Visma DataLøn A/S

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale med Visma DataLøns kunder, som anvender DataLøn-løsningen pr 24. september 2020

Indholdsfortegnelse

Sektion I - Ledelsens udtalelse 3

Sektion II – Uafhængig revisors erklæring 5

Sektion III – Beskrivelse af behandling 8

Karakteren af behandlingen 8

Personoplysninger 9

Praktiske tiltag 9

Risikovurdering 9

Kontrolforanstaltninger 10

Komplementerende kontroller hos de dataansvarlige 10

Sektion IV - Tests udført af EY 12

Formål og omfang 12

Udførte tests 12

Kontrolmål, kontrolaktivitet, test og resultat heraf 13

Sektion I - Ledelsens udtalelse

Visma DataLøn behandler personoplysninger på vegne af Visma DataLøns kunder, som anvender DataLøn-løsningen (herefter dataansvarlige) i henhold til databehandleraftale (Bilag 1 i *"Vilkår for DataLøn, Gældende fra 1. november 2019"*).

Medfølgende beskrivelse er udarbejdet til brug for Visma DataLøns kunder, der har anvendt DataLøn-løsningen, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført 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.

Visma DataLøn anvender underleverandører til datalagring eller infrastruktur. Beskrivelsen i sektion III medtager kun kontrolmål og kontrolaktiviteter hos Visma DataLøn og medtager således ikke kontrolmål og underliggende kontrolaktiviteter hos underleverandører. Beskrivelsen angiver også, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan nås, hvis underleverandørernes kontroller, der forudsættes i designet af vores kontroller, er passende designet og fungerer effektivt. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underleverandører.

Beskrivelsen angiver, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan opnås, hvis komplementerende kontroller hos de dataansvarlige, der forudsættes i designet af Visma DataLøns kontroller, er passende designet og fungerer effektivt sammen med relaterede kontroller hos Visma DataLøn. Beskrivelsen omfatter ikke kontrolaktiviteter udført af de dataansvarlige.

Visma DataLøn bekræfter, at:

a) Den medfølgende beskrivelse i sektion III, giver en retvisende beskrivelse af DataLøn-løsningen i Visma DataLøn, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen pr. 24. september 2020. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan DataLøn-løsningen var udformet og implementeret, herunder redegør for:

      i. De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger.

      ii. De processer i både manuelle og it-manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere, slette og begrænse behandling af personoplysninger.

      iii. De processer, der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige.

      iv. 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.

      v. 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.

vi. De processer, der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underrettelse til de registrerede.

vii. 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.

viii. Ydelser udført af underleverandører, hvis relevant, herunder om de er medtaget efter helhedsmetoden eller udeladt efter partielmetoden.

ix. Kontroller, som vi med henvisning til Visma DataLøns 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.

x Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger.

(ii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af DataLøn-løsningen til behandling af personoplysninger under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og derfor ikke kan omfatte ethvert aspekt ved DataLøn-løsningen, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og implementeret pr. 24. september 2020, hvis relevante kontroller hos underleverandører fungerer effektivt, og kunder har udført de komplementerende kontroller som forudsættes i designet af Visma DataLøns kontroller pr. 24. september 2020. Kriterierne anvendt for at give denne udtalelse var, at:

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

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

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.

København, 26. november 2020

Karina Wellendorph
Managing Director

Sektion II – Uafhængig revisors erklæring

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftale mellem Visma DataLøn og Visma DataLøns kunder.

Til: Visma DataLøn og Visma DataLøns kunder

Omfang

Vi har fået som opgave at afgive erklæring om Visma DataLøns beskrivelse i sektion III af DataLøn-løsningen i henhold til databehandleraftale med Visma DataLøns kunder, som anvender DataLøn-løsningen pr. 24. september 2020 (beskrivelsen) og om udformningen og implementeringen af 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.

Beskrivelsen angiver, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan opnås, hvis komplementerende kontroller hos de dataansvarlige, der forudsættes i designet af Visma DataLøns kontroller, er passende designet og fungerer effektivt sammen med relaterede kontroller hos Visma DataLøn. Beskrivelsen omfatter ikke kontrolaktiviteter udført af dataansvarlige. Vi har ikke udført handlinger vedrørende funktionaliteten af de komplementerende kontroller hos dataansvarlige, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

Visma DataLøn anvender underleverandører til datalagring eller infrastruktur. Beskrivelsen i sektion III medtager kun kontrolmål og relaterede kontroller hos Visma DataLøn og medtager således ikke kontrolmål og relaterede kontroller hos underleverandører. Beskrivelsen angiver også, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan nås, hvis underleverandørels kontroller, der forudsættes i designet af Visma DataLøns kontroller, er passende designet og fungerer effektivt sammen med de relaterede kontroller hos Visma DataLøn. Vores handlinger har ikke omfattet kontrolaktiviteter udført af underleverandører, og vi har ikke vurderet egnetheden af design eller den operationelle effektivitet af kontrolaktiviteter hos underleverandører.

