01. juni 2024

D-mærket

Virksomhedsrapport

D-mærkets kontrol af Complea A/S

1. Formål og tiltænkte brugere

Denne rapport er udarbejdet til Complea A/S (”**Virksomheden**”), dens ledelse og relevante interessenter af Mærkningsordningen for it-sikkerhed og ansvarlig dataanvendelse (”**Mærkningsordningen**”). Rapporten er et overordnet indblik i de kontrolmål, der er blevet udtaget til tilsyn, om fremgangsmåden for tilsynet i forbindelse med anmodning eller genanmodning om D-mærket, samt resultatet af tilsynet. Det er Virksomhedens egen vurdering, om de ønsker at dele rapporten.

2. Uafhængighed

Mærkningsordningens Auditors er uafhængige af øvrig kontrol, og deres beslutninger er uden ekstern påvirkning. Tilsyn og kontrol bliver udført ud fra grundlæggende principper om integritet, objektivitet, faglige kompetencer, fortrolighed samt professionel adfærd.

Virksomheden bliver testet og kvalitetskontrolleret af minimum to Auditors.

3. Virksomhedens ansvar

Som afslutning på Virksomhedens selvevaluering, og inden tilsynet og fremsendelse af dokumentation gennemføres, har Virksomheden underskrevet en tro- og loveerklæring, hvori de erklærer, at alle svar på spørgsmål og informationer givet af Virksomheden er korrekte.

Derudover finder vilkårene for D-mærket anvendelse, og Virksomheden er forpligtet til at følge dem.

4. Information om Virksomheden

Oversigt 1

Navn på virksomhed	Complea A/S				
Virksomhedsadresse	Bøgildsmindevej 7				
Postnummer	9400		**By**	Nørresundby	
Telefonnummer	+45 96 32 70 00		**CVR**	33153716	
URL	www.complea.dk				
Branche	Konsulentbistand vedrørende informationsteknologi				
Branchekode	620200				
Antal ansatte	☐0-9	☐10-49	☒50-249	☐250-999	☐>1000
Nettoomsætning ved seneste regnskab	☐0-7,9 mDKK	☒8-155,9 mDKK	☐156-313 mDKK	☐≥313 mDKK	
Kontaktperson	Christian Mørkeberg				
Titel	Project Manager		**E-mail**	CMN@complea.dk	

5. Omfang for audit

Mærkningsordningens Auditors fører tilsyn på Virksomhedens efterlevelse af D-mærkets krav ud fra udvalgte kontrolmål (niveau 3 kriterier) og tilhørende kontrolaktiviteter (krav). De specifikke udvalgte og fortrolige kontrolaktiviteter (krav) fremsendes ved tilsyn. Kontrolaktiviteterne og resultat af test heraf fremgår under afsnit 6.

Tilsynet er udført som et "*point in time*" tilsyn, hvorfor Virksomheden dokumenterer, at de udvalgte krav er designet og implementeret effektivt i Virksomheden. Indeværende rapport skal derfor anses som øjebliksbillede af Virksomhedens faktiske forhold.

Ved genanmodning om D-mærket vil tilsynet udføres som et "*over time*" tilsyn, hvorfor Virksomheden skal dokumentere den operationelle effektivitet af de udvalgte krav, hvor perioden fra første tildeling til genanmodning om D-mærket afdækkes.

