

Erklæring fra uafhængig revisor

Erklæringsafgivelse i forbindelse med overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov i rollen som databehandler for perioden 21-06-2019 til 31-05-2020

ISAE 3000

SpeedAdmin ApS

CVR-nr.: 34 59 01 76

Juni 2020

Indholdsfortegnelse

Afsnit 1:	SpeedAdmin ApS' udtalelse.....	1
Afsnit 2:	SpeedAdmin ApS' kontrolbeskrivelse ISAE 3000	3
Afsnit 3:	Uafhængig revisors erklæring om overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov i rollen som databehandler for perioden 21-06-2019 til 31-05-2020.....	7
Afsnit 4:	Kontrolmål, udførte kontroller, test og resultater heraf	9

Afsnit 1: SpeedAdmin ApS' udtalelse

Medfølgende beskrivelse er udarbejdet til brug for en bred kreds af dataansvarlige, der har anvendt SpeedAdmin, 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 bekræfter, at:

- a) Den medfølgende beskrivelse, afsnit 2, giver en retvisende beskrivelse af SpeedAdmin, der har behandlet personoplysninger for dataansvarlige omfattet af databeskyttelsesforordningen i hele perioden fra 21-06-2019 til 31-05-2020. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:
- (i) Redegør for, hvordan SpeedAdmin 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 SpeedAdmins 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 SpeedAdmin til behandling af personoplysninger foretaget i perioden fra 21-06-2019 til 31-05-2020
- (iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af den beskrevne SpeedAdmin 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 SpeedAdmin, som den enkelte dataansvarlige måtte anse vigtigt efter deres særlige forhold.
- b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 21-06-2019 til 31-05-2020. Kriterierne anvendt for at give denne udtalelse var, at:
- (i) De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret
- (ii) De identificerede kontroller ville, hvis udført som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål, og
- (iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 21-06-2019 til 31-05-2020.
- c) Der er etableret og opretholdt passende tekniske og organisatoriske foranstaltninger med henblik på at opfylde aftalerne med de dataansvarlige, god databehandleriskik og relevante krav til databehandlere i henhold til databeskyttelsesforordningen.

Sønderborg, 29. juni 2020



Torben Dueholm Rasmussen

Co-founder



Karsten G. Rasmussen

Co-founder

Afsnit 2: SpeedAdmin ApS' kontrolbeskrivelse ISAE 3000

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 udføre de 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 downloade 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 dataansvarlig foregår udelukkende kun efter den dataansvarliges instrukser. Databehandleren anvender ikke personoplysningerne til andre formål end de som er beskrevet i dataansvarliges instrukser.

Personoplysninger

- CPR-nummer (DK) og personnummer (NO og 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, de forskellige årlige revisioner, der foretages internt i SpeedAdmin.

Alle SpeedAdmins medarbejdere er orienteret om persondata og informationssikkerhed. Der bliver årligt holdt intern security awareness training 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 gjort på elever, værgere 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 databehandlaftaler, 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 medarbejders brugeradgange. Vi har en oversigt over alle medarbejders brugeradgange og opdaterer den, når der sker ændringer.

Proceduregennemgang

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 training dag, skal alle medarbejdere slette mails og diverse dokumenter, som indeholder personoplysninger.

Procedurer – adgangsstyring

Det er SpeedAdmins ledelse der står for beslutningen 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'er 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 gør 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 intern log.

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 "blot" 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 fokuset 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.

Væsentlige ændringer i perioden

Vi er gået fra at benytte Gmail til at benytte Microsoft Outlook. Ellers ingen væsentlige ændringer.

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 ansvarlige for at få dem slettet.
- De Dataansvarlige skal være obs. 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 3: Uafhængig revisors erklæring om overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov i rollen som databehandler for perioden 21-06-2019 til 31-05-2020

Til SpeedAdmin ApS, selskabets kunder i deres rolle som dataansvarlige og disses revisorer.

Vi har efter aftale undersøgt SpeedAdmin ApS' overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov for perioden 21-06-2019 til 31-05-2020.

