et trygt samfund med IT og data

Revisorerklæring

SpeedAdmin ApS

Uafhængig revisors ISAE 3000 erklæring om informationssikkerhed og foranstaltninger i henhold til databehandleraftaler med kunder pr. 21. juni 2021.

REVI-IT A/S | www.revi-it.dk
Højbro Plads 10, 1200 København K
CVR: 30 98 85 31 | Tlf. 33 11 81 00 | info@revi-it.dk
www.dpo-danmark.dk | www.revi-cert.dk

Juni 2021

Indholdsfortegnelse

Afsnit 1: SpeedAdmin ApS' beskrivelse af behandlingsværktøjer for leverancen af administrationssystemet SpeedAdmin til musik og kulturskoler

Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er: At levere administrationssystemet SpeedAdmin til musik- og kulturskoler.

Det er musik- og kulturskolerne, som har ansvaret for at levere de data de har behov for, for at kunne udførede daglige administrative driftsopgaver i SpeedAdmin. Dette gør musik- og kulturskolerne til dataansvarlig overfor de registrerede i systemet.

Behandling af personoplysninger er i henhold til hovedaftalen (licensaftalen) mellem SpeedAdmin ApS og musik- og kulturskolerne samt den databehandleraftale, som bliver indgået ved starten af leverancen.

Systemet er 100% webbaseret og der skal derfor ikke hentes eller downloades noget program til den pc man benytter. Dog er der mulighed for at downloade SpeedAdmins App på smartphones og tablets, som både kan benyttes af lærere, elever og værger.

Karakteren af behandlingen

Databehandlerens behandling af personoplysningerne på vegne af den dataansvarlige foregår udelukkende efter den dataansvarliges instrukser. Databehandleren anvender ikke personoplysningerne til andre formål end de som er beskrevet i dataansvarliges instrukser.

Personoplysninger

- CPR-nummer (DK) and personnummer (NO and SE)
- Fødselsdato (UK og DE)
- Adresse, postnummer
- Fulde navn
- E-mail
- Mobil- og telefonnummer

Kategorier af registrerede personer omfattet af databehandleraftalen:

- Musik- og kulturskolers ansatte
- Elever
- Værger
- Evt. kontaktpersoner på musik- og kulturskolens samarbejdspartnere

Praktiske tiltag

Ledelsen i SpeedAdmin har godkendt alle tiltag, interne standarder og de forskellige årlige revisioner, der foretages internt i SpeedAdmin.

Alle SpeedAdmins medarbejdere er orienteret om persondata og informationssikkerhed. Der bliver årligt afholdt intern security awareness træning for alle medarbejdere, hvor interne standarder gennemgås samt information knyttet til GDPR og IT-sikkerhed. Alle standarder ligger tilgængeligt for alle medarbejdere.

Ved større ændringer i standarderne bliver alle medarbejdere orienteret herom.

Systemet udfører automatiske logs. Blandt andet logges alle logins i systemet inkl. fejlede logins. Ændringer som bliver foretaget på elever, værger og lærere bliver logget. Herudover bliver personspecifikke søgninger i systemet også logget.

Udvikling i systemet som kan påvirke de registreredes rettigheder registreres i en log og SpeedAdmins DPO bliver involveret i processen. Eventuelle sikkerhedsbrud registreres, samt håndteringen af dem. Årligt vil denne log blive gennemgået med fokus på måden sikkerhedsbruddene er blevet håndteret på.

Risikovurdering

SpeedAdmin ApS har foretaget en risikoanalyse af potentielle trusler mod systemet og datasikkerheden. Truslerne er blevet vurderet ud fra sandsynligheden for, at truslen vil forekomme og hvor stor en konsekvens truslen ville have, hvis den blev realiseret.

Denne risikoanalyse gennemgås minimum én gang årligt. I denne gennemgang er der blandt andet fokus på, om der er kommet nye trusler til siden sidst. Derudover rettes risikoanalysen til, hvis tiltag er blevet realiseret eller hvis der er kommet nye løsningsforslag.