Visma DataLøns ansvar

Visma DataLøn er ansvarlig for udarbejdelsen af beskrivelsen i sektion III og tilhørende udtalelse i sektion I, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter; for at anføre kontrolmålene, identifikation af de risici, der påvirker opnåelsen af kontrolmålene; udvælgelsen af de kriterier, der er præsenteret i ledelsens udtalelse samt for at udforme, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Vores 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) og IESBA's Etiske regler, som er baseret på de grundlæggende principper om integritet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og 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.

Vores ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Visma DataLøns beskrivelse samt om udformningen og implementeringen 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 implementeret.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og implementeringen af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse af DataLøn-løsningen samt for kontrollernes udformning og implementering. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet og implementeret. 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 Visma DataLøn har specificeret og beskrevet i sektion I.

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 dataansvarlig

Visma DataLøns beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved DataLøn-løsningen, 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.

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 DataLøn-løsningen, således som denne var udformet og implementeret pr. 24. september 2020, i alle væsentlige henseender er retvisende, og

(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. 24. september 2020, hvis kontroller hos underleverandører fungerer effektivt, og hvis dataansvarlige har designet og implementeret de komplementerende kontroller, der forudsættes i designet af Visma DataLøns kontroller pr. 24. september 2020.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultater af disse tests fremgår i sektion IV.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i sektion IV er udelukkende tiltænkt dataansvarlige, der har anvendt DataLøn-løsningen, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen er overholdt.

København, den 26. november 2020
EY
Godkendt Revisionspartnerselskab
CVR-nr. 30 70 02 28

Nils B. Christiansen
statsaut. revisor
mne34106

Andreas Uldahl
Senior Manager, CISA

Sektion III – Beskrivelse af behandling

Visma DataLøn A/S leverer DataLøn, et standard IT-system, der laver løn for over 60.000 kunder, herunder over 500.000 lønsedler om måneden.

Systemet består af en lønmotor, der udfører beregninger, indberetninger til myndigheder og generer lønsedler. DataLøn systemet inkluderer:

- Standard set-up til at dække kundens lønbehov
- Mulighed for ubegrænsede prøveberegninger
- Opdateringer til at sikre overholdelse af dansk lovgivning
- Mulighed for lønbehandling med obligatorisk og valgfri indberetning til tredjeparter, herunder myndigheder og pensionsselskaber
- Tilbagelevering af data i elektronisk form
- Support til lønbehandling og brug af systemet

Visma DataLøn A/S anvender eksterne leverandører, herunder Nets Danmark A/S, ATEA A/S og Visma IT & Communications (VITC) til visse dele af IT leverancen (datalagring og infrastruktur). Disse leverandører håndteres igennem Visma Enterprise Operations afdeling, hvilket omfatter IT-infrastruktur, samt eksterne leverandører.

Visma DataLøn A/S anvender et internt system ("CRM") til kundehåndtering. CRM giver overblik over kunder, abonnementsstatus, oprettede supportsager og lignende. Systemet anvendes af Visma DataLøn A/S kundeservice samt marketing.

Til adgangsstyring anvendes SSO, som er vores fælles single sign on modul, der anvendes DataLøn frontends og API'er.
Systemet indeholder brugeroplysninger samt rettigheder (claims).

Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er levering af et en standard it-løsningen, der på baggrund af Kundens indberetninger til Visma DataLøn foretager lønbehandling for Kunden, i henhold til Visma DataLøns regler og vilkår (Hovedaftalen).

Karakteren af behandlingen
Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig om lønbehandling, herunder:

- beregne medarbejdernes løn
- foretage alle beregninger og indberetninger til og foranlediger pengeoverførsler til SKAT, ATP, ferie- og barselsfonde, pensionskasser m.v. på Kundens vegne
- foretage indberetning af statistik til arbejdsgiverforening og Danmarks Statistik på Kundens vegne
- sende lønsedler til Medarbejdernes e-Boks
- gemmer Kundens lønbilag i et elektronisk arkiv i fem år efter udløbet af det år, hvor lønbilaget produceres
- yde hjælp til opstart og oprettelse af Kunden og Medarbejderne
- levere support- og konsulentydelser telefonisk og online fra Visma DataLøns lønkonsulenter, når Kunden har brug for hjælp.

Visma DataLøn foretager ingen udvikling eller tilpasning af DataLøn i forhold til Kundens specifikke behov eller ønsker.