Erklæringen er alene udarbejdet til brug for SpeedAdmin ApS, selskabets kunder i rollen som dataansvarlige og disses revisorer til vurdering af de tilrettelagte forretningsgange, og kan ikke anvendes til andre formål.

Ledelsens ansvar

Ledelsen i SpeedAdmin ApS har ansvaret for at implementere og sikre opretholdelsen af forretningsgange som krævet af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov.

Revisors ansvar

Det er vores ansvar, på grundlag af det udførte arbejde, at udtrykke en konklusion om, hvorvidt selskabet overholder de krav, der er nævnt i databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov.

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 vores konklusion.

REVI-IT A/S er underlagt international standard om kvalitetsstyring, ISQC 1, og anvender således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende krav i lov og øvrig regulering.

Vi har overholdt kravene til uafhængighed og andre etiske krav i FSR – danske revisors retningslinjer for revisors etiske adfærd (Ethiske regler for revisorer), der bygger på de grundlæggende principper om integritet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

Vores arbejde har omfattet forespørgsler, observationer samt vurdering og stikprøvevis undersøgelse af den information, vi har modtaget.

På grund af begrænsninger i ethvert kontrolsystem kan der opstå fejl eller besvigelser, som ikke afdækkes af vort arbejde. Endvidere vil en anvendelse af vor konklusion på efterfølgende perioders transaktioner være undergivet en risiko for, at der foretages ændringer af systemer eller kontroller, ændring i kravene til behandling af oplysninger eller i selskabets overholdelse af de beskrevne politikker og procedurer, hvorved vores konklusion eventuelt ikke længere vil være gældende.

Begrænsninger i kontroller 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 SpeedAdmin, 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

Denne konklusion er udformet på grundlag af forståelsen af de kriterier, som der er redegjort for i erklæringens indledende afsnit, og som bygger på kravene i databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov.

Det er vores opfattelse, at SpeedAdmin ApS, i alle væsentlige henseender, lever op til ovennævnte kriterier for perioden 21-06-2019 til 31-05-2020

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt SpeedAdmin ApS' kunder, der har anvendt SpeedAdmin ApS' SpeedAdmin, i kundernes rolle som dataansvarlig, og de revisorer, som har tilstrækkelig forståelse til at vurdere den medfølgende beskrivelse sammen med anden information, herunder information om kontroller, som de dataansvarlige selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov er overholdt.

København, 29. juni 2020

REVI-IT A/S

Statsautoriseret revisionsaktieselskab



Henrik Paaske

Statsautoriseret revisor



Basel Obari

IT-revisor, CISA, CISM, Partner

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

Den følgende oversigt er udformet for at skabe et overblik over de kontroller, som SpeedAdmin ApS har implementeret i henhold til overholdelse af databeskyttelsesforordningen (GDPR) og tilhørende databeskyttelseslov. Vores test af design og implementering af kontroller har omfattet de kontroller, som vi har vurderet nødvendige for at kunne opnå en høj grad af sikkerhed for, at de anførte artikler for perioden 21-06-2019 til 31-05-2020 er efterlevet.

De krav, som fremgår direkte af forordningen eller loven, kan ikke fraviges. Derimod kan der justeres på, hvordan sikkerheden implementeres, da sikkerhedskravene i forordningen på flere punkter er af mere generel og overordnet karakter, som bl.a. skal tage hensyn til formål, behandlingens karakter, kategorien af personoplysninger mv. Herudover kan der være konkrete krav i de enkelte kundekontrakter, der kan have en rækkevidde, der går ud over databeskyttelseslovens almindelige krav. Disse er i givet fald ikke omfattet af nedenstående.

Kontroller udført hos SpeedAdmin ApS' kunder er herudover ikke omfattet af vores erklæring, idet kundernes egne revisorer må foretage denne gennemgang og vurdering.

