Uafhængig revisors erklæring med sikkerhed om
beskrivelsen af kontroller og deres udformning
i forbindelse med drift og vedligeholdelse af DPG-løsningen
pr. 16. januar 2019

ISAE 3402, type I

Timengo DPG A/S

CVR-nr. 35 83 36 84

Januar 2019

Indholdsfortegnelse

Afsnit 1: Timengo DPG A/S' udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt Timengo DPG A/S' DPG-løsning, 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 kundernes regnskaber. Timengo DPG A/S bekræfter, at:

(a) Den medfølgende beskrivelse, i afsnit 2, giver en retvisende beskrivelse af Timengo DPG A/S' drift og vedligeholdelse af DPG-løsningen til kunder pr. 16. januar 2019. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

(i) Redegør for, hvordan systemet 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 at igangsætte, registrere, behandle og om nødvendigt korrigere transaktionerne samt overføre disse til de rapporter, der er udarbejdet til kunder
- 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 identificerede 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 behandlingen og rapporteringen af kunders transaktioner.

(ii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af det beskrevne system 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 systemet, som den enkelte kunde måtte anse vigtigt efter deres særlige forhold.

(b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformede og fungerede effektivt pr. 16. januar 2019. Kriterierne for denne udtalelse var, at:

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

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

Ballerup, 16. januar 2019

Timengo DPG A/S

Martin Lundsgaard
Adm. direktør

Afsnit 2: Timengo DPG A/S' beskrivelse af DPG-løsningen samt interne kontroller

Formål

Formålet med denne beskrivelse er at levere information til Timengo DPG kunder og deres revisorer vedrørende Timengo DPG A/S' overholdelse af kravene i den internationale revisionsstandard for erklæringsopgaver om kontroller hos en serviceleverandør: ISAE 3402.

Denne beskrivelse har yderligere det formål at give information om de kontroller, der er anvendt for vores services i perioden.

Beskrivelsen omfatter de kontrolmål, kontroller og procedurer som omfatter vores standardleverancer. Individuelle kundeforhold er ikke medtaget i denne beskrivelse.

Timengo DPG

Timengo leverer en managed service: Timengo DPG - GDPR sikker post service (herefter: "Timengo DPG"), som er beskrevet yderligere på www.sikker-post.dk. Timengo DPG A/S er en førende leverandør af GDPR sikker/digital post løsninger siden 2011. Den er 100% dansk udviklet og drevet, og kan skalere fra 1-50.000 brugere og op til 100 mio. krypterede e-mails/døgn. Løsningen kan, som den eneste i det danske marked, tilbyde 100% garanti for sikker aflevering af e-mail til enhver e-mail modtager i verden.

Kunder kan sende og modtage sikker post i alle deres foretrukne e-mailprogrammer, på både Windows, Mac og Linux, samt tablets og telefoner. Timengo DPG leveres i 4 udgaver, der er tilpasset kunden behov og økonomi.

Der er også mulighed for at integrere med E-Boks. Det gør det muligt at sende til ethvert CPR/CVR nummer i Danmark. E-Boks integration understøtter også digital underskrift og tovejs kommunikation.

Denne informationssikkerhedspolitik omfatter vores leverance af Timengo DPG. Vores managed service kan leveres på 2 måder:

1. **On premise Timengo DPG.** Installeres i kundens eget IT driftsmiljø. Virksomheden udfører, i samarbejde med Timengo DPG, installation og konfiguration. I denne udgave er kunden ansvarlig for IT-platformen, som DPG installeres på.
2. **Cloud Timengo DPG**. Installeres på en server i Microsoft Azure cloud. Timengo DPG udfører installation og konfiguration. I denne udgave er Timengo DPG ansvarlig for IT-platformen, som DPG afvikles på.