Personoplysninger

- Almindelige personoplysninger
  - identifikationsoplysninger
  - stamoplysninger (ansættelsesoplysninger)
  - ferieafregning
  - pensionsafregning
  - skatteafregning
  - kontooplysninger
- Andre oplysninger
  - CPR-numre

Kategorier af registrerede personer omfattet af databehandleraftalen:

- Kunders ansatte
- Kundens kontaktperson

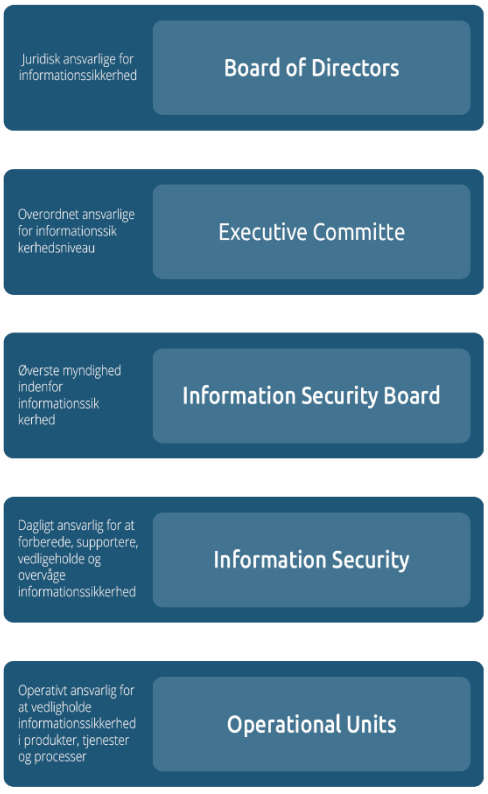
Praktiske tiltag

Visma DataLøn har etableret et ledelsesrammeværk til initiering og styring af implementering samt drift af informationssikkerhed og databeskyttelse.

Ansvar for databeskyttelse og informationssikkerhed varetages af Visma DataLøns Information Security Board, samt Data Protection Manager og Security Manager. Området understøttes derudover af Visma-koncernens DPO.

Visma DataLøn har implementeret politikker, kontroller og processer, som dækker de nedenfor beskrevne informationssikkerhedsområder:

- Organisering af informationssikkerhed
- Personalesikkerhed
- Styring af aktiver
- Adgangsstyring
- Kryptografi
- Fysisk sikring og miljøsikring
- Driftssikkerhed
- Kommunikationssikkerhed
- Anskaffelse, udvikling og vedligeholdelse af systemer
- Leverandørforhold
- Styring af informationssikkerhedsbrud
- Informationssikkerhedsaspekter ved nødberedskabs- og reetableringsstyring
- Compliance



Risikovurdering

Formålet med Risikovurdering er at give retning, forventninger og intentioner til styring af informationssikkerhedsrisici i Visma DataLøn.

- Vurderede sikkerhedsrisici skal analyseres.

- Trusler og sårbarheder skal vurderes.
- Konsekvenser (positive eller negative) af risiko på mål.
- Konsekvenser (positive eller negative) af risiko på aktiver.
- Sandsynligheden for, at disse konsekvenser kan forekomme.

I de særlige tilfælde, hvor en høj risiko indebærer, at den dataansvarlige skal foretage en konsekvensanalyse vedrørende databeskyttelse, beskrives tillige, hvordan databehandleren eventuelt har bistået hermed.

Rapportering og opfølgning på sikkerhedsrisici skal udføres i henhold til de definerede behov fra Division og Group.

Kontrolforanstaltninger

Visma DataLøn A/S har struktureret deres kontroller omkring de tekniske sikkerhedsforanstaltninger, med afsæt i ISO27001.

Metoden til udførelse af risikostyring i Visma DataLøn er baseret på internationalt anerkendte principper og standarder, der er tilpasset organisationen. Metoden giver vejledning og inkluderer processerne for, hvordan effektiv risikostyring skal udføres.

- Kontrolmål A
  Der er procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger kan efterleves i overensstemmelse med den indgående databehandleraftale.
- Kontrolmål B
  Der er procedurer og kontroller, som sikrer, at Visma DataLøn har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.
- Kontrolmål C
  Der er procedurer og kontroller, som sikrer, at Visma DataLøn har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.
- Kontrolmål D
  Der er procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres, såfremt der indgås aftale herom med den dataansvarlige.
- Kontrolmål E
  Der er procedurer og kontroller, som sikrer, at Visma DataLøn alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.
- 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.
- Kontrolmål G
  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.
- Kontrolmål H
  Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.

Komplementerende kontroller hos de dataansvarlige

Den Dataansvarlige har ansvaret for, at behandlingen af Personoplysninger lever op til kravene i Databeskyttelsesforordningen og Databeskyttelsesloven.

Den Dataansvarlige er ved brug af de tjenester, som Visma DataLøn stiller til rådighed i henhold til Hovedaftalen, forpligtet til at behandle Personoplysninger i overensstemmelse med bestemmelserne i gældende lovgivning, herunder bl.a. ved at:

- sikre sig, at behandlingen af Personoplysninger opfylder Databeskyttelsesforordningen.
- sikre sig, at de registrerede er oplyst om behandlingen af Personoplysninger.
- sikre sig, at instruksen er lovlig set i forhold til den til enhver tid gældende persondataretlige regulering.
- sikre sig, at instruksen er hensigtsmæssig set i forhold til denne databehandleraftale og hovedydelsen.
- sikre sig, at den dataansvarliges brugere er ajourførte.
- sikre sig, at de har indført detaljerede procedurer til varetagelse af den registreredes rettigheder.