Ændringer i risikoanalysen vil altid blive godkendt og underskrevet af en af SpeedAdmin ApS' ledere.

Behandlinger – instrukser

I vores databehandleraftaler, som vi har med vores kunder, er kundernes instrukser beskrevet i forbindelse med databehandlingen. Disse instrukser er udelukkende kun dem, som vi behandler data efter.

Vi har en standard for, hvordan vi internt håndterer en ulovlig instruks, hvis vi modtager en fra en kunde. Alle medarbejdere er bekendt med denne standard og kan derfor agere, hvis de modtager en ulovlig instruks.

Vi fører også en artikel 30-fortegnelse over de forskellige behandlinger af persondata vi foretager os, både som databehandler (på vegne af vores kunder) og som dataansvarlig (for vores underleverandører). Denne fortegnelse ligger også tilgængeligt for medarbejderne, så de har mulighed for at orientere sig i den.

Artikel 30-fortegnelsen bliver gennemgået og revideret minimum én gang årligt i starten af et nyt år eller løbende ved behov. Der er lavet påmindelser til de ansvarlige, så de får en reminder om, at revideringen skal gøres.

Foruden artikel 30-fortegnelsen administrerer vi også alle medarbejderes brugeradgange. Vi har en oversigt over alle medarbejderes brugeradgange og opdaterer den, når der sker ændringer.

Procedurekontrol

Én gang årligt eller ved behov bliver alle interne standarder gennemgået. Herudover bliver diverse fortegnelser og logs også gennemgået og revideret. På denne måde kan vi danne os et overblik over den samlede håndtering af de sager der har været og revidere, om der eventuelt skal ændres på en eller flere standarder.

Ved vores årlige security awareness trænings dag, skal alle medarbejdere slette mails og diverse dokumenter,som indeholder personoplysninger.

Procedurer - adgangsstyring

Det er SpeedAdmins ledelse der står for beslutningen om og administrationen af, hvilke adgange de forskellige medarbejdere skal have.

Alle adgange bliver registreret i et dokument. Dette dokument opdateres for hver ændring der foretages i forbindelse med adgange.

Der er personlige kodeord til både ansattes pc'ere og til selve systemet

Alle SpeedAdmins medarbejdere har adgang til kontoret i Sønderborg. Alle har modtaget en nøglebrik, som der er individuelle adgangskoder til, som kræver adgangskode uden for arbejdstiden. Hver nøglebrik er markeret med et nummer, som er registreret i adgangsdokumentet ud for hver medarbejder.

Ophører en medarbejder skal den gældende standard for dette efterleves i forbindelse med tilbagelevering af nøglebrik og stoppe de forskellige adgange den enkelte har.

I selve systemet er der rettighedsgrupper for brugerne. Det betyder, at ikke alle har de samme rettigheder i systemet, da hver rettighedsgruppe definerer, hvilke funktioner der skal være tilgængelig for den enkelte.

Foruden rettighedsgrupperne i systemet, logges der også de handlinger, som bliver gjort i systemet og hvem, der udfører handlingerne.

Procedurer – udvikling

Den interne standard, der indeholder udvikling af nye eller nuværende funktioner, som kan eller vil påvirke de registreredes rettigheder og/eller persondata, skal følges. Proceduren lyder på, at de udviklere, som arbejder på den enkelte udvikling, skal udviklingen logges i en internlog.

Foruden at forløbet skal logges, skal DPO'en også inddrages inden udviklingen bliver deployet (lagt ud i systemet). DPO'en skal være med til at sikre, at de registrerede i systemet, er beskyttet på den bedste måde og i overensstemmelse med persondataforordningen.

Procedurer – håndtering af persondataanmodninger

Persondataanmodninger fra registrerede må vi fra SpeedAdmin ikke behandle. Da vi "bare" er databehandler og dermed ikke dataansvarlige, må og skal vi ikke behandle disse anmodninger. Det er de dataansvarlige, altså vores kunder, som må og skal behandle persondataanmodninger.