Oversigt 2

Kompenserende kontroller	☐ [Indsæt krav hvor kompenserende kontroller er benyttet]
Virksomhedstype	☐ Gruppe I ☐ Gruppe II ☒ Gruppe III ☐ Gruppe IV
	☒ Virksomheden er leverandør af software eller it-tjenester til andre ☐ Virksomheden anvender leverandører (som benytter it) til behandling af personoplysninger og / eller forretningskritiske data ☐ Virksomheden udvikler software ☐ Virksomheden anvender eller udvikler algoritmer eller AI
Udvalgt kriterie (niveau 1)	**Udvalgte kontrolmål (niveau 3)**
☒ 1. Styring og forankring i ledelsen	☒ 1.1.1 Udpegning af ansvarlig person for it-sikkerhed og ansvarlig dataanvendelse ☒ 1.2.1 Overblik over personoplysninger ☒ 1.2.2 Overblik over forretningskritiske data ☒ 1.2.3 Overblik over it-systemer, tjenester, netværkskomponenter, enheder, software og aktivitetsbaserede algoritme/AI "use cases" ☒ 1.3.1 Risikovurdering og -håndtering ☒ 1.4.1 Politik for it-sikkerhed ☒ 1.5.1 It-beredskabsplan ☒ 1.6.1 Politik for behandling af personoplysninger ☒ 1.6.2 Politik for dataetik ☐ 1.7.1 Krav til udviklingsproces
☒ 2. Awareness og sikker adfærd	☐ 2.1.1 Træn bestyrelsen og den øverste ledelse i it-sikkerhed, databeskyttelse og dataetik ☒ 2.2.1 Træn alle ansattes og brugeres viden om it-sikkerhed kontinuerligt ☒ 2.3.1 Træn alle ansattes og brugeres viden om ansvarlig behandling af personoplysninger kontinuerligt ☐ 2.3.2 Træn alle ansatte og brugeres viden om dataetik kontinuerligt
☒ 3. Teknisk it-sikkerhed	☐ 3.1.1 Beskyttelse af administrative grænseflader, netværk og enheder ☐ 3.1.2 Kryptering af ekstern netværksadgang ☐ 3.2.1 Opsætning og vedligeholdelse af korrekt konfiguration ☒ 3.3.1 Beskyttelse af administrative brugerkonti ☒ 3.4.1 Implementering af beskyttelsesmekanismer mod malware ☐ 3.4.2 Beskyttelse mod uønskede e-mails. ☒ 3.5.1 Kontinuerlig opdatering af software og styresystemer ☒ 3.6.1 Procedure for automatisk og jævnlig backup ☐ 3.7.1 Overvågning af systemaktivitet gennem logning

☒ 4. Krav til leverandørers it-sikkerhed og ansvarlige dataanvendelse	☒ 4.1.1 Leverandørlivscyklus og risikovurdering ☒ 4.2.1 Krav til it-sikkerhed hos leverandører ☒ 4.3.1 Krav til persondatabehandling hos leverandører ☐ 4.3.2 Krav til dataetisk behandling hos leverandører
☒ 5. Transparens & kontrol med data	☒ 5.1.1 Oplysningspligt overfor den registrerede ☐ 5.1.2 Information om samarbejdspartnere, der deles data med ☐ 5.2.1 Cookie-information og -brugervenlighed ☒ 5.3.1 Brugerkontrol ☐ 5.4.1 Lettilgængelig klagevejledning vedrørende ansvarlig dataanvendelse og it-sikkerhed
☐ 6. Privacy & security by design & default	☐ 6.1.1 Risikovurdering ☐ 6.1.2 Tag stilling til persondatabeskyttelses- og sikkerhedsniveau ☐ 6.2.1 Minimering og begrænsning ☐ 6.2.2 Separering og skjul ☐ 6.2.3 Aggregering ☐ 6.2.4 Persondatabeskyttelse som standardindstilling (indlejring af persondatabeskyttelse) ☐ 6.2.5 Fuld funktionalitet og persondatabeskyttelse ☐ 6.3.1 Minimer angrebsflader ☐ 6.3.2 Højt niveau af sikkerhed som standardindstilling ☐ 6.3.3 Mindste sæt af rettigheder/rettighedsstyring ☐ 6.3.4 Kontrol af kode (egen og tredjepart) ☐ 6.4.1 Implementering igennem udviklingsproces
☐ 7. Pålidelige algoritmer & AI	☐ 7.1.1 Risikovurdering ☐ 7.1.2 Interessentinddragelse ☐ 7.1.3 Informationspligt og gennemsigtighed ☐ 7.1.4 Udfordringsret ☐ 7.1.5 Nødstop ☐ 7.2.1 Valg af inferensmetode og forklarlighed ☐ 7.2.2 Højkvalitetsdatagrundlag ☐ 7.2.3 Kontinuerlig evaluering af data og beregningslogik ☐ 7.3.1 Implementering igennem udviklingsproces
☒ 8. Dataetik	☒ 8.1.1 Dataetiske overvejelser