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

Metode	Overordnet beskrivelse
Forespørgsel	Forespørgsel af udvalgt personale hos virksomheden angående kontroller
Observation	Observation af, hvordan kontroller udføres
Inspektion	Gennemgang og stillingtagen til politikker, procedurer og dokumentation vedrørende kontrollers udførelse
Genudførelse af kontrol	Vi har selv genudført kontroller med henblik på at verificere, at kontrollen fungerer som forventet

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.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
A.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Vi har inspiceret informationsikkerhedspolitik, og påset, at der er taget stilling til, at behandling af personoplysninger alene må foretages efter instruks.</p> <p>Vi har inspiceret, at procedurer er opdaterede i perioden.</p> <p>Vi har stikprøvevis inspiceret nye databehandleraftaler, og påset, at der er beskrevet et krav om instruks.</p>	Ingen afvigelser konstateret.
A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Vi har stikprøvevis inspiceret databehandleraftaler, og påset at databehandleren overholder instruksen i disse.	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 forespurgt til, om der har været ulovlige instrukser i perioden.	<p>Vi er blevet oplyst, at der ikke har været ulovlige instrukser i perioden, hvorfor vi ikke kan teste effektiviteten af kontrollen.</p> <p>Ingen afvigelser konstateret i øvrigt.</p>