Det vil derfor også være et sjældent tilfælde, at vi overhovedet vil modtage nogle. Men da dette ikke er en garanti, har vi et punkt om dette i vores standard om de registreredes rettigheder.

Modtager vi en persondataanmodning fra en registreret, henviser vi vedkommende til at kontakte den tilknyttede skole. Derudover registrerer vi persondataanmodninger i en log, som ligeledes vil blive revideret ved behov, eller minimum én gang årligt, for at danne os et overblik over, om der skal ændres noget i standarden.

Procedurer - sikkerhedshændelser

SpeedAdmin ApS logger sikkerhedshændelser i henhold til den interne standard om sikkerhedsbrud. Det er blandt andet vigtigt, at man inddrager DPO'en lige så snart man er blevet gjort opmærksom på en hændelse eller et brud.

Ved sikkerhedsbrud skal der registreres i intern log, hvordan man har håndteret sagen. Den skal løbende opdateres – lige fra opdagelse af bruddet til sagen er færdigbehandlet.

Denne log bliver revideret en gang årligt. Ved revideringen gennemgås håndtering af de brud, som har været i det forgangne år. Ved denne gennemgang er fokus blandt andet på håndtering af bruddet og om der er behov for justeringer i standarden. Hvis standarden bliver justeret, bliver alle medarbejdere orienteret herom.

Underleverandører

Vi har valgt at benytte nogle underleverandører, da vi mener, at de er med til at give den bedste samlede løsning for alle vores kunder.

Underleverandørerne skal til enhver tid have sikret sig forsvarligt mod ulovlig elektronisk eller fysisk indtrængen, hærværk, tyveri, hacking, edb-virus, denial of service angreb og andre lignende sikkerhedsbrud. Derudover også sikre sig mod risiko for brand, storm, vandskade og andre forhold, der kan bringe SpeedAdmins opfyldelse af sine aftaler i fare.

Årligt føres der tilsyn med underleverandørerne. Vi indhenter underleverandørers it-revisionserklæring, hvis de får udarbejdet en. Ellers udsender vi årligt et spørgeskema, som omhandler deres måde og procedurer for at sikre en høj IT-sikkerhed.

Alt ikke-fortroligt materiale i forbindelse med vores tilsyn kan, efter ønske/forespørgsel fra dataansvarlig, blive fremsendt til den dataansvarlige.

Tredjelande

Der er internt besluttet, at SpeedAdmin hverken lagrer eller overfører data til tredjelande. Derfor er dette også altid en faktor, som bliver undersøgt, før SpeedAdmin beslutter sig for at benytte en eventuel ny underleverandør.

Medarbejdere

Når en medarbejder bliver ansat, gennemgås IT-sikkerhedspolitikken samt de interne standarder. Herudover skal en medarbejdererklæring underskrives, som også ligger som bilag til vores IT-sikkerhedspolitik.

Ved fratrædelse bliver standarden for dette fulgt.

Komplementerende kontroller

- Dataansvarlige er selv ansvarlige for at slette loggen.
- Superbrugere er de eneste som må anonymisere brugere i systemet.
- Hvis den Dataansvarlige downloader Excel regneark fra SpeedAdmin, er den dataansvarlige selv ansvarlig for at få dem slettet.
- De Dataansvarlige skal være opmærksom på de mails, der bliver sendt ud fra systemet om låste brugere.
- De Dataansvarlige har selv oplysningspligt overfor de registrerede i SpeedAdmin – vi bistår selvfølgelig med oplysninger om behandlingen.

Afsnit 2: SpeedAdmin ApS' udtalelse

SpeedAdmin behandler personoplysninger i overensstemmelse med databehandleraftaler, indgået med vores kunder.

Medfølgende beskrivelse er udarbejdet til brug for data ansvarlige, der har anvendt administrationssystemet SpeedAdmin til musik- og kulturskoler, og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført ved vurdering af, om kravene i EU's forordning om "Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger" (herefter "databeskyttelsesforordningen") er overholdt.