Sektion IV - Tests udført af EY

Formål og omfang

Vores test af kontrollers udformning og implementering har omfattet de kontrolmål og tilknyttede kontroller, der er udvalgt af ledelsen, og som fremgår af afsnit 1. Eventuelle andre kontrolmål, tilknyttede kontroller og kontroller hos underleverandører til Visma DataLøn, der anvender løsningen, beskrevet i afsnit 1, er ikke omfattet af vores test.

Test af design og implementering har omfattet de kontroller, som blev vurderet nødvendige for at kunne opnå høj grad af sikkerhed, for at de anførte kontrolmål blev opnået pr. 24. september 2020.

Udførte tests

De udførte tests i forbindelse med fastlæggelsen af kontrollers design og implementering er beskrevet nedenfor:

Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at blive effektive, hvis de implementeres. Desuden vurderes det ved en stikprøve på én, om kontroller overvåges og kontrolleres tilstrækkeligt. På de tekniske platforme, databaser og netværkskomponenter har vi testet den specifikke systemopsætning for at påse, om kontroller er designet og implementeret pr. 24. september 2020.
Forespørgsler	Forespørgsel af passende personale hos Visma DataLøn. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Vi har ved en stikprøve på én observeret kontrollens implementering.

Kontrolmål, kontrolaktivitet, test og resultat heraf

Kontrolmål A **Der er procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger kan efterleves i overensstemmelse med den indgående databehandleraftale.**			
Nr.	*Visma DataLøns kontrolaktivitet*	*Tests udført af EY*	*Resultat af test*
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der er krav om 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. Inspiceret, at procedurer er opdateret.	Ingen afvigelser konstateret.
A.2	Visma DataLøn 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.	Ingen afvigelser konstateret.

Kontrolmål A **Der er procedurer og kontroller, som sikrer, at instruks vedrørende behandling af personoplysninger kan efterleves i overensstemmelse med den indgående databehandleraftale.**			
Nr.	*Visma DataLøns kontrolaktivitet*	*Tests udført af EY*	*Resultat af test*
A.3	Visma DataLøn underretter omgående den dataansvarlige skriftligt, hvis en instruks efter Visma DataLøns 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. Inspiceret, at der er procedurer for underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. Forespurgt, om der er er konstateret tilfælde, hvor behandlingen af personoplysninger er vurderet i strid med lovgivningen.	Vi har fået oplyst at Visma DataLøn ikke har konstateret tilfælde, hvor instruksen har været i strid med lovgivningen, hvorfor det derfor ikke har været muligt at teste implementeringen af kontrollen. Ingen afvigelser konstateret.
A.4	Relevante lov-, myndigheds- og kontraktkrav samt organisationens metode til overholdelse af disse krav skal være klart identificeret, dokumenteret og opdateret for hvert informationssystem og for organisationen.	Inspiceret, at der er procedurer for identifikation og overvågning af relevante lov-, myndigheds- og kontraktkrav, samt at organisationens metode til overholdelse af disse krav er klart identificeret, dokumenteret og opdateret for hvert informationssystem og for organisationen:	Ingen afvigelser konstateret.
A.5	Privatlivets fred og personoplysninger skal beskyttes i overensstemmelse med relevant lovgivning og eventuelle forskrifter.	Inspiceret, at der er procedurer for privatlivets fred, og at personoplysninger er beskyttet i overensstemmelse med relevant lovgivning og eventuelle forskrifter. Inspiceret, at procedurer er opdateret.	Ingen afvigelser konstateret.

Kontrolmål B **Der er procedurer og kontroller, som sikrer, at Visma DataLøn har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Visma DataLøns kontrolaktivitet*	*Test udført af EY*	*Resultat af test*
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger. Inspiceret, at procedurer er opdateret. Inspiceret, at der er etableret de aftalte sikringsforanstaltninger i overensstemmelse med databehandleraftalen.	Ingen afvigelser konstateret.
B.2	Visma DataLøn 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. Inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger. Inspiceret, at databehandler har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen. Inspiceret, at databehandler har implementeret de sikringsforanstaltninger, der er aftalt med de dataansvarlige.	Ingen afvigelser konstateret.

Kontrolmål B Der er procedurer og kontroller, som sikrer, at Visma DataLøn har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som er opdateret.	Inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirus software. Inspiceret, at antivirus software er opdateret.	Ingen afvigelser konstateret.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall. Inspiceret, at firewall er konfigureret i henhold til intern politik herfor.	Ingen afvigelser konstateret.
B.5	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger. Inspiceret, at de aftalte tekniske foranstaltninger understøtter opretholdelsen af begrænsningen i brugernes arbejdsbetingede adgang til personoplysninger.	Ingen afvigelser konstateret.

