Experian A/S

Uafhængig revisors ISAE 3000-erklæring med sikkerhed om kontroller rettet mod databeskyttelse og behandling af personoplysninger på vegne af Experians kunder pr. 16. december 2025

Indhold

1	Ledelsens udtalelse	2
2	Uafhængig revisors ISAE 3000-erklæring med sikkerhed om kontroller rettet mod databeskyttelse og behandling af personoplysninger på vegne af Experians kunder	4
3	Beskrivelse	7
4	Kontrolmål, kontrolaktivitet, test og resultat heraf	10

1 Ledelsens udtalelse

Experian A/S (Experian) varetager databehandling af personoplysninger på vegne af Experians kunder, der er dataansvarlige i henhold til EU's forordning om *"Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger"* (herefter "databeskyttelsesforordningen") og *"Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger"* (herefter "databeskyttelsesloven").

Medfølgende beskrivelse i afsnit 4 af kontrolmål og kontrolaktiviteter relateret til behandling af personoplysninger på vegne af Experians kunder, som har indgået en standard databehandleraftale, er udarbejdet til brug for Experians kunder, der er dataansvarlige, som forudsættes at have en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som Experians kunder selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen og databeskyttelsesloven er overholdt.

Experian bekræfter, at:

1. Den medfølgende beskrivelse i afsnit 4 af kontrolmål og kontrolaktiviteter giver en retvisende beskrivelse af kontrolmål og kontrolaktiviteter relateret til behandling af personoplysninger, der er omfattet af databeskyttelsesforordningen og databeskyttelsesloven, og som er udført på vegne af Experians kunder pr. 16. december 2025.

    1.1 Redegør for, hvordan behandling af personoplysninger var udformet og implementeret, herunder redegør for:

    - i) De typer af ydelser, der er leveret, herunder typen af behandlede personoplysninger.
    - ii) 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.
    - iii) De processer, der er anvendt for at sikre, at den foretagne databehandling er sket i henhold til kontrakt, instruks eller aftale med den dataansvarlige.
    - iv) 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.
    - v) 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.
    - vi) De processer, der i tilfælde af brud på persondatasikkerheden understøtter, at den dataansvarlige kan foretage anmeldelse til tilsynsmyndigheden samt underrettelse til de registrerede.
    - vii) 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.
    - viii) Kontroller, som vi med henvisning til behandling af personoplysninger i Experians systems 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.
    - ix) Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen af personoplysninger.

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

2. De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse i afsnit 4, var hensigtsmæssigt udformet og implementeret pr. 16. december 2025. Kriterierne anvendt for at give denne udtalelse var, at

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

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

3. Der er etableret og opretholdt passende tekniske og organisatoriske foranstaltninger med henblik på at opfylde databehandleraftalerne med Experians kunder og relevante krav til databehandlere i henhold til databeskyttelsesforordningen og databeskyttelsesloven.

København, 2. marts 2026
Experian A/S

Andrew Rich
Country Managing Director, Northern Europe

2 Uafhængig revisors ISAE 3000-erklæring med sikkerhed om kontroller rettet mod databeskyttelse og behandling af personoplysninger på vegne af Experians kunder

Til ledelsen i Experian A/S og Experians kunder, som har indgået en databehandleraftale med Experian

Omfang

Vi har fået som opgave at afgive erklæring om Experians beskrivelse i afsnit 4 af kontrolmål og kontrolaktiviteter relateret til behandling af personoplysninger, der er omfattet af EU's forordning om *"Beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger"* (herefter “databeskyttelsesforordningen") og *"Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger"* (herefter "databeskyttelsesloven"), og som er udført på vegne af Experians kunder pr. 16. december 2025, og om udformningen og implementeringen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Experian anvender underleverandørerne Experian Ltd. og Experian Bulgaria. Beskrivelsen i sektion 3 medtager kun kontrolmål og relaterede kontroller hos Experian og medtager således ikke kontrolmål og relaterede kontroller hos underleverandørerne. Visse kontrolmål kan kun nås, hvis underleverandørens kontroller, der forudsættes i designet af Experians kontroller, er passende designet og implemenret sammen med de relaterede kontroller hos Experian. Vores handlinger har ikke omfattet kontrolaktiviteter udført af overstående underleverandører, og vi har ikke vurderet egnetheden af udformning og implementering af kontrolaktiviteter hos underleverandørerne.

Erklæringen dækker ikke IT-systemer, hvor der er delt adgang med Experians kunder, da Experian ikke kan kontrollere sikkerhedsforanstaltninger, der er rettet mod Experians kunders brugere.