SpeedAdmin ApS anvender underleverandørerne og underdatabehandlerne Microsoft, Zendesk, Unit-IT og Link Mobility. Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos SpeedAdmin ApS' underleverandører og underdatabehandlere.

SpeedAdmin ApS bekræfter at:

a) Den medfølgende beskrivelse, Afsnit 1, giver en retvisende beskrivelse af administrationssystemet SpeedAdmin til musik- og kulturskoler, der har behandlet personoplysninger på vegne af dataansvarlige og i henhold til databeskyttelsesforordningen pr. 21. juni 2021. Kriterierne anvendt for at give denne udtalelse var, at den følgende beskrivelse:

   (i) Redegør for, hvordan administrationssystemet SpeedAdmin til musik- og kulturskoler var udformet og implementeret, herunder redegør for:

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

de dataansvarlige og som, hvis det er nødvendigt for at nå de kontrolmål der er anført I beskrivelsen, er identificeret i beskrivelsen.

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

(ii) Indeholder relevante oplysninger om ændringer ved databehandlerens administrationssystem SpeedAdmin til musik- og kulturskoler, til behandling af personoplysninger, foretager pr. 21.juni 2021.

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

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og implementeret pr. 21. juni 2021. Kriterierne anvendt for at give denne udtalelse var, at

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

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

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

Sønderborg, 29. juni 2021
SpeedAdmin ApS

Torben Dueholm Rasmussen
CEO

Karsten Grau Rasmussen
CTO

Afsnit 3: Uafhængig revisors ISAE 3000 erklæring om informationssikkerhed og foranstaltninger i henhold til SpeedAdmin ApS' databehandleraftaler med kunder

Til SpeedAdmin ApS, deres kunder og disses revisorer.

Omfang

Vi har fået som opgave at afgive erklæring om a) SpeedAdmin ApS' beskrivelse af administrationssystemet SpeedAdmin til musik- og kulturskoler, i henhold til databehandleraftaler med deres kunder, i rollen som dataansvarlig pr. 21. juni 2021 og b) om udformningen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

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

SpeedAdmin ApS anvender underleverandørerne og underdatabehandlerne Microsoft, Zendesk, Unit-IT og Link Mobility. Denne erklæring omfatter ikke kontrolmål og tilknyttede kontroller hos SpeedAdmin ApS' underleverandører og underdatabehandlere.

Vores konklusion udtrykkes med høj grad af sikkerhed.

SpeedAdmin ApS' ansvar

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

Vores uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i såvel IESBA's Etiske regler som FSR – danske revisorers retningslinjer for revisors etiske adfærd (Etiske regler for revisorer), som er baseret på de grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd.

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

Revisors ansvar

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

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

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

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 af administrationssystemet SpeedAdmin til musik- og kulturskoler, samt for kontrollernes udformning. De valgte handlinger afhænger af revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke er implementeret. Vores handlinger har omfattet test af implementeringen af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev opnået.

En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, egnetheden af de heri anførte mål samt egnetheden af de kriterier, som databehandleren har specificeret og beskrevet i "Afsnit 1".

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

Begrænsninger i controller hos en databehandler

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

Konklusion

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

(a) at beskrivelsen af administrationssystemet SpeedAdmin til musik- og kulturskoler, således som dette var udformet og implementeret pr. 21 June 2021, i alle væsentlige henseender er retvisende og

(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. 21. juni 2021.

Beskrivelse af test af controller

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

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i det efterfølgende afsnit, Afsnit 4, er udelukkende tiltænkt dataansvarlige, der har anvendt SpeedAdmin ApS' administrationssystem; SpeedAdmin til musik- og kulturskoler, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen er overholdt.