Kontrolmål B Der er procedurer og kontroller, som sikrer, at Visma DataLøn har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
B.6	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 med alarmering.	Der er ikke etableret alarmering på systemovervågning internt hos Visma DataLøn. Ingen yderligere afvigelser konstateret.
B.7	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet.	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. Inspiceret, at der anvendes kryptering af transmissioner af følsomme og fortrolige personoplysninger via internettet eller med e-mail. Forespurgt, om der har været ukrypterede transmissioner af følsomme og fortrolige personoplysninger, samt om de dataansvarlige er behørigt orienteret herom.	Ingen afvigelser konstateret.

Kontrolmål B Der er procedurer og kontroller, som sikrer, at Visma DataLøn har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			

B.8	Der er etableret logning i systemer og databaser af følgende forhold:
	
	• Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder.
	• Sikkerhedshændelser omfattende:
	  ○ Ændringer i logopsætninger, herunder deaktivering af logning.
	  ○ Ændringer i systemrettigheder til brugere.
	  ○ Fejlede forsøg på log-on til systemer, databaser og netværk.
	
	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 på logs.
		
		Inspiceret, at logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, er konfigureret og aktiveret.
		
		Inspiceret, at opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod manipulation og sletning.
			Der foretages ikke periodisk opfølgning på aktiviteter udført af Visma DataLøns egne systemadministratorer og andre med særlige rettigheder. Vi er blevet informeret om, at logs kan gennemgås reaktivt ved behov.
			
			Ingen yderligere afvigelser konstateret.

B.9	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. Forespurgt , om der anvendes personoplysninger, der ikke er pseudonymiseret eller anonymiseret i udviklings- og testmiljøer.	Ingen afvigelser konstateret.

Kontrolmål B Der er procedurer og kontroller, som sikrer, at Visma DataLøn har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.			
B.10	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. Inspiceret ved stikprøve på tre typer af ændringer (Emergency, Ekstern og Intern), at procedurer for håndtering af ændringer til systemer, databaser og netværk er implementeret. Inspiceret ved gennemgang erklæringer fra underleverandører, at systemer, databaser og netværk er opdateret med aftalte ændringer og relevante opdateringer, patches og sikkerhedspatches.	Ingen afvigelser konstateret.
B.11	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. Inspiceret, at der foreligger formaliserede procedurer for opfølgning på, at brugeres adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov. Inspiceret ved en stikprøve på én medarbejders adgange til systemer og databaser, at de tildelte brugeradgange er godkendt, og at der er et arbejdsbetinget behov.	Procedurer for adgangsstyring ikke indeholder en beskrivelse af, hvordan en periodisk gennemgang af brugere og deres rettigheder skal foretages. Ingen yderligere afvigelser konstateret.

		Inspiceret ved en stikprøve på én fratrådt medarbejdere, at disses adgange til systemer og databaser er rettidigt deaktiveret eller nedlagt. Inspiceret, at der foreligger dokumentation for regelmæssig – mindst en gang årligt – vurdering og godkendelse af tildelte brugeradgange.	
Kontrolmål B **Der er procedurer og kontroller, som sikrer, at Visma DataLøn har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
B.12	Der er etableret fysisk adgangssikkerhed, så kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvor 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. Observeret, at kun autoriserede personer har fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger. Inspiceret ved gennemgang af erklæringer fra underleverandører, at der er etableret fysisk adgangssikkerhed, så kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvor der opbevares og behandles personoplysninger.	Ingen afvigelser konstateret.
B.13	Information skal klassificeres efter lovmæssige krav, værdi og efter, hvor følsom og kritisk informationen er i forhold til uautoriseret offentliggørelse eller ændring.	Inspiceret, at der vedligeholdes et klassificeringsskema, samt at dette er godkendt og gjort tilgængeligt for medarbejdere.	Ingen afvigelser konstateret.
B.14	Der skal udarbejdes og implementeres procedurer til håndtering af aktiver i overensstemmelse med det informationsklassifikationssystem, som organisationen har vedtaget.	Inspiceret, at et register over aktiver er vedligeholdt, godkendt og indeholder klassificering af: • Kategori • Miljø	Ingen afvigelser konstateret.