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

Experians ansvar

Experian er ansvarlig for udarbejdelsen af beskrivelsen af kontrolmål og kontrolaktiviteter relateret til behandlingen af personoplysninger samt for at udforme og implementere af udføre 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 samt FSR – danske revisorers retningslinjer for revisors etiske adfærd (Etiske regler for revisorer), der bygger på de grundlæggende principper om integritet, objektivitet, faglig kompetence og fornøden omhu, fortrolighed og professionel adfærd.

KPMG er underlagt international standard om kvalitetsstyring, ISQM 1, og anvender og opretholder således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og krav ifølge lov og øvrig regulering.

Vores ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Experians beskrivelse af kontrolmål og kontrolaktiviteter relateret til behandlingen af personoplysninger samt om udformningen og implementeringen af kontroller, der knytter sig til de anførte kontrolmål.

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. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for vores konklusion.

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

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 implementeret.

En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af Experians beskrivelse af kontrolmål og kontrolaktiviteter relateret til behandlingen af personoplysninger samt egnetheden af de heri anførte kontrolmål, som databehandleren har anvendt.

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

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

Begrænsninger i kontroller hos en databehandler

Experians beskrivelse er udarbejdet for at opfylde de almindelige behov hos den dataansvarlige og omfatter derfor ikke nødvendigvis alle de aspekter ved Experians ydelser, som den dataansvarlige måtte anse for vigtige. 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 effektiviteten 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. Det er vores opfattelse, at

- Experians beskrivelse i afsnit 4 af kontrolmål og kontrolaktiviteter i alle væsentlige henseender giver en retvisende beskrivelse af kontrolmål og kontrolaktiviteter relateret til behandling af personoplysninger, der er omfattet af databeskyttelsesforordningen og databeskyttelsesloven, og som er udført på vegne af Experians kunder pr. 16. december 2025.

- kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt designet og implementeret pr. 16. december 2025.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultater af disse test fremgår af afsnit 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt Experians kunder, som forudsættes at have en tilstrækkelig forståelse til at overveje erklæringen og beskrivelsen af test af kontroller sammen med anden information, herunder information om kontroller, som Experians kunder selv har udført, ved vurdering af, om kravene i databeskyttelsesforordningen og databeskyttelsesloven er overholdt.

København, 2. marts 2026
KPMG
Statsautoriseret Revisionspartnerselskab

Christopher Pedersen
registreret revisor
mne35392

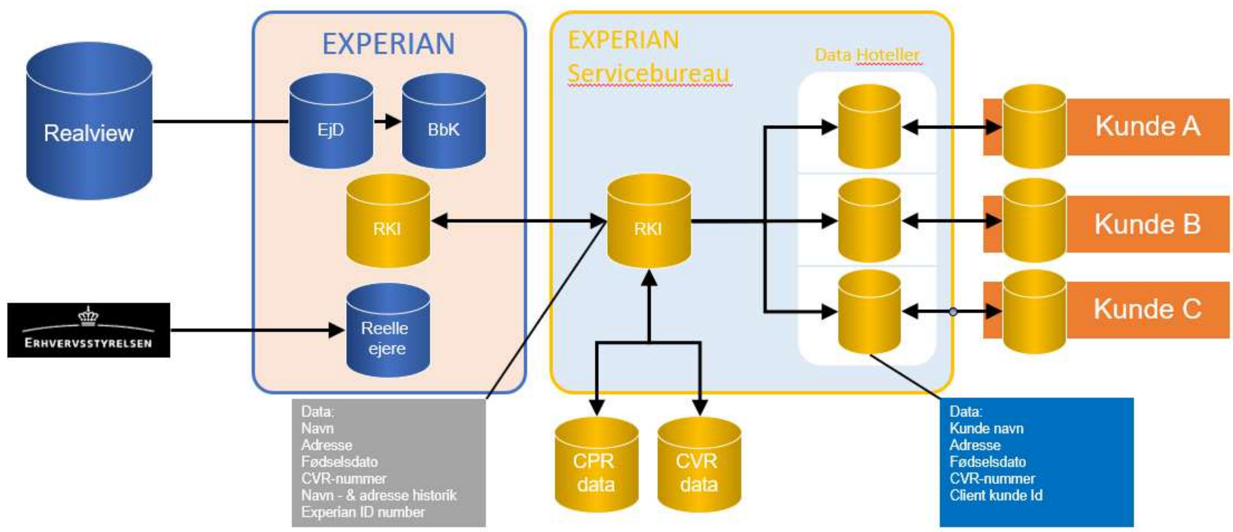
3 Beskrivelse

Formålet med databehandlerens behandling af personoplysninger på vegne af de dataansvarlige er at opbevare dataansvarliges data i forbindelse med deres overvågning igennem AKS-løsningen (Aktiv Kredit Sikring).

