MARTS 2019

IMS A/S

CVR-nummer 25862015

ISAE 3402 TYPE 1 ERKLÆRING

Revisors erklæring vedrørende overholdelse af sikkerhedsprocedurer omkring dataudveksling. Rammen for sikkerhedsprocedurer er angivet i bilag D jf. databehandleraftale.

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

www.beierholm.dk

BEIERHOLM
VI SKABER BALANCE

Erklæringsopbygning

Kapitel 1:
Ledelseserklæring.

Kapitel 2:
Beskrivelse af sikkerhedsprocedurer i forbindelse med dataudveksling.

Kapitel 3:
Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller og deres udformning.

KAPITEL 1:

Ledelseserklæring

Beskrivelsen af IMS A/S' kontrolmiljø i kapitel 2 er udarbejdet til brug for kunder, der har anvendt eller påtænker at anvender IMS' dataudvekslingsservice (jf. bilag D under databehandleraftale), og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som kunderne selv har anvendt, ved vurdering af risiciene for væsentlig fejlinformation i deres regnskaber. IMS A/S bekræfter hermed, at

(A) Den medfølgende beskrivelse, kapitel 2, giver en retvisende beskrivelse af IMS A/S' kontrolmiljø i tilknytning til dataudveksling pr. 28. februar 2019. Kriterierne for dette udsagn er, at den medfølgende beskrivelse:

(i) redegør for, hvordan kontrollerne var udformet og implementeret, herunder redegør for:
- de typer af ydelser, der er leveret, når det er relevant
- de processer i både it- og manuelle systemer, der er anvendt til styring af de sikkerhedsprocedurer
- relevante kontrolmål og kontroller udformet til at nå disse mål
- kontroller, som vi med henvisning til systemets udformning har forudsat ville være implementeret af brugervirksomheder, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen sammen med de specifikke kontrolmål, som vi ikke selv kan nå
- andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for de sikkerhedsprocedurer

(ii) 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 vigtig efter deres særlige forhold.

(B) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet pr. 28. februar 2019. Kriterierne for dette udsagn er, at:

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

(C) Den medfølgende beskrivelse og de tilhørende kriterier for opnåelse af kontrolmål og kontroller, kapitel 2, er udarbejdet med baggrund i overholdelse af IMS A/S' standardaftale, grundlaget for databehandling, herunder rammen for bilag D – dataudveksling og den tilhørende sikkerhedsprocedurer. Kriterierne for dette grundlag var:

(i) IMS A/S – Databehandleraftale for drift
(ii) Bilag D – Parternes regulering af andre forhold
(iii) IMS A/S – It-sikkerhedspolitik – version 1.0

Århus, den 1. marts 2019

Henrik Poulsen, Direktør

Tormod Ween, Teknisk chef

IMS A/S, Åbogade 25, 3., 8200 Århus N, CVR-nummer 25862015

KAPITEL 2:

Beskrivelse af sikkerhedsprocedurer i forbindelse med dataudveksling

Indledning

Formålet med nærværende beskrivelse er at levere information til IMS's kunder og deres revisorer vedrørende kravene i ISAE 3402, som er den internationale revisorstandard for erklæringsopgaver om kontroller hos serviceleverandører.

Nedenstående beskrivelse er en direkte reference til bilag D i henhold til databehandlingsaftalen.

Beskrivelsen giver herudover information om de kontroller, der er anvendt i forbindelser med databehandlingen omkring IMS's aktiviteter pr. 28. februar 2019.

Omfang for denne beskrivelse

Følgende procedurer omfatter behandling af data, som potentielt indeholder kundesensitiv information. I dette dokument beskrives de regler og tiltag, som skal følges, for at kundens data er sikret efter bedste evne i forbindelse med overførsler og opbevaring af data i IMS.

Ved databehandling er der typisk en dataleverandør og en datamodtager. Dataleverandør er den part, i som afleverer data til datamodtager. Datamodtager er modtager af data leveret fra dataleverandør. Både IMS og kunde kan i følgende dokument have begge roller.

Dokumentet tager udgangspunkt i det, som betegnes som sensitive data.