		• Klassificering • Acceptable use • Intellectual property rights	
B.15	Aktiver i relation til information og informationsbehandlingsfaciliteter skal identificeres, og der skal udarbejdes og vedligeholdes en fortegnelse over disse aktiver.	Inspiceret, at et register over aktiver er vedligeholdt, godkendt og indeholder relevant information og informationsbehandlingsaktiver.	Ingen afvigelser konstateret.
Kontrolmål B **Der er procedurer og kontroller, som sikrer, at Visma DataLøn har implementeret tekniske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
B.16	Regler for accepteret brug af information og aktiver i relation til information og informationsbehandlingsfaciliteter skal identificeres, dokumenteres og implementeres.	Inspiceret, at regler for brug af identificerede aktiver i relation til information og informationsbehandlingsfaciliteter er dokumenteret og implementeret. Inspiceret, at politikken for brug af informationsaktiver er kommunikeret og tilgængelig for medarbejdere.	Ingen afvigelser konstateret.
B.17	Organisationen skal fastlægge krav til informationssikkerhed og informationssikkerhedskontinuitet i kritiske situationer, fx i tilfælde af en krise eller katastrofe.	Inspiceret, at der foreligger en formaliseret politik for informationssikkerhed og informationssikkerhedskontinuitet i kritiske situationer, samt at denne er opdateret og godkendt.	Ingen afvigelser konstateret.
B.18	Organisationen skal fastlægge, dokumentere, implementere og vedligeholde processer, procedurer og kontroller for at sikre den nødvendige informationssikkerhedskontinuitet i en kritisk situation.	Inspiceret, at der er fastlagt, dokumenteret og implementeret procedurer og kontroller for at sikre den nødvendige informationssikkerhedskontinuitet i en kritisk situation, samt at disse er vedligeholdt og godkendt.	Ingen afvigelser konstateret.
B.19	Organisationen skal verificere de etablerede og implementerede kontroller vedrørende informationssikkerhedskontinuiteten med jævne mellemrum med henblik på at sikre, at de er tidssvarende og effektive i kritiske situationer.	Inspiceret, at der er fastlagt, dokumenteret og implementeret procedurer og kontroller for at sikre den nødvendige informationssikkerhedskontinuitet i en kritisk situation.	Ingen afvigelser konstateret.

		Inspiceret, at de underliggende procedurer for informationssikkerhedskontinuitet er verificeret og godkendt.	

Kontrolmål C **Der er procedurer og kontroller, som sikrer, at Visma DataLøn har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Visma DataLøns kontrolaktivitet*	*Tests udført af EY*	*Resultat af test*
C.1	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. It-sikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering.	Inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Inspiceret dokumentation for, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.	Ingen afvigelser konstateret.
C.2	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. Inspiceret ved et eksempel på en databehandleraftale, at kravene i aftalerne er dækket af informationssikkerhedspolitikkens krav til sikringsforanstaltninger og behandlingssikkerheden.	Ingen afvigelser konstateret.

Kontrolmål C **Der er procedurer og kontroller, som sikrer, at Visma DataLøn har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Visma DataLøns kontrolaktivitet*	*Tests udført af EY*	*Resultat af test*
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: • Referencer fra tidligere ansættelser • Straffeattest • Eksamensbevis	Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Inspiceret ved et eksempel på en nyansat medarbejder, at kravene til efterprøvning af medarbejdere i aftalerne er dækket af databehandlerens procedurer for efterprøvning. Inspiceret ved et eksempel på en nyansat medarbejder, at der er dokumentation for, at efterprøvningen har omfattet. • Referencer fra tidligere ansættelser • Straffeattest • Eksamensbevis	Ingen afvigelser konstateret.
C.4	Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.	Inspiceret ved et eksempel på en nyansat medarbejder, at den pågældende medarbejder har underskrevet en fortrolighedsaftale. Inspiceret ved et eksempel på en nyansat medarbejder, at den pågældende medarbejder er blevet introduceret til: • Informationssikkerhedspolitikken. • Procedurer vedrørende databehandling, samt anden relevant information.	Ingen afvigelser konstateret.

Kontrolmål C **Der er procedurer og kontroller, som sikrer, at Visma DataLøn har implementeret organisatoriske foranstaltninger til sikring af relevant behandlingssikkerhed.**			
Nr.	*Visma DataLøns kontrolaktivitet*	*Tests udført af EY*	*Resultat af test*
C.5	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 som adgangskort, pc, mobiltelefon osv. inddrages.	Ingen afvigelser konstateret.
C.6	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, 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. Inspiceret ved et eksempel på en fratrådt medarbejder, at der er dokumentation for opretholdelse af fortrolighedsaftale og generel tavshedspligt.	Ingen afvigelser konstateret.
C.7	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. Inspiceret dokumentation for, at alle medarbejdere, som enten har adgang til eller behandler personoplysninger, har gennemført den udbudte awareness-træning:	Ingen afvigelser konstateret.

