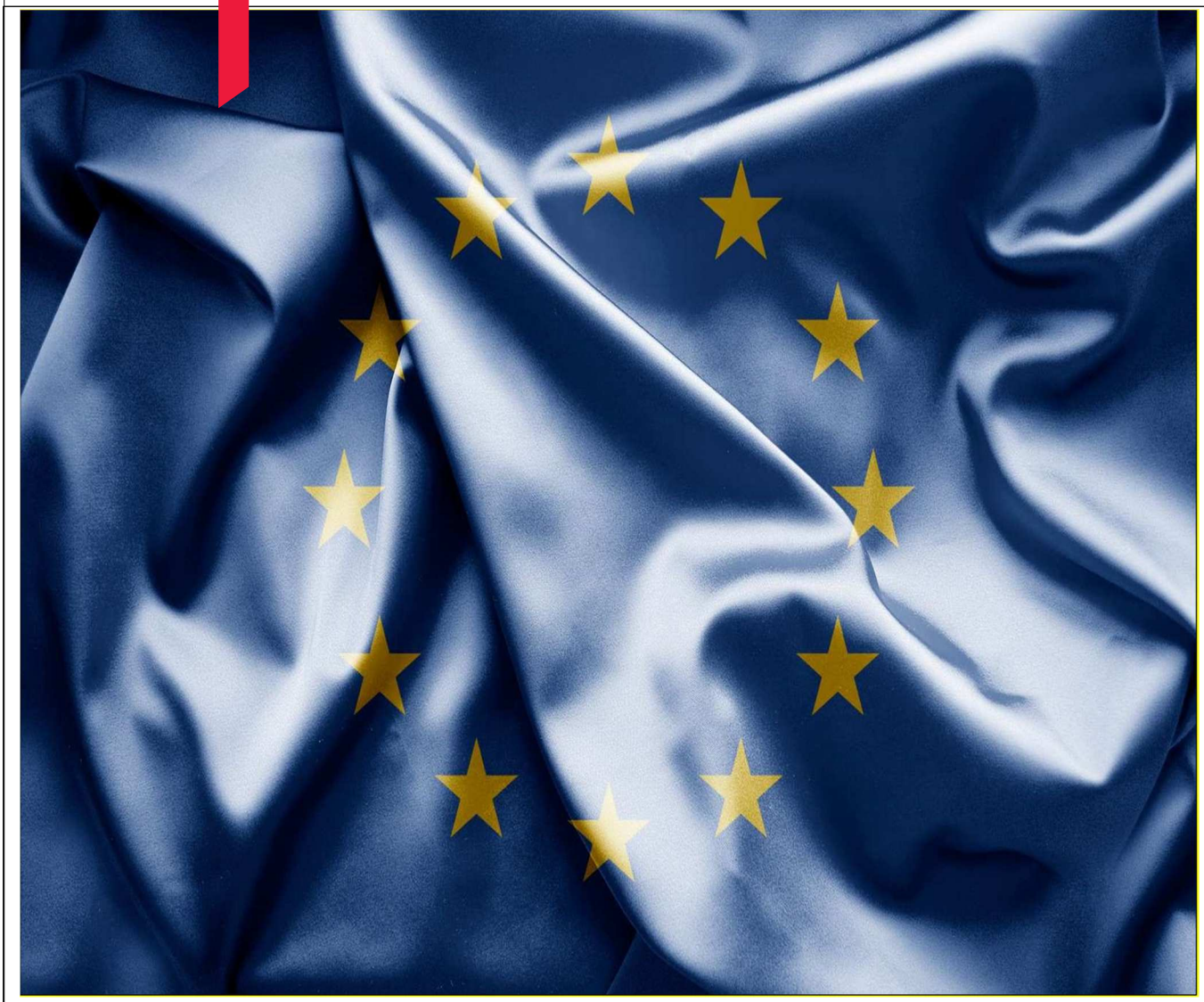

TIMEMSYSTEM APS

AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. JANUAR TIL 31. DECEMBER 2023 OM BESKRIVELSEN AF TIDSREGISTRERINGSSYSTEMET MTIME OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER OG DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

INDHOLD

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. JANUAR TIL 31. DECEMBER 2023 OM BESKRIVELSEN AF TIDSREGISTRERINGSSYSTEMET MTIME OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER OG DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

Til: Ledelsen i TIMEmSYSTEM ApS
TIMEmSYSTEM ApS' kunder (dataansvarlige)

Omfang

Vi har fået som opgave at afgive erklæring om den af TIMEmSYSTEM ApS (databehandleren) for hele perioden fra 1. januar til 31. december 2023 udarbejdede beskrivelse i sektion 3 af tidsregistreringssystemet mTIME og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, rettet mod behandling og beskyttelse af personoplysninger i henhold til Europa-Parlamentets og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordningen) og lov om supplerende bestemmelser til databeskyttelsesforordningen (databeskyttelsesloven), og om udformningen og den operationelle effektivitet af de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Databehandlerens ansvar

Databehandleren er ansvarlig for udarbejdelse af udtalelsen i sektion 2 og den medfølgende beskrivelse, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå udtalelsen og beskrivelsen er præsenteret. Databehandleren er endvidere ansvarlig for leveringen af de ydelser, beskrivelsen omfatter, ligesom databehandleren er ansvarlig for at anføre kontrolmålene samt udforme, implementere og effektivt udføre kontroller for at opnå de anførte kontrolmål.

Revisors 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.

BDO Statsautoriseret revisionsaktieselskab anvender International Standard on Quality Management 1, ISQM 1, som kræver, at vi designer, implementerer og driver et kvalitetsstyringssystem, herunder politikker eller procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om databehandlerens beskrivelse samt om udformningen og den operationelle effektivitet af kontroller, der knytter sig til de kontrolmål, som er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3000 om andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og den operationelle effektivitet af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse samt for kontrollernes udformning og operationelle effektivitet. De valgte handlinger afhænger af databehandlerens 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 den operationelle effektivitet 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 kontrolmål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i sektion 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

Databehandlerens beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved anvendelsen af tidsregistreringssystemet mTIME, som hver enkelt dataansvarlig måtte anse for vigtigt 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 den operationelle effektivitet af kontroller til fremtidige perioder undergivet risikoen for, at kontroller hos en databehandler kan blive utilstrækkelige eller svigte.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i databehandlerens udtalelse i sektion 2. Det er vores opfattelse:

a. at beskrivelsen af tidsregistreringssystemet mTIME og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, rettet mod behandling og beskyttelse af personoplysninger i henhold til databeskyttelsesforordningen og databeskyttelsesloven, således som de var udformet og implementeret i hele perioden fra 1. januar til 31. december 2023, i alle væsentlige henseender er retvisende, og

b. at de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 1. januar til 31. december 2023, og

c. at de testede tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som var de, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. januar til 31. december 2023.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, og resultater af disse tests fremgår i sektion 4.

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt dataansvarlige, der har anvendt databehandlerens tidsregistreringssystemet mTIME, og som har en tilstrækkelig forståelse til at vurdere den sammen med anden information, herunder de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen og databeskyttelsesloven er overholdt.

København, den 17. Januar 2024

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

Mikkel Jon Larssen
Partner, chef for Risk Assurance, CISA, CRISC

2. TIMEMSYSTEM APS' UDTALELSE

TIMEmSYSTEM ApS varetager behandling af personoplysninger i forbindelse med tidsregistreringssystemet mTIME for vores kunder, der er dataansvarlige i henhold til Europa-Parlaments og Rådets forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesforordningen) og lov om supplerende bestemmelser til databeskyttelsesforordningen (databeskyttelsesloven).

Medfølgende beskrivelse er udarbejdet til brug for de dataansvarlige, der har anvendt tidsregistreringssystemet mTIME, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen og databeskyttelsesloven er overholdt.

TIMEmSYSTEM ApS anvender underdatabehandlere. Disse underdatabehandleres relevante kontrolmål og tilknyttede tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller indgår ikke i den medfølgende beskrivelse.