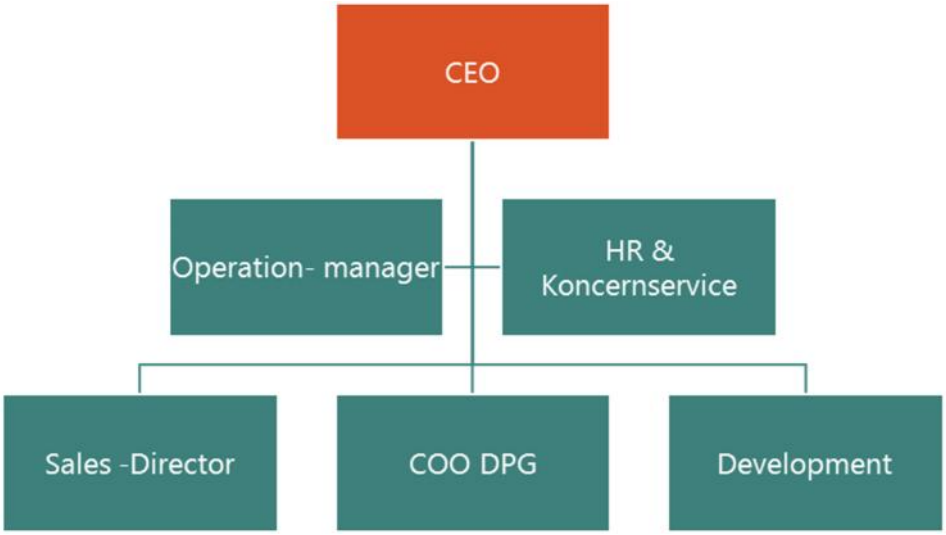
Timengo DPG A/S' hovedaktiviteter er:

- Implementering og udvikling af Timengo DPG - Sikker Post
- Rådgivning og support
- Salg og uddannelse

Timengo DPG behandler kun sikre e-mails og Timengo DPG har ikke adgang til resten af kundens e-mails og løsningen indgår ikke i kundens mailflow. Mail bliver krypteret/dekrypteret uden at personale hos Timengo DPG A/S, kan tilgå indholdet i mailen. Vi har dermed minimal berøring med vores kunders data. Vi sikrer løbende at vores procedurer og kontrolmål overholdes og det er Timengo DPG A/S ledelse, som overordnet beskriver, hvordan drift og produktion sikres således, at det til hver en tid kan dokumenteres, at virksomheden drives ansvarligt og har opsat en række procedurer og retningslinjer, som understøtter dette.

Detaljeringsgraden i informationssikkerhedspolitikken kan variere og vil blive udspecificeret i bilag og/eller procesbeskrivelser, som vil udgøre det samlede detaljerede overblik.

Organisation og ansvar



Timengo DPG beskæftiger 8 medarbejdere og er inddelt i 3 afdelinger; salg, drift og udvikling.

Risikovurdering og -håndtering

Risikovurdering

It- risikoanalyse

Vi har procedurer for løbende risikovurdering af vores forretning. Dermed sikrer vi, at de risici, som er forbundet med de services og ydelser vi stiller til rådighed, er minimeret til et acceptabelt niveau.

Risikovurdering foretages periodisk, samt når vi laver ændringer eller tilfører funktioner som vi vurderer at give anledning til at revurdere vores generelle risikovurdering.

Ansvaret for risikovurderinger ligger hos virksomhedens COO og skal efterfølgende forankres og godkendes hos ledelsen.

Håndtering af sikkerhedsrisici

Procedure for risikohåndtering

Vi har indført et pointsystem til at vurdere de risici, der er forbundet med vores levering af Timengo DPG.

Vi vurderer sandsynligheden for, at en given hændelse kan ske og holder det op imod den konsekvens en sådan hændelse måtte have. Det tages løbende op til vurdering om vi kan nedbringe risici og iværksætte tiltag, der kan forbedre vores sikkerhed.

Sikkerhedspolitik

Informationssikkerhedspolitik

Informationssikkerhedsdokument

Vi har indført politikker, procedurer og retningslinjer der sikrer, at vores leverancer er ensartede og gennemsigtige. Vi ønsker med dette at leve op til vores målsætning om at levere stabil og sikker drift til vores kunder.

