# SAMESYSTEM A/S

## AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3000-ERKLÆRING MED SIKKERHED PR. 5. SEPTEMBER 2023 OM BESKRIVELSEN AF SAMESYSTEM OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER OG DERES UDFORMNING, 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 PR. 5. SEPTEMBER 2023 OM BESKRIVELSEN AF SAMESYSTEM OG DE TILHØRENDE TEKNISKE OG ORGANISATORISKE SIKKERHEDSFORANSTALTNINGER OG ØVRIGE KONTROLLER OG DERES UDFORMNING, RETTET MOD BEHANDLING OG BESKYTTELSE AF PERSONOPLYSNINGER I HENHOLD TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN**

Til: Ledelsen i Samesystem A/S
Samesystem A/S´ kunder (dataansvarlige)

## Omfang

Vi har fået som opgave at afgive erklæring om den af Samesystem A/S (databehandleren) pr. 5. september 2023 udarbejdede beskrivelse i sektion 3 af Samesystem 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 af de tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

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

## 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 og implementere 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 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.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen og udformningen af kontroller hos en databehandler omfatter udførelse af handlinger for at opnå bevis for oplysningerne i databehandlerens beskrivelse samt for kontrollernes udformning. 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. 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.

Som nævnt ovenfor har vi ikke udført handlinger vedrørende den operationelle effektivitet af de kontroller, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

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

**Begrænsninger i kontroller hos en 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 Samesystem, 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.

**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 Samesystem og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller, rettet mod behandling og beskyttelses af personoplysninger i henhold til databeskyttelsesforordningen og databeskyttelsesloven, således som de var udformet og implementeret pr. 5. september 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 pr. 5. september 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 Samesystem, 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, 26. september 2023

**BDO Statsautoriseret revisionsaktieselskab**

Nicolai T. Visti
Partner, Statsautoriseret revisor

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

## 2. SAMESYSTEM A/S´UDTALELSE

SameSystem A/S varetager behandling af personoplysninger i forbindelse med SameSystem 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 SameSystem, 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.

SameSystem A/S anvender underdatabehandlere. Disse underdatabehandleres relevante kontrolmål og tilknyttede tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller indgår ikke i den medfølgende beskrivelse.

SameSystem A/S bekræfter, at den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af SameSystem og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller pr. 5. september 2023. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for SameSystem, og hvordan de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og 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 SameSystem 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. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af SameSystem 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 SameSystem, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.

SameSystem A/S 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 pr. 5. september 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.

SameSystem A/S bekræfter, at der er implementeret 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 26. september 2023

**Samesystem A/S**

Carsten Fensholt
Adm. direktør

# 3. SAMESYSTEM A/S´ BESKRIVELSE AF SAMESYSTEM

## SAMESYSTEM A/S

SameSystem er en Nasdaq First North børsnoteret virksomhed, der udvikler og driver en online workforce management løsning til retail og foodservice, der håndterer planlægning og administration.

Workforce management løsningen (SameSystem) fokuserer udelukkende på det, der betyder noget inden for butikker, caféer og restauranter: at booste vækst, reducere udgifter, spare tid og sikre motiverede medarbejdere.

SameSystem har udviklings- og salgskontorer i Danmark og Litauen, samt salgskontorer i Spanien, Tyskland og Norge. SameSystem's ca. 100 medarbejdere er specialiserede inden for systemudvikling, serverdrift, support, salg samt informationssikkerhed. SameSystem er organiseret i følgende afdelinger:

| | |
|---|---|
| Product | Udvikling og drift af SameSystem platformen |
| Customer Success | Implementering, support og key account management |
| Sales | Opsøgende salg af SameSystem platformen |
| Administration | Bogholderi, IT, Jura, med mere |

Administrationsafdelingen styrer SameSystem's persondatasikkerhed i forhold til den behandling, som SameSystem 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 og procedurer og lignende.

## SAMESYSTEM OG BEHANDLING AF PERSONOPLYSNINGER

SameSystem leverer SameSystem platformen som en Software-as-a-Service (SaaS) løsning. SameSystem platformen består af en webapplikation med tilhørende mobil app.

SameSystem platformen udvikles i Danmark og Litauen, men afvikles fra hosting-centre i Tyskland og Finland. Der benyttes andre underdatabehandlere til opbevaring af backup, udsendelse af mail og tekstbeskeder, chat og digitale underskrifter. SameSystem har indgået databehandleraftaler med disse underdatabehandlere.

SameSystem behandler personoplysninger på vegne af sine kunder, der er dataansvarlige, når disse anvender SameSystem platformen til workforce management. SameSystem har indgået databehandleraftaler med de dataansvarlige om denne behandling.

De personoplysninger, der behandles, henhører under databeskyttelsesforordningens artikel 6.1.b (Kontraktlig aftale) om almindelige personoplysninger, og omfatter blandt andet personnavn, e-mail, telefonnummer, personnummer, bank information samt anden HR og løn data på den dataansvarliges ansatte.

## STYRING AF PERSONDATASIKKERHED

SameSystem har opstillet krav til etablering, implementering, vedligeholdelse og løbende forbedring af et ledelsessystem for persondatasikkerhed, der sikrer opfyldelse af indgåede aftaler med de dataansvarlige, god databehandlerskik og relevante krav til databehandlere i henhold til databeskyttelsesforordningen og databeskyttelsesloven.

De tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller til beskyttelse af personoplysninger er udformet i henhold til risikovurderinger, og implementeres for at sikre fortrolighed, integritet og tilgængelighed samt overholdelse af den gældende databeskyttelseslovgivning. Sikkerhedsforanstaltninger og kontroller er i videst muligt omfang automatiserede og teknisk understøttet af it-systemer.

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<br>Artikel 29<br>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. |
| Artikel 44 – 49 | Overførsel af personoplysninger til tredjelande |

## RISIKOVURDERING

SameSystem styrer risici i sine leverancer med udgangspunkt i en risikostyringsproces. Risikostyringen omfatter bl.a. følgende:

- Identifikation af potentielle risici, der kan få indflydelse på de enkelte leverancer både ud fra en teknisk og en forretningsmæssig synsvinkel.
- Vurdering af de identificerede potentielle risici, væsentlighed, sandsynlighed og konsekvenser for de enkelte leverancer.
- At tiltag, til reduktion af sandsynligheden for at risici indtræder, implementeres på en kost-effektiv måde.

Kontrolmål og kontroller, der imødegår risiciene, er udvalgt fra Databeskyttelsesforordningen og tilpasset i fornødent omfang, herunder med inspiration fra ISO 27001. Beskrivelse af kontrolmål fremgår af afsnittet, revisors resultater af test af kontroller.

I risikovurderingen indgår kortlægning af alle de kendte risici, behandlingen medfører, og en kategorisering (scoring, sandsynlighed og alvorlighed) heraf samt tiltag til minimering af kortlagte risici. Formålet er, at SameSystem lever op til høje standarder med fokus på høj fortrolighed, integritet og tilgængelighed.

Baseret på risikovurderingen er der udarbejdet og implementeret en informationssikkerhedspolitik med en lang række procedurer for specifikke områder.

Det vurderes ikke, at SameSystem leverancer indebærer en høj risiko ved behandling af personoplysninger. Såfremt dette er tilfældet, vil SameSystem indgå i tæt dialog med den dataansvarlige og i samarbejde med den dataansvarlige foretage en konsekvensanalyse vedrørende databeskyttelse.

## 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.

### Databehandlerens garantier

SameSystem har indført politikker og procedurer, der sikrer, at SameSystem 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. SameSystem har implementeret en af ledelsen godkendt IT sikkerhedspolitik, der løbende gennemgås og opdateres. Der forefindes procedurer for rekruttering og fratrædelse af medarbejdere.

### Databehandleraftale

SameSystem indgår databehandlingsaftaler med kunderne, der sikrer, at SameSystem i tilknytning til kundekontrakten indgår en databehandleraftale, der angiver betingelserne for behandling af personoplysninger på vegne af den dataansvarlige. SameSystem anvender en skabelon for databehandleraftaler i overensstemmelse med de tjenester, der leveres, herunder information om brugen af underdatabehandlere. Databehandleraftalerne er digitalt underskrevet og opbevares elektronisk.

### Instruks for behandling af personoplysninger

SameSystem har indført politikker og procedurer, der sikrer, at SameSystem handler efter den instruks, som den dataansvarlige har givet i databehandleraftalen. Instruksen opretholdes ved procedurer, der instruerer medarbejderne i, hvorledes behandling af personoplysninger skal ske, herunder hvem der hos den dataansvarlige kan give bindende instruks til SameSystem. Proceduren sikrer desuden, at SameSystem informerer den dataansvarlige, når dennes instruks er i strid med databeskyttelseslovgivningen.

### Underdatabehandlere

SameSystem vurderer underdatabehandleren og dennes garantier, før der indgås aftale, for at sikre at underdatabehandleren kan overholde de forpligtelser, som er pålagt SameSystem.

