Grant Thornton

Revisorerklæring

Visma timemsystem ApS

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

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

Juni 2023

Penneo dokumentnøgle: GAP5O-N7NXV-LS0VG-7KBKG-ODVNI-7EAQD

Indholdsfortegnelse

Afsnit 1:	Visma timemsystem ApS' beskrivelse af behandlingsaktivitet for leverancen af mTIME	1
Afsnit 2:	Visma timemsystem ApS' udtalelse	3
Afsnit 3:	Uafhængig revisors erklæring med høj grad af sikkerhed om informationssikkerhed og foranstaltninger i henhold til databehandleraftaler med kunder i perioden fra 1. januar 2022 til 31. december 2022	5
Afsnit 4:	Kontrolmål, udførte kontroller, test og resultater heraf	8

Penneo dokumentnøgle: GAP5O-N7NXV-LS0VG-7KBKG-ODVNI-7EAQD

Afsnit 1: Visma timemsystem ApS' beskrivelse af behandlingsaktivitet for leverancen af mTIME

Visma timemsystem ApS' beskrivelse af behandlingsaktivitet for leverancen af mTIME

Visma timemsystem

Visma timemsystem ApS er et selskab i VISMA, som udvikler produkter, komponenter og tilbyder rådgivning til det offentlige og private marked samt uddannelsesinstitutioner landet over.

Visma timemsystem udvikler mTIME som er et tids- og aktivitetsregistreringssystem.

Visma timemsystem har ca. 30 medarbejdere og er specialiserede inden for systemudvikling, support og informationssikkerhed. Visma timemsystem er organiseret i en udviklingsafdeling, drift- og supportafdeling og en administrationsafdeling.

Visma timemsystem har kontor i København.

Behandling af personoplysninger i mTIME

Tids og aktivitetsregistreringssystemet mTIME udvikles i Danmark og afvikles fra et hostingcenter inden for EU.

Databehandlingen består i support, fejlrettelser samt ændring og opdatering af tidsregistreringssystemet.

Databaser med kunders data bliver anonymiseret i forbindelse med hjemtagelse.

Personoplysninger

Kategori A

Almindelige personoplysninger, herunder oplysninger om navn, CPR-nummer, e-mailadresser, lønnummer, ansættelsesdato, ferieberegningsdato, fratrædelsesdato, normtid, ansættelsesvilkår, børn fødselsdage (af hensyn til omsorgsdage), oplysninger om sygefravær og sygdomsperioder, forudsat at sygdommens art ikke er nævnt, samt andet fravær fra arbejdet.

Kategori B

Ingen følsomme personoplysninger

Styring af persondatasikkerhed

Sikkerhedsgruppen i Visma timemsystem styrer persondatasikkerhed i forhold til den behandling, som Visma timemsystem varetager på vegne af sine kunder, herunder indgåelse af databehandleraftaler, besvarelse af henvendelser fra den dataansvarlige, underretning om brud på persondatasikkerheden, efterlevelse af interne politikker, procedurer og lignende.

Visma timemsystem har indført politikker, processer og procedurer, som sikrer, at Visma timemsystem kan stille tilstrækkelige garantier til at gennemføre passende tekniske og organisatoriske sikkerhedsforanstaltninger på en sådan måde, at behandlingen opfylder kravene i databeskyttelsesforordningen og sikrer beskyttelse af den registreredes rettigheder.

Visma timemsystem sørger for at uddanne medarbejdere i retningslinjerne i Visma timemsystems GDPR-håndbog samt at give instruktion i processer og procedurer. Dette sker gennem et årligt sikkerhedskursus. Endvidere er der GDPR-orientering, i forbindelse med fællesmøder i Visma timemsystem hvert kvartal.

Penneo dokumentnøgle: GAP5O-N7NXV-LS0VG-7KBKG-ODVNI-7EAQD

Derudover er der løbende awareness aktiviteter på Visma timemsystems intranet og interne månedlige nyhedsbreve.

Persondata sikkerhedspolitikken som er beskrevet i Visma timemsystems GDPR-håndbog er operationaliseret gennem den tilhørende persondata sikkerhedsinstruks, som oplister en række tilbagevendende handlinger og kontroller, samt en række regler for konfigurering og anvendelse af virksomhedens IT-systemer, der tilsammen sikrer, at persondata behandles forsvarligt.