Vores informationssikkerhedspolitik er udarbejdet med reference til ovenstående og er gældende for alle medarbejdere og for alle leverancer.

Vores informationssikkerhedspolitik er inddelt i følgende kontrolområder og er dermed defineret med reference til ISO 27002.

- Kontrol
- Risikovurdering og håndtering
- Risikoidentifikation
- Kvantificering af risici
- Prioritering af risici
- Planer for risikorespons
- Overvågning af planudførsel samt risikostyringens effektivitet
- Sikkerhedspolitik
- Organisering af informationssikkerhed
- Sikkerhed i forhold til HR
- Styring af aktiver
- Adgangskontrol
- Kryptografi
- Fysiske og miljømæssige sikringer
- Sikkerhed i forbindelse med drift
- Kommunikationssikkerhed
- Anskaffelse, udvikling og vedligehold
- Leverandørforhold
- Styring af sikkerhedshændelser
- Informationssikkerhedsaspekter ved beredskabsstyring
- Overensstemmelse

Vi foretager løbende forbedringer af vores politikker, procedurer og den operationelle drift.

Evaluering af informationssikkerhedspolitikken

Vi opdaterer løbende informationssikkerhedspolitikken og som minimum én gang årligt.

Organisering af informationssikkerhed

Intern organisering

Delegering af ansvar for informationssikkerhedspolitikken

Vi har en klar opdelt organisation og har ansvars og -rollebeskrivelser på alle vores medarbejdere.

Der er etableret fortrolighed for alle medarbejdere og for alle involverede i vores forretning. Dette sker via vores ansættelseskontrakter.

Funktionsadskillelse
Gennem løbende dokumentation og processer sikrer vi at kunne udelukke eller minimere nøglepersonafhængighed. Opgaver tildeles og fastsættes via procedure for styring af den operative drift.

Mobilt udstyr og fjernarbejdspladser

Mobilt udstyr og kommunikation
Vores medarbejdere og udviklere har mulighed for at arbejde hjemmefra og vores bærbare enheder er sikret med login og kryptering.

Adgang til vores systemer sker kun for autoriserede personer og kun hvor der anvendes VPN og 2 factor beskyttelse, kan der kobles op udefra.

Sikkerhed i forhold til HR

Inden ansættelse

Screening
Vi har interne procedure for ansættelse af medarbejdere, der sikrer at vi ansætter den rigtige kandidat i forhold til erfaring og kompetencer. Vi har ved ansættelsen rolle og ansvarsbeskrivelse så alle kender deres ansvar og arbejdsområde.

Ansættelsesforhold
Generelle vilkår for ansættelse, herunder fortrolighed om egne og kunders forhold er beskrevet i hver medarbejders ansættelseskontrakt. I kontrakten er beskrevet sanktioner ved brud beskrevet.

Under ansættelse

Ledelsens ansvar
Ved indgåelse af ansættelse underskriver nye medarbejdere en kontrakt, hvori det er indeholdt, at den ansatte skal overholde de til hver en tid gældende politikker og procedurer. En del af kontrakten er ligeledes en stillingsbeskrivelse hvor den ansattes rolle og forpligtelser fremgår.

Uddannelse og træning i informationssikkerhed
Vi fører løbende kontrol med, at alle medarbejdere overholder vores sikkerhedsretningslinjer, dog minimum årligt. Medarbejdere, og eksterne parter hvor det er relevant at inkludere disse, bliver periodisk orienteret om vores sikkerhedsretningslinjer samt, når der sker ændringer.

Sanktioner
Generelle vilkår for ansættelse, herunder fortrolighed om egne og kunders forhold, er beskrevet i hver medarbejders kontrakt, hvor forhold omkring ansættelsen er angivet, samt sanktioner ved evt. sikkerhedsbrud.

Ansættelse ophør
Når en medarbejders ansættelse ophører, følger vi en udførlig procedure for at sikre at alle aktiver, adgange til bygninger, systemer og data inddrages.

Det overordnede ansvar for sikring af alle kontroller i fratrædelsen ligger hos virksomhedens COO.