SameSystem har ført tilsyn med sine underdatabehandlere, baseret på en risikovurdering af den konkrete behandling af personoplysninger, ved blandt andet at indhente revisorerklæringer af typen ISAE 3000 eller SOC 2 eller lignende dokumentation, hvor dette er muligt.

### Fortrolighed og lovbestemt tavshedspligt

Alle ansatte hos SameSystem har forpligtet sig til fortrolighed ved at underskrive en ansættelseskontrakt, der indeholder vilkår om tavshed og fortrolighed.

### Tekniske og organisatoriske sikkerhedsforanstaltninger

Risikovurdering

SameSystem har gennemført de tekniske og organisatoriske sikkerhedsforanstaltninger på baggrund af en vurdering af risici i forhold til fortrolighed, integritet og tilgængelighed. Der henvises til særskilt afsnit herom.

Beredskabsplaner

SameSystem kan rettidigt genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af fysiske eller tekniske hændelser. SameSystem har etableret et kriseberedskab, der træder i kraft i disse tilfælde. Organisering af kriseberedskabsgruppe er etableret, og der er indført retningslinjer for aktivering af kriseberedskabet.

Opbevaring af personoplysninger

SameSystem sikrer, at personoplysninger kun opbevares i overensstemmelse med kontrakten med den dataansvarlige og i henhold til listen over lokationer i den tilhørende databehandleraftale.

Fysisk adgangskontrol
SameSystem 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.

SameSystem's hostingleverandør har indført procedurer, der sikrer, at adgang til serverrum er tildelt ud fra et arbejdsbetinget behov. Serviceleverandører, der har behov for adgang for at varetage opsyn eller vagt, er godkendt af ledelsen. Tildelte adgange til serverrum gennemgås og revideres ved ændringer og mindst én gang årligt på leverandørens ansvar.

Fysisk sikkerhed
SameSystem har indført procedurer, der sikrer, at servere er beskyttet mod uautoriseret adgang, beskadigelse, driftsafbrydelser og lignende hændelser ved særlige sikkerhedsforanstaltninger.

Servere er således opbevaret hos eksterne hosting partnere i særligt indrettet serverrum med fysisk og elektronisk adgangskontrol og logning af adgange. Serverrummet er sikret mod miljømæssige trusler som brand, vandindtrængning, fugt, overophedning, strømudfald og overspænding. Systemer til miljømæssig sikring af driftsfaciliteter er serviceret og vedligeholdt løbende efter de respektive leverandørers forskrifter. Driftsmiljøet er overvåget af SameSystem.

Logisk adgangssikkerhed
SameSystem 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.

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

Der er udformet tekniske foranstaltninger, der sikrer, at alle SameSystem ansattes adgang til persondata i SameSystem platformen er beskyttet med to-faktor autentifikation, lige meget hvorfra systemet tilgås.

Fjernarbejdspladser og fjernadgang til systemer og data
SameSystem har indført procedurer, der sikrer, at adgang til backend systemer og udviklingsmiljøer uden for SameSystems lokaler samt fjernadgang til systemer og data sker via VPN-forbindelser og to-faktor autentifikation.

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

Kryptering af personoplysninger
SameSystem har indført procedurer, der sikrer, at databaser, der indeholder personoplysninger, er krypterede, og at tilsvarende gælder sikkerhedskopier. Genoprettelsesnøgler og certifikater opbevares på forsvarlig vis.

SameSystem har indført procedurer, der sikrer, at data på personlige enheder er krypteret ved ibrugtagning, så data kun kan tilgås af autoriserede brugere. Genoprettelsesnøgler og certifikater opbevares på forsvarlig vis.

Firewall
SameSystem har indført tekniske foranstaltninger, der sikrer, at trafik mellem internettet og netværket kontrolleres af firewall. Adgang udefra via porte i firewallen er begrænset mest muligt, og adgangsrettigheder tildeles via konkrete porte til specifikke segmenter. Arbejdsstationer benytter firewall.

Antivirusprogram
SameSystem har indført antivirus, der sikrer, at enheder med adgang til netværk og applikationer er beskyttet mod virus og malware. Der sker en løbende opdatering og tilpasning af antivirusprogrammer og andre beskyttelsessystemer.

Sårbarhedsscanning og penetrationstests
SameSystem har indført procedurer, der sikrer, at systemer er indført med henblik på at identificere og imødegå tekniske sårbarheder i applikationer, services og infrastruktur, så tab af fortrolighed, integritet og tilgængelighed af systemer og data undgås.

Sikkerhedskopiering og retablering af data
SameSystem har indført backup, der sikrer, at systemer og data synkroniseres til redundant og geografisk adskilt miljø i Tyskland og Finland, samt at al data sikkerhedskopieres for at imødegå tab af data eller tab af tilgængelighed ved nedbrud.
Sikkerhedskopier opbevares på alternativ cloud lokation, og er beskyttet med fysiske og logiske sikkerhedsforanstaltninger, der forhindrer, at data kommer uvedkommende i hænde, eller at sikkerheds-kopier ødelægges ved brand, vand, hærværk eller hændelig skade.

Vedligeholdelse af systemsoftware
SameSystem's systemer driftes i et Docker Cloud miljø. Når man deployer i et Docker Cloud miljø, får man hver gang automatisk de nyeste versioner af systemmiljøerne. Der er derfor ingen formeld proces eller procedure for vedligeholdelse af systemsoftware, da det sker automatisk.

Logning i systemer, databaser og netværk
SameSystem har indført VPN og logning, der er opsat i henhold til forretningsmæssige behov, baseret på en risikovurdering af systemer og det aktuelle trusselsniveau. Omfang og kvalitet af logdata er tilstrækkelig til at identificere og påvise eventuelt misbrug af systemer eller data. Logdata er sikret mod tab og sletning.
Ekstern adgang til Databaser skal godkendes af 4 personer. Handlinger i databasen bliver logget.

Overvågning
SameSystem har indført overvågning af systemets resourcer og fejl. Dette håndteres reaktivt i Kibana, der sikrer, at der sker løbende overvågning af systemer og indførte tekniske sikkerhedsforanstaltninger.

Reparation og service samt bortskaffelse af it-udstyr
SameSystem udleverer ikke lagermedier til destruktion. Ved reparation er harddiske krypteret, og kan ikke tilgås uden brugerens password.
Alle PCér er sat op med kryptering af lagermedier, samt Microsoft Endpoint Manager.
Login til PCér foregår via 2 Factor Authentication.

Afprøvning, vurdering og evaluering
SameSystem har indført procedurer for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger til sikring af behandlingssikkerheden gennem implementering af årshjul og governance værktøj.

**Databeskyttelse gennem design og standardindstillinger**

SameSystem har indført politikker og procedurer for udvikling og vedligeholdelse af SameSystem platformen, der sikrer en styret ændringsproces. Der anvendes et Change Management system til styring af udviklings- og ændringsopgaver, og enhver opgave følger en ensartet proces.

Udviklings- og produktionsmiljø er adskilte. Enhver udviklingsopgave gennemløber et testforløb, og der anvendes anonymiserede persondata i et udviklingsmiljø. Der er indført procedurer for versionskontrol, logning og sikkerhedskopiering, så det er muligt at geninstallere tidligere versioner.

**Sletning og tilbagelevering af personoplysninger**

SameSystem har indført politikker og procedurer, 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**

SameSystem har indført politikker og procedurer, der sikrer, at SameSystem kan bistå den dataansvarlige med at opfylde dennes forpligtelse til at besvare anmodninger om udøvelse af de registreredes rettigheder.

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

SameSystem har indført politikker og procedurer, der sikrer, at SameSystem kan stille alle oplysninger, der er nødvendige for at påvise overholdelse af kravene til databehandlere, til rådighed for den dataansvarlige. SameSystem 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**

SameSystem har indført politikker og procedurer, 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.

**Underretning om brud på persondatasikkerheden**

SameSystem har indført politikker og procedurer, der sikrer, at brud på persondatasikkerheden registreres med detaljeret information om hændelsen, og at dataansvarlige underrettes uden unødig forsinkelse, efter at SameSystem er blevet opmærksom på, at der er sket brud på persondatasikkerheden. De registrerede informationer gør den dataansvarlige i stand til at vurdere, om bruddet på persondatasikkerheden skal anmeldes til tilsynsmyndigheden, og om de registrerede skal underrettes.

**Overførsel af personoplysninger til tredjelande**

SameSystem har indført politikker og procedurer, der sikrer, at overførslen af personoplysninger til underdatabehandlere i lande uden for EU sker i henhold til databeskyttelsesforordningens SCC (standardkontrakt) eller andet gyldigt overførselsgrundlag og ifølge instruks fra den dataansvarlige. SameSystem bestræber sig på, at leverandører og data er placeret inden for EU's grænser.

## 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 databeskyttelseslovgivningen:

- Den dataansvarlige skal sikre, at instruksen fra den dataansvarlige er lovlig i forhold til den til enhver tid gældende databeskyttelseslovgivning, og at instruksen er hensigtsmæssig i forhold til den indgåede kontrakt og databehandleraftalen.
- Den dataansvarlige har ansvaret for at sikre, at administratorernes brug af SameSystem platformen og den behandling af personoplysninger, der foretages i systemet, sker i overensstemmelse med databeskyttelseslovgivningen.