De anførte kontroller og handlinger er indeholdt i et årshjul, der angiver, hvornår aktiviteterne skal gennemføres.

Resultaterne af de gennemførte kontroller bliver derefter indført i en logbog og andre sikkerhedshændelser indføres ligeledes i logbogen. Dette udgør virksomhedens dokumentation for, at Visma timemsystem lever op til forordningens krav.

Tredjelande

Der overføres ikke data til tredjelande.

Væsentlige ændringer i perioden

Der har ikke været væsentlige ændringer i perioden.

Komplementerende kontroller hos de dataansvarlige

Den dataansvarlige er forpligtet til at implementere følgende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller for at opnå kontrolmålene og dermed opfylde databeskyttelsesforordningen og databeskyttelsesloven:

- Visma timemsystem har gjort opmærksom på, at der ikke må indtastes følsomme personoplysninger i kommentarfelterne i mTIME. Det er den dataansvarliges ansvar, hvis der alligevel indtastes følsomme personoplysninger i disse felter.
- Den dataansvarlige har ansvaret for at sikre, at administratorernes brug af mTIME og den behandling af personoplysninger, der foretages i systemet, sker i overensstemmelse med databeskyttelseslovgivningen.
- Den dataansvarlige styrer brugerrettighederne (roller og rettigheder) i mTIME, herunder hvilke personer der tildeles administratoradgang, og hvilke rettigheder de enkelte administratorer tildeler de enkelte brugere, når der bliver oprettet brugere.
- Den dataansvarlige skal altid igennem en brugeraccepttest, før de accepterer at tage mTIME i brug i forbindelse med fejlrettelser og opdateringer.
- Den dataansvarlige skal give besked til Visma timemsystem, når der er en medarbejder, der stopper, således at Visma timemsystem kan fjerne brugeradgangen til Kundecenteret.
- Den dataansvarlige har ansvaret for, at logning for den enkelte medarbejder i mTIME slettes.

Penneo dokumentnøgle: GAP5O-N7NXV-LS0VG-7KBKG-ODVNI-7EAQD

Afsnit 2: Visma timemsystem ApS' udtalelse

Medfølgende beskrivelse er udarbejdet til brug for Visma timemsystem ApS' kunder, som har indgået en databehandleraftale med Visma timemsystem ApS, 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 timemsystem ApS anvender underleverandørerne og underdatabehandlerne IT Relation og TimeEdit AB. Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos Visma timemsystem ApS' underleverandører og underdatabehandlere. Visse kontrolmål i beskrivelsen kan kun nås, hvis underleverandørens kontroller, der forudsættes i designet af vores kontroller, er passende designet og er operationelt effektive. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underleverandører.

Enkelte af de kontrolmål, der er anført i Visma timemsystem ApS' beskrivelse i afsnit 1 af mTIME, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos Visma timemsystem ApS. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disses komplementerende kontroller.

Visma timemsystem ApS bekræfter, at:

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

   (i) Redegør for, hvordan Visma timemsystem ApS' processer og kontroller relateret til databeskyttelse var udformet og implementeret, herunder redegør for:

   - De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger
   - De processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere, slette og begrænse behandling af personoplysninger
   - De processer, der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige
   - De processer, der sikrer, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt
   - De processer, der ved ophør af databehandling sikrer, at der efter den dataansvarliges valg sker sletning eller tilbagelevering af alle personoplysninger til den dataansvarlige, medmindre lov eller regulering foreskriver opbevaring af personoplysningerne
   - De processer, der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underrettelse til de registrerede
   - De processer, der sikrer passende tekniske og organisatoriske sikringsforanstaltninger for behandlingen af personoplysninger under hensyntagen til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet
   - Kontroller, som vi med henvisning til mTIME's 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

Penneo dokumentnøgle: GAP5O-N7NXV-LS0VG-7KBKG-ODVNI-7EAQD

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

(ii) Indeholder relevante oplysninger om ændringer ved databehandlerens mTIME til behandling af personoplysninger foretaget i perioden fra 1. januar 2022 til 31. december 2022