Kontrolmål D **Der er procedurer og kontroller, som sikrer, at personoplysninger kan slettes eller tilbageleveres, såfremt der indgås aftale herom med den dataansvarlige.**			
Nr.	*Visma DataLøns kontrolaktivitet*	*Tests udført af EY*	*Resultat af test*
D.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurer er opdateret.	Inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
D.2	Der er aftalt følgende specifikke krav til databehandlerens opbevaringsperioder og sletterutiner: • Visma DataLøn optager telefonsamtaler, såfremt der er givet samtykke hertil, mellem Kunden og Visma DataLøns kundecentre for at kunne fastslå samtalernes indhold. Samtalerne opbevares i seks måneder, hvorefter de slettes. • Dokumenter på aktive kunder slettes efter løbende + fem år. • Grundmateriale opbevares i 45 dage.	Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner. Inspiceret ved en stikprøve på en databehandling fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger opbevares i overensstemmelse med de aftalte opbevaringsperioder. Inspiceret ved en stikprøve på en databehandling fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at personoplysninger er slettet i overensstemmelse med de aftalte sletterutiner.	Ingen afvigelser konstateret.
D.3	Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: • tilbageleveret til den dataansvarlige og/eller • slettet, hvor det ikke er i modstrid med anden lovgivning.	Inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger. Inspiceret ved en stikprøve på en ophørt databehandling, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført.	Ingen afvigelser konstateret.

Kontrolmål E **Der er procedurer og kontroller, som sikrer, at Visma DataLøn alene opbevarer personoplysninger i overensstemmelse med aftalen med den dataansvarlige.**			
Nr.	*Visma DataLøn kontrolaktivitet*	*Tests udført af EY*	*Resultat af test*
E.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Inspiceret, at procedurerne er opdateret. Inspiceret ved en stikprøve på en databehandling fra databehandlerens oversigt over behandlingsaktiviteter, at der er dokumentation for, at databehandlingen sker i henhold til databehandleraftalen.	Ingen afvigelser konstateret.
E.2	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. Inspiceret ved et eksempel på en databehandling 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.	Ingen afvigelser konstateret.

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.**			
Nr.	*Visma DataLøns kontrolaktivitet*	*Tests udført af EY*	*Resultat af test*
F.1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
F.2	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. Inspiceret ved et eksempel på en underdatabehandler fra databehandlerens oversigt over underdatabehandlere, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalen – eller i øvrigt er godkendt af den dataansvarlige.	Ingen afvigelser konstateret.
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underretters den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Inspiceret dokumentation for, at den dataansvarlige er blevet underrettet ved seneste ændring i anvendelse af underdatabehandlerne.	Ingen afvigelser konstateret.

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.**			
Nr.	*Visma DataLøns kontrolaktivitet*	*Tests udført af EY*	*Resultat af test*
F.4	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. Inspiceret ved en stikprøve på en underdatabehandleraftale, at denne indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Ingen afvigelser konstateret.
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: • Navn • CVR-nr. • Adresse • Beskrivelse af behandlingen	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.	Ingen afvigelser konstateret.

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.**			
Nr.	*Visma DataLøns kontrolaktivitet*	*Tests udført af EY*	*Resultat af test*
F.6	Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. 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. Inspiceret dokumentation for, at der er foretaget en risikovurdering af den enkelte underdatabehandler og den aktuelle behandlingsaktivitet hos denne. Inspiceret dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerheden hos de anvendte underdatabehandlere, tredjelands overførselsgrundlag og lignende.	Ingen afvigelser konstateret.

Kontrolmål G **Der efterleves procedurer og kontroller, som sikrer, at databehandleren kan bistå den dataansvarlige med udlevering, rettelse, sletning eller begrænsning af oplysninger om behandling af personoplysninger til den registrerede.**			
Nr.	*Visma DataLøns kontrolaktivitet*	*Tests udført af EY*	*Resultat af test*
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder. Inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
G.2	Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	Forespurgt, om der foreligger procedurer for bistand til den dataansvarlige, som indeholder detaljerede procedurer for: • Udlevering af oplysninger. • Rettelse af oplysninger. • Sletning af oplysninger. • Begrænsning af behandling af personoplysninger. • Oplysning om behandling af personoplysninger til den registrerede.	Der er ikke detaljerede procedurer i relation til håndteringen af den registreredes rettigheder. Der henvises til komplementerende kontroller hos dataansvarlige. Vi har konstateret, at der ikke er modtaget henvendelser, og det har dermed ikke været muligt at teste implementeringen af kontrollen. Ingen yderligere afgivelser konstateret.

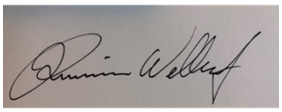
Kontrolmål H **Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.**			
Nr.	*Visma DataLøns kontrolaktivitet*	*Tests udført af EY*	*Resultat af test*
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Inspiceret, at proceduren er opdateret.	Der er ikke angivet passende frister for rapportering af brud på persondatasikkerheden. Ingen yderligere afvigelser konstateret.
H.2	Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: • Awareness hos medarbejdere. • Logning af tilgang til personoplysninger. • Scanning af dark websites og markedspladser for læk af personoplysninger.	Inspiceret, at databehandler udbyder awarenesstræning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden. Inspiceret dokumentation for, at netværkstrafik overvåges, samt at der sker opfølgning på anormaliteter, overvågningsalarmer, overførsel af store filer m.v. Inspiceret dokumentation for, at der sker rettidig opfølgning på logning af adgang til personoplysninger, herunder opfølgning på gentagne forsøg på adgang. Observeret, at der er implementeret løsning, som scanner dark websites og markedspladser for læk af personoplysninger.	Der er ikke etableret periodisk opfølgning på logaktiviteter for at identificere eventuelle brud på persondatasikkerheden. Ingen yderligere afvigelser konstateret.