- Den dataansvarlige styrer brugerrettighederne i SameSystem platformen, herunder hvilke personer der tildeles administratoradgang, og hvilke rettigheder de enkelte administratorer tildeles.
- Den dataansvarlige frarådes at bruge platformene til behandling, herunder opbevaring, af følsomme persondata, og det er den dataansvarliges ansvar at sikre, at sådanne persondata ikke indgår i eller uploades til platformene.

# 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 Samesystem A/S´ beskrivelse af Samesystem samt for udformningen 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.

BDO's test af udformningen af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller samt implementeringen heraf har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, der er udvalgt af SameSystem A/S, 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 pr. 5. september 2023.

## Udførte testhandlinger

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

| Type | Beskrivelse |
|---|---|
| Forespørgsel | Forespørgsler hos passende personale er udført for alle væsentlige kontrolaktiviteter.<br><br>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.<br><br>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. |

For de ydelser, som Hetzner Online GmbH har leveret i perioden inden for hosting, har vi modtaget ISO 27001-certificering gældende til 26. september 2025 og en SoA-rapport pr. 30. maj 2022 for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller.

For de ydelser, som Scaleway SAS leverer inden for backup, har vi modtaget ISO 27001-certificering gældende til 14. februar 2024 for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller.

For de ydelser, som Link Mobility Group leverer inden for levering af tekstbeskeder, har vi modtaget ISAE 3000-erklæring pr. 15. marts 2023 for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller.

For de ydelser, som SMTP.DK ApS leverer inden for levering af e-mails, har vi modtaget databehandlerens udførte tilsyn i form af et udfyldt spørgeskema pr. 16. august 2023 for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller.

For de ydelser, som E-Signatur Danmark A/S leverer inden for digitale signaturer, har vi modtaget ISAE 3000-erklæring pr. 30. juni 2022 for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller gældende.

For de ydelser, som Sendbird, Inc. leverer inden for chat- og kommunikationstjenester, har vi modtaget ISO 27001-certificering gældende til 24. juli 2024 for underdatabehandlerens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller gældende.

Disse underdatabehandleres relevante kontrolmål og tilknyttede kontroller indgår ikke i SameSystem A/S´ beskrivelse af SameSystem og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller. Vi har således alene inspiceret den modtagne dokumentation, og testet de kontroller hos SameSystem A/S´, der sikrer udførelsen af et behørigt tilsyn med underdatabehandlerens opfyldelse af den mellem underdatabehandleren og databehandleren indgåede databehandleraftale 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 eller implementeret.

## 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 |
|---|---|---|
| **Informationssikkerhedspolitik**<br><br>▶ Databehandleren har udarbejdet og implementeret en informationssikkerhedspolitik. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens informationssikkerhedspolitik og observeret, at denne er implementeret.<br><br>Vi har foretaget inspektion af, at der er udført træning af databehandlerens ansatte med afsæt i informationssikkerhedspolitikken. | Ingen afvigelser konstateret. |
| **Gennemgang af informationssikkerhedspolitik**<br><br>▶ Databehandlerens informationssikkerhedspolitik bliver gennemgået og opdateret minimum en gang årligt. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens årshjul, hvoraf det fremgår, at informationssikkerhedspolitikken bliver gennemgået og opdateret minimum en gang årligt. | Ingen afvigelser konstateret. |
| **Organisering af informationssikkerhed**<br><br>▶ Databehandleren har dokumenteret og etableret ledelsesstyring af informationssikkerhed. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens informationssikkerhedspolitik og observeret, at den øverste ledelse har det overordnede ansvar for informationssikkerheden.<br><br>Vi har foretaget inspektion af databehandlerens årshjul og observeret, at databehandleren har etableret ledelsesstyring af informationssikkerheden. | Ingen afvigelser konstateret. |

| Artikel 28, stk. 1: Databehandlerens garantier | | |
|---|---|---|
| **Kontrolmål**<br>▶ *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**<br>▶ Databehandleren udfører screening af potentielle medarbejdere før ansættelse. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens procedure for rekruttering af medarbejdere, hvoraf det fremgår, at databehandleren udfører screening af potentielle medarbejdere før ansættelse.<br><br>Vi har for seneste ansatte medarbejder inspiceret at proceduren er fulgt. | Ingen afvigelser konstateret. |
| **Fratrædelse af medarbejdere**<br>▶ Databehandleren har udarbejdet og implementeret en procedure for off-boarding af fratrådte medarbejdere. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens procedure for fratrædelse af medarbejdere.<br><br>Vi har for seneste fratrådte medarbejder inspiceret dokumentation for, at proceduren er fulgt. | Ingen afvigelser konstateret. |
| **Uddannelse og instruktion af medarbejdere, der behandler personoplysninger**<br>▶ Databehandleren afholder awareness-træning af nye medarbejdere i henhold til databeskyttelse og informationssikkerhed i forlængelse af ansættelsen.<br>▶ Der afholdes introduktionskursus for nye medarbejdere, herunder om behandling af dataansvarliges personoplysninger. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har inspiceret dokumentation for, at databehandleren har udført awareness-træning for medarbejdere om databeskyttelse og informationssikkerhed. | Ingen afvigelser konstateret. |

| Artikel 28, stk. 1: Databehandlerens garantier | | |
|---|---|---|
| **Kontrolmål**<br>▶ *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** |
| ▶ Databehandleren foretager løbende uddannelse af medarbejdere i henhold til databeskyttelse og informationssikkerhed samt håndtering heraf. | Vi har inspiceret dokumentation for, at databehandleren har udført introduktionskursus om behandling af dataansvarliges personoplysninger for nye ansatte.<br><br>Vi har foretaget inspektion af databehandlerens årshjul og observeret, at databehandleren løbende udfører uddannelse af medarbejdere i henhold til databeskyttelse og informationssikkerhed samt håndtering heraf.<br><br>Vi har inspiceret dokumentation for, at databehandleren har udført løbende uddannelse af medarbejdere i henhold til databeskyttelse og informationssikkerhed samt håndtering heraf. | |
| **Awareness og oplysningskampagner for medarbejdere**<br><br>▶ Databehandleren udfører løbende awareness-kampagner i form af, opslag, morgenmøder mv.<br>▶ Databehandleren udfører oplysningskampagner for medarbejdere om databeskyttelse og informationssikkerhed. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har inspiceret dokumentation for, at databehandleren løbende har afholdt awareness-kampagner.<br><br>Vi har inspiceret dokumentation for, at databehandleren løbende har afholdt oplysningskampagner om databeskyttelse og informationssikkerhed. | Ingen afvigelser konstateret. |

## 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**<br><br>- Databehandleren anvender en databehandleraftaleskabelon eller lignende for indgåelse af databehandleraftaler.<br>- Gældende databehandleraftaler opbevares elektronisk.<br>- Databehandleraftaler indeholder informationer om brugen af underdatabehandlere. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens skabelon for databehandleraftaler, samt indgåede databehandleraftaler.<br><br>Vi har inspiceret dokumentation for, at gældende databehandleraftaler opbevares elektronisk.<br><br>Vi har foretaget inspektion af databehandlerens databehandleraftaler og observeret, at disse indeholder informationer om brugen af underdatabehandlere. | Ingen afvigelser konstateret. |