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne mTIME 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 mTIME, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i perioden fra 1. januar 2022 til 31. december 2022, hvis relevante kontroller hos underleverandører var operationelt effektive, og dataansvarlige har udført de komplementerende kontroller, som forudsættes i designet af Visma timemsystem ApS' kontroller i perioden fra 1. januar 2022 til 31. december 2022. Kriterierne anvendt for at give denne udtalelse var, at:

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

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

(iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i perioden fra 1. januar 2022 til 31. december 2022

c) Der er etableret og opretholdt passende tekniske og organisatoriske foranstaltninger med henblik på at opfylde aftalerne med de dataansvarlige, god databehandlerskik og relevante krav til databehandlere i henhold til databeskyttelsesforordningen.

København, den 20. juni 2023
Visma timemsystem ApS

Khanh Bao Nguyen-Cong
Adm. direktør

Penneo dokumentnøgle: GAP5O-N7NXV-LS0VG-7KBKG-ODVNI-7EAQD

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

Til Visma timemsystem ApS og Visma timemsystem ApS' kunder i rollen som dataansvarlige.

Omfang

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

Visma timemsystem ApS anvender underleverandørerne og underdatabehandlerne IT Relation og TimeEdit AB. Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos Visma timemsystem ApS' underleverandører og underdatabehandlere. Visse kontrolmål i beskrivelsen kan kun nås, hvis underdatabehandlernes kontroller, der forudsættes i designet af Visma timemsystem ApS´ kontroller, er passende designet og fungerer effektivt sammen med de relaterede kontroller hos Visma timemsystem ApS.

Enkelte af de kontrolmål, der er anført i Visma timemsystem ApS' beskrivelse i afsnit 1 af mTIME, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos Visma timemsystem ApS. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disses komplementerende kontroller.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Visma timemsystem ApS' ansvar

Visma timemsystem ApS er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i "Afsnit 2", herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for at udforme, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Grant Thorntons uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i International Ethics Standards Board for Accountants' internationale retningslinjer for revisorers etiske adfærd (IESBA Code), der bygger på de grundlæggende principper om integritet, objektivitet, professionel kompetence og fornøden omhu, fortrolighed og professionel adfærd, samt etiske krav gældende i Danmark.

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

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

Penneo dokumentnøgle: GAP5O-N7NXV-LS0VG-7KBKG-ODVNI-7EAQD

Revisors ansvar

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

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

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

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

Begrænsninger i kontroller hos en databehandler

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

Penneo dokumentnøgle: GAP5O-N7NXV-LS0VG-7KBKG-ODVNI-7EAQD

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 mTIME, således som denne var udformet og implementeret i perioden fra 1. januar 2022 til 31. december 2022, i alle væsentlige henseender er retvisende, og

(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i perioden fra 1. januar 2022 til 31. december 2022, for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, ville blive opnået, hvis kontroller hos underleverandører var operationelt effektive, og hvis dataansvarlige har designet og implementeret de komplementerende kontroller, der forudsættes i designet af Visma timemsystem ApS' kontroller i perioden fra 1. januar 2022 til 31. december 2022, og

(c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i perioden fra 1. januar 2022 til 31. december 2022.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i det efterfølgende afsnit, Afsnit 4, er udelukkende tiltænkt dataansvarlige, der har anvendt Visma timemsystem ApS' mTIME, 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 20. juni 2023

Grant Thornton
Statsautoriseret Revisionspartnerselskab

Jacob Helly Juell-Hansen
Statsautoriseret revisor

Basel Rimon Obari
Executive director, CISA, CISM

Penneo dokumentnøgle: GAP5O-N7NXV-LS0VG-7KBKG-ODVNI-7EAQD

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

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

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

Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos Visma timemsystem ApS' underleverandører og underdatabehandlere.

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

Vi har udført vores tests af kontroller hos Visma timemsystem ApS via følgende handlinger:

Metode	Overordnet beskrivelse
Forespørgsel	Forespørgsel af passende personale hos Visma timemsystem ApS. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Observation af, hvordan kontroller udføres
Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at blive effektive, hvis de implementeres.
Genudførelse af kontrol	Vi har gentaget udførelse af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

Penneo dokumentnøgle: GAP5O-N7NXV-LS0VG-7KBKG-ODVNI-7EAQD

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

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

Artikler og punkter markeret med fed angiver primære områder.