TIMEmSYSTEM ApS bekræfter, at den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af tidsregistreringssystemet mTIME og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller i hele perioden fra 1. januar til 31. december 2023. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for tidsregistreringssystemet mTIME, og hvordan de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger øvrige kontroller var udformet og implementeret, herunder redegør for:
    - De typer af ydelser der er leveret, herunder typen af behandlede personoplysninger.
    - De processer i både it-systemer og forretningsgange der er anvendt til at behandle personoplysninger og, om nødvendigt, at korrigere og slette personoplysninger samt at 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 underretning til de registrerede.
    - De processer der sikrer passende tekniske og organisatoriske sikkerhedsforanstaltninger 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.
    - De kontroller, som vi med henvisning til afgrænsningen af tidsregistreringssystemet mTIME har forudsat ville være udformet og implementeret af de dataansvarlige, og som, hvis det er nødvendigt for at nå kontrolmålene, er identificeret i beskrivelsen.
    - De andre aspekter ved kontrolmiljøet, risikovurderingsprocessen, informationssystemerne og kommunikationen, kontrolaktiviteterne og overvågningskontrollerne, som har været relevante for behandlingen af personoplysninger.

2. Indeholder relevante oplysninger om ændringer i tidsregistreringssystemet mTIME og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der er foretaget i perioden fra 1. januar til 31. december 2023.

3. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af tidsregistreringssystemet mTIME og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller under hensyntagen til, at denne beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af dataansvarlige og derfor ikke kan omfatte ethvert aspekt ved tidsregistreringssystemet mTIME, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

TIMEmSYSTEM ApS bekræfter, at de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der knytter sig til de kontrolmål, som er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 1. januar til 31. december 2023. Kriterierne anvendt for at give denne udtalelse var, at:

1. De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret.

2. 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.

3. Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse, i hele perioden fra 1. januar til 31. december 2023.

TIMEmSYSTEM ApS bekræfter, at der er implementeret og opretholdt passende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller med henblik på at opfylde aftalerne med de dataansvarlige, god databehandlerskik og relevante krav til databehandlere i henhold til databeskyttelsesforordningen og databeskyttelsesloven.

København, den 17. januar 2024

TIMEmSYSTEM ApS

Khanh Bao Nguyen-Cong
Direktør og Partner

3. TIMEMSYSTEM APS' BESKRIVELSE AF TIDSREGISTRERINGSSYSTEMET MTIME

TIMEMSYSTEM APS

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

TIMEmSYSTEM udvikler mTIME, som er et tids- og aktivitetsregistreringssystem.

TIMEmSYSTEM har ca. 26 medarbejdere og er specialiserede inden for systemudvikling, support og informationssikkerhed. TIMEmSYSTEM er organiseret i en udviklingsafdeling, drift- og supportafdeling og en administrationsafdeling.

Visma timemsystem har kontor i Carlsbergbyen.

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.

TIDSREGISTRERINGSSYSTEMET MTIME OG BEHANDLING AF PERSONOPLYSNINGER

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, 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 TIMEmSYSTEM styrer persondatasikkerhed i forhold til den behandling, som 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.

TIMEmSYSTEM har indført politikker, processer og procedurer, som sikrer, at 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.

TIMEmSYSTEM sørger for at uddanne medarbejdere i retningslinjerne i TIMEmSYSTEM 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 TIMEmSYSTEM hvert kvartal. Derudover er der løbende awareness aktiviteter på Visma Space og learning zone.

Persondata sikkerhedspolitikken som er beskrevet i TIMEmSYSTEMs GDPR-håndbog er operationaliseret gennem den tilhørende persondatasikkerhedsinstruks, 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 TIMEmSYSTEM lever op til forordningens krav.

Styringen af persondatasikkerheden samt de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller er struktureret i følgende hovedområder, for hvilke der er defineret kontrolmål og kontrolaktiviteter:

ARTIKEL	OMRÅDE
Artikel 28, stk. 1	Databehandlerens garantier
Artikel 28, stk. 3	Databehandleraftale
Artikel 28, stk. 3, litra a og h, og stk. 10 Artikel 29 Artikel 32, stk. 4	Instruks for behandling af personoplysninger
Artikel 28, stk. 2 og 4	Underdatabehandlere
Artikel 28. stk. 3, litra b	Fortrolighed og lovbestemt tavshedspligt
Artikel 28, stk. 3, litra c	Tekniske og organisatoriske sikkerhedsforanstaltninger
Artikel 25	Databeskyttelse gennem design og standardindstillinger
Artikel 28, stk. 3, litra g	Sletning og tilbagelevering af personoplysninger
Artikel 28, stk. 3, litra e, f og h	Bistand til den dataansvarlige
Artikel 30, stk. 2, 3 og 4	Fortegnelse over kategorier af behandlingsaktiviteter
Artikel 33, stk. 2	Underretning om brud på persondatasikkerheden

RISIKOVURDERING

Sikkerhedsgruppen i TIMEmSYSTEM er ansvarlig for, at der foretages identifikation af sikkerhedsrisici, at der sker kategorisering af sikkerhedsrisici med udgangspunkt i sandsynlighed og påvirkningsgraden for den registreredes rettigheder, samt at der er etableret de nødvendige sikkerhedsforanstaltninger.

Sikkerhedsgruppen i TIMEmSYSTEM sørger for en årlig gennemgang af nuværende og fremtidige sikkerhedsrisici og sikkerhedsforanstaltninger.

Der anvendes en GDPR risikobaseret tilgang ved enhver rettelse og videreudvikling i mTIME. Den belyser risici i forhold til den registreredes rettigheder ved uautoriseret adgang til persondata, tilintetgørelse af oplysningerne, tab af oplysningerne, ændring af oplysningerne samt for uautoriseret adgang til følsomme personoplysninger eller CPR-nr. Risikovurderingen understøtter, at der bliver etableret de nødvendige sikkerhedsforanstaltninger (kontroller).

TIMEmSYSTEM har som databehandler ikke valgt at udarbejde en konsekvensanalyse vedrørende databeskyttelse (Data Protection Impact Assessment), fordi TIMEmSYSTEM har vurderet, at kriterierne for udarbejdelsen af konsekvensanalysen ikke er til stede.

TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER

De tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller vedrører alle processer og systemer, som behandler personoplysninger på vegne af den dataansvarlige. De i kontrolskemaet anførte kontrolmål og kontrolaktiviteter er en integreret del af den efterfølgende beskrivelse.

Instruks for behandling af personoplysninger

TIMEmSYSTEM har indført politikker og procedurer, der sikrer, at medarbejdere som tilgår kunders miljø, handler efter instruks. TIMEmSYSTEM's ansvar skal som databehandler følge beskrevne Standard Operation Procedures, hvoraf det fremgår, at medarbejderne skal have læst kundens databehandleraftale. Dette er med et særligt fokus på instruksen og hvilke typer af persondata, der er indeholdt i aftalen. Medarbejderne er samtidig opmærksom på at informere dataansvarlige, såfremt der sker en ulovlig instruks, som er i strid med databeskyttelseslovgivningen.

Underdatabehandler og tilsyn hermed

TIMEmSYSTEM benytter Cloud Factory som underdatabehandler. TIMEmSYSTEM har med Cloud Factory indgået en underdatabehandleraftale, hvor det er aftalt, at Cloud Factory skal fremsende en ISAE 3402 type 2-erklæring. Der udarbejdes et referat, der samler det årlige tilsyn med Cloud Factory, som er lokaliseret i Danmark, Vestergade 4, 6800 Varde. Der føres et årligt tilsyn med underdatabehandleren, som fremgår af vores årshjul.

Fortrolighedsaftale med leverandører

TIMEmSYSTEM sikrer, at der indgås tavsheds- og fortrolighedsaftaler med leverandører, der ikke er underdatabehandlere, og som kan have adgang til personoplysninger.

Fortrolighed og lovbestemt tavshedspligt

Alle personer, der arbejder med personoplysninger i TIMEmSYSTEM er underlagt tavshedspligt. Ved ansættelsen underskrives en fortroligheds- og tavshedserklæring, som opbevares i medarbejderens personalemappe digitalt og i fysisk arkiv.

Databeskyttelse gennem design og standardindstillinger

Ændringsstyring

TIMEmSYSTEM har et workflow, der indeholder en procesbeskrivelse i tilfælde af fejl, som er fundet i produktionsmiljøet, eller ved ændringsønsker, der kommer fra en kunde, og som kræver koderettelse. Den beskriver flowet mellem supportafdelingen, udviklingsafdelingen og testafdelingen.