København, den 29. juni 2021

REVI-IT A/S
Statsautoriseret revisionsaktieselskab

Henrik Paaske
Statsautoriseret revisor

Basel Rimon Obari
Partner, CISA, CISM

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

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

Vores test af udformningen har omfattet de kontrolmål og tilknyttede kontroller, der er udvalgt af ledelsen, og som fremgår af kontrolmålene A-I nedenfor. Vores test har omfattet de kontroller, som blev vurderet nødvendige for at kunne opnå en høj grad af sikkerhed for, at de anførte kontrolmål blev nået pr. 21. juni 2021.

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

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

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

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

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

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

Artikler og punkter markeret med fed angiver primære områder.

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

G.2	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1,** 7.5.2, 7.5.3, 7.5.4, **8.4.2,** 8.5.2, 8.5.3	13.2.1
G.3	15, 30, **44, 45,** 46, 47, 48, 49	**6.10.2.1, 7.5.1**, 7.5.2, 7.5.3, 7.5.4, 8.5.3	13.2.1
H.1	12, **13, 14,** 15, 20**,** 21	**7.3.5, 7.3.8, 7.3.9**	*Nyt område ift. ISO 27001/2*
H.2	12, **13, 14,** 15, 20**,** 21	**7.3.5, 7.3.8, 7.3.9**	*Nyt område ift. ISO 27001/2*
I.1	**33, 34**	**6.13.1.1**	16.1.1-5
I.2	**33, 34**, 39	6.4.2.2, **6.13.1.5, 6.13.1.6**	16.1.5-6
I.3	**33, 34**	**6.13.1.4**	16.1.5
I.4	**33, 34**	**6.13.1.4,** 6.13.1.6	16.1.7

Kontrolmål A – Instruks vedrørende behandling af personoplysninger

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

Nr.	*SpeedAdmin ApS' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat of test*
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks. Vi har inspiceret, at procedurer er opdateret.	Ingen afvigelser konstateret.
A.2	Databehandleren udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Vi har stikprøvevist inspiceret, at behandlinger af personoplysninger foregår i overensstemmelse med instruks.	Ingen afvigelser konstateret.
A.3	Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning.	Ingen afvigelser konstateret.

Kontrolmål B – Tekniske foranstaltninger

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

Nr.	*SpeedAdmin ApS' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat of test*
B.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der etableres aftalte sikringsforanstaltninger for behandling af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret at der foreligger formaliserede procedurer der sikrer at de aftalte sikringsforanstaltninger etableres. Vi har inspiceret, at procedurer er opdaterede.	Ingen afvigelser konstateret.
B.2	Databehandleren har foretaget en risikovurdering og på baggrund heraf implementeret de tekniske foranstaltninger, der er vurderet relevante for at opnå en passende sikkerhed, herunder etableret de med dataansvarlige aftalte sikringsforanstaltninger.	Vi har inspiceret risikovurderingen og sikret at databehandlingen er blevet vurderet. Vi har inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger.	Ingen afvigelser konstateret.
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Vi har stikprøvevist, inspiceret servere og stikprøvevist sikret at antivirus er implementeret og opdateret.	Ingen afvigelser konstateret.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Vi har stikprøvevist, inspiceret implementeringen af firewall, inklusive regler for ind- og udgående data trafik.	Ingen afvigelser konstateret.
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Vi har inspiceret netværks diagrammer og anden netværk dokumentation for at sikre passende segmentering.	Ingen afvigelser konstateret.
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Vi har inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger. Vi har stikprøvevist inspiceret, at brugeres adgange til systemer og databaser er begrænset til medarbejdernes arbejdsbetingede behov.	Ingen afvigelser konstateret.