AKS-løsningen er bygget op omkring såkaldte Datahoteller, hvor Experians kunder lægger deres portefølje af kunder til overvågning. Hvert datahotel er specifik til den enkelte kunde, således at ingen kundedata blandes sammen. Når der sker en ændring i en person eller virksomheds data, skubbes disse nye opdaterede data ud til Experians kunder.

Data indhentes af Experian i egne databaser – f.eks. RKI-registreringer eller fra offentlige kilder – f.eks. Erhvervsstyrelsen (virksomheds- og regnskabsdata) og Statstidende eller fra andre kilder – f.eks. Realview (ejendomsdata, tingbogsoplysninger).

AKS-løsningen:



Karakteren af behandlingen

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig både om kreditoplysninger, stamoplysninger og andre offentlige data. Databehandler varetager drift og monitorering af AKS og er i forbindelse hermed ansvarlig for at sikre driften og funktionen af kontrolsystemer med henblik på at forebygge og opdage fejl, herunder bevidste fejl, med henblik på overholdelse af persondataforordning, kontrakter og god skik.

Der stilles et system til rådighed for dataansvarlige data

Data i AKS er fordelt på beskedtyper, hvor den enkelte kunde (client) kan vælge, hvilke data de vil have overvåget afhængig af kundens relation til personen / virksomheden. Er der ikke en kreditrelation, må der således ikke overvåges på kreditoplysninger. Det beskrives i kontrakten, at den dataansvarlige har ansvaret for data, der ligges på AKS. Der er følgende beskedtyper:

Beskedtype	Person	Firma	Kreditoplysning
Navneændring	√	√	
Adresseændring	√	√	
Statusændring	√	√	
Navne/adr.-beskyttelse	√		
Betalingsanmærkning (RKI)	√	√	√
Kreditadvarsel	√		√
Reklamebeskyttelse	√	√	
Værge	√		
Commercial Delphi Score		√	√
Revisorforbindelser		√	
Bankforbindelser		√	
Direktionsmedlemmer		√	
Bestyrelsesmedlemmer		√	
Ejerkoncernforhold		√	
Tegningsret		√	
Regnskab Inddateret		√	
Regnskab fysisk		√	
Regnskabsperiode		√	
Fusion		√	
Spaltning		√	
Betalingserfaringer		√	√
Pant		√	√
Opløsningsstatus		√	
Rating		√	√
Ejendomsejere	√	√	
Ejendom	√	√	
Energimærke	√	√	
Ejendomshæftelse	√	√	
Endelig Ejer / UBO		√	
Bobestyrer (Dødsbo data modtaget)	√		
Kurator (Konkursbo)		√	

Udover ovenstående behandles fødselsdato på privatpersoner samt CVR-nummer på virksomheder til brug for matching af data.

- Kategorier af registrerede personer omfattet af databehandleraftalen:
  - Privatpersoner
  - Enkeltmandsvirksomheder / Personligt ejet mindre virksomhed
  - Selskaber (A/S og ApS)
  - Øvrige virksomhedstyper.

Praktiske tiltag

For at sikre den dataansvarliges data er der implemeteret en række sikkerhedstiltag, der er baseret på ISO 27001:2022-standarden. Datacenteret er ISO 27001:2022-certificeret.

Adgang til Servicebureauet med henblik på varetagelse af systemtekniske opgaver er udelukkende udstedt til IT-medarbejdere med opgaver inden for teknisk drift, udvikling og fejlretning.

Adgang til Servicebureauet med henblik på varetagelse af opgaver i forbindelse med Servicebureauets behandling af personoplysninger, fx besvarelse af indsigtsanmodning fra de registrerede, udstedes udelukkende til medarbejderne i Experian Forbrugerservice.

Alle ansatte med adgang til data i Servicebureauet har underskrevet en udvidet NDA.

Experian har etableret kontroller i relation til databeskyttelse og behandling af persondata med afsæt i den gældende persondatalov suppleret med Experians krav fra interne sikkerhedspolitikker og interne Technical Security Baselines.

Risikovurdering

Risikovurderingen af AKS følger de politikker og regler, der er gældende for alle produkter i Experian. Det er klassificeringen af data samt adgangsmulighederne, der afgør sikkerhedsniveauet.

AKS er en integreret API-løsning hos kunderne, og data har højeste klassificeringniveau, hvilket betyder, at AKS og infrastrukturen, denne er bygget på, er omfattet af de højeste sikkerhedskrav defineret i Experian. Dette omfatter bl.a. årlig sikkerhedsgennemgang (SAQ, Security Assessment Questionnaire), som følger Experians sikkerhedspolikker og TSB'er (Technical Security Baselines), herunder penetrationtests, Veracode-skanninger (malicious code) m.v.