Styring af aktiver

Ansvar for aktiver

Fortegnelse af aktiver
Hardware, netværksudstyr samt fortegnelse over servere er registreret til brug ved dokumentation og gennemgås årligt.

Ejerskab af aktiver
Via ansvarsfordeling og rollebeskrivelser, er vores aktiver tilegnet systemansvarlige i vores virksomhed. Kundens data og systemer er tilegnet kundens kontaktperson.

Acceptabel brug af aktiver
Medarbejderes brug af aktiver er beskrevet i vores personalehåndbog.

Mediehåndtering

Styring af bærbare medier
Vi søger at vores medarbejderes bærbare medier er konfigureret sikkerhedsmæssigt lige så højt som resten af vores miljø samt, at de opdateres når vi foretager nye sikkerhedstiltag.

Adgangskontrol

Forretningskrav til adgangskontrol

Politikker for adgangsstyring
I vores informationssikkerhedspolitik er procedure for adgangsstyring beskrevet.

Administration af bruger adgange

Bruger oprettelse og nedlæggelse
Brugere, i vores kunders system, oprettes kun efter vores kunders ønske og de er dermed ansvarlige for oprettelse og nedlæggelse.

Håndtering af fortrolige logon informationer
Alle personlige logons er kun kendt af medarbejderen og er underlagt vores passwordpolitik.

Evaluering af brugeradgangsrettigheder
Virksomhedens egne brugere bliver gennemgået, som minimum årligt, i vores interne systemer. Oprettede bruger og adgangsniveau gennemgås for at sikre mod uautoriseret adgang.

Brugeransvar

Brug af fortrolig adgangskode
Vores informationssikkerhedspolitik beskriver at medarbejderes kodeord er strengt fortroligt. I forbindelse med nye versioner af vores informationssikkerhedspolitik, skriver medarbejderne under op at de har læst og forstået den.

Kontrol af adgang af systemer og data

Begrænset adgang til data
Vores medarbejdere har kun adgang til de systemer, som er relevante for deres arbejde.

System for administration af adgangskoder
Alle brugere har en adgangskode og det er styringsmæssigt sat op at den skal være kompleks og skriftes regelmæssigt.

Fysiske og miljømæssige sikringer

Sikker bortskaffelse af udstyr
Alt databærende udstyr destrueres inden bortskaffelse.

Sikkerhed i forbindelse med drift

Logning og overvågning
Vi følger og logger vores kunders sager og vores support overvåger dette. Vi prioriterer vores hændelser i vores support system, hvori det også dokumenteres.

Hændelseslogning
Alle hændelser logges i vores ITSM system.

Beskyttelse af logoplysninger
Oplysninger beskyttes af sikkerheden i vores ITSM system.

Kommunikationssikkerhed

Sikring af netværkstjenester
Adgang til kunders DPG server i Azure sikre via netværkssikkerheds grupper (firewall) konfigureret efter best-practise i Azure.

Vi er ansvarlige for driften og sikkerheden i Azure løsningen. Vores kunder er selv ansvarlige for at kunne tilgå internettet sikkert.

Leverandørforhold

Styring af serviceydelser fra tredjepart

Styring af ændringer af serviceydelser
Når det sker ændringer i politikker og procedurer i vores virksomhed eller hvis der sker ændringer til vores ydelser eller ydelser fra vores eksterne samarbejdspartnere, foretages en risikovurdering for at afdække ændringernes indflydelse.

Overvågning af ydelser fra tredjepart
Vi overvåger løbende og mindst én gang årligt at de ydelser, som leveres af tredjepart, overholder de krav og vilkår vi har indgået med disse.

Styring af sikkerhedshændelser

Styring af informationssikkerhedsbrud og forbedringer

Ansvar og procedurer
Vi har en procedure der beskriver hvorledes vi holder os ajour med vores underleverandørers udmeldinger om sikkerheds patches, der skal lukke potentielle sikkerhedshuller i vores løsning.