Kontrolmål B – Tekniske foranstaltninger

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

Nr.	*SpeedAdmin ApS' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat of test*
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	Vi har inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysninger, er etableret systemovervågning med alarmering.	Ingen afvigelser konstateret.
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Vi har stikprøvevist inspiceret transmission af personoplysninger over internettet og stikprøvevist sikret at transmissionen er krypteret.	Ingen afvigelser konstateret.
B.9	Der er etableret logning i systemer, databaser og netværk. Logoplysninger er beskyttet mod manipulation og tekniske fejl og gennemgås løbende.	Vi har inspiceret politikken for logning og sikret at der er taget stilling til beskyttelse af personoplysninger. Vi har stikprøvevist inspiceret opsætning af logfiler og sikret at dette er i overensstemmelse med politikken.	Ingen afvigelser konstateret.
B.10	Personoplysninger, der anvendes til udvikling, test eller lignende, er altid i pseudonymiseret eller anonymiseret form. Anvendelse sker alene for at varetage den ansvarliges formål i henhold til aftale og på dennes vegne.	Vi har stikprøvevist inspiceret udviklingsserveren og sikret at datasæt er anonymiserede.	Ingen afvigelser konstateret.
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	Vi har stikprøvevis inspiceret penetrationstest og stikprøvevist sikret at sårbarheder bliver håndteret.	Ingen afvigelser konstateret.
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Vi har inspiceret procedure for ændringer. Vi har stikprøvevist inspiceret ændringer og stikprøvevist sikret at ændringer er i overensstemmelse med proceduren.	Ingen afvigelser konstateret.

Nr.	SpeedAdmin ApS' kontrolaktivitet	REVI-IT A/S' udførte test	Resultat of test
B.13	Der er formaliseret forretningsgang for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetinget behov.	Vi har inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Vi har stikprøvevist inspiceret, at medarbejderes adgange til systemer og databaser er godkendt, og at der er et arbejdsbetinget behov. Vi har stikprøvevist inspiceret adgange og stikprøvevist sikret at nye medarbejdere bliver allokeret i overensstemmelse med proceduren. Vi har inspiceret, at der foreligger dokumentation for regelmæssig – og mindst en gang årligt – vurdering og godkendelse af tildelte brugeradgange.	Ingen afvigelser konstateret.
B.14	Adgang til systemer og databaser, hvori der sker behandling af personoplysninger, der medfører højrisiko for de registrerede, sker som minimum ved anvendelse af to-faktor autentifikation.	Vi har stikprøvevist inspiceret, at brugernes adgang til at udføre behandling af personoplysninger, alene kan ske ved anvendelse af to-faktor autentifikation.	Ingen afvigelser konstateret.
B.15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Vi har inspiceret dokumentation for, at adgang til data behandlerens lokaler bliver evalueret.	Ingen afvigelser konstateret.

Kontrolmål C – Organisatoriske foranstaltninger

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

Nr.	*SpeedAdmin ApS' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat of test*
C.1	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. It-sikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst en gang årligt – vurdering af, om it-sikkerhedspolitikken skal opdateres.	Vi har inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Vi har sikret at persondatapolitikken er tilgængelig for de ansatte. Vi har inspiceret kontrollen af informationssikkerhedspolitikken og sikret os at denne bliver regelmæssigt opdateret.	Ingen afvigelser konstateret.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Vi har inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler.	Ingen afvigelser konstateret.
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.	Vi har inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Vi har stikprøvevist inspiceret at der er dokumentation for at relevante screeninger bliver udført.	Ingen afvigelser konstateret.
C.4	Ved ansættelse underskriver medarbejdere en fortrolighedsaftale. Endvidere bliver medarbejderen introduceret til informationssikkerhedspolitik og procedurer vedrørende databehandling samt anden relevant information i forbindelse med medarbejderens behandling af personoplysninger.	Vi har stikprøvevist inspiceret, at nyansatte medarbejdere har underskrevet en fortrolighedsaftale Vi har stikprøvevist, inspiceret at nyansatte medarbejdere bliver introduceret til de relevante procedurer og politikker.	Ingen afvigelser konstateret.