Der anvendes en GDPR risikobaseret tilgang ved enhver rettelse og videreudvikling i mTIME. Den belyser risici i forhold til den registreredes rettigheder ved uautoriseret adgang til persondata, tilintetgørelse af oplysningerne, tab af oplysningerne, ændring af oplysningerne samt for uautoriseret adgang til følsomme personoplysninger eller cpr-nr. Risikovurderingen understøtter, at der bliver etableret de nødvendige sikkerhedsforanstaltninger (kontroller).

Hjemtagelse af kundedatabaser

I tilfælde af, at der er behov for hjemtagelse af en database for at reproducere en fejl, og for at sikre, at fejlrettelsen fungerer efter hensigten, vil proceduren for hjemtagning af databaser benyttes. Proceduren sørger for at hente anonymiserede data fra kundens produktionsmiljø eller testmiljø.

Tekniske og organisatoriske sikkerhedsforanstaltninger

Risikovurdering
TIMEmSYSTEM har gennemført de tekniske og organisatoriske sikkerhedsforanstaltninger på baggrund af en vurdering af risici i forhold til fortrolighed, integritet og tilgængelighed.

Træning og uddannelse (it-sikkerhedskursus)
TIMEmSYSTEM sørger for at uddanne medarbejdere i retningslinjerne i TIMEmSYSTEMs it-sikkerhedsforanstaltninger samt at give instruktion i processer og procedurer. Dette sker gennem et årligt sikkerhedskursus.

Opbevaring
TIMEmSYSTEM opbevarer ind- og uddatamateriale, så uvedkommende ikke kan få adgang til at gøre sig bekendt med de personoplysninger, der er indeholdt i mTIME-systemet.

Brugerstyring
TIMEmSYSTEM har indført procedurer, der sikrer, at adgang til systemer og data er beskyttet af et autorisationssystem. Bruger oprettes med unik brugeridentifikation og password, og brugeridentifikation anvendes ved tildeling af adgang til ressourcer og systemer. Al tildeling af rettigheder i systemer sker ud fra et arbejdsbetinget behov. Der foretages mindst en gang årligt en evaluering af brugernes fortsatte arbejdsbetingede behov for adgang, herunder aktualitet og korrekthed for tildelte brugerrettigheder. Procedurer og kontroller understøtter processen for oprettelse, ændring og nedlæggelse af brugere og tildeling af rettigheder samt gennemgang heraf.

Udformning af krav til blandt andet længde, kompleksitet, løbende udskiftning og historik af password samt lukning af brugerkonto efter forgæves adgangsforsøg følger best practise for en sikker logisk adgangskontrol. Der er udformet tekniske foranstaltninger, der understøtter disse krav.

Kryptering af personoplysninger
TIMEmSYSTEM har indført procedure for at sende krypterede e-mails.

TIMEmSYSTEM har indført procedurer, der sikrer, at eksterne kommunikationsforbindelser er sikret med stærk kryptering, og at e-mails og anden kommunikation, der indeholder følsomme personoplysninger, er krypteret i forsendelsen ved anvendelse af TLS.

Hjemmearbejdspladser
TIMEmSYSTEM har indført procedurer, der sikrer, at adgang fra arbejdspladser uden for TIMEmSYSTEM's lokaler og fjernadgang til systemer og data sker via VPN-forbindelser med to-faktor autentifikation.

Fysisk sikkerhed
TIMEmSYSTEM har indført procedurer, der sikrer, at lokaler er beskyttet mod uautoriseret adgang. Kun personer med et arbejdsbetinget eller andet legitimt behov har adgang til lokalerne, og særlige sikkerhedsmæssige foranstaltninger er indført for områder, hvor der foretages behandling af personoplysninger. Kunder, leverandører og andre besøgende ledsages.

Reparation og service samt bortskaffelse af it-udstyr
TIMEmSYSTEM har indført procedurer, der sikrer, at udstyr, som udleveres til tredjemand for service, reparation eller bortskaffelse, udleveres uden datadiske, og at brugte og kasserede datamedier wipes inden destruktion.

Logning i systemer, databaser og netværk
TIMEmSYSTEM har indført procedurer, der sikrer, at logning er opsat i henhold til lovgivningens krav og forretningsmæssige behov, baseret på en risikovurdering af systemer og det aktuelle trusselsniveau. Logdata er sikret mod tab og sletning.

Der foretages følgende logning i mTIME:
- Registrering: Hvem har registreret oplysningen og tidspunkt for registreringen.
- Medarbejdergodkendelse: Hvem har foretaget egen godkendelsen og tidspunkt for godkendelsen.
- Ledergodkendelse: Hvem har foretaget ledergodkendelsen og tidspunkt for godkendelsen.
- Fraværsgodkendelse: Hvem har godkendt fraværet og tidspunkt for godkendelsen.

Egenkontrol
TIMEmSYSTEM har udarbejdet et årshjul, som benyttes til at udføre egenkontrol.

TIMEmSYSTEM har indført procedurer, der sikrer, at der sker løbende overvågning af indførte tekniske sikkerhedsforanstaltninger. Der foretages løbende opfølgning af medarbejdernes brugeradgange til kunders miljøer.

Ændring af datalokation
TIMEmSYSTEM anvender kun godkendte underdatabehandlere i forhold til behandling af personoplysninger uden for det almindelige datamiljø i overensstemmelse med indgåede databehandleraftaler.

Sletning og tilbagelevering af personoplysninger

TIMEmSYSTEM har indført en procedure, der sikrer, at personoplysninger slettes eller tilbageleveres i henhold til instruks fra den dataansvarlige, når behandlingen af personoplysninger ophører ved udløb af kontrakten med den dataansvarlige.

Bistand til den dataansvarlige

TIMEmSYSTEM har indført en proces, der sikrer, at TIMEmSYSTEM kan bistå den dataansvarlige med at opfylde dennes forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder.

TIMEmSYSTEM har indført en proces, der sikrer, at TIMEmSYSTEM kan bistå den dataansvarlige med at sikre overholdelse af forpligtelserne i artikel 32 om behandlingssikkerhed, artikel 33 og 34 om anmeldelse og underretning af brud på persondatasikkerheden samt artikel 35 og 36 om konsekvensanalyser.

TIMEmSYSTEM har indført en proces, der sikrer, at TIMEmSYSTEM kan stille alle oplysninger, der er nødvendige for at påvise overholdelse af kravene til databehandlere, til rådighed for den dataansvarlige. TIMEmSYSTEM giver desuden mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller andre, som er bemyndiget hertil af den dataansvarlige.

Fortegnelse over kategorier af behandlingsaktiviteter

TIMEmSYSTEM har indført en proces, der sikrer, at der føres en fortegnelse over kategorier af behandlingsaktiviteter, der foretages på vegne af den dataansvarlige. Fortegnelsen opdateres regelmæssigt og kontrolleres under den årlige gennemgang af politikker og procedurer mv. Fortegnelsen opbevares elektronisk og kan stilles til rådighed for tilsynsmyndigheden efter anmodning.

Brud på persondatasikkerheden

TIMEmSYSTEM har indført en proces, der sikrer, at brud på persondatasikkerheden registreres med detaljeret information om hændelsen, og at der sker underretning af den dataansvarlige uden unødig forsinkelse, efter at TIMEmSYSTEM er blevet opmærksom på, at der er sket brud på persondatasikkerheden. De registrerede informationer gør den dataansvarlige i stand til at foretage en vurdering af, om bruddet på persondatasikkerheden skal anmeldes til tilsynsmyndigheden, og om de registrerede skal underrettes.

ÆNDRINGER I PERIODEN 1. JANUAR TIL 31. DECEMEBR 2023

TIMEmSYSTEM skiftede lokation fra Glostrup til Carlsbergbyen i slutningen af december 2022/starten af januar 2023.

TIMEmSYSTEM skiftede den 1/5-2023 underdatabehandler fra IT-Relation til Cloud Factory. Endvidere har vi i perioden taget et nyt egenudviklet kundecenter i brug, hvor komponenten Mailjet anvendes.

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:

- 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 TIMEmSYSTEM, når der er en medarbejder, der stopper, således at TIMEmSYSTEM kan fjerne brugeradgangen til Kundecenteret.

4. KONTROLMÅL, KONTROLAKTIVITETER, TEST OG RESULTAT AF TEST

Formål og omfang

BDO har udført sit arbejde i overensstemmelse med ISAE 3000 om andre erklæringsopgaver med sikkerhed end revision eller review af historiske finansielle oplysninger.