Kontrolforanstaltninger

Datacenter er ISO 27001:2022-certificeret, og Experian har på global plan udarbejdet foranstaltninger gennem deres politikker, som overholdes af AKS. Af væsentlige områder kan fremhæves:

1. Data krypteres under opbevaring (AES128/AES256) og under overførsel (TLS 1.2.)
2. Adgangsstyring inkl. logning og overvågning
3. BCP inkl. test
4. Backup og test
5. Login med 2-faktor
6. Logning og monitoring af sikkerhedshændelser
7. Funktionsadskillelse.

Komplementerende kontroller hos de dataansvarlige

Den dataansvarlige har følgende forpligtelser:

- Vedligeholdelse af borgernes bevilling gennem den adgang, de kontraktretligt er sikret
- Opsætning og styring af egne brugere i løsningen i produktionsmiljøet (Identity and Access Management)
- Proces og kontrol af, at data udelukkende anvendes til formål beskrevet i kontrakten med Experian, samt at den dataansvarlige har hjemmel til at behandle data m.fl., og at den dataansvarlige vedligeholder data.

4 Kontrolmål, kontrolaktivitet, test og resultat heraf

Introduktion

Dette afsnit er udformet med henblik på behandling af personoplysninger på vegne af kunder, som har indgået en databehandleraftale med Experian. Kontrolmiljøet bygger på fastlæggelsen af arten, timingen og omfanget af Experians forretningsprocesser.

Vores test af kontroller er afgrænset til kontrolmålene og de relaterede kontroller, der er anført i matriceoversigten i denne sektion af rapporten. Vores test omfatter ikke kontroller, der er beskrevet i systembeskrivelsen, som ikke er inkluderet i de nævnte matriceoversigter, eller kontroller, der eventuelt udføres hos brugerorganisationerne. Hver kunde og deres revisor er ansvarlige for at vurdere disse informationer i forhold til de kontroller, der er på plads i hver organisation. Hvis visse komplementære kontroller ikke er etableret hos brugerorganisationerne, kan kontrollerne muligvis ikke opveje disse svagheder.

Test af kontroller

De udførte tests i forbindelse med fastlæggelsen af kontrollers design og implementering består af en eller flere af følgende metoder:

Metode	Beskrivelse
Forespørgsel	Forespørgsel hos udvalgt personale hos Experian.
Observation	Observation af kontrollens udførelse.
Inspektion	Inspektion af dokumenter og rapporter, som indeholder angivelse omkring udførelse af kontroller. 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. Endvidere vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Genudførelse af kontrollen	Gentagelse af den relevante kontrol med henblik på at verificere, at kontrollen fungerer som forudsat.

Resultat af test

Resultatet af tests af kontroller omfatter en tilkendegivelse af, hvorvidt der i forbindelse med den beskrevne test af kontrollen er konstateret afvigelser. En afvigelse i en kontrol foreligger, når:

- en kontrol er udformet og implementeret på en sådan måde, at den ikke rettidigt kan forebygge eller opdage og korrigere fejl i processer eller systemer, eller
- der mangler en kontrol, der er nødvendig for rettidigt at forebygge eller opdage og korrigere fejl i processer eller systemer.

Resultat af test

Kontrolmål A

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

Nr.	Databehandlerens kontrolaktivitet	Test udført af KPMG	Resultat af revisors test
A.1	Der foreligger skriftlige procedurer, som indeholder krav om, at der alene må foretages behandling af personoplysninger, når der foreligger en instruks.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at behandling af personoplysninger alene foregår i henhold til instruks.	Ingen bemærkninger.
A.2	Databehandler udfører alene den behandling af personoplysninger, som fremgår af instruks fra dataansvarlig.	Inspiceret, at alle databehandleraftaler og behandling af personoplysninger foregår i henhold til instruks. Inspiceret, at der i databehandleraftaler med de dataansvarlige foreligger en instruks.	Ingen bemærkninger.
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.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer kontrol af, at behandling af personoplysninger ikke er i strid med databeskyttelsesforordningen eller anden lovgivning. Inspiceret, at der er procedurer for underretning af den dataansvarlige i tilfælde, hvor behandling af personoplysninger vurderes at være i strid med lovgivningen. Endvidere forespurgt og fået oplyst, at der ikke er foretaget behandling af personoplysninger, som er vurderet at være i strid med lovgivningen.	Oplyst, at der ikke er foretaget behandling af personoplysninger, som er vurderet i strid med lovgivningen. Ingen bemærkninger.