6. Kriterier, krav, test og resultat af test

Kriterie 1: Styring og forankring i ledelsen Virksomhedens øverste ledelse tager aktivt ansvar for arbejdet med it-sikkerhed og ansvarlig dataanvendelse. Det er dog ikke nødvendigvis den øverste ledelse, som er udførende på de definerede krav.			
Ref.	**Virksomhedens udvalgte krav**	**Tilsynets udførte test**	**Resultat af test**
1.1.1.1	Virksomheden skal udpege mindst én navngiven person, der har ansvaret for it-sikkerhed og ansvarlig dataanvendelse. Denne person skal i øvrigt have ressourcer, kompetencer og mandat til at udfylde denne rolle; uanset om vedkommende har andre roller internt i virksomheden. Den eller de navngivne personer med ansvaret for it-sikkerhed og ansvarlig dataanvendelse skal kunne rapportere direkte til den øverste ledelse. Der kan sagtens være flere personer, som er udførende på opgaverne, men ansvaret kan ikke delegeres.	Inspiceret, at ansvaret for it- sikkerhed og ansvarlig dataanvendelse er tildelt en person. Vurderet, at personen med ansvaret for it- sikkerhed og ansvarlig dataanvendelse har det nødvendige mandat, ressourcer og kompetencer.	Ingen væsentlige afvigelser konstateret
1.2.1.1	Virksomheden skal udarbejde og vedligeholde en kortlægning af alle typer personoplysninger om registrerede, som indgår i virksomhedens aktiviteter. Kortlægningen skal som minimum indeholde oplysninger om de it-systemer og tjenester, som er kortlagt i 1.2.3.1.	Inspiceret, at der foreligger en kortlægning af alle typer af personoplysninger, som indgår i virksomhedens aktiviteter. Inspiceret, at kortlægningen omfatter de it-systemer og tjenester, som er kortlagt i 1.2.3.1.	Ingen væsentlige afvigelser konstateret
1.2.2.1	Virksomheden skal udarbejde en ledelsesgodkendt definition af forretningskritiske data. Forretningskritiske data udgør kernen af virksomhedens aktiviteter, og denne type data kan have væsentlige konsekvenser for virksomhedsdrift, omdømme, kunder og/eller økonomi, hvis: 1. Enten fortrolighed, integritet eller tilgængelighed påvirkes eller 2. Data misbruges Kravet opstiller en ramme, som virksomheden skal benytte til at udarbejde en definition af forretningskritiske data. Virksomheden opfordres dog til at tænke forretningsbehov og andet ind i definitionen, så den er dækkende for virksomheden.	Inspiceret, at der foreligger en definition at forretningskritisk data. Inspiceret, at definition af forretningskritisk data er ledelsesgodkendt.	Ingen væsentlige afvigelser konstateret

Kriterie 1: Styring og forankring i ledelsen Virksomhedens øverste ledelse tager aktivt ansvar for arbejdet med it-sikkerhed og ansvarlig dataanvendelse. Det er dog ikke nødvendigvis den øverste ledelse, som er udførende på de definerede krav.			
Ref.	**Virksomhedens udvalgte krav**	**Tilsynets udførte test**	**Resultat af test**
1.2.2.2	Virksomheden skal udarbejde og vedligeholde en kortlægning af hvor de forretningskritiske data indgår i virksomhedens aktiviteter. Kortlægningen skal som minimum indeholde oplysninger om de it-systemer og tjenester, som er kortlagt i 1.2.3.1.	Inspiceret, at forretningskritiske data og hvor de indgår i virksomhedens aktiviteter er kortlagt. Inspiceret, at kortlægningen indeholder it-systemer og tjenester, som benyttes til behandling af forretningskritisk data.	Ingen væsentlige afvigelser konstateret
1.2.3.1	Virksomheden skal udarbejde og vedligeholde en kortlægning af: 1. It-systemer 2. Tjenester 3. Netværkskomponenter 4. Enheder 5. Software Kortlægning af de fem kategorier kan udarbejdes i én og samme løsning eller hver for sig.	Inspiceret, at en kortlægning af it-systemer, tjenester, netværkskomponenter, enheder og software er udarbejdet og vedligeholdes.	Ingen væsentlige afvigelser konstateret
1.2.3.3	Virksomheden skal udarbejde og vedligeholde en kortlægning af virksomhedens eksternt rettede aktiviteter.	Inspiceret, at de eksternt rettede aktiviteter er kortlagt. Inspiceret, at kortlægning fyldestgørende beskriver de eksternt rettede aktiviteter.	Ingen væsentlige afvigelser konstateret
1.3.1.2	Virksomheden skal udarbejde og vedligeholde en proces for risikovurderinger. Processen skal indeholde følgende faser: • Identifikation • Analyse • Evaluering • Behandling • Afsluttende accept af restrisiko De identificerede risici skal vurderes ud fra sandsynlighed og konsekvens og skal tildeles en vægtning, som hjælper virksomheden til at prioritere sin indsats. Virksomhedens risikovurderinger kan give anledning til, at virksomheden skal implementere flere foranstaltninger end de krav, som virksomheden skal efterleve i forbindelse med D-mærket.	Forespurgt, om processerne for identificering og behandling af risici. Inspiceret, at procedure for risikovurderinger indeholder faserne identifikation, analyse, evaluering, behandling og accept. Inspiceret, at identificerede risici er vurderet og tildelt en vægtning ud fra sandsynlighed og konsekvens.	Ingen væsentlige afvigelser konstateret