BDO har udført handlinger for at opnå bevis for oplysningerne i TIMEmSYSTEM ApS' beskrivelse af tidsregistreringssystemet mTIME samt for udformningen og den operationelle effektivitet af de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. De valgte handlinger afhænger af BDO's vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt.

BDO's test af udformningen og den operationelle effektivitet af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, der er udvalgt af TIMEmSYSTEM ApS, og som fremgår af efterfølgende kontrolskema.

I kontrolskemaet har BDO beskrevet de udførte test, der blev vurderet som nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået, og at de tilhørende kontroller var hensigtsmæssigt udformet og har fungeret effektivt i hele perioden fra 1. januar til 31. december 2023.

Udførte testhandlinger

Test af udformningen af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller samt implementeringen heraf er udført ved forespørgsel, inspektion, observation og genudførelse.

Type	Beskrivelse
Forespørgsel	Forespørgsler hos TIMEmSYSTEM ApS' passende personale er udført for alle væsentlige kontrolaktiviteter. Forespørgslerne blev udført for blandt andet at opnå viden og yderligere oplysninger om indførte politikker og procedurer, herunder hvordan kontrolaktiviteterne udføres, samt at få bekræftet beviser for politikker, procedurer og kontroller.
Inspektion	Dokumenter og rapporter, der indeholder angivelse om udførelse af kontrollen, er gennemlæste med det formål at vurdere udformningen og overvågningen af de specifikke kontroller, herunder om kontrollerne er udformede, således at de kan forventes at blive effektive, hvis de implementeres, og om kontrollerne overvåges og kontrolleres tilstrækkeligt og med passende intervaller. Test af væsentlige systemopsætninger af tekniske platforme, databaser og netværksudstyr er udført for at påse, om kontroller er implementerede, herunder eksempelvis vurdering af logning, sikkerhedskopiering, patch management, autorisationer og adgangskontroller, datatransmission samt besigtigelse af udstyr og lokaliteter.
Observation	Anvendelsen og eksistensen af specifikke kontroller er observeret, herunder test for at påse, at kontrollen er implementeret.
Genudførelse	Kontroller er genudført for at verificere, at kontrollen fungerer som forudsat.

For de ydelser, som IT Relation leverer inden for hosting af TIMEmSYSTEMs kundecenter, har vi modtaget en ISAE 3402 type 2-erklæring om de generelle it-kontroller for perioden 1. januar til 31. december 2022.

For de ydelser, som Cloud Factory leverer inden for Hosting af mTIMEs kundecenter, har vi modtaget en ISAE 3402 type 2-erklæring om de generelle it-kontroller for perioden 1. januar til 31. december 2022.

Disse underdatabehandleres relevante kontrolmål og tilknyttede kontroller indgår ikke i TIMEmSYSTEM ApS' beskrivelse af tidsregistreringssystemet mTIME og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. Vi har således alene inspiceret den modtagne dokumentation og

testet de kontroller hos TIMEmSYSTEM ApS, der sikrer udførelsen af et behørigt tilsyn med underdatabehandlernes opfyldelse af den mellem underdatabehandlernes og databehandleren indgåede databehandleraftaler og opfyldelse af databeskyttelsesforordningen og databeskyttelsesloven.

Resultat af test

Resultatet af de udførte test af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller angiver, om den beskrevne test har givet anledning til at konstatere afvigelser.

En afvigelse foreligger, når:

- Tekniske eller organisatoriske sikkerhedsforanstaltninger eller øvrige kontroller mangler at blive udformet og implementeret for at kunne opfylde et kontrolmål.
- Tekniske eller organisatoriske sikkerhedsforanstaltninger eller øvrige kontroller, der knytter sig til et kontrolmål, ikke er hensigtsmæssigt udformet og implementeret eller ikke har fungeret effektivt i perioden.

Artikel 28, stk. 1: Databehandlerens garantier		
Kontrolmål ▶ *At sikre, at databehandleren kan stille de fornødne garantier til beskyttelse af den dataansvarliges personoplysninger i overensstemmelse med kravene i databeskyttelsesforordningen og beskyttelsen af den registreredes rettigheder.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Informationssikkerhed- og databeskyttelse ▶ TIMEmSYSTEM har udarbejdet og implementeret en IT-sikkerhedspolitik, som bliver opdateret minimum en gang årligt ved vurderet behov herfor. ▶ TIMEmSYSTEM har udarbejdet og implementeret en GDPR-Håndbog, som bliver opdateret minimum en gang årligt ved vurderet behov herfor.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's IT-sikkerhedspolitik samt GDPR-Håndbogen og observeret, at disse er implementeret hos TIMEmSYSTEM. Vi har observeret, at IT-sikkerhedspolitikken og GDPR-Håndbogen kommunikeres til medarbejdere i forbindelse med ansættelsen og ved løbende awareness-kampagner. Vi har på forespørgsel blevet oplyst, at IT-sikkerhedspolitikken fra 2022 har været gældende i hele 2023 og vil blive opdateret igen i 2024, og observeret at GDPR-Håndbogen er blevet opdateret den 14. november 2023.	Ingen afvigelser konstateret.
Organisering af informationssikkerhed ▶ TIMEmSYSTEM har dokumenteret og etableret ledelsesstyring af informationssikkerhed. ▶ TIMEmSYSTEM har dokumenteret og etableret ledelsesstyrring af databeskyttelse.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's IT-sikkerhedspolitik samt GDPR-Håndbogen. Vi har observeret, at TIMEmSYSTEM har etableret ledelsesstyring af informationssikkerhed og databeskyttelse gennem politikker, der ajourføres af IT-sikkerhedsgruppen og den GDPR-ansvarlige.	Ingen afvigelser konstateret.

Artikel 28, stk. 1: Databehandlerens garantier		
Kontrolmål ▶ *At sikre, at databehandleren kan stille de fornødne garantier til beskyttelse af den dataansvarliges personoplysninger i overensstemmelse med kravene i databeskyttelsesforordningen og beskyttelsen af den registreredes rettigheder.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Rekruttering af medarbejdere ▶ TIMEmSYSTEM har udarbejdet og implementeret en procedure for rekruttering af nye medarbejdere, herunder screening af medarbejder før ansættelse.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's procedure for rekruttering af nye medarbejdere. Vi har observeret, at denne indeholder procedure for rekruttering og ansættelse af medarbejdere, herunder screening af potentielle medarbejdere. Vi har ved en stikprøve af nyansatte inspiceret dokumentation for, at databehandleren har foretaget screening af medarbejdere før ansættelse.	Ingen afvigelser konstateret.
Fratrædelse af medarbejdere ▶ TIMEmSYSTEM's har udarbejdet og implementeret en procedure for fratrædelse af medarbejdere ved ophør af ansættelse. ▶ Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's procedure for fratrædelse af medarbejdere og observeret, at proceduren sikrer beskyttelse af den dataansvarliges personoplysninger i overensstemmelse med kravene i databeskyttelsesforordningen og databeskyttelsesloven. Vi har ved en stikprøve af fratrådte medarbejdere inspiceret dokumentation for, at systemadgange er slettet i henhold til proceduren. Vi har ved en stikprøve af fratrådte medarbejdere observeret at medarbejderen ved fratrædelse er blevet orienteret om, at den underskrevne fortrolighedsaftale fortsat er gældende efter fratrædelse.	Ingen afvigelser konstateret.