Rapportering af informationssikkerhedshændelser
Vi håndterer alle sikkerhedshændelser i vores ITSM system, hvor kunderne har adgang til at læse disse

Rapportering af sikkerhedssvagheder
Vores medarbejdere og eksterne sikkerheds partnere er forpligtede til at anmelde en hver sikkerhedshændelse til nærmeste leder.

Beredskabsstyring

Informationssikkerhedsaspekter ved beredskabsstyring

Beredskabsplanlægning
Beredskabsplanen er forankret i vores risikoanalyse og vedligeholdes minimum årligt.

Prøvning, vedligeholdelse og revurdering af beredskabsplaner
Planen testes en gang årligt som en del af vores beredskab, så vi sikrer at kunderne i mindst muligt omfang vil opleve forstyrrelser i driften, i forbindelse med en eventuel nødsituation.

Overensstemmelse

Review af informationssikkerhed

Uafhængig evaluering af informationssikkerhed
Vi får foretaget evaluering af ekstern it-revisor med udarbejdelse af ISAE 3402 erklæring og vil årligt blive evalueret.

Overensstemmelse med sikkerhedspolitikker og procedurer
Vi har løbende kontroller for at sikre at vores medarbejdere overholder gældende procedurer og sikkerhedsforanstaltninger som er beskrevet i vores informationssikkerhedspolitik.

Afsnit 3: Uafhængig revisors erklæring om beskrivelsen af kontroller og deres udformning

Til ledelsen hos Timengo DPG A/S, Timengo DPG A/S' kunder og deres revisorer.

Omfang

Vi har fået til opgave at afgive erklæring om Timengo DPG A/S' beskrivelse, som er gengivet i afsnit 2. Beskrivelsen, som i afsnit 1 er bekræftet af Timengo DPG A/S' ledelse, dækker virksomhedens behandling af kunders transaktioner på virksomhedens DPG-løsning pr. 16. januar 2019 samt udformningen af de kontroller der knytter sig til de kontrolmål, 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.

Timengo DPG A/S' ansvar

Timengo DPG A/S er ansvarlig for udarbejdelsen af beskrivelsen (afsnit 2) og tilhørende udtalelse (afsnit 1), herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelse er præsenteret. Timengo DPG A/S er herudover ansvarlig for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmål, og for udformningen, implementeringen og effektiviteten af kontrollerne for at nå de anførte kontrolmål.

REVI-IT A/S' uafhængighed og kvalitetsstyring

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

Firmaet 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.

REVI-IT A/S' ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Timengo DPG A/S' beskrivelse (afsnit 2) og om udformningen af de kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse. Vi har udført vores arbejde i overensstemmelse med ISAE 3402, "Erklæringer med sikkerhed om kontroller hos en serviceleverandør", som er udstedt af IAASB. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå en høj grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er retvisende, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformede.

Opgaven med afgivelse af en erklæring med sikkerhed om beskrivelsen og udformningen af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system samt for kontrollernes udformning. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformede. En erklæringsopgave med sikkerhed af denne type omfatter endvidere en vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden

af de heri anførte mål samt hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet i afsnit 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 en serviceleverandør

Timengo DPG A/S' beskrivelse i afsnit 2 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 vigtige efter sine særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller afdække 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. Kriterierne, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i Timengo DPG A/S' beskrivelse i afsnit 2, og det er på den baggrund vores vurdering,

(a) at beskrivelsen af DPG-løsningen, således som den var udformet og implementeret pr. 16. januar 2019, i alle væsentlige henseender er retvisende

(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformede pr. 16. januar 2019.

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt kunder, der har anvendt Timengo DPG A/S' DPG-løsning, og deres revisorer, som har en tilstrækkelig kompetence til at vurdere den medfølgende beskrivelse sammen med anden information, herunder information om kunders egne kontroller. Denne information tjener til opnåelse af en forståelse af kundernes informationssystemer, som er relevante for regnskabsaflæggelsen.

København, 16. januar 2019

REVI-IT A/S
Statsautoriseret revisionsaktieselskab

Henrik Paaske
Statsautoriseret revisor

Martin Brogaard Nielsen
It-revisor, CISA, CIPP/E, CRISC, adm. direktør