Kontrolmål B

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

Nr.	Databehandlerens kontrolaktivitet	Test udført af KPMG	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.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at der etableres de aftalte sikkerhedsforanstaltninger.	Ingen bemærkninger.
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.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at databehandler foretager en risikovurdering for at opnå en passende sikkerhed. Inspiceret, at den foretagne risikovurdering er opdateret og omfatter den aktuelle behandling af personoplysninger. Inspiceret, at databehandler har implementeret de tekniske foranstaltninger, som sikrer en passende sikkerhed i overensstemmelse med risikovurderingen.	Ingen bemærkninger.
B.3	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, installeret antivirus, som løbende opdateres.	Inspiceret, at der for de systemer og databaser, der anvendes til behandling af personoplysninger, er installeret antivirus-software.	Ingen bemærkninger.
B.4	Ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, sker gennem sikret firewall.	Inspiceret, at ekstern adgang til systemer og databaser, der anvendes til behandling af personoplysninger, alene sker gennem en firewall. Inspiceret, at firewall er konfigureret i henhold til intern politik herfor.	Ingen bemærkninger.

Kontrolmål B

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

Nr.	Databehandlerens kontrolaktivitet	Test udført af KPMG	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.	Forespurgt, om interne netværk er segmenteret med henblik på at sikre begrænset adgang til systemer og databaser, der anvendes til behandling af personoplysninger. Inspiceret netværksdiagrammer og anden netværksdokumentation for at sikre behørig segmentering.	Ingen bemærkninger.
B.6	Adgang til personoplysninger er isoleret til brugere med arbejdsbetinget behov herfor.	Inspiceret, at der foreligger formaliserede procedurer for begrænsning af brugeres adgang til personoplysninger. Inspiceret, at der foreligger formaliserede procedurer for opfølgning på, at brugeres adgang til personoplysninger er i overensstemmelse med deres arbejdsbetingede behov.	Ingen bemærkninger.
B.7	Der er for de systemer og databaser, der anvendes til behandling af personoplysninger, etableret systemovervågning med alarmering.	Inspiceret, at der for systemer og databaser, der anvendes til behandling af personoplysning, er etableret passende systemovervågning med alarmering.	Igen bemærninger.
B.8	Der anvendes effektiv kryptering ved transmission af fortrolige og følsomme personoplysninger via internettet og med e-mail.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at transmission af følsomme og fortrolige oplysninger over internettet er beskyttet af stærk kryptering baseret på en anerkendt algoritme.	Ingen bemærninger.

Kontrolmål B

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

Nr.	Databehandlerens kontrolaktivitet	Test udført af KPMG	Resultat af revisors test
B.9	Der er etableret logning i systemer, databaser og netværk af følgende forhold: • Aktiviteter, der udføres af systemadministratorer og andre med særlige rettigheder • Sikkerhedshændelser omfattende: - Ændringer i logopsætninger, herunder deaktivering af logning - Ændringer i systemrettigheder til brugere - Fejlede forsøg på log-on til systemer, databaser og netværk Logoplysninger er beskyttet mod manipulation.	Inspiceret, at der foreligger formaliserede procedurer for opsætning af logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, herunder gennemgang og opfølgning på logs. Inspiceret, at logning af brugeraktiviteter i systemer, databaser og netværk, der anvendes til behandling og transmission af personoplysninger, er konfigureret og aktiveret. Forespurgt, om der er etableret procedurer for, hvorledes opsamlede oplysninger om brugeraktivitet i logs er beskyttet mod manipulation og sletning.	Ingen bemærkninger.
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.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af personoplysninger til udvikling, test og lignende, der sikrer, at anvendelsen alene sker i pseudonymiseret eller anonymiseret form.	Ingen bemærkninger.
B.11	De etablerede tekniske foranstaltninger testes løbende ved sårbarhedsscanninger og penetrationstests.	Inspiceret, at der foreligger formaliserede procedurer for løbende tests af tekniske foranstaltninger, herunder til udførelse af sårbarhedsscanninger og penetrationstests.	Ingen bemærkninger.

Kontrolmål B

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

Nr.	Databehandlerens kontrolaktivitet	Test udført af KPMG	Resultat af revisors test
B.12	Ændringer til systemer, databaser og netværk følger fastlagte procedurer, som sikrer vedligeholdelse med relevante opdateringer og patches, herunder sikkerhedspatches.	Inspiceret, at der foreligger formaliserede procedurer for håndtering af ændringer til systemer, databaser og netværk, herunder håndtering af relevante opdateringer, patches og sikkerhedspatches. Inspiceret et eksempel af en ændring i håndtering af ændringsproces.	Ingen bemærninger.
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.	Inspiceret, at der foreligger formaliserede procedurer for tildeling og afbrydelse af brugernes adgang til systemer og databaser, som anvendes til behandling af personoplysninger. Inspiceret, at der foreligger dokumentation for seneste udførte periodiske revurdering og godkendelse af tildelte brugeradgange.	Ingen bemærkninger.
B.14	Adgange til systemer, netværk, databaser og datafiler indeholdende persondata er beskyttet med adgangskode. Der er opsat kvalitetskrav til adgangskoder, således at der kræves en minimumslængde, kompleksitet og maksimal løbetid, ligesom adgangskodeopsætninger medfører, at adgangskoder ikke kan genbruges. Endvidere bliver brugeren lukket ude ved gentagne fejlagtige forsøg på log-in.	Inspiceret ved analyse af konfigurationsudtræk, at adgangskoder til systemer, netværk, databaser og datafiler indeholdende persondata overholder gældende kvalitetskrav.	Ingen bemærkninger.