Kontrolmål B – Tekniske foranstaltninger

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

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors 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.	Vi har inspiceret informationssikkerhedspolitikken, og påset, at der er taget stilling til, at der skal etableres aftalte sikringsforanstaltninger for behandling af persondata. Vi har inspiceret ved en stikprøve på 4 databehandleraftaler, at der er etableret de aftalte sikringsforanstaltninger.	Ingen afvigelse 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 påset, at den tager udgangspunkt i de registreredes rettigheder. Vi har inspiceret risikovurderingen, og påset, at denne er blevet opdateret i perioden.	Ingen afvigelser konstateret.
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, er implementeret beskyttelse mod malware, som løbende opdateres.	Vi har stikprøvevis inspiceret implementering af beskyttelse mod malware, og påset, at disse er korrekt konfigureret og løbende bliver opdateret.	Ingen afvigelser konstateret.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Vi har stikprøvevis inspiceret implementering af firewall, herunder reglerne for in-/outbound regler. Vi har inspiceret erklæring fra driftsleverandør, og påset, at de har opstillet firewalls.	Ingen afvigelser konstateret.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B.5	Interne netværk er segmenteret for at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger.	Vi har inspiceret oversigt over netværk, og påset, at miljøer er adskilt. Vi har inspiceret erklæring fra driftsleverandør, og påset, at netværket er tilstrækkeligt segmenteret.	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 stikprøvevis inspiceret rettigheder for nye medarbejdere i perioden, og påset, at disse har et arbejdsbetinget behov for adgang.	Ingen afvigelser konstateret.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	Vi har stikprøvevis inspiceret overvågning af kapacitet, og påset, at dette gøres løbende.	Ingen afvigelser konstateret.
B.8	Der anvendes effektiv kryptering ved transmission af personoplysninger via internettet og med e-mail.	Vi har inspiceret politikken for kryptering, og påset, at denne tager stilling til transmission af personoplysninger. Vi har stikprøvevis inspiceret SSL-certifikater, og påset, at disse er korrekt konfigureret.	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 påset, at der er taget stilling til beskyttelse af personoplysninger. Vi har stikprøvevis inspiceret opsætning af logning på systemer, og påset, at dette stemmer i overens med politikken. Vi har stikprøvevis inspiceret adgang til logfiler, og påset, at adgangen er begrænset til et arbejdsbetinget behov.	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 stikprøvevis inspiceret udviklingsserveren, og påset, at datasættet er anonymiseret.	Ingen afvigelser konstateret.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrations-tests.	Vi har forespurgt til, formaliserede procedurer for løbende tests af tekniske foranstaltninger. Vi har inspiceret erklæring fra driftsleverandør, og påset, at der er løbende patching af operativsystemer.	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 proceduren for ændringer, og påset, der bliver taget hensyn til registreredes rettigheder. Vi har stikprøvevis inspiceret ændringer i perioden, og påset, at dette er sket i overensstemmelse med proceduren.	Ingen afvigelser konstateret.
B.13	Der er formaliseret forretningsgange for tildeling og afbrydelse af brugeradgange til personoplysninger. Brugeres adgang revurderes regelmæssigt, herunder at rettigheder fortsat kan begrundes i et arbejdsbetiget 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 stikprøvevis inspiceret adgange, og påset, at nye medarbejdere har fået tildelt adgange efter proceduren. Vi har stikprøvevis inspiceret adgange, og påset, at fratrådte medarbejdere har fået frataget adgange efter proceduren. Vi har inspiceret, at der foreligger dokumentation for regelmæssig – som minimum årlig – 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 forespurgt til, om virksomhedens anvender tofaktor autentifikation.	Vi er blevet informeret om at SpeedAdmin ikke behandler følsomme personoplysninger, hvorfor SpeedAdmin har valgt ikke at anvende to-faktor autentifikation. Vi har dog påset, at der anvendes VPN ved oprettelse af forbindelse til interne netværk. Ingen afvigelser konstateret i øvrigt.
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 politikken for fysisk sikring, og påset, at der er taget stilling til den fysiske sikkerhed. Vi har inspiceret erklæring fra driftsleverandør, og påset, at der er etableret fysisk sikring af servere.	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.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
C.1	Databehandlerens ledelse har godkendt en skriftlig informationssikkerhedspolitik, som er kommunikeret til alle relevante interessenter, herunder databehandlerens medarbejdere. Informationssikkerhedspolitikken tager udgangspunkt i den gennemførte risikovurdering. Der foretages løbende – og mindst én 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 perioden. Vi har påset, at informationssikkerhedspolitikken er tilgængelig for medarbejderne. Vi har inspiceret kontrollen af informationssikkerhedspolitikken, og påset, at denne bliver løbende vurderet.	Ingen afvigelser konstateret.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Vi har stikprøvevis inspiceret databehandleraftaler, og påset, at informationssikkerhedspolitikken er i overensstemmelse med aftalerne.	Ingen afvigelser konstateret.
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse.	Vi har stikprøvevis inspiceret nye ansættelser, og påset, at ansættelsen har fulgt proceduren for ansættelse.	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 stikprøvevis inspiceret ansættelsesaftaler på nye medarbejdere i perioden, og påset, at de har forpligtet sig til fortrolighed. Vi har stikprøvevis inspiceret erklæringer, underskrevet af nye medarbejdere i perioden, og påset, at de har bekræftet at have læst virksomhedens politikker og procedurer.	Ingen afvigelser konstateret.
C.5	Ved fratrædelse er der hos databehandleren implementeret en proces, som sikrer, at brugerens rettigheder bliver inaktive eller ophører, herunder at aktiver inddrages.	Vi har inspiceret procedurer, der sikrer, at fratrædte medarbejders rettigheder deaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages. Vi har stikprøvevis inspiceret lukning af adgange og tilbagelevering af aktiver på tidligere ansatte, og påset, at dette er sket i overensstemmelse med proceduren.	Ingen afvigelse konstateret.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
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 stikprøvevis inspiceret fortrolighedsaftaler, og påset, at disse også er gældende efter fratrædelsen.	Ingen afvigelser konstateret.
C.7	Der gennemføres løbende awarenessstræning af databehandlerens medarbejdere i relation til it-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Vi har stikprøvevis inspiceret materiale fra awarenessstræning i perioden, og påset, at dette relaterer sig til it-sikkerhed.	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 og bliver inddraget i relevante områder.	Vi har stikprøvevis inspiceret kontroller og procedurer, og påset, at databeskyttelsesrådgiveren har været indblandet.	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.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors 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 informationsikkerhedspolitikken, og påset, at der er taget stilling til, at sletning sker i overensstemmelse med aftaler. Vi har inspiceret proceduren for sletning, og påset, at denne er blevet opdateret i perioden. Vi har inspiceret kontrollen af proceduren, og påset, at proceduren bliver løbende opdateret.	Ingen afvigelser konstateret.
D.2	Der er aftalt krav til databehandlerens opbevaringsperioder og sletterutiner.	Vi har stikprøvevis inspiceret nye databehandleraftaler, og påset, 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: <ul style="list-style-type: none">) 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 inspiceret ved en stikprøve på én ophørt databehandling i erklæringsperioden, at der er dokumentation for, at den aftalte sletning eller tilbagelevering af data er udført.	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.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
E.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at der alene foretages opbevaring af personoplysninger i overensstemmelse med aftalen med den dataansvarlige.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Vi har inspiceret informations sikkerhedspolitikken, og vi har påset, at der er taget stilling til opbevaring af data.</p> <p>Vi har inspiceret politikken, og påset, at denne er opdateret i perioden.</p>	Ingen afvigelser konstateret.
E.2	Databehandlerens databehandling inklusive opbevaring må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	<p>Vi har inspiceret databehandleraftaler, og påset, at lokationen for opbevaring er i overensstemmelse med aftalerne.</p> <p>Vi har inspiceret oversigten over backups i perioden, og stikprøvevis påset, at disse er korrekt konfigureret.</p>	<p>Vi har observeret, at backup ikke har været konfigureret efter databehandlerens politik i perioden. Vi har efterfølgende modtaget dokumentation for, at dette er blevet rettet.</p> <p>Ingen afvigelser konstateret i øvrigt.</p>