Kriterie 1: Styring og forankring i ledelsen Virksomhedens øverste ledelse tager aktivt ansvar for arbejdet med it-sikkerhed og ansvarlig dataanvendelse. Det er dog ikke nødvendigvis den øverste ledelse, som er udførende på de definerede krav.			
Ref.	**Virksomhedens udvalgte krav**	**Tilsynets udførte test**	**Resultat af test**
1.3.1.3	Virksomheden skal udarbejde og vedligeholde en oversigt over risici, som skal indgå i virksomhedens risikovurderinger. Oversigten skal både indeholde risici mod virksomheden og den registrerede.	Forespurgt, om processen for vedligeholdelse af oversigt over risici. Inspiceret, at der forefindes risikovurderinger som indeholder risici mod virksomheden og den registrerede. Inspiceret, at risikovurderingen er revideret indenfor det seneste år.	Ingen væsentlige afvigelser konstateret
1.4.1.1	Virksomheden skal udarbejde og vedligeholde en politik for it-sikkerhed.	Forespurgt, hvorledes politik for it-sikkerheds vedligeholdes og kommunikeres internt. Inspiceret at politikken for it-sikkerhed er revideret indenfor det seneste år	Ingen væsentlige afvigelser konstateret
1.4.1.2	Politik for it-sikkerhed skal definere: · Virksomhedens mål · Anvendelsesområde · Ansvar · Udmøntning · Opfølgning, herunder rapportering til ledelsen	Inspiceret, at politik for it-sikkerhed indeholder og definerer: - Virksomhedens mål - Anvendelsesområde - Ansvar - Udmøntning - Opfølgning, herunder rapportering til ledelsen	Ingen væsentlige afvigelser konstateret
1.5.1.1	Virksomheden skal udarbejde og minimum årligt vedligeholde en it-beredskabsplan og relaterede handlingsplaner for de it-systemer og tjenester, som benyttes til behandling af personoplysninger (1.2.1.1) og forretningskritiske data (1.2.2.2). It-beredskabsplanen skal indeholde følgende: · Hvem man skal kontakte, internt og eksternt, hvis der er it-problemer. · Alle leverandører som er med til at understøtte de identificerede it-systemer og tjenester og deres kontaktdetaljer og tilgængelighed (åbningstider og kommunikationskanaler) · Hvordan data/it kan gendannes jf. krav i 3.6.1	Inspiceret, at it-beredskabsplan og relaterede handlingsplaner på tilstrækkelig vis beskriver: - Hvem man skal kontakte, internt og eksternt, hvis der er it-problemer - Alle leverandører, som er med til at understøtte de identificerede it-systemer og tjenester og deres kontaktdetaljer og tilgængelighed - Hvordan data/it kan gendannes jf. krav i 3.6.1. Inspiceret, at it-beredskabsplan og	Ingen væsentlige afvigelser konstateret