| Artikel 28, stk. 3 og 10, artikel 29 og artikel 32, stk. 4: Instruks for behandling af personoplysninger | | |
|---|---|---|
| **Kontrolmål**<br>▶ *At sikre, at databehandleren alene handler efter dokumenteret instruks fra den dataansvarlige.*<br>▶ *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**<br><br>▶ Indgået databehandleraftale indeholder en instruks fra den dataansvarlige.<br>▶ Databehandler indhenter instruks for behandling af personoplysninger fra den dataansvarlige, i forbindelse med indgåelse af databehandleraftale. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af indgåede databehandleraftaler og observeret, at disse indeholder instruks fra den dataansvarlige. | Ingen afvigelser konstateret. |
| **Efterlevelse af instruks for behandling af personoplysninger**<br><br>▶ Databehandler udfører alene behandling af personoplysninger, som fremgår af instruks fra dataansvarlige.<br>▶ Databehandleren udfører egenkontrol af efterlevelse af instruks i indgåede databehandleraftaler. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens fortegnelse over behandlingsaktiviteter som databehandler og observeret, at behandlingerne er i overensstemmelse med instruks fra dataansvarlige.<br><br>Vi har foretaget inspektion af databehandlerens årshjul og observeret, at databehandleren har udført egenkontrol af efterlevelse af instruks i indgåede databehandleraftaler. | Ingen afvigelser konstateret. |
| **Underretning af den dataansvarlige ved ulovlig instruks**<br><br>▶ Databehandleren underretter straks den dataansvarlige i tilfælde, hvor den dataansvarliges instruks strider mod databeskyttelseslovgivningen. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har på forespørgsel fået oplyst, at der ikke har været tilfælde af instrukser, der er vurderet i strid med databeskyttelseslovgivningen, hvorfor vi ikke har kunnet teste kontrollen for implementering. | 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 |
|---|---|---|
| **Underdatabehandleraftale og instruks**<br><br>▶ Ved brug af underdatabehandler indgår databehandleren en databehandleraftale, der pålægger underdatabehandleren de samme databeskyttelsesforpligtelser, som databehandleren er pålagt.<br>▶ Instrukser fra dataansvarlig er videregivet til underdatabehandler.<br>▶ Databehandleraftaler med underdatabehandler opbevares elektronisk.<br>▶ Databehandleraftalen med underdatabehandler indeholder informationer om brugen af underdatabehandlere. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens indgåede databehandleraftaler med underdatabehandlere og observeret, at underdatabehandlerne pålægges de samme databeskyttelsesforpligtelser, som databehandleren er pålagt.<br><br>Vi har foretaget inspektion af databehandlerens indgåede databehandleraftaler med underdatabehandlere og observeret, at de dataansvarliges instrukser til databehandleren er videregivet til underdatabehandleren.<br><br>Vi har inspiceret, at databehandleraftaler med underdatabehandlere opbevares elektronisk.<br><br>Vi har foretaget inspektion af databehandlerens indgåede databehandleraftaler med underdatabehandlere og observeret, at aftalerne indeholder information om brugen af underdatabehandlere. | Ingen afvigelser konstateret. |
| **Godkendelse af underdatabehandlere**<br><br>▶ Databehandler anvender kun godkendte underdatabehandlere. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af, at databehandleren har indgået aftale med alle underdatabehandlerne.<br><br>Vi har for indgåede databehandleraftaler observeret, at disse indeholder information om brugen af de godkendte underdatabehandlere. | 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 |
|---|---|---|
| **Ændringer i godkendte underdatabehandlere**<br><br>▶ Databehandler har udarbejdet en passende proces med dataansvarlig for udskiftning af godkendte underdatabehandlere.<br>▶ Databehandler underretter dataansvarlig ved udskiftning af underdatabehandler i forbindelse med generel godkendelse af underdatabehandler.<br>▶ Dataansvarlig har mulighed for at gøre indsigelse vedr. udskiftning af underdatabehandler. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens procedure vedrørende udskiftning af godkendte underdatabehandlere og observeret, at den omhandler proces for underretning af dataansvarlige, samt mulighed for dataansvarlige for at gøre indsigelse inden for en frist på 60 dage.<br><br>Vi har inspiceret, at databehandleren i ét tilfælde har taget en ny underdatabehandler i brug før fristen for dataansvarliges mulighed for indsigelse var udløbet. Det har medført at dataansvarliges persondata er overført til en underdatabehandler uden dataansvarliges samtykke. Vi har på forespørgsel fået oplyst, at den overførsel er foretaget i testøjemed og at persondata er krypteret.<br><br>Vi har inspiceret, at de overførte persondata var krypteret. | Vi har konstateret, at databehandleren i ét tilfælde har taget en ny underdatabehandler i brug før fristen for dataansvarliges mulighed for indsigelse var udløbet. Underdatabehandleren blev taget i brug den 1. juli 2023 og fristen for indsigelse udløb den 30. august 2023.<br><br>Ingen yderligere afvigelser konstateret. |
| **Oversigt over godkendte underdatabehandlere**<br><br>▶ Databehandler 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 databehandleren.<br><br>Vi har foretaget inspektion af, at databehandleren har en oversigt over godkendte underdatabehandlere og observeret, at den indeholder de relevante informationer. | 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 |
|---|---|---|
| **Tilsyn med underdatabehandlere**<br><br>▶ Databehandleren udfører tilsyn, herunder indhenter og gennemgår underdatabehandlers revisorerklæringer, certificeringer og lignende.<br>▶ Databehandleren udfører tilsyn af underdatabehandleren baseret på en risikovurdering.<br>▶ Databehandler udfører tilsyn af underdatabehandler minimum en gang om året, baseret på en risikovurdeirng. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens årshjul og observeret, at databehandleren årligt udfører tilsyn af underdatabehandlere.<br><br>Vi har inspiceret dokumentation for, at databehandleren har indhentet og gennemgået underdatabehandleren Hetzner Online GmbH's ISO 27001-certificering gældende til 26. september 2025 og en SoA-rapport pr. 30 maj 2022 og observeret, at databehandleren har forholdt sig til materialet baseret på en risikovurdering.<br><br>Vi har inspiceret dokumentation for, at databehandleren har indhentet og gennemgået underdatabehandleren Scaleway SAS's ISO 27001-certificering gældende til 14. februar 2024 og observeret, at databehandleren har forholdt sig til materialet baseret på en risikovurdering.<br><br>Vi har inspiceret dokumentation for, at databehandleren har indhentet og gennemgået underdatabehandleren Link Mobility's ISAE 3000-erklæring pr. 15. marts 2023 og observeret, at databehandleren har forholdt sig til materialet baseret på en risikovurdering.<br><br>Vi har inspiceret dokumentation for, at databehandleren har indhentet og gennemgået underdatabehandleren SMTP.DK ApS' udfyldte spørgeskema pr. 16. august 2023 og observeret, at databehandleren har forholdt sig til materialet baseret på en risikovurdering.<br><br>Vi har inspiceret dokumentation for, at databehandleren har indhentet og gennemgået underdatabehandleren E-Signatur | 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 |
|---|---|---|
| | Danmark A/S' ISAE 3000-erklæring pr. 30. juni 2022 og observeret, at databehandleren har forholdt sig til materialet baseret på en risikovurdering.<br><br>Vi har inspiceret dokumentation for, at databehandleren har indhentet og gennemgået underdatabehandleren Sendbird, Inc.'s ISO 27001-certificering gældende til 24. juli 2024 og observeret, at databehandleren har forholdt sig til materialet baseret på en risikovurdering. | |

| Artikel 28, stk. 3, litra b: Fortrolighed og lovbestemt tavshedspligt | | |
|---|---|---|
| **Kontrolmål**<br>▶ *At sikre, at de personer, der er autoriseret til at behandle personoplysninger, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.* | | |
| **Kontrolaktivitet** | **Test udført af BDO** | **Resultat af test** |
| **Lovbestemt tavshedspligt**<br><br>▶ Alle medarbejdere er underlagt lovbestemt tavshedspligt efter straffelovens bestemmelser. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens procedure for ansættelser og observeret, at medarbejdere underskriver en ansættelseskontrakt indeholdende krav om tavshedspligt.<br><br>Vi har for den seneste ansatte medarbejder foretaget inspektion af, at medarbejderen har underskrevet aftale om tavshedspligt i ansættelseskontrakten. | Ingen afvigelser konstateret. |
| **Tavsheds- og fortrolighedsaftale med medarbejdere**<br><br>▶ Alle medarbejdere har underskrevet en ansættelseskontrakt, der indeholder en bestemmelse om tavshedspligt.<br>▶ Eksterne leverandører/konsulenter er underlagt tavshedspligt ved indgåelse af kontrakt. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens procedure for ansættelser og observeret, at medarbejdere underskriver en ansættelseskontrakt indeholdende krav om tavshedspligt.<br><br>Vi har for seneste ansættelse foretaget inspektion af, at medarbejderen har underskrevet aftale om tavshedspligt i ansættelseskontrakten.<br><br>Vi er på forespørgsel blevet oplyst om, at ingen eksterne konsulenter har adgang til persondata, hvorfor vi ikke har kunnet teste kontrollen. | Ingen afvigelser konstateret. |

## Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

**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 rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *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**<br><br>▶ Der foretages løbende og som minimum en gang årligt en risikovurdering af SameSystem baseret på potentielle risici for datas tilgængelighed, fortrolighed og integritet i forhold til den registreredes rettigheder og frihedsrettigheder.<br>▶ Sårbarheden af systemer og processer vurderes ud fra identificerede trusler.<br>▶ Risici minimeres ud fra vurderingen af deres sandsynlighed, konsekvens og afledte implementeringsomkostninger.<br>▶ Risikovurderinger opdateres løbende efter behov, men minimum en gang årligt. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens risikovurdering af SameSystem og observeret, at den er baseret på potentielle risici for datas tilgængelighed, fortrolighed og integritet i forhold til den registreredes rettigheder og frihedsrettigheder.<br><br>Vi har observeret, at sårbarheden af systemer og processer vurderes ud fra identificerede trusler.<br><br>Vi har inspiceret, at databehandleren har implementeret kompenserende handlinger på baggrund af risikoens sandsynlighed og konsekvens.<br><br>Vi har inspiceret databehandlerens årshjul og observeret, at databehandleren årligt foretager gennemgang af risikovurderingen.<br><br>Vi har inspiceret dokumentation for, at databehandleren har foretaget den årlige gennemgang og opdatering af risikovurderingen og observeret, at denne senest er foretaget den 8. marts 2023, samt at der i løbet af 2023 løbende er sket opdatering af risikovurderingen. | Ingen afvigelser konstateret. |

## Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

**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 rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *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 |
|---|---|---|
| **Beredskabsplaner i tilfælde af fysisk eller teknisk hændelse**<br><br>▶ Databehandleren har etableret en beredskabsplan, der sikrer hurtig responstid til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.<br>▶ Databehandleren har etableret periodisk afprøvning af beredskabsplanen med henblik på at sikre, beredskabsplanerne er tidssvarende og effektive i kritiske situationer.<br>▶ Beredskabstest dokumenteres og evalueres. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af, at databehandleren har etableret en beredskabsplan med det formål at sikre en hurtig responstid til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.<br><br>Vi har foretaget inspektion af databehandlerens årshjul og observeret, at databehandleren har etableret periodisk afprøvning af beredskabsplanen med henblik på at sikre, at beredskabsplanerne er tidssvarende og effektive i kritiske situationer. | Ingen afvigelser konstateret. |
| **Opbevaring af personoplysninger**<br><br>▶ Personoplysninger opbevares utilgængeligt for andre.<br>▶ Adgang til personoplysninger tildeles på baggrund af arbejdsbetinget behov/need-to-know principper.<br>▶ Fortroligheden af digitale personoplysninger opbevares i krypteret form i backup, og når data transporteres.<br>▶ Personoplysninger opbevares kun så længe, der er hjemmel/en legitim grund. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens procedure for, hvordan personoplysninger skal opbevares utilgængeligt for andre og observeret, at denne er implementeret.<br><br>Vi har foretaget inspektion af, at databehandleren tildeler adgang til personoplysninger på baggrund af arbejdsbetinget behov/need-to-know principper. | Ingen afvigelser konstateret. |

## Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

**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 rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *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 foretaget inspektion af databehandlerens årshjul og observeret, at databehandleren løbende foretager kontrol af brugere med adgang til personoplysninger.<br><br>Vi har for medarbejdere med adgang til personoplysninger observeret, at de har et arbejdsbetinget behov.<br><br>Vi har foretaget inspektion af data i backup og transit og observeret, at disse data er krypteret.<br><br>Vi har foretaget inspektion af databehandlerens procedure for, at personoplysninger opbevares kun så længe der er hjemmel/en legitim grund og observeret, at denne er implementeret. | |
| **Fysisk adgangskontrol**<br><br>- Der er etableret fysiske adgangskontroller, som forebygger sandsynligheden for uautoriseret adgang til databehandlerens kontorer, faciliteter og personoplysninger, herunder sikring af, at kun autoriserede personer har adgang.<br>- Alle adgange registreres og logges.<br>- Der foretages løbende og som minimum en gang om året gennemgang af den fysiske adgang til databehandlerens kontorer og faciliteter. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har observeret, at adgang til databehandlerens kontor er beskyttet med adgangskort til selve bygningen.<br><br>Vi har foretaget inspektion af databehandlerens adgangslog og observeret, at indgange af hoveddøren logges.<br><br>Vi har foretaget inspektion af databehandlerens årshjul og observeret, at databehandleren løbende gennemgår adgangslog. | Ingen afvigelser konstateret. |

## Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

**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 rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *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 |
|---|---|---|
| **Fysisk sikkerhed**<br><br>▸ Der er etableret fysisk perimetersikring til at beskytte områder, der indeholder personoplysninger. Den fysiske perimetersikring er i overensstemmelse med de vedtagne sikkerhedskrav.<br>▸ Databehandleren har etableret kontroller til beskyttelse mod eksterne og miljømæssige trusler, herunder efterlevelse af specificerede krav til serverrum omfattende følgende forhold:<br>○ Bygning<br>○ Gulve<br>○ Klima<br>○ Strøm<br>○ Adgang<br>○ Alarmmonitorering<br>○ Brandslukning<br>○ Kabling | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har observeret at den fysiske sikring af servere pr. 5. september 2023 har ligget hos underdatabehandlerne Hetzner Online GmbH og Scaleway SAS.<br><br>Vi har inspiceret dokumentation for, at databehandleren har indhentet og gennemgået underdatabehandleren Hetzner Online GmbH's ISO 27001-certificering gældende til 26. september 2025 og en SoA-rapport pr. 30. maj 2022 og observeret, at der ikke har været konstateret afvigelser vedrørende den fysiske sikkerhed.<br><br>Vi har inspiceret dokumentation for, at databehandleren har indhentet og gennemgået underdatabehandleren Scaleway SAS' ISO 27001-certificering gældende til 14. februar 2024 og derigennem udledt, at Scaleway SAS har passende fysiske kontrolforanstaltninger. | Ingen afvigelser konstateret. |
| **Logisk adgangskontrol**<br><br>▸ Databehandleren har implementeret procedure for brugeradministration, der sikrer, at brugeroprettelser og -nedlæggelser følger en styret proces, og at alle brugeroprettelser er autoriserede.<br>▸ Brugerrettigheder tildeles ud fra et arbejdsbetinget behov. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens procedure for brugeradministration med det formål at sikre, at brugeropret- | Ingen afvigelser konstateret. |

## Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

**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 rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *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 |
|---|---|---|
| ▶ Privilegerede (administrative) adgangsrettigheder tildeles til systemer og enheder ud fra arbejdsbetinget behov.<br>▶ Der foretages halvårlig gennemgang af brugere og brugerrettigheder.<br>▶ Der foretages logning af alle adgange til systemer og data.<br>▶ Databehandleren har etableret logisk adgangskontrol til systemer med personoplysninger, herunder to-faktor autentifikation.<br>▶ Databehandleren har etableret regler for krav til adgangskoder, som skal følges af alle medarbejdere samt eksterne konsulenter. | telser og -nedlæggelser følger en styret proces, og at alle brugeroprettelser er autoriserede og observeret, at disse er implementeret.<br><br>Vi har foretaget inspektion af, at databehandleren tildeler adgang til personoplysninger og privilegerede rettigheder på baggrund af arbejdsbetinget behov/need-to-know principper.<br><br>Vi har for medarbejdere med adgang til personoplysninger observeret, at de har arbejdsbetinget behov.<br><br>Vi har foretaget inspektion af databehandlerens årshjul og observeret, at databehandleren halvårligt foretager kontrol af brugere med adgang til personoplysninger.<br><br>Vi har foretaget inspektion af, at databehandleren foretager logning af alle brugeradgange til systemer og data.<br><br>Vi har foretaget inspektion af, at databehandleren har etableret logisk adgangskontrol til systemer med personoplysninger og observeret, at der anvendes to-faktor autentifikation, og at databehandleren har etableret regler for krav til adgangskoder. | |
| **Fjernarbejdspladser og fjernadgang til systemer og data**<br><br>▶ Fjernadgang til databehandlerens systemer og data sker via en krypteret VPN-forbindelse.<br>▶ Fjernadgang skal foregå via to-faktor autentifikation. | Vi har udført forespørgsel hos passende personale hos databehandleren. | Ingen afvigelser konstateret. |

## Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

**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 rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *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 inspiceret databehandlerens netværkstopologi og faktiske opsætning og observeret, at fjernadgang til databehandlerens systemer og data sker via krypteret VPN-forbindelse.<br><br>Vi har foretaget inspektion af, at der skal anvendes to-faktor autentifikation ved fjernadgang. | |
| **Eksterne kommunikationsforbindelser**<br><br>- Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall og VPN.<br>- Udveksling af personoplysninger via email sker vha. sikkermail løsning.<br>- Eksterne kommunikationsforbindelser er krypteret.<br>- Databehandleren har en oversigt over, hvilke eksterne kommunikationsforbindelser der har tilladelse til at tilgå deres netværk. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har inspiceret at databehandlerens netværkstopologi og faktiske opsætning og observeret, at ekstern adgang til systemer og databaser sker gennem sikret firewall og VPN.<br><br>Vi har foretaget inspektion af databehandlerens SMTP opsætning og observeret, at den understøtter TLS 1.2, samt at databehandleren anvender Microsoft Exchanges standardindstillinger. | Ingen afvigelser konstateret. |
| **Kryptering af personoplysninger**<br><br>- Databehandleren har implementeret en krypteringspolitik for kryptering af persondata. Politikken definerer styrken og protokollen for kryptering.<br>- Bærbare medier med personlysninger er krypteret. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens krypteringspolitik for kryptering af persondata og observeret at den er implementeret via databehandlerens informationssikkerhedspolitik. VI har observeret at politikken definerer, hvordan data skal | Ingen afvigelser konstateret. |

## Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

**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 rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *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 |
|---|---|---|
| ▶ Der anvendes kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og e-mail. | krypteres, og hvilke protokoller der er accepteret samt den er implementeret.<br><br>Vi har foretaget inspektion af databehandlerens krypteringsopsætning på bærbare medier og observeret, at disse er krypteret.<br><br>Vi har foretaget inspektion af data i transit og observeret, at disse data er krypteret. | |
| **Firewall**<br><br>▶ Databehandler har konfiguret firewall korrekt efter best-practice standard.<br>▶ Databehandler anvender kun services/porte, som de har behov for.<br>▶ Firewalls er konfigureret og valideret periodisk efter behov, således at service/porte kun er åbne efter behov. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har inspiceret databehandlerens netværkstopologi og faktiske opsætning af firewall og observeret, at firewall er konfigureret efter best-practice standard, og at der kun er åbnet for services/porte, der er behov for.<br><br>Vi har foretaget inspektion af, at databehandleren har sikret, at firewalls er konfigureret og valideret periodisk efter behov, således at service/porte kun er åbne efter behov. | Ingen afvigelser konstateret. |
| **Netværkssikkerhed**<br><br>▶ Netværkstopologien er struktureret efter best-practice principper, hvilket betyder at servere, som driver applikationer, ikke kan nås direkte fra internettet. | Vi har udført forespørgsel hos passende personale hos databehandleren. | Ingen afvigelser konstateret. |

## Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

**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 rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *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 |
|---|---|---|
| ▶ Databehandlers netværk er segmenteret, så interne services/servere ikke kan kommunikere direkte med internettet.<br>▶ Databehandleren anvender kendte netværksteknologier og mekanismer(Firewall/Intrusion DetectionSystem/Intrusion Prevention System) for at beskytte internt netværk. | Vi har foretaget inspektion af databehandlerens netværkstopologi og faktiske opsætning og observeret, at adgange sker via firewall og VPN forbindelse, og dermed ikke kan nås direkte igennem internettet.<br><br>Vi har foretaget inspektion af databehandlerens netværkstopologi og faktiske opsætning og observeret, at der er niveausegmenteret. | |
| **Antivirusprogram**<br><br>▶ Der er installeret antivirus-software på alle arbejdsstationer.<br>▶ Antivirus-software opdateres løbende og opdateret med seneste version. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens generelle antivirus-politik, der er aktiveret på alle arbejdsstationer og observeret, at disse ikke kan fravælges. Vi har observeret, at politikken sikrer at antivirus er aktiveret på alle arbejdsstationer og løbende opdateres.<br><br>Vi har foretaget inspektion af én udvalgt arbejdsstation og observeret, at der er installeret opdateret antivirus og observeret. | Ingen afvigelser konstateret. |
| **Penetrationstests**<br><br>▶ 1 gang årligt foretages der en penetrationstest af en ekstern leverandør af databehandlerens netværk. Databehandleren gennemgår rapporten og følger op på konstaterede svagheder. | Vi har udført forespørgsel hos passende personale hos databehandleren. | Ingen afvigelser konstateret. |

## Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

**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 rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *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 |
|---|---|---|
| ▶ Databehandler håndterer/mitigerer eventuelle sårbarheder ud fra en risikovurdering.<br>▶ Databehandler har dokumenteret deres håndtering/mitigering af fundne sårbarheder. | Vi har foretaget inspektion af databehandlerens årshjul og observeret, at databehandleren årligt får foretaget penetrationstest af ekstern leverandør.<br><br>Vi har foretaget inspektion af, at databehandleren har fået udført en ekstern penetrationstest og observeret, at databehandleren på baggrund af testens resultater har planlagt mitigerende handlinger og dokumentation heraf. | |
| **Sikkerhedskopiering og retablering af data**<br><br>▶ Der foretages dagligt backup af systemer og data.<br>▶ Drift og opbevaring af backup er outsourcet til underdatabehandler.<br>▶ Der udføres restore-tests 2 gange årligt. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens konfiguration af backup og observeret, at der foretages daglige backups af systemer og data, der uploades til underdatabehandleren Scaleway SAS.<br><br>Vi har inspiceret underdatabehandleren Scaleway SAS' ISO 27001-certificering gældende til 14. februar 2024 og derigennem udledt, at Scaleway har passende kontrolforanstaltninger i forhold til sikkerhedskopiering.<br><br>Vi har inspiceret databehandlerens årshjul og observeret at databehandleren foretager restore-test minimum 2 gange årligt. Senest test blev foretaget i juni 2023 og næste er planlagt til december 2023. | Ingen afvigelser konstateret. |

## Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

**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 rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *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 |
|---|---|---|
| **Vedligeholdelse af systemsoftware**<br><br>▸ Operativsystem-software på servere og arbejdsstationer opdateres løbende.<br>▸ Databehandleren har implementeret en proces for opdatering af systemsoftware med henblik på at sikre systemers tilgængelighed og sikkerhed. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens procedure for opdatering af systemsoftware og observeret, at denne er implementeret. Vi har observeret, at der er opsat automatisk opdatering af arbejdsstationer og manuel opdateringsproces for servere.<br><br>Vi har foretaget inspektion af en udvalgt arbejdspc og observeret, at denne er opdateret.<br><br>Vi har foretaget inspektion af en udvalgt server og observeret, at denne er opdateret. | Ingen afvigelser konstateret. |
| **Logning i systemer, databaser og netværk, herunder logning af anvendelse af personoplysninger**<br><br>▸ Alle succesfulde og mislykkede adgangsforsøg til databehandlerens systemer og data logges.<br>▸ Alle brugerændringer i system og databaser logges.<br>▸ Loggen slettes efter den fastsatte retentionsperiode.<br>▸ Databehandler monitorerer og logger netværkstrafik.<br>▸ Databehandler opbevarer logs i 6 måneder. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har inspiceret dokumentation for, at databehandleren har opsat logning af adgangsforsøg til databehandlerens systemer og data.<br><br>Vi har inspiceret dokumentation for, at databehandleren har opsat logning af brugerændringer i systemet.<br><br>Vi har inspiceret dokumentation for, at databehandleren har opsat logning af netværkstrafik. | Ingen afvigelser konstateret. |

## Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

**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 rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *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 inspiceret dokumentation for, at logs slettes eller anonymiseres efter 6 måneder. | |
| **Overvågning**<br>- Databehandleren har etableret et overvågningssystem til overvågning af produktionsmiljø, herunder oppetid, ydeevne og kapacitet.<br>- Databehandleren notificeres om identificerede alarmer, og følger op herpå. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af, at databehandleren har etableret et overvågningssystem til overvågning af produktionsmiljø, herunder oppetid, ydeevne og kapacitet og observeret, at systemet genererer notifikationer om alarmer til databehandleren. | Ingen afvigelser konstateret. |
| **Reparation og service samt bortskaffelse af it-udstyr**<br>- Databehandleren sender it-udstyr til reparation og service uden indhold af personoplysninger.<br>- Databehandleren bortskaffer it-udstyr ved fysisk destruktion af databærende medier.<br>- Databehandleren foretager sikker sletning af data på databærende medier(overskrivning/forvanskning, kryptering)<br>- Databehandleren fører en oversigt af destrueret it-udstyr. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af, at databehandleren har en oversigt over defekt og destrueret it-udstyr.<br><br>Vi har inspiceret databehandlerens indgåelse af aftale med en ekstern leverandør om varetagelse af reparation af defekt it-udstyr og bortskaffelse ved fysisk destruktion af databærende medier.<br><br>Vi har på forespørgsel fået oplyst, at der ikke har været defekt udstyr siden indgåelse af aftalen med den eksterne leverandør, hvorfor vi ikke har kunnet teste kontrollen for implementering. | Ingen afvigelser konstateret. |