Med sensitive data menes

- Data som indeholder information om kundens interne miljøer (konfigurationer, brugernavn, passwords serverinformationer etc.). Dette kan f.eks. være installationspakker, som er konfigureret til kundens interne IT-miljø.
- Al data genereret af kunde. Her tages der ikke stilling til, om data er af sensitiv natur eller ej. Al data genereret af kunde behandles som sensitiv data. Dette er for eksempel:
  - Kundegenererede dokumenter (Office dokumenter, PDF dokumenter mm)
  - Databaser tilknyttet IMS systemer
  - Databaser tilknyttet eksterne systemer
  - Systemfiler som benyttes til kommunikation med eksterne systemer (Navision, e-Boks m.fl.)
  - Digital Post

Følgende områder dækkes af procedurer

- Overførsel af sensitive data fra IMS til kunde
- Opbevaring af kundedata hos IMS
- Overførsel af sensitiv data fra kunde til IMS, hvor IMS udfører overførsel

Følgende områder dækkes ikke

- Dataopbevaring hos kunde efter endt overførsel.
- Sikring af data efter endt overførsel til kundes miljø.
- Procedurer tager ikke højde for kunder, som selv vælger at stille data til rådighed via usikre systemer. Det kan f.eks. være kunder, som sender sensitiv information via e-mail. IMS kan dog rådgive i sikre overførselsmetoder på kundens opfordring.

Følgende type data dækkes af procedurer

- Data som betegnes ”sensitiv data” som beskrevet ovenfor
- Data som befinder sig i en gråzone når det er tale, om den er sensitiv eller ej.

Følgende type data dækkes ikke af procedurer

- Data af en ikke-sensitiv natur. Dette kan for eksempel være:
  - Softwarepakker, som ikke er konfigureret specifikt til kunde, og som ikke indeholder sensitiv information om kundes eller IMS' miljøer.
  - Anden type data, som ikke indeholder tilpasset kundedata eller data som på ingen måde kan belaste kunden.

Dataoverførsler

Følgende regler gælder for overførsler af data, hvor IMS er dataleverandør, eller hvor IMS er både dataleverandør og datamodtager.

1. Datatrafik krypteres altid ved overførsel. Der benyttes primært FTPS til dette formål, hvor en intern filserver fungerer som FTPS server. WINSCP eller anden kompatibel FTPS klient benyttes som software ved overførsel på klientside.
2. Dataleverandør og datamodtager skal begrænse tilgang til data til det minimumsantal personer, som er nødvendige for at udføre det pågældende formål med dataudvekslingen.
3. Dataoverførsler udføres kun ved skriftligt samtykke fra kunden.

IMS som dataleverandør

1. Data bliver gjort tilgængelig på FTPS, hvor en unik konto bliver udleveret til datamodtager (kunden).
2. Password genereres unikt til hver enkelt kunde. Kontoinformation afleveres til aftalt person hos datamodtager.
3. Passwords og brugernavn må ikke sendes sammen.
4. Datamodtager er selv ansvarlig for at holde styr på, hvem der har tilgang til denne konto og dermed kan tilgå data.
5. Hos dataleverandør (IMS) vil konto kun være tilgængelig for de personer, som er direkte involveret i overførsel af data.
6. Konto lukkes, så snart opgaven relateret til dataoverførsel er udført.

NB. Ønsker dataleverandør selv at stille systemer til rådighed til overførsel, tager IMS ingen ansvar for sikkerhed i overførsel.

IMS som datamodtager

1. IMS gør en unik FTPS konto klar, hvortil dataleverandør kan uploade data.
2. Kontoinformation videregives til dataleverandør.
3. Password genereres unikt til hver enkelt kunde. Konto information afleveres til aftalt person hos datamodtager.
4. Passwords og brugernavn må ikke sendes sammen.

NB. Ønsker dataleverandør selv at stille systemer til rådighed til overførsel, tager IMS ingen ansvar for sikkerhed i overførsel.

IMS som mellemled i dataoverførsel fra kunde til anden leverandør - eller omvendt

IMS påtager sig ikke overførsler af data mellem kunde og tredjepartsleverandør. Dette skal kunde og tredjepart selv sørge for. IMS kan dog hjælpe med klargøring af data inden overførsel.

Kunden som dataleverandør

Kunden er selv ansvarlig for at stille data til rådighed på en sikker måde. Kunden er selv ansvarlig for sikkerheden af data, indtil den pågældende data er modtaget af IMS.

Kunden som datamodtager

IMS skal som dataleverandør sikre, at kunden kan modtage data på en sikker måde i henhold til ovenstående regler. Så snart data er modtaget, har kunden selv ansvar for sikring af data i henhold til egne interne procedurer.

NB. Ønsker datamodtager selv at stille systemer til rådighed til overførsel, tager IMS ingen ansvar for sikkerhed i overførsel.

Opbevaring af kundedata hos IMS

Ved behov for opbevaring af sensitiv kundedata hos IMS gælder følgende regler:

1. Tilgængelighed til sensitiv kundedata er altid begrænset til kun at omfatte de personer, som enten er medvirkende til at overførsel af data kan finde sted, eller som efterfølgende skal behandle data på baggrund af den pågældende opgave.
2. Efter data er overført til intern FTPS server hos IMS, flyttes den overførte data ud i et arbejdsområde, hvortil kun personer med direkte relation til arbejdsopgaven har adgang. Dette kan f.eks. være udviklers egen virtuelle maskine, som kun udviklere har adgang til.
3. Sensitiv data opbevares på dedikeret FTPS-placering, samt arbejdsområdet til de involverede. Ved behov for backups af data i forbindelse med udførelse af opgaven laves dette lokalt på den lukkede server.
4. Data slettes permanent fra al intern lagring umiddelbart efter, at opgaven er udført. Hos IMS er det den person, der udfører opgaven, som har ansvar for sletning af data.
5. Hvis det i opgaven er nødvendig at behandle data, skal der laves en databehandleraftale, inden opgave kan udføres.