Kontrolmål H **Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.**			
Nr.	*Visma DataLøns kontrolaktivitet*	*Tests udført af EY*	*Resultat af test*
H.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse og senest 24 timer efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Forespurgt underdatabehandlerne, om de har konstateret nogen brud på persondatasikkerheden. Inspiceret, at databehandleren har medtaget eventuelle brud på persondatasikkerheden hos underdatabehandlere i databehandlerens oversigt over sikkerhedshændelser. Inspiceret, at et eksempel på et registreret brud på persondatasikkerheden hos databehandleren eller underdatabehandlerne er meddelt de berørte dataansvarlige uden unødig forsinkelse og senest 24 timer efter, at databehandleren er blevet opmærksom på brud på persondatasikkerheden.	Ingen afvigelser konstateret.

Kontrolmål H **Der efterleves procedurer og kontroller, som sikrer, at eventuelle sikkerhedsbrud kan håndteres i overensstemmelse med den indgåede databehandleraftale.**			
Nr.	*Visma DataLøns kontrolaktivitet*	*Tests udført af EY*	*Resultat af test*
H.4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: • Karakteren af bruddet på persondatasikkerheden. • Sandsynlige konsekvenser af bruddet på persondatasikkerheden. • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	Inspiceret, at de foreliggende procedurer for underretning af de dataansvarlige ved brud på persondatasikkerheden indeholder detaljerede procedurer for: • Beskrivelse af karakteren af bruddet på persondatasikkerheden. • Beskrivelse af sandsynlige konsekvenser af bruddet på persondatasikkerheden. • Beskrivelse af foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden. Inspiceret dokumentation for, at de foreliggende procedurer understøtter, at der træffes foranstaltninger for håndtering af bruddet på persondatasikkerheden.	Foranstaltninger, som Visma DataLøn har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, fremgår ikke klart af procedure for videreformidling af brud på persondatasikkerheden til dataansvarlige. Ingen yderligere afvigelser konstateret.

The document is signed using Visma Addo digital signing service.
The signatures in this document are legally binding. The signers identities are registered and listed below.

"With my signature, I confirm the content of the document above."



Karina Wellendorph
Managing Director
(Signer's name supplied by Majken Havn)
26-11-2020 10:48

Andreas Uldahl
Senior Manager
(Signer's name supplied by Majken Havn)
26-11-2020 10:48

Nils B Christiansen
Associate Partner
(Signer's name supplied by Majken Havn)
26-11-2020 12:20

In addition to this document, one or more documents and attachments can be associated with the transaction.
All documents included in the transaction are listed below. The event log
describes signers' events related to the signing of the document.

Documents in the transaction

This document
Visma Dataløn - ISAE 3000 GDPR pr. 24.09.2020.pdf

The documents and attachemnts above have been signed and sent to all parties by e-mail or as a download link. Signer is responsible for downloading and securing the content of the documents and attachments.

Download documents
As a signer you have received a link to download the documents. The documents will be available for 10 days whereupon they will be deleted from Visma Addo.

Event log for document

Event log for the document

2020-11-26 10:43	The signing process has started
2020-11-26 10:43	The signing process has started
2020-11-26 10:43	The signing process has started
2020-11-26 10:43	A notification has been sent to Karina Wellendorph
2020-11-26 10:43	A notification has been sent to Nils B Christiansen
2020-11-26 10:43	A notification has been sent to Andreas Uldahl
2020-11-26 10:47	The authentication screen has been accessed via the link sent to Karina Wellendorph with method 2 faktor identifikation from IP address: 128.76.231.196
2020-11-26 10:47	The authentication screen has been accessed via the link sent to Andreas Uldahl with method 2 faktor identifikation from IP address: 93.162.215.81
2020-11-26 10:47	The document was opened via the link sent to Karina Wellendorph
2020-11-26 10:48	The document was opened via the link sent to Andreas Uldahl
2020-11-26 10:48	The document was signed by Karina Wellendorph (IP: 128.76.231.196)
2020-11-26 10:48	All documents have been signed by Karina Wellendorph
2020-11-26 10:48	The document was signed by Andreas Uldahl (IP: 93.162.215.81)
2020-11-26 10:48	All documents have been signed by Andreas Uldahl
2020-11-26 12:10	The authentication screen has been accessed via the link sent to Nils B Christiansen with method 2 faktor identifikation from IP address: 213.32.242.143
2020-11-26 12:10	The document was opened via the link sent to Nils B Christiansen
2020-11-26 12:20	The document was signed by Nils B Christiansen (IP: 213.32.242.143)
2020-11-26 12:20	All documents have been signed by Nils B Christiansen