## Artikel 28, stk. 3, litra c: Tekniske og organisatoriske sikkerhedsforanstaltninger

**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 rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.*
- *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 |
|---|---|---|
| **Afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske sikkerhedsforanstaltninger**<br><br>▶ Databehandler afprøver, vurderer og evaluerer effektiviteten af, at de tekniske og organisatoriske sikkerhedsforanstaltninger er passende ift. de data, som varetages på vegne af den dataansvarlige. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens årshjul og observeret, at databehandler afprøver, vurderer og evaluerer effektiviteten af, at de tekniske og organisatoriske sikkerhedsforanstaltninger er passende ift. de data, som varetages på vegne af den dataansvarlige.<br><br>Vi har observeret at databehandleren i marts 2023 har gennemført den beskrevne kontrol. | 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 |
|---|---|---|
| **Udvikling og vedligeholdelse af systemer**<br><br>▶ Databehandleren arbejder ud fra privacy-by-design principper i udvikling og vedligeholdelsesopgaver.<br>▶ Mindst én gang om året i forbindelse med opdatering af den generelle risikovurdering, vurderes det, om databeskyttelsen gennem design og standardindstillinger i de etablerede tekniske og organisatoriske foranstaltninger er passende. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens procedure vedrørende udvikling og vedligeholdelsesopgaver og observeret, at proceduren omhandler indarbejdelse af privacy-by-design principper i udvikling og vedligeholdelsesopgaver.<br><br>Vi har observeret, at databehandlerens udviklingsproces indeholder krav til beskrivelse af ønsket udvikling/vedligehold i en ticket, hvor udviklingen risikovurderes i beskyttelse af personoplysninger. Den efterfølgende kvalitetssikring, test, mv. baseres på denne risikovurdering. Processen indeholder derudover krav til udvikling, kvalitetssikring, test, ibrugtagning og tilbagerulning.<br><br>Vi har foretaget inspektion af en udvalgt udviklingsopgave og observeret, at procedurens krav er efterlevet i den pågældende udviklingsproces.<br><br>Vi har foretaget inspektion af databehandlerens årshjul og observeret, at databehandleren årligt foretager en generel risikovurdering, herunder vurdering af databeskyttelsen gennem design og standardindstillinger. | Ingen afvigelser konstateret. |
| **Informationssikkerhed i udvikling og ændringer**<br><br>▶ Databehandler arbejder ud fra security-by-design principper i udviklings- og ændringsopgaver.<br>▶ Rollback-plan er implementeret i tilfælde af fejl i produktionsmiljøet.<br>▶ Mindst én gang om året i forbindelse med opdatering af den generelle risikovurdering, vurderes det, om informationssikkerheden gennem design og udvikling i | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens procedure vedrørende udvikling og ændringsopgaver og observeret, at proceduren omhandler indarbejdelse af security-by-design principper i udvikling og ændringsopgaver. | 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 |
|---|---|---|
| de etablerede tekniske og organisatoriske foranstaltninger er passende. | Vi har observeret, at databehandlerens udviklingsproces indeholder krav til beskrivelse af ønsket udvikling/vedligehold i en ticket, hvor udviklingen risikovurderes i it-sikkerhed. Den efterfølgende kvalitetssikring, test, mv. baseres på denne risikovurdering. Processen indeholder derudover krav til udvikling, kvalitetssikring, test, ibrugtagning og tilbagerulning.<br><br>Vi har foretaget inspektion af en udvalgt udviklingsopgave og observeret, at procedurens krav er efterlevet i den pågældende udviklingsproces.<br><br>Vi har foretaget inspektion af databehandlerens årshjul og observeret, at databehandleren årligt foretager en generel risikovurdering, herunder vurdering af informationssikkerheden gennem design og udvikling. | |
| **Adskillelse af udviklings-, test og produktionsmiljø**<br><br>▶ Der er indført funktionsadskillelse mellem udvikling og drift.<br>▶ Ændringer af funktionalitet testes, inden det sættes i drift.<br>▶ Udvikling og test udføres i udviklingsmiljøer, som er adskilte fra produktionssystemer.<br>▶ Der benyttes et versionsstyringssystem som registrerer alle ændringer i kildekode. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har inspiceret, at der er funktionsadskillelse mellem udvikling og drift.<br><br>Vi har inspiceret udviklingsprocessen og observeret, at denne indeholder brug af test, inden en ny funktionalitet implementeres.<br><br>Vi har foretaget inspektion af databehandlerens it-miljøer og observeret, at udviklingsmiljøet er adskilt fra produktionsmiljøet.<br><br>Vi har inspiceret databehandlerens versionsstyringssystem og observeret, at der registreres ændringer i kildekoden. | Ingen afvigelser konstateret. |

| Artikel 25: Databeskyttelse gennem design og standardindstillinger | | |
|---|---|---|
| **Kontrolmål**<br>▶ *At sikre, at databehandleren gennemfører databeskyttelse gennem design og standardindstillinger.* | | |
| **Kontrolaktivitet** | **Test udført af BDO** | **Resultat af test** |
| | Vi har foretaget inspektion af en udvalgt udviklingsopgave og observeret, at denne er udviklet i et særskilt udviklingsmiljø, og er testet og ibrugtaget via et versionsstyringssystem. | |
| **Personoplysninger i udviklings- og testmiljø**<br>▶ Der anvendes anonymiseret testdata i udviklings- og testmiljø. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af udviklingsmiljøet og observeret, at databehandleren har anonymiseret data i udvikling- og testsmiljøet. | Ingen afvigelser konstateret. |
| **Supportopgaver**<br>▶ Supporteres adgange og håndtering af personoplysninger ved supportopgaver sker ud fra support tickets og supporterens arbejdsbetingede behov. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens log over supportsager og observeret, at supportsager behandles på baggrund af support tickets.<br><br>Vi har inspiceret dokumentation for at supportere, der har adgang til persondata, har et arbejdsbetinget behov.<br><br>Vi har foretaget inspektion af databehandlerens årshjul og observeret, at databehandleren gennemgår supporternes adgangsrettigheder. | Ingen afvigelser konstateret. |

| Artikel 28, stk. 3, litra g: Sletning og tilbagelevering af personoplysninger | | |
|---|---|---|
| **Kontrolmål**<br>▶ *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 af personoplysninger**<br><br>▶ Databehandleren sletter den dataansvarliges personoplysninger efter instruks, ved ophør af hovedaftalen. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens generelle databehandleraftale med dataansvarlige og observeret, at databehandleren er forpligtet til at slette eller tilbagelevere den dataansvarliges personoplysninger efter instruks, ved ophør af hovedaftalen.<br><br>Vi har inspiceret, at data er slettet i databehandlerens systemer for databehandlerens seneste ophørte kunde. | Ingen afvigelser konstateret. |
| **Tilbagelevering af personoplysninger**<br><br>▶ Databehandlerens system har en funktion, som sikrer, at ophørte kunder selv kan hente deres egne data | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af, at databehandleren har opsat en funktion, som sikrer, at ophørte kunder selv kan hente deres egne data. | Ingen afvigelser konstateret. |

| Artikel 28, stk. 3, litra e, f og h: Bistand til den dataansvarlige | | |
|---|---|---|
| **Kontrolmål**<br>▶ *At sikre, at databehandleren kan bistå den dataansvarlige med opfyldelse af de registreredes rettigheder.*<br>▶ *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).*<br>▶ *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**<br><br>▶ Databehandler har udarbejdet en procedure for bistand til den dataansvarlige ved opfyldelse af de registreredes rettigheder.<br>▶ Det er muligt at give indsigt i alle oplysninger, der er registreret. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har inspiceret databehandlerens procedure vedrørende bistand til dataansvarlige og observeret, at den sikrer bistand til den dataansvarlige ved opfyldelse af de registreredes rettigheder.<br><br>Vi har på forespørgsel fået oplyst, at der har ikke har været henvendelse vedrørende de registreredes rettigheder, hvorfor vi ikke har kunnet teste proceduren for implementering. | Ingen afvigelser konstateret. |
| **Forpligtelser om behandlingssikkerhed, brud på persondatasikkerheden og konsekvensanalyser**<br><br>▶ Der er udarbejdet procedurer for bistand til den dataansvarlige ved opfyldelse af bistand i forhold til artikel 32-36. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har inspiceret databehandlerens procedure for bistand til den dataansvarlige og observeret, at der er udarbejdet procedurer for bistand til den dataansvarlige ved opfyldelse af bistand i forhold til artikel 32-36.<br><br>Vi har på forespørgsel fået oplyst, at databehandleren ikke har modtaget henvendelser fra den dataansvarlige vedrørende de registreredes rettigheder og de særlige krav i forordningen, hvorfor vi ikke har kunnet teste proceduren for implementering. | Ingen afvigelser konstateret. |

## Artikel 28, stk. 3, litra e, f og h: Bistand til den 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 |
|---|---|---|
| **Revision og inspektion**<br><br>▶ Databehandler er forpligtet til at få udarbejdet en ISAE 3000-erklæring om de tekniske og organisatoriske sikkerhedsforanstaltninger, rettet mod behandling og beskyttelse af personoplysninger.<br>▶ Databehandleren stiller den fornødne information til rådighed for den dataansvarlige og tilsynsmyndigheden på anmodning i forbindelse med revision og inspektion af databehandleren. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har inspiceret databehandlerens indgåede databehandleraftaler og observeret, at databehandleren er forpligtet til at få udarbejdet en ISAE 3000-erklæring om de tekniske og organisatoriske sikkerhedsforanstaltninger rettet mod behandling og beskyttelse af personoplysninger. Vi har udarbejdet nærværende ISAE 3000-erklæring til brug for databehandlerens forpligtelser i denne relation.<br><br>Vi har observeret, at databehandleren på baggrund af anmodning fra den dataansvarlige skal stå til rådighed for den dataansvarlige, og stille den fornødne information til rådighed for den dataansvarlige og tilsynsmyndigheden i forbindelse med revision og inspektion af databehandleren.<br><br>Vi har ved forespørgsel fået oplyst, at der de seneste 12 måneder har været anmodning fra en dataansvarlig om levering af informationer.<br><br>Vi har inspiceret, at databehandleren har videregivet de fornødne informationer til den dataansvarlige. | Ingen afvigelser konstateret. |

| Artikel 30, stk. 2, 3 og 4: Fortegnelse over kategorier af behandlingsaktiviteter | | |
|---|---|---|
| **Kontrolmål**<br>▶ *At sikre, at databehandleren udarbejder en skriftlig fortegnelse over alle kategorier af behandlingsaktiviteter, der foretages på vegne af den dataansvarlige.*<br>▶ *At sikre, at databehandleren opbevarer fortegnelsen skriftligt, herunder elektronisk.*<br>▶ *At sikre, at databehandleren kan stille fortegnelsen til rådighed for tilsynsmyndigheden.* | | |
| **Kontrolaktivitet** | **Test udført af BDO** | **Resultat af test** |
| **Fortegnelse over kategorier af behandlingsaktiviteter**<br>▶ Databehandleren har etableret en fortegnelse over behandlingsaktiviteter som databehandler.<br>▶ Fortegnelsen opdateres løbende ved væsentlige ændringer.<br>▶ Fortegnelsen opdateres minimum en gang årligt under det årlige review. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har inspiceret, at databehandleren har etableret en fortegnelse over behandlingsaktiviteter som databehandler.<br><br>Vi har foretaget gennemgang af databehandlerens årshjul og observeret, at databehandleren løbende opdaterer fortegnelsen og minimum én gang årligt. | Ingen afvigelser konstateret. |
| **Opbevaring af fortegnelsen**<br>▶ Fortegnelsen opbevares elektronisk i databehandlerens system/fil-drev. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens fortegnelse og observeret, at fortegnelsen opbevares elektronisk i databehandlerens filsystem. | Ingen afvigelser konstateret. |
| **Datatilsynets adgang til fortegnelsen**<br>▶ Databehandleren udleverer fortegnelsen på anmodning fra Datatilsynet. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens procedure for udlevering af fortegnelsen over behandlingsaktiver og observeret, at databehandleren kan udlevere fortegnelsen til Datatilsynet ved forespørgsel.<br><br>Vi har på forespørgsel fået oplyst, at databehandleren ikke har modtaget anmodninger fra Datatilsynet vedrørende udlevering af fortegnelsen, hvorfor vi ikke har kunnet teste for implementering. | Ingen afvigelser konstateret. |