Kriterie 1: Styring og forankring i ledelsen Virksomhedens øverste ledelse tager aktivt ansvar for arbejdet med it-sikkerhed og ansvarlig dataanvendelse. Det er dog ikke nødvendigvis den øverste ledelse, som er udførende på de definerede krav.			
Ref.	**Virksomhedens udvalgte krav**	**Tilsynets udførte test**	**Resultat af test**
		relaterede handlingsplaner er revideret indenfor det seneste år.	
1.6.1.1	Virksomheden skal udarbejde og vedligeholde en politik for behandling af personoplysninger.	Forespurgt, hvorledes politik for behandling af personoplysninger vedligeholdes og kommunikeres internt. Inspiceret, at politik for behandling af personoplysninger er udarbejdet og indenfor det seneste år blevet revideret.	Ingen væsentlige afvigelser konstateret
1.6.1.2	Politik for behandling af personoplysninger (1.6.1.1) skal definere: - Virksomhedens mål - Anvendelsesområde - Ansvar - Udmøntning - Opfølgning, herunder rapportering til ledelsen	Inspiceret, at der foreligger en politik for behandling af personoplysninger, der bl.a. definerer: - Virksomhedens mål - Anvendelsesområde - Ansvar - Udmøntning - Opfølgning, herunder rapportering til ledelsen	Ingen væsentlige afvigelser konstateret
1.6.2.1	Virksomheden skal udarbejde og vedligeholde en politik for dataetik.	Forespurgt, hvorledes politik for dataetik vedligeholdes og kommunikeres internt. Inspiceret, at politik for dataetik er udarbejdet og indenfor det seneste år blevet revideret.	Ingen væsentlige afvigelser konstateret
1.6.2.2	Politik for dataetik (1.6.2.1) skal definere: - Virksomhedens mål - Anvendelsesområde - Ansvar - Udmøntning - Opfølgning, herunder rapportering til ledelsen	Inspiceret, at der foreligger en politik for dataetik, der bl.a. definerer: - Virksomhedens mål - Anvendelsesområde - Ansvar - Udmøntning - Opfølgning, herunder rapportering til ledelsen	Ingen væsentlige afvigelser konstateret

Kriterie 2: Awareness og sikker adfærd Virksomheden skal sikre, at bestyrelsen og den øverste ledelse modtager træning i it-sikkerhed og ansvarlig dataanvendelse. Virksomheden skal yderligere sikre, at ansatte, konsulenter og leverandører løbende og med jævne mellemrum bliver trænet i awareness og handlingskompetencer i relation til it-sikkerhed og ansvarlig dataanvendelse.			
Ref.	**Virksomhedens udvalgte krav**	**Tilsynets udførte handling**	**Resultat af test**
2.1.1.1	Virksomheden skal sørge for at bestyrelsen og den øverste ledelse årligt modtager særlig træning i it-sikkerhed og databeskyttelse. Træningen skal klæde bestyrelsen og den øverste ledelse på til at: - Forstå virksomhedens risikobillede indenfor it-sikkerhed og databeskyttelse og sikre relevant risikostyring - Forstå hensigtsmæssig organisering, rapportering og allokering af ressourcer, for at virksomheden effektivt kan arbejde med it-sikkerhed og databeskyttelse. - Forstå og kunne føre effektiv kontrol med virksomhedens risici inden for it-sikkerhed og databeskyttelse	Forespurgt, hvorledes personale og ledelse bliver trænet i it-sikkerhed og databeskyttelse. Inspiceret, at der foreligger en formaliseret procedure, der bl.a. inkluderer emner om it-sikkerhed og databeskyttelse. Inspiceret, at awareness træning har været afholdt for ansatte og ledelsen indenfor det seneste år.	Ingen væsentlige afvigelser konstateret
2.2.1.5	Virksomheden skal skriftligt dokumentere deltagelsen i træningsprogrammet.	Inspiceret, at deltagelse i awareness træning om it-sikkerhed dokumenteres skriftligt. Inspiceret, at awareness træning har været afholdt for ansatte og ledelsen indenfor det seneste år.	Ingen væsentlige afvigelser konstateret
2.3.1.1	Virksomheden skal etablere et træningsprogram om ansvarlig behandling af personoplysninger for alle ansatte og brugere, som arbejder med personoplysninger.	Forespurgt, hvorledes relevant personale og ledelse bliver trænet i behandling af personoplysninger. Inspiceret, at der foreligger en formaliseret procedure, der bl.a. inkluderer emner om behandling af personoplysninger. Inspiceret, at awareness træning har været afholdt for ansatte og ledelsen indenfor det seneste år.	Ingen væsentlige afvigelser konstateret
2.3.1.5	Virksomheden skal skriftligt dokumentere deltagelsen i træningsprogram om ansvarlig håndtering af personoplysninger (2.3.1.1).	Inspiceret, at awareness træning har været afholdt for ansatte og ledelsen indenfor det seneste år.	Ingen væsentlige afvigelser konstateret