Kontrolmål B

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

Nr.	Databehandlerens kontrolaktivitet	Test udført af KPMG	Resultat af revisors test
B.15	Der er etableret fysisk adgangssikkerhed, således at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger.	Forudspurgt, at der foreligger formaliserede procedurer, der sikrer, at kun autoriserede personer kan opnå fysisk adgang til lokaler og datacentre, hvori der opbevares og behandles personoplysninger. Inspiceret, at Experian er ISO 27001:2022-certificeret.	Ingen bemærkninger.
B.16	En formaliseret proces er etableret for automatisk backup af alle forretningskritiske systemer og data.	Inspiceret, at der er en formaliseret politik for backup. Inspiceret, at der foreligger dokumentation for, at backup er taget på systemet. Inspiceret, at der foretages vedligeholdelse af parametre, der styrer backup.	Ingen bemærkninger.
B.17	Planlagte tests af organisationens beredskabsprocedurer gennemføres mindst én gang årligt.	Inspiceret, at der foreligger dokumentation for test af beredskabsplanen og kontinuitetsplanen. Inspiceret, at der foreligger dokumentation for seneste udførte test af beredskabsplanen.	Ingen bemærkninger.

Kontrolmål C

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

Nr.	Databehandlerens kontrolaktivitet	Test udført af KPMG	Resultat af revisors 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.	Inspiceret, at der foreligger en informationssikkerhedspolitik, som ledelsen har behandlet og godkendt inden for det seneste år. Forespurgt og fået oplyst, at informationssikkerhedspolitikken er kommunikeret til relevante interessenter, herunder databehandlerens medarbejdere.	Ingen bemærkninger.
C.2	Databehandlerens ledelse har sikret, at informationssikkerhedspolitikken ikke er i modstrid med indgåede databehandleraftaler.	Inspiceret dokumentation for ledelsens vurdering af, at informationssikkerhedspolitikken generelt lever op til kravene om sikringsforanstaltninger og behandlingssikkerheden i indgåede databehandleraftaler. Inspiceret, at indgåede databehandleraftaler er dækket af informationssikkerhedspolitikkens krav til sikringsforanstaltninger og behandlingssikkerheden.	Ingen bemærkninger.
C.3	Der udføres en efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse. Efterprøvningen omfatter i relevant omfang: • Reference indhentes.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer efterprøvning af databehandlerens medarbejdere i forbindelse med ansættelse, samt at efterprøvningen har omfattet: • Reference indhentes.	Informeret, at der ingen ansættelser har været omkring tidspunktet for revisionen. Ingen yderligere bemærkninger.
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.	Inspiceret, at der foreligger fortrolighedsaftale, samt at medarbejder er blevet introduceret til gældende Informationssikkerhedspolitik og -procedurer vedrørende databehandling.	Informeret, at der ingen ansættelser har været omkring tidspunktet for revisionen. Ingen yderligere bemærkninger.

Kontrolmål C

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

Nr.	Databehandlerens kontrolaktivitet	Test udført af KPMG	Resultat af revisors 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.	Inspiceret procedurer, der sikrer, at fratrådte medarbejderes rettigheder inaktiveres eller ophører ved fratrædelse, og at aktiver som adgangskort, pc, mobiltelefon etc. inddrages. Inspiceret ved en stikprøve for seneste fratrådte medarbejder, at rettigheder er inaktiveret eller ophørt, samt at aktiver er inddraget. Forespurgt og fået oplyst, at der ingen fratrædelser har været omkring tidspunktet for revisionen.	Informeret, at der ingen fratrædelser har været omkring tidspunktet for revisionen. Ingen yderligere bemærkninger.
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.	Inspiceret, at der foreligger formaliserede procedurer, der sikrer, at fratrådte medarbejdere gøres opmærksom på opretholdelse af fortrolighedsaftalen og generel tavshedspligt. Forespurgt, om der har været fratrædelser omkring tidspunktet for revisionen.	Informeret, at der ingen fratrædelser har været omkring tidspunktet for revisionen. Ingen yderligere bemærkninger.
C.7	Der gennemføres løbende bevidsthedstræning af databehandlerens medarbejdere i relation til IT-sikkerhed generelt samt behandlingssikkerhed i relation til personoplysninger.	Inspiceret, at databehandleren udbyder bevidsthedstræning til medarbejderne omfattende generel IT-sikkerhed og behandlingssikkerhed i relation til personoplysninger.	Ingen bemærkninger.