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

Penneo dokumentnøgle: GAP5O-N7NXV-LS0VG-7KBKG-ODVNI-7EAQD

Kontrolmål A – Instruks vedrørende behandling af personoplysninger

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

Nr.	*Visma timemsystem ApS' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Vi har forespurgt til opdatering af proceduren.	Vi har observeret, at proceduren for håndtering af instrukser sidst er opdateret i 2020. Vi har fået oplyst, at der ikke har været ændringer til hvordan man håndterer instrukser siden sidste opdatering af proceduren. Ingen yderligere afvigelser konstateret.
A.2	Databehandleren udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Vi har stikprøvevis inspiceret, at behandlinger af personoplysninger foregår i overensstemmelse med instruks.	Ingen afvigelser konstateret.
A.3	Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning. Vi har inspiceret, at der er procedurer for underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. Vi har inspiceret, at den dataansvarlige er underrettet i tilfælde, hvor behandlingen af personoplysninger er vurderet at være i strid med lovgivningen.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: GAP5O-N7NXV-LS0VG-7KBKG-ODVNI-7EAQD

Kontrolmål B – Tekniske foranstaltninger

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

Nr.	*Visma timemsystem ApS' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at de aftalte sikkerhedsforanstaltninger etableres. Vi har inspiceret, at procedurer er opdaterede.	Ingen afvigelser konstateret.
B.2	Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de med dataansvarlige aftalte sikringsforanstaltninger.	Vi har inspiceret, at risikovurderingen er opdateret og omfatter relevante emner i forbindelse med behandlingen af personoplysninger.	Ingen afvigelser konstateret.
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Vi har forespurgt til om netværk er segmenteret.	Vi er blevet informeret om, at netværk ikke er tilstrækkeligt segmenteret hos underdatabehandler. Ingen yderligere afvigelser konstateret.
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Vi har inspiceret, at der en formel proces for tildeling af adgange, som sikrer, at der er et arbejdsbetinget behov for adgang. Vi har stikprøvevis inspiceret adgange, og stikprøvevis påset, at der er et arbejdsbetinget behov.	Ingen afvigelser konstateret.
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Vi har stikprøvevis inspiceret transmission over internettet, og stikprøvevis påset, at dette sker med effektiv kryptering.	Vi har observeret, at databehandleren understøtter forældet transportkryptering. Vi har fået oplyst, at der er igangværende arbejde for at udbedre forholdet. Ingen yderligere afvigelser konstateret.

Penneo dokumentnøgle: GAP5O-N7NXV-LS0VG-7KBKG-ODVNI-7EAQD

Kontrolmål B – Tekniske foranstaltninger

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

Nr.	*Visma timemsystem ApS' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
B.9	Der er etableret logning i systemer, databaser og netværk.	Vi har stikprøvevis inspiceret systemer, som opbevarer personoplysninger, og stikprøvevis påset, at der sker logning.	Ingen afvigelser konstateret.
B.10	Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.	Vi har inspiceret, at der foreligger procedurer for anvendelse af personoplysninger til udvikling, test og lignende, der sikrer, at anvendelsen alene sker i pseudonymiseret eller anonymiseret form. Vi har stikprøvevis inspiceret, at personoplysninger er pseudonymiseret eller anonymiseret i udviklings- og testdatabaser.	Ingen afvigelser konstateret.
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger.	Vi har stikprøvevis inspiceret, at der er dokumentation for løbende tests af de etablerede tekniske foranstaltninger.	Ingen afvigelser konstateret.
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Vi har stikprøvevis inspiceret ændringer, og vi har stikprøvevis påset, at ændringerne følger en formel procedure.	Ingen afvigelser konstateret.
B.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Vi har inspiceret, at der er en formel proces for tildeling og afbrydelse af adgange. Vi har stikprøvevis inspiceret dokumentation for afbrydelse af adgange for fratrådte medarbejdere. Vi har inspiceret dokumentation for gennemgang af adgange i perioden.	Ingen afvigelser konstateret.
B.14	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører højrisiko for de registrerede, sker som minimum ved anvendelse af to-faktor autentifikation.	Vi har stikprøvevis inspiceret adgange, og stikprøvevis påset, at adgang med to-faktor autentifikation.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: GAP5O-N7NXV-LS0VG-7KBKG-ODVNI-7EAQD