## Artikel 33, stk. 2: Underretning om 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 |
|---|---|---|
| **Underretning om brud på persondatasikkerheden**<br><br>▶ Databehandleren underretter den dataansvarlige om brud på persondatasikkerheden uden unødig forsinkelse.<br>▶ Databehandleren ajourfører den dataansvarlige med alle relevante og nødvendige oplysninger, når de er til rådighed for databehandleren.<br>▶ Kommunikation mellem databehandler og den dataansvarlige dokumenteres og gemmes. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens procedure for databrud og underretning af den dataansvarlige om brud på persondatasikkerheden og observeret, at denne er implementeret.<br><br>Vi har observeret, at proceduren omhandler ajourføring af den dataansvarlige med alle relevante og nødvendige oplysninger og forhold omkring dokumentering af kommunikationen med den dataansvarlige.<br><br>Vi har på forespørgsel fået oplyst, at der ikke har været brud på persondatasikkerheden siden etablering af proceduren, hvorfor vi ikke har kunnet teste for implementering. | Ingen afvigelser konstateret. |
| **Identifikation af brud på persondatasikkerheden**<br><br>▶ Databehandleren uddanner relevant personale i Identifikation af brud på persondatasikkerheden.<br>▶ Databehandleren har udarbejdet en procedure for vurdering og identifikation af brud på persondatasikkerheden. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har inspiceret dokumentation for, at databehandleren har uddannet relevant personale i Identifikation af brud på persondatasikkerheden.<br><br>Vi har foretaget inspektion af databehandlerens procedure for databrud og observeret at deres incident response indeholder afsnit omkring vurdering og identifikation af databrud. | Ingen afvigelser konstateret. |

## Artikel 33, stk. 2: Underretning om 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 |
|---|---|---|
| **Registrering af brud på persondatasikkerheden**<br><br>▶ Databehandleren registrerer brud på persondatasikkerheden i databrudsloggen.<br>▶ Databehandleren har udarbejdet og implementeret en procedure for erfaringsopsamling ved brud på persondatasikkerheden. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens procedure for databrud, herunder registrering af brud på persondatasikkerheden i databrudsloggen og observeret, at denne er implementeret.<br><br>Vi har observeret, at proceduren også omhandler erfaringsopsamling ved brud på persondatasikkerheden.<br><br>Vi har på forespørgsel fået oplyst, at der ikke har været brud på persondatasikkerheden siden etablering af proceduren, hvorfor vi ikke har kunnet teste for implementering. | Ingen afvigelser konstateret. |

| Artikel 44 – 49: Overførsel af personoplysninger til tredjelande | | |
|---|---|---|
| **Kontrolmål**<br>▶ *At sikre, at databehandleren kun overfører personoplysninger til et tredjeland eller en international organisation, når betingelserne i artikel 45-49, opfyldes.*<br>▶ *At sikre, at databehandleren kun overfører personoplysning i henhold til instruks fra den dataansvarlige og i henhold til et gyldigt overførselsgrundlag (artikel 45-49).* | | |
| **Kontrolaktivitet** | **Test udført af BDO** | **Resultat af test** |
| **Overførsel af personoplysninger til tredjelande**<br><br>▶ Der foreligger skriftlige procedurer for overførsel af personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.<br>▶ Databehandlerens procedure gennemgås og vurderes løbende, og som minimum en gang årligt, om proceduren skal opdateres. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens procedure for overførsel af personoplysninger til tredjelande eller internationale organisationer og observeret, at den er i overensstemmelse med databehandlerens generelle databehandleraftale.<br><br>Vi har foretaget inspektion af databehandlerens procedure og observeret, at databehandlerens procedure gennemgås og vurderes løbende, og som minimum en gang årligt. | Ingen afvigelser konstateret. |
| **Instruks fra den dataansvarlige**<br><br>▶ Databehandleren overfører kun personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.<br>▶ Databehandleren dokumenterer indhentet instruks vedrørende overførsel af personoplysninger til tredjelande eller internationale organisationer fra den dataansvarlige. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens generelle databehandleraftale og observeret, at databehandler kun må overføre data til tredjeland efter instruks fra den dataansvarlige. Vi har videre observeret, at denne instruks er dokumenteret i bilag i den generelle databehandleraftale. | Ingen afvigelser konstateret. |
| **Gyldigt overførselsgrundlag**<br><br>▶ Databehandleren vurderer og dokumenterer, at der eksisterer et gyldigt overførselsgrundlag i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer. | Vi har udført forespørgsel hos passende personale hos databehandleren.<br><br>Vi har foretaget inspektion af databehandlerens transfer impact assessment og observeret, at databehandleren har vurderet overførselsgrundlaget for en amerikansk underdatabehandler, Sendbird Inc. | Vi har observeret, at databehandleren anvender en amerikanskejet underdatabehandler, og at databehandleren ikke har et gyldigt overførselsgrundlag ved overførsel af den dataansvarliges persondata til den amerikanske underdatabehandler Sendbird, Inc. EU-Kommissionen har den 10. juli 2023 truffet afgørelse om, at det såkaldte "EU-U.S. Data Privacy Framework" sikrer et tilstrækkeligt beskyttelsesniveau i forbindelse med overførsel af personoplysninger fra EU til USA, og dermed kan |

| Artikel 44 – 49: Overførsel af personoplysninger til tredjelande | | |
|---|---|---|
| **Kontrolmål**<br>▶ *At sikre, at databehandleren kun overfører personoplysninger til et tredjeland eller en international organisation, når betingelserne i artikel 45-49, opfyldes.*<br>▶ *At sikre, at databehandleren kun overfører personoplysning i henhold til instruks fra den dataansvarlige og i henhold til et gyldigt overførselsgrundlag (artikel 45-49).* | | |
| **Kontrolaktivitet** | **Test udført af BDO** | **Resultat af test** |
| | Vi har foretaget inspektion af databehandlerens oversigt over underdatabehandlere og observeret, at databehandleren anvender en underdatabehandler i et tredjeland. Det drejer sig om den amerikanske underdatabehandler Sendbird Inc.<br><br>Den 10. juli 2023 har EU-kommisionen truffet afgørelse om, at det såkaldte "EU-U.S. Data Privacy Framework" sikrer et tilstrækkeligt beskyttelsesniveau i forbindelse med overførsel af personoplysninger fra EU til USA, og dermed kan fungere som et gyldigt overførselsgrundlag. Tilstrækkelighedsafgørelsen kan dog alene anvendes som overførselsgrundlag, ved overførsel af personoplysninger til organisationer i USA, der har certificeret sig under EU-U.S. Data Privacy Framework hos det amerikanske handelsministerium.<br><br>Vi har undersøgt, om Sendbird Inc; er certificeret under det nye overførselsgrundlag EU-U.S. Data Privacy Framework, som EU-Kommissionen tiltrådte den 10. juli 2023 pr. 5. september 2023. Vi har observeret, at Sendbird Inc. ikke har et aktivt certifikat, og dermed har databehandleren ikke et gyldigt overførselsgrundlag til overførsel af den dataansvarliges persondata til underdatabehandleren Sendbird Inc. | fungere som et gyldigt overførselsgrundlag. Tilstrækkelighedsafgørelsen kan dog alene anvendes som overførselsgrundlag, ved overførsel af personoplysninger til organisationer i USA, der har certificeret sig under EU-U.S. Data Privacy Framework hos det amerikanske handelsministerium. Underdatabehandleren Sendbird Inc. har ikke haft et gyldigt certifikat pr. 5. september 2023, og derfor har databehandleren ikke haft et gyldigt overførselsgrundlag.<br><br>Ingen yderligere afvigelser konstateret. |

**BDO STATSAUTORISERET REVISIONSAKTIESELSKAB**

**KYSTVEJEN 29**
**8000 AARHUS C**

**CVR-NR. 20 22 26 70**