KAPITEL 3:

Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller og deres udformning

Til kunder/ brugere af IMS A/S' dataudvekslingsservice og deres revisorer

Omfang

Vi har fået som opgave at afgive erklæring om IMS A/S' beskrivelse i kapitel 2, som er en beskrivelse af sikkerhedsprocedurer i forbindelse med IMS' dataudvekslingsservice pr. 28. februar 2019 samt udformningen af de kontroller, som er anført i beskrivelsen.

Vi har ikke udført handlinger vedrørende funktionaliteten af de kontroller, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Erklæringen er afgivet efter helhedsmetoden, hvilket betyder, at denne erklæring omfatter alle it-sikkerhedsmæssige kontroller og kontrolaktiviteter som er tilknyttet dataudvekslingsservice hos IMS A/S. Erklæringen afdækker ikke kundespecifikke forhold. Desuden dækker erklæringen ikke de komplementerende kontroller og kontrolaktiviteter, som udføres af brugervirksomheden.

Den nuværende it-sikkerhedspolitik med arbejdsgangsbeskrivelser er blevet udarbejdet og færdigimplementeret i januar måned 2019. Udviklingen omkring it-sikkerhed har medført, at supplerende kontroller er udformet og implementeret i løbet af implementeringsperioden. Vores udgangspunkt har været, at hele it-sikkerhedsframeworket og de tilhørende it-sikkerhedskontroller har virket fra ultimo februar 2019.

IMS A/S' ansvar

IMS A/S er ansvarlig for udarbejdelsen af beskrivelsen (kapitel 2), herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen er præsenteret; for leveringen af IMS A/S' dataudvekslingsservice som beskrivelsen omfatter; for at anføre kontrolmålene samt for udformningen og implementeringen for at nå de anførte kontrolmål.

Beierholms uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i FSR's Etiske Regler, som er baseret på grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd. Vi anvender ISQC 1 og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder samt gældende krav ifølge lov og øvrig regulering.

Revisors ansvar

Vores ansvar er, på grundlag af vores handlinger, at udtrykke en konklusion om IMS A/S' beskrivelse samt om udformningen af kontroller, der knytter sig til kontrolmål, der er anført i denne beskrivelse. Vi har udført vores arbejde i overensstemmelse med ISAE 3402, Erklæringer med sikkerhed om kontroller hos serviceleverandør, som er udstedt af IAASB. Denne standard kræver, at vi overholder etiske krav samt 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.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelse og udformning af kontroller hos serviceleverandøren omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sikkerhedsprocedurer tilknyttet IMS A/S' dataudvekslingsservice samt for kontrollernes udformning. De valgte handlinger afhænger af serviceleverandørens revisor vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte kontrolmål og hensigtsmæssigheden af de kriterier, som IMS A/S har specificeret og beskrevet i kapitel 2. Som nævnt ovenfor har vi ikke udført handlinger vedrørende funktionaliteten af de kontroller, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

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

Begrænsninger i kontroller hos IMS A/S

IMS A/S' beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved systemet, som hver enkelt kunde måtte anse for vigtig efter deres særlige forhold. Endvidere vil kontroller hos en serviceleverandør, som følge af deres art, muligvis ikke forhindre eller opdage alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner.

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 kriterier, der er beskrevet i kapitel 1 i ledelsens erklæring. Det er vores opfattelse,

a) at beskrivelsen af de af IMS A/S' sikkerhedsprocedurer i tilknytning til IMS A/S' dataudvekslingsservice, således som de var udformet og implementeret pr. 28. februar 2019, 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 pr. 28. februar 2019.

Vi skal bemærke, at der for de enkelte kunder kan være specifikke forhold, som gør, at den generelle konklusion ikke er dækkende. Hvis det er aftalt mellem kunden og IMS A/S, at der udarbejdes en specifik erklæring vedrørende kundens kontrakt, vil forholdene fremgå af denne kontrakt.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen er udelukkende tiltænkt IMS 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 7. marts 2019

Beierholm
Statsautoriseret Revisionspartnerselskab
CVR-nr. 32 89 54 68

Kim Larsen
Statsautoriseret revisor

Jesper Aaskov Pedersen
IT-auditor, Manager