Kontrolmål B – Tekniske foranstaltninger

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

Nr.	*Visma timemsystem ApS' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
B.15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Vi har inspiceret dokumentation for, at databehandleren har oversigter over nøgler til kontoret.	Ingen afvigelser konstateret.

Kontrolmål C – Organisatoriske foranstaltninger

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

Nr.	*Visma timemsystem ApS' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
C.1	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. It-sikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Vi har inspiceret informationssikkerhedspolitikken og at den er opdateret og ledelsesgodkendt i perioden. Vi har inspiceret dokumentation for, at politikken er tilgængelig for medarbejderne.	Ingen afvigelser konstateret.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Vi har stikprøvevis inspiceret at kravene i databehandleraftalerne er dækket af informationssikkerhedspolitikkens krav til sikringsforanstaltninger og behandlingssikkerheden.	Ingen afvigelser konstateret.
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.	Vi har inspiceret, at der er en formel procedure for screening. Vi har stikprøvevis forespurgt til screening af medarbejdere i perioden.	Vi er blevet informeret om, at der er blevet udført screening i perioden, dog har vi ikke kunnet få dokumentation for dette. Ingen yderligere afvigelser konstateret.

Penneo dokumentnøgle: GAP5O-N7NXV-LS0VG-7KBKG-ODVNI-7EAQD

Kontrolmål C – Organisatoriske foranstaltninger

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

Nr.	*Visma timemsystem ApS' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
C.4	Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.	Vi har stikprøvevis inspiceret, at nyansatte medarbejdere har underskrevet en fortrolighedsaftale. Vi har stikprøvevis inspiceret, at nyansatte medarbejdere er blevet introduceret til relevante politikker og procedurer.	Vi har observeret, at der i én ud af fire stikprøver, har onboardingsprocessen ikke været fulgt. Ingen yderligere afvigelser konstateret.
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Vi har inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder deaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages. Vi har stikprøvevis inspiceret, at rettigheder er deaktiveret eller ophørt, samt at aktiver er inddraget for fratrådte medarbejdere.	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.	Vi har inspiceret dokumentation for, at fratrådte medarbejdere er underlagt en generel tavshedspligt.	Ingen afvigelser konstateret.
C.7	Der gennemføres løbende awarenesstræning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Vi har inspiceret dokumentation for at der er afholdt awareness træning i perioden, hvor behandling af personoplysninger bliver gennemgået.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: GAP5O-N7NXV-LS0VG-7KBKG-ODVNI-7EAQD

Kontrolmål C – Organisatoriske foranstaltninger

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

Nr.	*Visma timemsystem ApS' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
C.8	Databehandleren har vurderet behovet for en DPO, og har sikret, at DPO'en har tilstrækkelig faglighed til at udføre sine opgaver, samt at DPO'en bliver inddraget i relevante områder.	Vi har inspiceret dokumentation, der viser vurderingen af behovet for en DPO.	Ingen afvigelser konstateret.
C.9	Der foreligger hos databehandleren en fortegnelse over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige.	Vi har inspiceret fortegnelsen over behandlingsaktiviteter og at den er godkendt af ledelsen i perioden.	Ingen afvigelser konstateret.

Kontrolmål D -Tilbagelevering og sletning af personoplysninger

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

Nr.	*Visma timemsystem ApS' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
D.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Vi har forespurgt til opdatering af proceduren.	Vi har observeret, at proceduren er blevet opdateret efter periodens afslutning. Ingen yderligere afvigelser konstateret.
D.2	Der er aftalt specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.	Vi har stikprøvevis inspiceret databehandleraftaler, hvor krav for sletning og tilbagelevering af personoplysninger står beskrevet. Vi har forespurgt til ophørte kunder i perioden.	Vi er blevet oplyst om at der ikke har været nogle ophørte kunder i perioden og vi kan derfor ikke teste effektiviteten af kontrollen. Ingen afvigelser konstateret.