Artikel 28, stk. 1: Databehandlerens garantier		
Kontrolmål ▶ *At sikre, at databehandleren kan stille de fornødne garantier til beskyttelse af den dataansvarliges personoplysninger i overensstemmelse med kravene i databeskyttelsesforordningen og beskyttelsen af den registreredes rettigheder.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Uddannelse og instruktion af medarbejdere, der behandler personoplysninger ▶ Der afholdes introduktionskursus for nye medarbejdere, herunder om behandling af dataansvarliges personoplysninger. ▶ TIMEmSYSTEM foretager løbende uddannelse af medarbejdere i henhold til databeskyttelse og informationssikkerhed samt håndtering heraf.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's GDPR-håndbog og kursusmateriale, hvoraf det fremgår, at TIMEmSYSTEM instruerer alle medarbejdere om reglerne for håndtering og behandling af personoplysninger som databehandler. Vi har på forespørgsel fået oplyst, at der afholdes introduktionskursus for nye medarbejdere om systemer og adgang til disse samt om behandling af dataansvarliges personoplysninger. Vi har foretaget inspektion af stikprøvevis udvalgt dokumentation for medarbejderes deltagelse på GDPR-kurset hos TIMEmSYSTEM og observeret, at TIMEmSYSTEM's medarbejdere efter gennemført kursus svarer på kontrolspørgsmål om deres ansvar og retningslinjer for håndtering og behandling af personoplysninger. Vi har foretaget inspektion og observeret, at TIMEmSYSTEM via sikkerhedskurset og teamopfølgningsmøder løbende uddanner medarbejdere i henhold til databeskyttelse og informationssikkerhed samt håndtering heraf.	Ingen afvigelser konstateret.
Awareness og oplysningskampagner for medarbejdere ▶ TIMEmSYSTEM udfører løbende awareness-kampagner i form af, opslag, team-opfølgningsmøder. ▶ TIMEmSYSTEM udfører oplysningskampagner for medarbejdere om databeskyttelse og informationssikkerhed.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's GDPR-håndbog og kursusmateriale, hvoraf det fremgår, at TIMEmSYSTEM instruerer alle medarbejdere om reglerne for håndtering og behandling af personoplysninger som databehandler.	Ingen afvigelser konstateret.

Artikel 28, stk. 1: Databehandlerens garantier		
Kontrolmål ▶ *At sikre, at databehandleren kan stille de fornødne garantier til beskyttelse af den dataansvarliges personoplysninger i overensstemmelse med kravene i databeskyttelsesforordningen og beskyttelsen af den registreredes rettigheder.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har observeret, at TIMEmSYSTEM løbende udfører awareness-kampagner i form af, opslag, team-opfølgningsmøder i henhold til databeskyttelse og informationssikkerhed samt håndtering heraf.	

Artikel 28, stk. 3: Databehandleraftale

Kontrolmål

- *At sikre, at databehandleren indgår en skriftlig kontrakt med den dataansvarlige, der fastsætter vilkårene for behandlingen af den dataansvarliges personoplysninger, og at kontrakten opbevares elektronisk.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Indgåelse af databehandleraftale med den dataansvarlige - TIMEmSYSTEM har procedurer for indgåelse af skriftlige databehandleraftaler, der er i overensstemmelse med de ydelser, som TIMEmSYSTEM leverer. - TIMEmSYSTEM anvender en databehandleraftaleskabelon for indgåelse af databehandleraftaler. - Ved indgåelse af skriftlige databehandleraftaler baseret på den dataansvarliges skabelon, anvender TIMEmSYSTEM en tjekliste, som fastlægger hvad TIMEmSYSTEM kan leve op til. - Databehandleraftaler underskrives og opbevares elektronisk. - Databehandleraftaler indeholder informationer om brugen af underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's procedure for indgåelse af skriftlige databehandleraftaler, er i overensstemmelse med de ydelser, som leveres. Vi har foretaget inspektion af TIMEmSYSTEM's skabeloner for databehandleraftaler. Vi har observeret, at disse er i overensstemmelse med kravene i databeskyttelsesforordningens artikel 28. stk. 3, og at disse indeholder informationer om brugen af underdatabehandlere. Vi har på forespørgsel fået oplyst, at ved indgåelse af skriftlige databehandleraftaler baseret på den dataansvarliges skabelon, gennemlæser og vurdere TIMEmSYSTEM aftalerne, for at sikre, at TIMEmSYSTEM kan leve op til dem. Vi har inspiceret udvalgte stikprøver af indgåede databehandleraftaler med dataansvarlige ud fra fortegnelse over kategorier af behandlingsaktiviteter. Vi har observeret, at disse databehandleraftaler er i overensstemmelse med de ydelser, som TIMEmSYSTEM leverer, og følger skabelon for databehandleraftale. Vi har observeret, at disse databehandleraftaler er underskrevet af begge parter. Vi har observeret, at disse databehandleraftaler indeholder informationer om brugen af underdatabehandlere. Vi har observeret, at TIMEmSYSTEM opbevarer sine indgåede databehandleraftaler med de dataansvarlige elektronisk.	Ingen afvigelser konstateret.

Artikel 28, stk. 3 og 10, artikel 29 og artikel 32, stk. 4: Instruks for behandling af personoplysninger

Kontrolmål

- *At sikre, at databehandleren alene handler efter dokumenteret instruks fra den dataansvarlige.*
- *At sikre, at databehandleren underretter den dataansvarlige, hvis en instruks er i strid med databeskyttelsesforordningen og databeskyttelsesloven.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Instruks for behandling af personoplysninger ▶ Databehandler indhenter instruks for behandling af personoplysninger fra den dataansvarlige, i forbindelse med indgåelse af databehandleraftale. ▶ Databehandler udfører alene behandling af personoplysninger, som fremgår af instruks fra dataansvarlig. ▶ TIMEmSYSTEM underretter den dataansvarlige, hvis en instruks er i strid med databeskyttelseslovgivningen.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har inspiceret indgåede databehandleraftaler og observeret, at TIMEmSYSTEM indhenter instruks for behandling af personoplysninger fra den dataansvarlige, i forbindelse med indgåelse af databehandleraftale. Vi har inspiceret indgåede databehandleraftaler og observeret, at TIMEmSYSTEM alene udfører behandling af personoplysninger, som fremgår af instruks fra dataansvarlig. Vi har foretaget inspektion af TIMEmSYSTEM's GDPR-håndbog og skabelon for databehandleraftale. Vi har observeret, at TIMEmSYSTEM skal underrette den dataansvarlige, hvis det vurderes, at en instruks er i strid med databeskyttelseslovgivningen. Vi har ved en stikprøve af indgåede databehandleraftaler observeret, at TIMEmSYSTEM er forpligtet til at underrette den dataansvarlige, såfremt en instruks efter TIMEmSYSTEM's vurdering er i strid med databeskyttelseslovgivningen. Vi har på forespørgsel fået oplyst, at der ikke har været en instruks, der har været i strid med databeskyttelseslovgivningen, derfor er kontrollen ikke efterprøvet.	Ingen afvigelser konstateret.

Artikel 28, stk. 2 og 4:Underdatabehandlere

Kontrolmål

- *At sikre, at underdatabehandleren er pålagt de samme databeskyttelsesforpligtelser, som databehandleren er pålagt af den dataansvarlige, ved indgåelse af en skriftlig kontrakt med tilhørende instruks.*
- *At sikre, at den dataansvarlige har givet en forudgående specifik eller generel skriftlig godkendelse af underdatabehandlere.*
- *At sikre, at underdatabehandleren kan stille de fornødne garantier til beskyttelse af personoplysningerne i overensstemmelse med kontrakten.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Databehandleraftaler med underdatabehandlere, herunder dokumenteret instruks ▶ TIMEmSYSTEM har en oversigt over godkendte underdatabehandlere. Oversigt over godkendte underdatabehandlere indeholder blandt andet hvem der er kontaktperson, lokation for behandling samt hvilken type af behandling og kategori af personoplysninger, som underdatabehandler foretager.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's procedure for indgåelse af databehandleraftaler og skabelon for databehandleraftale, hvoraf procedure for indgåelse af underdatabehandleraftaler fremgår samt retningslinjer for brugen af underdatabehandlere. Vi har foretaget inspektion af indgået databehandleraftale mellem TIMEmSYSTEM og deres underdatabehandlere og observeret, at databehandleraftalen opfylder kravene i indgået databehandleraftale med dataansvarlig og databeskyttelsesforordningens artikel 28. Vi har desuden observeret, at databehandleraftalen er underskrevet af begge parter og opbevaret elektronisk. Vi har foretaget inspektion af indgåede databehandleraftaler med dataansvarlige og observeret, at relevante underdatabehandlere er angivet som underdatabehandler.	Ingen afvigelser konstateret.
Tilsyn med underdatabehandler ▶ TIMEmSYSTEM udfører og dokumenterer sit tilsyn med underdatabehandleren IT Relation, herunder at den sikkerhed, der i underdatabehandleraftalen er stillet krav om, lever op til de krav, som den dataansvarlige har stillet i sin aftale med TIMEmSYSTEM.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's skabelon for databehandleraftale og GDPR årshjul. Vi har observeret, at TIMEmSYSTEM årligt fører tilsyn med samtlige underdatabehandlere, der udføres ved indhentelse af en ISAE 3402 type 2-erklæring, og ved gennemgang af en liste over underdatabehandlerens anvendte underdatabehandlere i forhold til TIMEmSYSTEM.	Ingen afvigelser konstateret.