Kontrolmål C – Organisatoriske foranstaltninger

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

Nr.	*SpeedAdmin ApS' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat of test*
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Vi har inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages Vi har stikprøvevist inspiceret, at rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget for fratrådte medarbejdere.	Ingen afvigelser konstateret.
C.6	Ved fratrædelse orienteres medarbejderen om, at den underskrevne fortrolighedsaftale fortsat er gældende, samt at medarbejderen er underlagt en generel tavshedspligt i relation til behandling af personoplysninger, databehandleren udfører for de dataansvarlige.	Vi har stikprøvevist inspiceret at fratrådte medarbejdere gøres opmærksom på deres generelle tavshedspligt.	Ingen afvigelser konstateret.
C.7	Der gennemføres løbende awareness-træning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Vi har inspiceret, at databehandleren udbyder awareness træning til medarbejderne omfattende generel it-sikkerhed og behandlingssikkerhed i relation til personoplysninger.	Ingen afvigelser konstateret.
C.8	Databehandleren har vurderet behovet for en DPO, og har sikret, at DPO'en har tilstrækkelig faglighed til at udføre sine opgaver, samt at DPO'en bliver inddraget i relevante områder.	Vi har stikprøvevist inspiceret kontroller og procedurer der sikrer at DPO'en bliver inddraget.	Ingen afvigelser konstateret.
C.9	Der foreligger hos databehandleren en fortegnelse over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige.	Vi har inspiceret fortegnelsen over behandlinger og sikret at den indeholder relevante oplysninger. Vi har inspiceret at behandlingskategorierne er blevet opdateret og godkendt af ledelsen.	Ingen afvigelser konstateret.

Kontrolmål D -Tilbagelevering og sletning af personoplysninger

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

Nr.	*SpeedAdmin ApS' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat of test*
D.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der foretages opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.	Vi har inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Vi har inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
D.2	Der er aftalt specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.	Vi har stikprøvevist inspiceret nye databehandleraftaler og sikret at der er taget stilling til opbevaringsperioder og sletterutiner.	Ingen afvigelser konstateret.
D.3	Ved ophør af behandling af personoplysninger for den dataansvarlige er data i henhold til aftalen med den dataansvarlige: • Tilbageleveret til den dataansvarlige og/eller • Slettet, hvor det ikke er i modstrid med anden lovgivning.	Vi har inspiceret, at der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger. Vi har stikprøvevist inspiceret, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført for ophørte databehandlinger.	Ingen afvigelser konstateret.

Kontrolmål E – Opbevaring af personoplysninger

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

Nr.	*SpeedAdmin ApS' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat of test*
E.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne. Vi har inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Vi har stikprøvevist inspiceret databehandleraftaler og stikprøvevist sikret at personoplysninger kun opbevares på godkendte lokaliteter.	Ingen afvigelser konstateret.

Kontrolmål F – Anvendelse af underdatabehandlere

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

Nr.	*SpeedAdmin ApS' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat of test*
F.1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks. Vi har inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Vi har stikprøvevist inspiceret databehandlingsaftaler og sikret at behandleren enten har en generel, eller specifik tilladelse til at bruge underdatabehandlere.	Ingen afvigelser konstateret.
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underretters den dataansvarlige rettidigt i forhold til at kunne gøre indsigelse gældende og/eller trække persondata tilbage fra databehandleren. Ved ændringer i anvendelse af specifikt godkendte underdatabehandlere er dette godkendt af den dataansvarlige.	Vi har inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere.	Ingen afvigelser konstateret.
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Vi har stikprøvevist inspiceret databehandleraftaler med nye underdatabehandlere og stikprøvevist sikret at underdatabehandleren er underlagt den samme eller lignende forpligtelser som den dataansvarlige.	Ingen afvigelser konstateret.
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere.	Vi har inspiceret listen over underdatabehandlere og sikret at alle relevante underdatabehandlere fremgår af listen.	Ingen afvigelser konstateret.

Kontrolmål F – Anvendelse af underdatabehandlere

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

Nr.	*SpeedAdmin ApS' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat of test*
F.6	Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende. Den dataansvarlige orienteres om den opfølgning, der er foretaget hos underdatabehandleren.	Vi har stikprøvevist inspiceret at databehandleren har vurderet underdatabehandleren og har indsamlet relevant materiale.	Ingen afvigelser konstateret.