Penneo dokumentnøgle: GAP5O-N7NXV-LS0VG-7KBKG-ODVNI-7EAQD

Kontrolmål D -Tilbagelevering og sletning af personoplysninger

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

Nr.	*Visma timemsystem ApS' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
D.3	Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: • Tilbageleveret til den dataansvarlige og/eller • Slettet, hvor det ikke er i modstrid med anden lovgivning.	Vi har forespurgt til ophørte kunder i perioden.	Vi er blevet oplyst om at der ikke har været nogle ophørte kunder i perioden og vi kan derfor ikke teste effektiviteten af kontrollen. Ingen afvigelser konstateret.

Kontrolmål E – Opbevaring af personoplysninger

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

Nr.	*Visma timemsystem ApS' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
E.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret.
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Vi har stikprøvevis inspiceret, at der er dokumentation for, at databehandlingen, herunder opbevaring af personoplysninger, alene foretages på de lokaliteter, der fremgår af databehandleraftalen – eller i øvrigt er godkendt af den dataansvarlige.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: GAP5O-N7NXV-LS0VG-7KBKG-ODVNI-7EAQD

Kontrolmål F – Anvendelse af underdatabehandlere

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

Nr.	*Visma timemsystem ApS' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
F.1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks.	Vi har inspiceret dokumentation for, at der er en formel proces, som sikrer, at der bliver taget stilling til relevante krav inden der bliver indgået en underdatabehandleraftale med underdatabehandlere.	Ingen afvigelser konstateret.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Vi har inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere. Vi har stikprøvevis inspiceret, at der er dokumentation for, at underdatabehandlerens databehandling fremgår af databehandleraftalerne – eller i øvrigt er godkendt af den dataansvarlige.	Ingen afvigelser konstateret.
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underretters den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Vi har inspiceret proceduren for udskiftning af underdatabehandlere. Vi har forespurgt til udskiftning af underdatabehandlere i perioden.	Vi er blevet informeret om at der ikke har været udskiftning af underdatabehandlere i perioden. Vi har derfor ikke kunnet teste effektiviteten af kontrollen. Ingen afvigelser konstateret.
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Vi har inspiceret dokumentation for at underdatabehandlere bliver underlagt de samme databeskyttelsesforpligtelser som dem der er forudsat i databehandleraftalen med den dataansvarlige.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: GAP5O-N7NXV-LS0VG-7KBKG-ODVNI-7EAQD

Kontrolmål F – Anvendelse af underdatabehandlere

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

Nr.	*Visma timemsystem ApS' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere.	Vi har inspiceret listen over godkendte underdatabehandlere. Vi har stikprøvevis inspiceret databehandler aftaler, der alle indeholder de godkendte underdatabehandlere.	Ingen afvigelser konstateret.
F.6	Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende.	Vi har inspiceret dokumentation for, at der er udført skriftligt tilsyn med de underdatabehandlere der benyttes.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: GAP5O-N7NXV-LS0VG-7KBKG-ODVNI-7EAQD

Kontrolmål G – Overførsel af personoplysninger til tredjelande

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

Nr.	*Visma timemsystem ApS' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der er en formel politik for overførsler til tredjelande. Vi har inspiceret dokumentation for, at politikken er opdateret.	Ingen afvigelser konstateret.
G.2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	Vi har stikprøvevis inspiceret databehandleraftaler, og stikprøvevis påset, at der er taget stilling til tredjelandsoverførsler. Vi har forespurgt, om databehandleren har overført personoplysninger til tredjelande eller internationale organisationer.	Vi er blevet informeret om, at personoplysninger ikke overføres til tredjelande eller internationale organisationer, og vi finder dette sandsynliggjort på baggrund af vores testhandlinger. Ingen afvigelser konstateret.
G.3	Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	Vi har forespurgt, om databehandleren har overført personoplysninger til tredjelande eller internationale organisationer.	Vi er blevet informeret om, at personoplysninger ikke overføres til tredjelande eller internationale organisationer, og vi finder dette sandsynliggjort på baggrund af vores testhandlinger. Ingen afvigelser konstateret.