Kontrolmål D

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

Nr.	Databehandlerens kontrolaktivitet	Test udført af KPMG	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.	Inspiceret, at der foreligger formaliserede procedurer for opbevaring og sletning af personoplysninger i overensstemmelse med aftalen med den dataansvarlige. Forespurgt om, ansvarsfordelingen mellem Experian og deres kunder for oprettelse og sletning af personoplysninger.	Informeret, at den dataansvarlige er ansvarlig for oprettelse og sletning af personoplysninger. Experian foretager ikke noget i den forbindelse. Ingen yderligere bemærkninger.
D.2	Der er aftalt specifikke krav til databehandlerens opbevaringsperioder og sletterutiner i de indgåede databehandleraftaler.	Inspiceret, at de foreliggende procedurer for opbevaring og sletning indeholder de specifikke krav til databehandlerens opbevaringsperioder og sletterutiner.	Informeret, at den dataansvarlige er ansvarlig for oprettelse og sletning af personoplysninger. Experian foretager ikke noget i den forbindelse. Ingen yderligere bemærkninger.
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.	Forespurgt om, hvorvidt der foreligger formaliserede procedurer for behandling af den dataansvarliges data ved ophør af behandling af personoplysninger. Forespurgt, om der har været ophør af behandling af personoplysninger for den dataansvarlige.	Informeret, at den dataansvarlige er ansvarlig for oprettelse og sletning af personoplysninger. Experian foretager ikke noget i den forbindelse. Ingen yderligere bemærkninger.

Kontrolmål E

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

Nr.	Databehandlerens kontrolaktivitet	Test udført af KPMG	Resultat af revisors 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.	Inspiceret, at der foreligger formaliserede procedurer for, at der alene foretages opbevaring og behandling af personoplysninger i henhold til databehandleraftalerne.	Ingen bemærkninger.
E.2	Databehandlerens databehandling, inklusive opbevaring, må kun finde sted på de af den dataansvarlige godkendte lokaliteter, lande eller landområder.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over behandlingsaktiviteter med angivelse af lokaliteter, lande eller landområder. Forespurgt, om der er dokumentation for, at databehandlingen, herunder opbevaring af personoplysninger, alene foretages på de lokaliteter, der fremgår af databehandleraftalen – eller i øvrigt er godkendt af den dataansvarlige.	Ingen bemærkninger.

Kontrolmål F

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	Test udført af KPMG	Resultat af revisors test
F.1	Der foreligger skriftlige procedurer, som indeholder krav til databehandleren ved anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler og instruks.	Inspiceret, at der foreligger formaliserede procedurer for anvendelse af underdatabehandlere, herunder krav om underdatabehandleraftaler.	Ingen bemærkninger.
F.2	Databehandleren anvender alene underdatabehandlere til behandling af personoplysninger, der er specifikt eller generelt godkendt af den dataansvarlige.	Inspiceret, om databehandleren har en samlet og opdateret oversigt over anvendte underdatabehandlere, samt om disse indgår i databehandleraftalerne og er godkendt af den dataansvarlige.	Ingen bemærkninger.
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.	Inspiceret, at der foreligger formaliserede procedurer for underretning til den dataansvarlige ved ændringer i anvendelse af underdatabehandlere. Forespurgt og fået oplyst, at der ikke er foretaget ændringer i anvendelsen af underdatabehandlere, efter seneste aftalte databehandleraftale er indgået med den dataansvarlige.	Ingen bemærkninger.
F.4	Databehandleren har pålagt underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er forudsat i databehandleraftalen el.lign. med den dataansvarlige.	Forespurgt om, hvorvidt der foreligger en procedure for at fremsende en oversigt af de sikkerhedskrav, der skal overholdes, og som er indgået med den dataansvarlige ved anvendelse af underdatabehandlere. Inspiceret, at underdatabehandleraftalerne indeholder samme krav og forpligtelser, som er anført i databehandleraftalerne mellem de dataansvarlige og databehandleren.	Ingen bemærkninger.

Kontrolmål F

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	Test udført af KPMG	Resultat af revisors test
F.5	Databehandleren har en oversigt over godkendte underdatabehandlere med angivelse af: • Navn • CVR-nr. • Adresse • Beskrivelse af behandlingen.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over anvendte og godkendte underdatabehandlere. Inspiceret, at oversigten som minimum indeholder de krævede oplysninger om de enkelte underdatabehandlere.	Ingen bemærkninger.
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.	Inspiceret, at der foreligger formaliserede procedurer for opfølgning på behandlingsaktiviteter hos underdatabehandlerne og overholdelse af underdatabehandleraftalerne. Forespurgt dokumentation for, at der er foretaget behørig opfølgning på tekniske og organisatoriske foranstaltninger, behandlingssikkerheden hos de anvendte underdatabehandlere, tredjelands overførselsgrundlag og lignende.	Ingen bemærkninger.

