Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige. | Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere.<br><br>Inspiceret ved en stikprøve på underdatabehandlere fra databehandlerens oversigt over underdatabehandlere, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |
| Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underretters den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige. | Inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere.<br><br>Forespurgt om der har været ændringer af underdatabehandlere i kontrolperioden.<br><br>Vi har fået bekræftet, at der ikke har været ændringer af underdatabehandlere i kontrolperioden. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |
| Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige. | Inspiceret, at der foreligger underskrevne underdatabehandleraftaler med anvendte underdatabehandlere, som fremgår af databehandlerens oversigt.<br><br>Inspiceret ved en stikprøve på underdatabehandleraftaler, at disse indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |

KONTROLMÅL F:

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

| Docpoints kontroller | Revisors test af kontroller | Resultat af test |
|---|---|---|
| Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af:<br>• Navn<br>• CVR-nr.<br>• Adresse<br>• Beskrivelse af behandlingen | Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere.<br><br>Inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |
| Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren. | Inspiceret, at der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne.<br><br>Inspiceret dokumentation for, at der er foretaget en risikovurdering af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne.<br><br>Inspiceret dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerheden hos de anvendte underdatabehandlere, tredjelands overførselsgrundlag og lignende. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |

KONTROLMÅL G:

| 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. | | |
|---|---|---|
| Docpoints kontroller | Revisors test af kontroller | Resultat af test |
| 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.<br><br>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres. | Vi har forespurgt på dokumentation for procedurer vedr. overførsel af personoplysninger til tredjelande.<br><br>Inspiceret, at der foreligger procedurer, der sikrer, at personoplysninger alene overføres til tredjelande eller internationale organisationer ved specifik godkendelse fra den dataansvarlige.<br><br>Inspiceret, at procedurerne er opdateret.<br><br>Forespurgt om databehandleren har assisteret med overførsler til tredjelande.<br><br>Vi har bekræftet, at der ikke sket overførsler til tredjelande i kontrolperioden. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |

KONTROLMÅL H:

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

| Docpoints kontroller | Revisors test af kontroller | Resultat af test |
|---|---|---|
| Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder.<br><br>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres. | Inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder.<br><br>Inspiceret, at procedurerne er opdateret.<br><br>Forespurgt om databehandleren har bistået dataansvarlige i relation til de registreredes rettigheder.<br><br>Vi har fået bekræftet, at der ikke er sket bistand i kontrolperioden. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |

KONTROLMÅL I:

| Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale. | | |
|---|---|---|
| Docpoints kontroller | Revisors test af kontroller | Resultat af test |
| Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden.<br><br>Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres. | Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden.<br><br>Inspiceret, at proceduren er opdateret. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |
| Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden:<br><br>• Awareness hos medarbejdere | Inspiceret, at databehandler udbyder awareness-træning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |
| Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler. | Inspiceret, at databehandleren har procedurer for registrering og vurdering af sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden.<br><br>Forespurgt underdatabehandlerne, om de har konstateret nogen brud på persondatasikkerheden i erklæringsperioden.<br><br>Vi kan bekræfte, at der har været én sikkerhedshændelse ved en dataansvarlig i kontrolperioden.<br><br>Inspiceret, at databehandleren har medtaget eventuelle brud på persondatasikkerheden hos underdatabehandlere i databehandlerens oversigt over sikkerhedshændelser.<br><br>Inspiceret, at samtlige registrerede brud på persondatasikkerheden hos databehandleren eller underdatabehandlerne er meddelt de berørte dataansvarlige uden unødig forsinkelse, at databehandleren er blevet opmærksom på brud på persondatasikkerheden. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |

KONTROLMÅL I:

| Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale. | | |
|---|---|---|
| Docpoints kontroller | Revisors test af kontroller | Resultat af test |
| Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet:<br>• Karakteren af bruddet på persondatasikkerheden<br>• Sandsynlige konsekvenser af bruddet på persondatasikkerheden<br>• Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. | Inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede procedurer for:<br>• Beskrivelse af karakteren af bruddet på persondatasikkerheden<br>• Beskrivelse af sandsynlige konsekvenser af bruddet på persondatasikkerheden<br>• Beskrivelse af foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden<br>Inspiceret dokumentation for, at der ved brud på persondatasikkerheden er truffet foranstaltninger, som har håndteret bruddet på persondatasikkerheden. | Vi har ikke ved vores test konstateret væsentlige afvigelser. |

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

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

**Allan Nielsen** (CVR valideret)
**BEIERHOLM, STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 32895468**
**Seniorkonsulent, IT-revision**
På vegne af: Beierholm Statsautoriseret Revisionspar…
*Serienummer: b664e0da-9557-4d4e-8f3d-9853cddff7c1*
*IP: 212.98.xxx.xxx*
*2024-04-26 06:29:11 UTC*

**Kim Holm Larsen** (CVR valideret)
**BEIERHOLM, STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 32895468**
**Statsautoriseret revisor**
På vegne af: Beierholm Statsautoriseret Revisionspar…
*Serienummer: bff7239f-6800-4339-865f-dbc13a357020*
*IP: 104.28.xxx.xxx*
*2024-04-26 06:39:47 UTC*

**Søren Kvorning** (CVR valideret)
**DOCPOINT A/S CVR: 35641807**
**Direktør**
På vegne af: Docpoint A/S
*Serienummer: 8a0c046a-32e1-4b01-9e5d-b401144b5611*
*IP: 109.70.xxx.xxx*
*2024-04-29 06:16:36 UTC*