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.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
F.1	<p>Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instrukser.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Vi har inspiceret politikken for krav til underleverandører, og påset, at der er taget stilling til underdatabehandleraftaler.</p> <p>Vi har inspiceret, at politikken er opdateret i perioden.</p>	Ingen afvigelser konstateret.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Vi har stikprøvevis inspiceret nye databehandleraftaler i perioden, og påset, at databehandleren enten har generel eller specifik tilladelse til anvendelse af underdatabehandlere.	Ingen afvigelser konstateret.
F.3	Ved ændringer i anvendelsen af generelt godkendte underdatabehandlere underrettes 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 forespurgt til, om der har været ændringer af underdatabehandlere i perioden, og vi har stikprøvevis inspiceret underretning af dataansvarlige.	Ingen afvigelser konstateret.
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen eller lignende med den dataansvarlige.	Vi har inspiceret databehandleraftaler med nye underdatabehandleraftaler, og påset, at underdatabehandleren er forpligtet til samme eller tilsvarende databeskyttelsesforpligtelser.	Ingen afvigelser konstateret.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere.	Vi har inspiceret listen over underdatabehandlere, og påset, at relevante underdatabehandlere fremgår.	Ingen afvigelser konstateret.
F.6	Databehandleren foretager, på baggrund af ajourført risikovurdering af den enkelte underdatabehandler og den aktivitet, der foregår hos denne, en løbende opfølgning herpå ved møder, inspektioner, gennemgang af revisionserklæring eller lignende.	Vi har stikprøvevis inspiceret løbende tilsyn af underdatabehandlere, og påset, at dette er sket i overensstemmelse med proceduren.	Ingen afvigelser konstateret.