Kontrolmål G

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

Nr.	Databehandlerens kontrolaktivitet	Test udført af KPMG	Resultat af revisors 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.	Inspiceret, at der foreligger formaliserede procedurer om overførsler af persondata til tredjelande eller internationale organisationer. Forespurgt, om der er overført til tredjelande, udover til Experian, egen lokalisation, samt at alle dataansvarlige har godkendt behandlingen i databehandleraftalen.	Ingen bemærkninger.
G.2	Databehandleren må kun overføre personoplysninger til tredjelande eller internationale organisationer efter instruks fra den dataansvarlige.	Inspiceret, at databehandleren har en samlet og opdateret oversigt over overførsler af personoplysninger til tredjelande eller internationale organisationer.	Ingen bemærkninger.
G.3	Databehandleren har i forbindelse med overførsel af personoplysninger til tredjelande eller internationale organisationer vurderet og dokumenteret, at der eksisterer et gyldigt overførselsgrundlag.	Inspiceret dataoverførsler fra databehandlerens oversigt over overførsler, at der er dokumentation for et gyldigt overførselsgrundlag i databehandleraftalen med den dataansvarlige.	Ingen bemærkninger.

Kontrolmål H

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	Test udført af KPMG	Resultat af revisors test
H.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal bistå den dataansvarlige i relation til de registreredes rettigheder.	Inspiceret, at der foreligger formaliserede procedurer for databehandlerens bistand af den dataansvarlige i relation til de registreredes rettigheder. Forespurgt om ansvarsfordelingen mellem Experian og deres kunder for oprettelse og sletning af personoplysninger.	Informeret, at den dataansvarlige har ansvaret for opbevaring og sletning af data, da de selv vælger at uploade og dele persondata. Ingen yderligere bemærkninger.
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.	Inspiceret, at der er etableret procedurer for at bistand til den dataansvarlige, som indeholder detaljerede procedurer for: • Udlevering af data • Rettelse af data • Sletning af data • Begrænsning af behandling af personoplysninger • Oplysning om behandling af personoplysninger til den registrerede.	Informeret, at den dataansvarlige har ansvaret for opbevaring og sletning af data, da de selv vælger at uploade og dele persondata. Ingen yderligere bemærkninger.

Kontrolmål I

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

Nr.	Databehandlerens kontrolaktivitet	Test udført af KPMG	Resultat af revisors test
I.1	Der foreligger skriftlige procedurer, som indeholder krav om, at databehandleren skal underrette de dataansvarlige ved brud på persondatasikkerheden.	Inspiceret, om der foreligger formaliserede procedurer, der indeholder krav til underretning af de dataansvarlige ved brud på persondatasikkerheden.	Ingen bemærkninger.
I.2	Databehandleren har etableret følgende kontroller for identifikation af eventuelle brud på persondatasikkerheden: • Bevidsthedstræning hos medarbejdere.	Inspiceret, at databehandler udbyder bevidsthedstræning til medarbejderne i relation til identifikation af eventuelle brud på persondatasikkerheden.	Ingen bemærkninger.
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.	Forespurgt, om der er konstateret brud på persondatasikkerheden.	Informeret, at der ikke har været konstateret brud omkring tidspunktet for revisionen. Ingen bemærkninger.
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.	Inspiceret, at der foreligger procedurer for, hvordes bistand til den dataansvarlige ved dennes anmeldelse til Datatilsynet skal behandles.	Ingen bemærkninger.

PENNEO

The signatures in this document are legally binding. The document is signed using Penneo™ secure digital signature. The identity of the signers has been recorded, and are listed below.

"By my signature I confirm all dates and content in this document."

Andrew Rich
Direktionsmedlem
Serial number: andy.rich@experian.com
IP: 131.229.xxx.xxx
2026-03-02 12:44:34 UTC

Andrew Rich
Country Managing Director, Northern Europe
Serial number: andy.rich@experian.com
IP: 131.229.xxx.xxx
2026-03-02 12:44:34 UTC

Christopher Anders Pedersen
Partner
On behalf of: KPMG Statsautoriseret Revisionspartners…
Serial number: f5fb37d2-9f41-450f-9b19-ceb4439fde75
IP: 83.151.xxx.xxx
2026-03-02 14:18:32 UTC

MitID

Penneo document key: JS2M6-P80ME-6WTFD-8DGX5-I6AMA-RVA7D