Artikel 28, stk. 2 og 4:Underdatabehandlere

Kontrolmål

- *At sikre, at underdatabehandleren er pålagt de samme databeskyttelsesforpligtelser, som databehandleren er pålagt af den dataansvarlige, ved indgåelse af en skriftlig kontrakt med tilhørende instruks.*
- *At sikre, at den dataansvarlige har givet en forudgående specifik eller generel skriftlig godkendelse af underdatabehandlere.*
- *At sikre, at underdatabehandleren kan stille de fornødne garantier til beskyttelse af personoplysningerne i overensstemmelse med kontrakten.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har foretaget inspektion af TIMEmSYSTEM's dokumentation for udførelse af tilsyn med deres underdatabehandlere, herunder TIMEmSYSTEM's vurdering af kontroller i ISAE 3402 type 2-erklæringen og tillægsspørgsmål i forhold til underdatabehandlerens opfyldelse af databehandleraftalen og databeskyttelseslovgivningen. Vi har observeret, at TIMEmSYSTEM har ført tilsyn med samtlige underdatabehandlere i overensstemmelse med proceduren herfor. Vi har foretaget inspektion af den af IT Relation og Cloud Factory udarbejdede ISAE 3402 type 2-erklæringer om generelle it-kontroller i relation til hosting services for perioden fra 1. januar til 31. december 2022.	

Artikel 28, stk. 3, litra b: Tavsheds- og fortrolighedsaftaler		
Kontrolmål ▶ *At sikre, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende tavshedspligt.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Fortrolighedsaftale med leverandører ▶ TIMEmSYSTEM har indgået fortrolighedsaftale med eventuelle leverandører, der ikke er underdatabehandlere.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's leverandører, der ikke er underdatabehandlere og observeret, at TIMEmSYSTEM har sikret, at leverandører er underlagt tavshedspligt i overensstemmelse med indgået databehandleraftale med dataansvarlige.	Ingen afvigelser konstateret.
Tavsheds- og fortrolighedsaftaler ▶ TIMEmSYSTEM har indgået tavsheds- og fortrolighedsaftale med medarbejdere.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's GDPR-håndbog og observeret, at TIMEmSYSTEM har en procedure for håndtering af tavsheds- og fortrolighedsaftaler med medarbejdere. Vi har ved udtagelse af en stikprøve og observeret, at de pågældende medarbejdere har underskrevet en tavsheds- og fortrolighedsaftale.	Ingen afvigelser konstateret.

Artikel 25: Databeskyttelse gennem design og standardindstillinger

Kontrolmål

- *At sikre, at databehandleren gennemfører databeskyttelse gennem design og standardindstillinger.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Ændringsstyring • TIMEmSYSTEM foretager en betryggende ændringsstyring, herunder sikrer identifikation, planlægning og test af ændringer, vurdering af konsekvenser, godkendelse, verifikation af konsekvenser for informationssikkerhed, kommunikation til den dataansvarlige, procedurer for tilbagerulning ved mislykkede ændringer samt nødændringer ved brud på persondatasikkerheden.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's procedurer for "mTime-styring af fejlrapport", "Løsning af supportsag" og "Opdatering af mTime" samt "Vejledning til GDPR-risikovurdering ved videreudvikling af mTime". Vi har ved en stikprøve inspiceret dokumentation for processen for håndtering af ændringsstyring, udvikling, tests og idriftsættelse, herunder vurdering af konsekvenser og godkendelse af releases. Vi har observeret, at der er implementeret den nødvendige funktionsadskillelse mellem udvikling, test og idriftsættelse for såvel platforme som for medarbejdere. Vi har observeret, at TIMEmSYSTEM kan tilbagerulle en version, hvis denne er fejlbehæftet. Vi har observeret, at TIMEmSYSTEM kan udføre nødændringer (hotfixes) for at imødegå brud på persondatasikkerheden.	Ingen afvigelser konstateret.
Hjemtagelse af kundedatabaser i forbindelse med opgaveløsning • TIMEmSYSTEM har passende procedurer og kontroller i forhold til at hjemtage kundedatabaser i forbindelse med test, fejlrettelser og lignende.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's procedure for hjemtagning af databaser via styringsværktøjet Manage Optimize Processes og for manuel hjemtagning. Vi har observeret hjemtagning af database, herunder at data er anonymiseret før hjemtagningen sker.	Ingen afvigelser konstateret.

Artikel 25: Databeskyttelse gennem design og standardindstillinger		
Kontrolmål ▶ *At sikre, at databehandleren gennemfører databeskyttelse gennem design og standardindstillinger.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har observeret, at hjemtagne databaser slettes efter 30 dage ved en automatisk kørsel.	

Artikel 28, stk. 3, litra c med henvisning til artikel 32: Tekniske og organisatoriske sikkerhedsforanstaltninger (behandlingssikkerhed)

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Risikovurdering ▶ TIMEmSYSTEM har som databehandler foretaget en vurdering af de risici, der er forbundet med behandling af personoplysninger på vegne af den dataansvarlige, ud fra det aktuelle tekniske niveau, implementeringsomkostninger samt risiciene for sandsynlighed og konsekvens for den registrerede (risikovurdering). ▶ TIMEmSYSTEM har indført procedure for udførelse af risikovurderinger, herunder principper og metoder for risikovurdering, opdateringsfrekvens og versionsstyring. ▶ TIMEmSYSTEM har gennemført passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de identificerede risici.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's procedure for risikovurdering, vejledning til GDPR-risikovurdering ved videreudvikling af mTIME og skabelon til databehandleraftale. Vi har observeret, at TIMEmSYSTEM har foretaget vurdering af risici i forbindelse med behandling af personoplysninger på vegne af den dataansvarlige i forhold til sandsynlighed og konsekvens samt arten af data. Vi har observeret, at TIMEmSYSTEM har indført procedure for udførelse af risikovurderinger. Vi har observeret, at TIMEmSYSTEM har gennemført passende tekniske og organisatoriske foranstaltninger, baseret på risikovurderingen. Vi har observeret, at risikovurderingen vedligeholdes og opdateres løbende og mindst en gang årligt.	Ingen afvigelser konstateret.
Brugerstyring ▶ TIMEmSYSTEM opbevarer ind- og uddatamateriale, så uvedkommende ikke kan få adgang til at gøre sig bekendt med de personoplysninger, der er indeholdt i mTIME-systemet. ▶ TIMEmSYSTEM har indført procedurer og kontroller, der sikrer, at kun medarbejdere, der er autoriseret	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har observeret, at TIMEmSYSTEM opbevarer ind- og uddatamateriale, så uvedkommende ikke kan få adgang til de personoplysninger, der er indeholdt i mTIME.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c med henvisning til artikel 32: Tekniske og organisatoriske sikkerhedsforanstaltninger (behandlingssikkerhed)