Penneo dokumentnøgle: GAP5O-N7NXV-LS0VG-7KBKG-ODVNI-7EAQD

Kontrolmål H – De registreredes rettigheder

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

Nr.	*Visma timemsystem ApS' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder. Vi har inspiceret, at procedurerne er opdaterede.	Ingen afvigelser konstateret
H.2	Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	Vi har forespurgt, om databehandleren har modtaget anmodninger fra den dataansvarlige i relation til de registreredes rettigheder.	Vi er blevet informeret om, at databehandleren ikke har modtaget anmodninger fra den dataansvarlige i relation til de registreredes rettigheder, hvorfor vi ikke har testet effektiviteten af databehandlerens procedurer. Ingen afvigelser konstateret

Penneo dokumentnøgle: GAP5O-N7NXV-LS0VG-7KBKG-ODVNI-7EAQD

Kontrolmål I – Håndtering af persondatasikkerhedsbrud

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

Nr.	*Visma timemsystem ApS' kontrolaktivitet*	*Grant Thorntons udførte test*	*Resultat af test*
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret procedure for håndteringen af brud på persondatasikkerheden samt at denne er opdateret og gennemgået i perioden.	Ingen afvigelser konstateret.
I.2	Databehandleren har etableret kontroller for identifikation af eventuelle brud på persondatasikkerheden.	Vi har inspiceret dokumentation for, at der er opsat kontroller for at opdage brud på informationssikkerheden. Vi har stikprøvevis inspiceret dokumentation for løbende identificering og udbedring af fejl i perioden.	Ingen afvigelser konstateret.
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Vi har inspiceret GDPR logbog for om der har været brud på persondatasikkerheden i perioden. Vi har forespurgt til, om der har været brud i perioden.	Vi er blevet informeret om, at der ikke har været nogle persondatasikkerhedsbrud i perioden og vi kan derfor ikke teste effektiviteten af kontrollen. Ingen afvigelser konstateret.
I.4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden.	Vi har inspiceret dokumentation for at der er opsat procedurer for hvordan den dataansvarlige bistås ved anmeldelse af persondatasikkerhedsbrud til datatilsynet.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: GAP5O-N7NXV-LS0VG-7KBKG-ODVNI-7EAQD

PENNEO

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

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

Navnet er skjult
Underskriver 1
Serienummer: d27bc15d-62cf-42d3-9b84-d15cce84f4ff
IP: 176.22.xxx.xxx
2023-06-20 11:51:44 UTC

MitID

Basel Rimon Obari
GRANT THORNTON,STATSAUTORISERET REVISIONSPARTNERSELSKAB
CVR: 34209936
Underskriver 2
Serienummer: 83192c2a-26a4-4658-812e-ed0c3d0b45d6
IP: 62.243.xxx.xxx
2023-06-20 12:39:48 UTC

MitID

Jacob Helly Juell-Hansen
Underskriver 3
Serienummer: CVR:34209936-RID:50904197
IP: 62.243.xxx.xxx
2023-06-21 07:17:08 UTC

NEM ID

Penneo dokumentnøgle: GAP5O-N7NXV-LS0VG-7KBKG-ODVNI-7EAQD

Dette dokument er underskrevet digitalt via **Penneo.com**. Signeringsbeviserne i dokumentet er sikret og valideret ved anvendelse af den matematiske hashværdi af det originale dokument. Dokumentet er låst for ændringer og tidsstemplet med et certifikat fra en betroet tredjepart. Alle kryptografiske signeringsbeviser er indlejret i denne PDF, i tilfælde af de skal anvendes til validering i fremtiden.

Sådan kan du sikre, at dokumentet er originalt
Dette dokument er beskyttet med et Adobe CDS certifikat. Når du åbner dokumentet i Adobe Reader, kan du se, at dokumentet er certificeret af **Penneo e-signature service <penneo@penneo.com>**. Dette er din garanti for, at indholdet af dokumentet er uændret.

Du har mulighed for at efterprøve de kryptografiske s igneringsbeviser i ndlejret i dokumentet ved at anvende Penneos validator på følgende websted: **https://penneo.com/validator**