Kontrolmål G – Overførsel af personoplysninger til tredjelände

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

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
G.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren alene overfører personoplysninger til tredjelände eller internationale organisationer i overensstemmelse med aftalen med den dataansvarlige på baggrund af et gyldigt overførselsgrundlag. Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.	Vi har inspiceret skriftlig procedure, som indeholder krav om, at personoplysninger ikke må overføres til tredjelände uden instruks fra den dataansvarlige. Vi har inspiceret dokumentation for, at proceduren er blevet opdateret i perioden.	Vi er blevet informeret og har observeret at data ikke overføres til tredjelände, hvorfor kontrollen ikke vurderes relevant. Ingen afvigelser konstateret.
G.2	Databehandleren må kun overføre personoplysninger til tredjelände eller internationale organisationer efter instruks fra den dataansvarlige.	Vi har stikprøvevis inspiceret databehandleraftaler på nye dataansvarlige perioden for instruks om tredjeländsoverførsel, og påset, at der er taget stilling til tredjeländsoverførsler.	Ingen afvigelser konstateret.
G.3	Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelände eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	Vi har stikprøvevis inspiceret databehandleraftaler på nye dataansvarlige i perioden for instruks om tredjeländsoverførselse.	Vi er blevet informeret og har observeret at data ikke overføres til tredjelände, hvorfor kontrollen ikke vurderes relevant. 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.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
H.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Vi har inspiceret proceduren for håndtering af anmodninger, og påset, at der er taget stilling til bi-stand til den dataansvarlige.</p> <p>Vi har inspiceret proceduren, og påset, at denne er blevet opdateret i perioden.</p>	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 stikprøvevis inspiceret anmodninger i perioden, og påset, at disse er blevet håndteret efter proceduren.	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.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
I.1	<p>Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden.</p> <p>Der foretages løbende – og mindst én gang årligt – vurdering af, om procedurerne skal opdateres.</p>	<p>Vi har inspiceret proceduren for brud på persondatasikkerheden, og påset, at der er taget stilling til underrettelse af den dataansvarlige i forbindelse med brud.</p> <p>Vi har inspiceret proceduren og påset, at denne er blevet opdateret i perioden.</p> <p>Vi har inspiceret kontroller, og påset, at sikkerhedsbrud bliver løbende gennemgået.</p>	Ingen afvigelser konstateret.
I.2	Databehandleren har etableret kontroller for identifikation af eventuelle brud på persondatasikkerheden:	Vi har inspiceret, at databehandler udbyder awarenessstræning 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 unødigt forsinkelse efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en underdatabehandler.	Vi har inspiceret loggen over sikkerhedsbrud i perioden.	<p>Vi har observeret at der ikke har været konstateret sikkerhedsbrud i revisionsperioden, hvorfor vi ikke har kunne teste effektiviteten af proceduren.</p> <p>Ingen afvigelser konstateret i øvrigt.</p>
I.4	Databehandleren har etableret procedurer for bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet.	Vi har inspiceret proceduren, og påset, at der er etableret bistand til den dataansvarlige.	<p>Vi har observeret at der ikke har været konstateret sikkerhedsbrud i revisionsperioden, hvorfor vi ikke har kunnet teste effektiviteten af proceduren.</p> <p>Ingen afvigelser konstateret i øvrigt.</p>

Kontrolmål J – Betingelser for samtykke og oplysningspligt

Der efterleves procedurer og kontroller, som sikrer, at de registrerede har givet skriftligt samtykke til behandling af personoplysninger, og hvori det sikres, at den registrerede har modtaget den dataansvarliges kontaktoplysninger, oplysning om formål med behandling af personoplysningerne samt anden information, der er nødvendig for opfyldelse af oplysningspligten.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
J.1	Der foreligger skriftlige procedurer for indhentelse af skriftligt samtykke til behandling af personoplysninger.	Vi har forespurgt til håndtering af samtykke og oplysningspligt.	Vi har fået oplyst, at virksomheden ikke indhenter samtykke fra de registrerede i forbindelse med de reviderede ydelser, hvorfor punktet ikke er relevant. Ingen afvigelser konstateret i øvrigt.

Kontrolmål K – Fortegnelse over behandlingsaktiviteter

Der efterleves procedurer og kontroller, som sikrer, at databehandleren fører en fortegnelse over kategorier af behandlingsaktiviteter, der foretages på vegne af de dataansvarlige.

Nr.	Databehandlerens kontrolaktivitet	Revisors udførte test	Resultat af revisors test
K.1	Der foreligger hos databehandleren en fortegnelse over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige.	Vi har inspiceret fortegnelsen, og påset, at den lever op til kravene i forordningen.	Ingen afvigelser konstateret.
K.2	Der foretages løbende – og mindst én gang årligt – vurdering af, hvorvidt fortegnelsen over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige skal opdateres.	Vi har inspiceret fortegnelsen, og påset, at denne er blevet opdateret i perioden.	Ingen afvigelser konstateret.
K.3	Ledelsen har sikret, at fortegnelsen over kategorier af behandlingsaktiviteter for de enkelte dataansvarlige er fyldestgørende, opdateret og korrekt.	Vi har inspiceret fortegnelsen, og påset, at ledelsen har godkendt fortegnelsen.	Ingen afvigelser konstateret.