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
hertil, har adgang til de personoplysninger, der behandles, og at der kun autoriseres medarbejdere, for hvem adgang til personoplysningerne er nødvendige med henblik på varetagelse af drifts- og systemtekniske opgaver. ▶ TIMEmSYSTEM vedligeholder en liste over medarbejdernes adgang og autorisation til at tilgå den dataansvarliges systemer, og TIMEmSYSTEM følger op på disse mindst en gang årligt for vurdering af, om der fortsat er behov for adgang, herunder opfylder kravene i databehandleraftalen til brugeradministrationen. ▶ TIMEmSYSTEM tildeler medarbejdere med adgang til systemet et personligt login, som er personhenførbart, og som ikke må deles med andre, heller ikke ansatte i TIMEmSYSTEM. ▶ TIMEmSYSTEM har indført procedurer og kontroller, der sikrer, at medarbejdernes login overholder krav til længde, specialtegn, store bogstaver mv. og de øvrige krav til adgang og adgangskoder i den indgåede databehandleraftale.	Vi har stikprøvevis observeret, at TIMEmSYSTEM ikke har adgang til ind- og uddatamateriale med undtagelse af support-afdelingens medarbejdere. Vi har foretaget inspektion af TIMEmSYSTEM's GDPR-håndbog og checkliste over til- og fratrådte medarbejdere. Vi har foretaget inspektion af liste over tilsyn med brugeradgange i 2023, Password Policy og Policy for skærmlås fra Active Directory og konfiguration af brugere og brugerrettigheder i styringsværktøjet Manage Optimize Processes. Vi har observeret, at den i Active Directory konfigurerede Password Policy og Policy for skærmlås stemmer overens med TIMEmSYSTEM's password politik samt politik for skærmlås. Vi har observeret, at TIMEmSYSTEM's medarbejdere er oprettet med personligt login, der er personhenførbart. Vi har observeret, at TIMEmSYSTEM har indført procedurer og kontroller til sikring at medarbejdernes login overholder de krav, som er specificeret i indgåede databehandleraftaler.	
Kryptering ▶ TIMEmSYSTEM har opsat stærk kryptering ved transmittering af personoplysninger via eksterne kommunikationsforbindelser. ▶ TIMEmSYSTEM har indført procedurer og kontroller, der sikrer, at adgang ved brug af hjemmearbejdspladser sker i overensstemmelse med den indgåede data-	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's GDPR-håndbog og password politik og observeret, at den stemmer overens med gældende procedure.	Vi har konstateret, at databehandleren fra 01.01.2023 til 30.04.2023 har anvendt forældet transportkryptering, men fra 01.05.2023 ved overgang til Cloud Factory som underdatabehandler er overgået til opdateret TLS kryptering. Ingen yderligere afvigelser konstateret.

Artikel 28, stk. 3, litra c med henvisning til artikel 32: Tekniske og organisatoriske sikkerhedsforanstaltninger (behandlingssikkerhed)		
Kontrolmål ▶ *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.* ▶ *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.* ▶ *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.* ▶ *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
behandleraftale, at adgang opnås gennem en VPN-klient, der autentificeres via sikkerheden i TIMEmSYSTEM's Active Directory, og at adgang til personoplysninger er sikret med login til server, der afvikler mTIME.	Vi har foretaget inspektion af TIMEmSYSTEM's krypteringscertifikat i forbindelse med eksterne kommunikationsforbindelser. Vi har observeret, at TIMEmSYSTEM anvender TLS-kryptering ved transmittering af personoplysninger via eksterne kommunikationsforbindelser, samt at adgang fra hjemmearbejdspladser sker via krypteret VPN-forbindelse. Vi har observeret, at TIMEmSYSTEM gør brug af to-faktor godkendelse i overensstemmelse med indgået databehandleraftale. Vi har foretaget inspektion af udtræk af Password Policy og Policy for skærmlås fra Active Directory og observeret, at disse stemmer overens med TIMEmSYSTEM's password politik.	
Fysisk sikkerhed ▶ TIMEmSYSTEM har indført procedurer og kontroller for fysiske sikkerhedsforanstaltninger i forhold til beskyttelse af personoplysninger, herunder adgang til TIMEmSYSTEM's bygning, lokaler, kontorer og øvrige faciliteter.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's GDPR-håndbog og observeret, at TIMEmSYSTEM har en procedure for fysisk sikkerhed til TIMEmSYSTEM's bygning, lokaler, kontorer og øvrige faciliteter. Vi har observeret, at indgangen til TIMEmSYSTEM's lokaler altid er låst både i og udenfor arbejdstiden, og at gæster modtages af en receptionist ved indgangen til kontoret.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c med henvisning til artikel 32: Tekniske og organisatoriske sikkerhedsforanstaltninger (behandlingssikkerhed)

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Reparation og service af udstyr ▶ TIMEmSYSTEM har indført procedurer og kontroller, der sikrer, at der ved reparation og service af udstyr, der indeholder personoplysninger, samt ved salg og kassation af anvendt udstyr, herunder datamedier, træffes de nødvendige foranstaltninger for at sikre, at personoplysninger ikke kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med databeskyttelseslovgivningen.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's GDPR-håndbog og observeret, at TIMEmSYSTEM har en procedure og kontroller for afskaffelse af udstyr, der indeholder personoplysninger. Der har ikke været nogle sager, og vi har derfor ikke haft mulighed for at teste.	Ingen afvigelser konstateret.
Logning og monitorering ▶ TIMEmSYSTEM foretager logning af anvendelsen af personoplysninger og sikrer, at loggen som minimum indeholder oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrører, eller det anvendte søgekriterium.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's GDPR-håndbog og procedure for logning i mTIME. Vi har observeret, at TIMEmSYSTEM foretager logning af personoplysninger, og at loggen indeholder oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, oplysningerne vedrører, eller anvendte søgekriterium. Vi har observeret, at der foretages følgende logning i mTIME: • Registreringer • Medarbejdergodkendelse • Ledergodkendelse • Fraværsgodkendelse	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra c med henvisning til artikel 32: Tekniske og organisatoriske sikkerhedsforanstaltninger (behandlingssikkerhed)

Kontrolmål

- *At sikre, at databehandleren har implementeret passende tekniske og organisatoriske sikkerhedsforanstaltninger under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder (risikovurdering), herunder en løbende gennemgang og ajourføring af risikovurdering og sikkerhedsforanstaltninger.*
- *At sikre, at risikovurderingen tager hensyn til risici for hændelig, eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.*
- *At sikre fortrolighed, integritet og tilgængelighed og robusthed af behandlingssystemer og -tjenester.*
- *At sikre regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har observeret, at logning i mTIME findes i databasen, og kan tilgås i brugerinterfacet.	
Egenkontrol ▶ TIMEmSYSTEM foretager en dokumenteret gennemgang af de sikkerhedsmæssige foranstaltninger mindst en gang årligt.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's GDPR-håndbog og årshjulet. Vi har observeret, at TIMEmSYSTEM løbende gennemgår og afprøver de sikkerhedsmæssige foranstaltninger samt tilsyn med underdatabehandler, anonymiseringskørsler, og at relevante sletninger er foretaget.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra g: Sletning og tilbagelevering af personoplysninger

Kontrolmål

- *At sikre, at databehandleren kan slette og tilbagelevere personoplysninger, efter at tjenesten vedrørende behandlingen er ophørt, i henhold til instruks fra den dataansvarlige.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Sletning og tilbagelevering af personoplysninger ▶ TIMEmSYSTEM sletter eller tilbageleverer personoplysninger, herunder ind- og uddatamateriale, i henhold til lovgivning og den indgåede databehandleraftale.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's procedure for sletning og tilbagelevering af personoplysninger. Vi har foretaget inspektion af en stikprøve af indgåede databehandleraftaler med de dataansvarlige samt skabelon for databehandleraftale. Vi har observeret, at databehandleraftalerne forpligter TIMEmSYSTEM til at slette og tilbagelevere personoplysninger i forbindelse med ophør af aftalen med de dataansvarlige. Vi har på forespørgsel fået oplyst, at der på erklæringstidspunktet ikke har været ophør af aftaler med dataansvarlige, hvorfor vi ikke har kunnet efterprøve kontrollen.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra e, f og h: Bistand til dataansvarlige

Kontrolmål

- *At sikre, at databehandleren kan bistå den dataansvarlige med opfyldelse af de registreredes rettigheder.*
- *At sikre, at databehandleren kan bistå den dataansvarlige i forhold til behandlingssikkerhed (artikel 32), brud på persondatasikkerheden (artikel 33-34) og konsekvensanalyser (artikel 35-36).*
- *At sikre, at databehandleren kan bistå den dataansvarlige i forhold til revision og inspektion.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
De registreredes rettigheder ▶ TIMEmSYSTEM bistår den dataansvarlige med at opfylde de registreredes rettigheder i henhold til artikel 28, stk. 3, litra e, med henvisning til kapitel III.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's GDPR-håndbog og skabelon for databehandleraftale. Vi har observeret, at TIMEmSYSTEM forpligter sig til at bistå den dataansvarlige med opfyldelse af den dataansvarliges forpligtelser i forhold til den registreredes rettigheder. Vi har foretaget inspektion af en stikprøve af indgåede databehandleraftaler og observeret, at databehandleraftalerne forpligter TIMEmSYSTEM til at bistå den dataansvarlige med opfyldelse af de registreredes rettigheder, og er i overensstemmelse med TIMEmSYSTEM's procedure og skabelon for databehandleraftale. Vi har observeret, at TIMEmSYSTEM kan give indsigt i alle de personoplysninger, der opbevares i mTIME i forbindelse med den behandling, som TIMEmSYSTEM varetager på vegne af de dataansvarlige. Vi har på forespørgsel fået oplyst, at der ikke har været henvendelser fra de dataansvarlige vedrørende bistand i forhold til de registreredes rettigheder, eller er blevet kontaktet direkte af de registrerede. Det har derfor ikke været muligt at teste kontrollen.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra e, f og h: Bistand til dataansvarlige