Kontrolmål G – Overførsel af personoplysninger til tredjelande

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

Nr.	*SpeedAdmin ApS' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat of test*
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelande eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag.	Vi har stikprøvevist inspiceret tilfældigt udvalgte databehandleraftaler og sikret at der er taget stilling til overførsel til tredjelande. Vi har inspiceret lokation for opbevaring af data. Vi har forespurgt om overførsel af data til tredjelande.	Vi er blevet oplyst at data behandleren ikke overfører personoplysninger til tredjelande og vi finder dette sandsynligt, baseret på vores udførte tests. Ingen afvigelser konstateret.
G.2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	Vi har stikprøvevist inspiceret tilfældigt udvalgte databehandleraftaler og sikret at der er taget stilling til overførsel til tredjelande. Vi har inspiceret lokation for opbevaring af data. Vi har forespurgt om overførsel af data til tredjelande.	Vi er blevet oplyst at data behandleren ikke overfører personoplysninger til tredjelande og vi finder dette sandsynligt, baseret på vores udførte tests. Ingen afvigelser konstateret.
G.3	Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	Vi har stikprøvevist inspiceret tilfældigt udvalgte databehandleraftaler og sikret at der er taget stilling til overførsel til tredjelande. Vi har inspiceret lokation for opbevaring af data. Vi har forespurgt om overførsel af data til tredjelande.	Vi er blevet oplyst at data behandleren ikke overfører personoplysninger til tredjelande og vi finder dette sandsynligt, baseret på vores udførte tests. Ingen afvigelser konstateret.

Kontrolmål H – De registreredes rettigheder

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

Nr.	*SpeedAdmin ApS' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat of test*
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder. Vi har inspiceret, at procedurerne er opdateret.	Ingen afvigelser konstateret.
H.2	Databehandleren har etableret procedurer, som i det omfang, dette er aftalt, muliggør en rettidig bistand til den dataansvarlige i relation til udlevering, rettelse, sletning eller begrænsning af og oplysning om behandling af personoplysninger til den registrerede.	Vi har forespurgt om, hvorvidt der har været forespørgsler. Vi har stikprøvevist inspiceret teknisk dokumentation for at forespørgsler kan behandles.	Vi er blevet informeret om at der ikke har været nogle forespørgsler og vi har derfor ikke kunnet teste implementeringen af data behandlerens procedurer. Ingen afvigelser konstateret.

Kontrolmål I – Håndtering af persondatasikkerhedsbrud

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

Nr.	*SpeedAdmin ApS' kontrolaktivitet*	*REVI-IT A/S' udførte test*	*Resultat of test*
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden. Der foretages løbende – og mindst en gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret, at der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden. Vi har inspiceret, at proceduren er opdateret.	Ingen afvigelser konstateret.
I.2	Databehandleren har etableret kontroller for identifikation af eventuelle brud på persondatasikkerheden.	Vi har inspiceret, at databehandler udbyder awareness-træning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden.	Ingen afvigelser konstateret.
I.3	Databehandleren har ved eventuelle brud på persondatasikkerheden underrettet den dataansvarlige uden unødig forsinkelse efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Vi har inspiceret, at databehandleren har en oversigt over sikkerhedshændelser med angivelse af, om den enkelte hændelse har medført brud på persondatasikkerheden. Vi har forespurgt om brud på persondatasikkerheden.	Vi er blevet oplyst at der ikke har være brud på persondatasikkerheden og vi har derfor ikke kunnet teste implementeringen af databehandlerens procedurer. Ingen afvigelser konstateret.
I.4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet: • Karakteren af bruddet på persondatasikkerheden • Sandsynlige konsekvenser af bruddet på persondatasikkerheden • Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden	Vi har inspiceret procedure og sikret at der er etableret bistand til den dataansvarlige.	Ingen afvigelser konstateret.