Kontrolmål

- *At sikre, at databehandleren kan bistå den dataansvarlige med opfyldelse af de registreredes rettigheder.*
- *At sikre, at databehandleren kan bistå den dataansvarlige i forhold til behandlingssikkerhed (artikel 32), brud på persondatasikkerheden (artikel 33-34) og konsekvensanalyser (artikel 35-36).*
- *At sikre, at databehandleren kan bistå den dataansvarlige i forhold til revision og inspektion.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Forpligtelser om behandlingssikkerhed, brud på persondatasikkerheden og konsekvensanalyser - TIMEmSYSTEM bistår den dataansvarlige med at sikre overholdelse af forpligtelserne i medfør af artikel 32 (behandlingssikkerhed), jf. også artikel 28, stk. 3, litra c. - TIMEmSYSTEM bistår den dataansvarlige med at sikre overholdelse af forpligtelserne i medfør af artikel 33 og 34 (anmeldelse og underretning af brud på persondatasikkerheden), jf. også artikel 33, stk. 2. - TIMEmSYSTEM bistår den dataansvarlige med at sikre overholdelse af forpligtelserne i medfør af artikel 35 og 36 (konsekvensanalyser).	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's GDPR-håndbog og skabelon for databehandleraftale. Vi har observeret, at TIMEmSYSTEM har procedure for at bistå den dataansvarlige med opfyldelse af den dataansvarliges forpligtelser i forhold til behandlingssikkerhed og brud på persondatasikkerheden. Vi har foretaget inspektion af TIMEmSYSTEM's vurdering af kriterier i forhold til, om en konsekvensanalyse skal udarbejdes. Vi har observeret, at TIMEmSYSTEM kan bistå den dataansvarlige med udarbejdelse af konsekvensanalyse og forudgående høring. Vi har foretaget inspektion af en stikprøve af indgåede databehandleraftaler og observeret, at databehandleraftalerne forpligter TIMEmSYSTEM til at bistå hermed. Vi har observeret, at der på erklæringstidspunktet ikke har været anmodninger fra dataansvarlige vedrørende bistand med opfyldelse af artikel 32-36, hvorfor vi ikke har kunnet observere de indførte kontroller.	Ingen afvigelser konstateret.
Revision og inspektion - TIMEmSYSTEM stiller alle oplysninger, der er nødvendige, for at påvise overholdelse af kravene til databehandlere til rådighed for den dataansvarlige. - TIMEmSYSTEM giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige, eller en anden revisor, som er bemyndiget af den dataansvarlige.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's GDPR-håndbog og observeret, at kravene til TIMEmSYSTEM som databehandler er beskrevet heri.	Ingen afvigelser konstateret.

Artikel 28, stk. 3, litra e, f og h: Bistand til dataansvarlige

Kontrolmål

- *At sikre, at databehandleren kan bistå den dataansvarlige med opfyldelse af de registreredes rettigheder.*
- *At sikre, at databehandleren kan bistå den dataansvarlige i forhold til behandlingssikkerhed (artikel 32), brud på persondatasikkerheden (artikel 33-34) og konsekvensanalyser (artikel 35-36).*
- *At sikre, at databehandleren kan bistå den dataansvarlige i forhold til revision og inspektion.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har observeret, at TIMEmSYSTEM på anmodning fra den dataansvarlige eller repræsentant for den dataansvarlige kan stille alle de nødvendige oplysninger til rådighed for den dataansvarlige. Vi har observeret, at TIMEmSYSTEM stiller relevant personale til rådighed for at bidrage til revisioner, der foretages af den dataansvarliges repræsentant, som er bemyndiget af den dataansvarlige.	

Artikel 30, stk. 2 og 4: Fortegnelse over kategorier af behandlingsaktiviteter		
Kontrolmål ▶ *At sikre, at databehandleren udarbejder en skriftlig fortegnelse over alle kategorier af behandlingsaktiviteter, der foretages på vegne af den dataansvarlige.* ▶ *At sikre, at databehandleren opbevarer fortegnelsen skriftligt, herunder elektronisk.* ▶ *At sikre, at databehandleren kan stille fortegnelsen til rådighed for tilsynsmyndigheden.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Fortegnelse over kategorier af behandlingsaktiviteter ▶ TIMEmSYSTEM fører en fortegnelse over dataansvarlige med angivelse af blandt andet kategorier af behandlingsaktiviteter. ▶ Fortegnelsen opdateres løbende ved væsentlige ændringer eller minimum en gang årligt.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's fortegnelse som databehandler og har observeret, at der er udarbejdet fortegnelse over kategorier af behandlingsaktiviteter som databehandler. Vi har observeret, at TIMEmSYSTEM løbende opdaterer fortegnelsen over kategorier af behandlingsaktiviteter som databehandler.	Ingen afvigelser konstateret.
Opbevaring af fortegnelsen ▶ Fortegnelsen opbevares elektronisk i TIMEmSYSTEMs system/fil-drev.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af dokumentation, som bekræfter, at fortegnelsen opbevares elektronisk.	Ingen afvigelser konstateret.
Datatilsynets adgang til fortegnelsen ▶ TIMEmSYSTEM udleverer fortegnelsen på anmodning fra Datatilsynet.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har på forespørgsel fået oplyst, at TIMEmSYSTEM stiller fortegnelsen til rådighed på anmodning fra Datatilsynet. Vi har på forespørgsel fået oplyst, at der i erklæringsperioden ikke har været anmodning fra Datatilsynet vedrørende adgang til fortegnelsen, og det har derfor ikke været muligt at efterprøve kontrollen.	Ingen afvigelser konstateret.

Artikel 33, stk. 2: Brud på persondatasikkerheden

Kontrolmål

- *At sikre, at databehandleren uden unødig forsinkelse underretter den dataansvarlige om brud på persondatasikkerheden.*
- *At sikre, at den dataansvarlige underrettes om alle nødvendige oplysninger, så bruddet kan vurderes med henblik på anmeldelse til tilsynsmyndigheden og underretning til den registrerede.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Brud på persondatasikkerheden ▶ TIMEmSYSTEM har indført en procedure for håndtering af brud på persondatasikkerheden, herunder hvorledes den enkelte medarbejder skal forholde sig, hvornår der er tale om et brud på persondatasikkerheden, og hvorledes den dataansvarlige uden unødig forsinkelse underrettes. ▶ TIMEmSYSTEM fører et register over brud på persondatasikkerheden som dokumentation for opfyldelse af artikel 33, stk. 2. ▶ TIMEmSYSTEM har indført en procedure, der sikrer dokumenteret underretning af den dataansvarlige uden unødig forsinkelse ved brud på persondatasikkerheden eller ved andre sikkerhedsbrister i systemet.	Vi har udført forespørgsel hos passende personale hos TIMEmSYSTEM. Vi har foretaget inspektion af TIMEmSYSTEM's procedure for brud på persondatasikkerheden Vi har observeret, at TIMEmSYSTEM har en procedure for brud på persondatasikkerheden, hvor de agerer som databehandler. Vi har observeret, at proceduren indeholder en proces for, hvordan medarbejdere skal forholde sig, såfremt der er et brud på persondatasikkerheden, og at den dataansvarlige skal underrettes i overensstemmelse med indgået databehandleraftale, herunder hvilke oplysninger underretningen skal indeholde. Vi har foretaget inspektion af TIMEmSYSTEM's register over brud på persondatasikkerheden og procedure for brud på persondatasikkerheden. Vi har observeret, at registret og proceduren tilsammen opfylder kravene til indholdet af et register over brud på persondatasikkerheden efter databeskyttelsesforordningens artikel 33, stk. 2.	Ingen afvigelser konstateret.

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

KYSTVEJEN 29
8000 AARHUS C

CVR-NR. 20 22 26 70