Kriterie 3: Teknisk IT-sikkerhed Virksomhedens systemer og enheder skal være sikret, så virksomheden reducerer sandsynligheden for sikkerhedshændelser baseret på de mest udbredte trusler. Målet er både at nedbringe risikoen for angreb og databrud og sætte virksomheden i stand til hurtigt og effektivt at opdage, inddæmme og afbøde konsekvenserne samt genoprette vigtige data og systemer, når sikkerhedsbruddet eller angrebet sker.			
Ref.	**Virksomhedens udvalgte krav**	**Tilsynets udførte handling**	**Resultat af test**
3.3.1.1	Virksomheden skal anvende flerfaktorautentifikation for at beskytte administrative grænseflader i it-systemer, tjenester, netværkskomponenter, enheder og software som benyttes til henholdsvis behandling af personoplysninger (1.2.1.1) og forretningskritiske data (1.2.2.2).	Inspiceret, at der foreligger procedure, som fastlægger krav om brug af flerfaktorautentifikation. Inspiceret, ved en stikprøve af relevante systemer at flerfaktorautentifikation er konfigureret og etableret.	Ingen væsentlige afvigelser konstateret
3.3.1.2	Brugerkonti med administrative rettigheder skal være adskilte fra almindelige brugerkonti, så aktiviteter såsom e-mail, internet browsing og andre almindelige brugeraktiviteter ikke udføres med administratorrettigheder.	Inspiceret, at der foreligger en procedure for oprettelse af adminbrugere er udarbejdet. Inspiceret, at brugere med almindelige roller og privilegerede roller er opdelte.	Ingen væsentlige afvigelser konstateret
3.3.1.4	Virksomheden skal definere en proces for at tildele administrative adgangsrettigheder til brugere, som sikrer at tildelinger bliver vurderet, godkendt og dokumenteret.	Inspiceret, at der foreligger en procedure for adgangsstyring, herunder tildeling af administrative adgangsrettigheder. Inspiceret, ved en stikprøve af brugere med privilegerede rettigheder at: - Adgangene er vurderet - Adgangene er godkendt - Adgangene er dokumenteret	Ingen væsentlige afvigelser konstateret
3.4.1.1	Virksomheden skal installere anti-malwaresoftware på it-systemer og enheder, som er defineret i kortlægningen i 1.2.3.1.	Inspiceret, at der foreligger en procedure for anvendelsen af anti-malwaresoftware. Inspiceret, at der stilles krav om installation af anti-malwaresoftware på virksomhedens it-systemer og enheder jf. kortlægningen i 1.2.3.1.	Ingen væsentlige afvigelser konstateret
3.4.1.3	Anti-malwaresoftwaren (3.4.1.1) og alle tilknyttede malware-signaturfiler skal holdes opdateret. Der skal kontrolleres for opdateringer, mindst på daglig basis.	Inspiceret, at der foreligger en procedure for opdatering af anti-malwaresoftware, herunder malware-signaturfiler. Inspiceret, at seneste opdatering af anti-malware er foretaget indenfor det seneste døgn.	Ingen væsentlige afvigelser konstateret

Kriterie 3: Teknisk IT-sikkerhed Virksomhedens systemer og enheder skal være sikret, så virksomheden reducerer sandsynligheden for sikkerhedshændelser baseret på de mest udbredte trusler. Målet er både at nedbringe risikoen for angreb og databrud og sætte virksomheden i stand til hurtigt og effektivt at opdage, inddæmme og afbøde konsekvenserne samt genoprette vigtige data og systemer, når sikkerhedsbruddet eller angrebet sker.			
Ref.	**Virksomhedens udvalgte krav**	**Tilsynets udførte handling**	**Resultat af test**
3.5.1.1	Virksomheden skal definere en proces for at holde soft- og firmware opdateret. Processen skal tage udgangspunkt i kortlægningen over it-systemer, netværkskomponenter, enheder og software defineret i 1.2.3.1.	Inspiceret, at der foreligger en procedure for opdatering af soft- og firmware, som tager udgangspunkt i kortlægningen i 1.2.3.1.	Ingen væsentlige afvigelser konstateret
3.6.1.1	Virksomheden skal med udgangspunkt i hhv. kortlægning af personoplysninger (1.2.1.1), forretningskritiske data (1.2.2.2) og it-systemer, tjenester, netværkskomponenter, enheder og software (1.2.3.1) dokumentere hvilke data, der skal tages backup af.	Inspiceret, at der foreligger en procedure for backup, som angiver hvilke data, der skal tages backup af.	Ingen væsentlige afvigelser konstateret
3.6.1.6	Virksomheden skal udarbejde og vedligeholde en dokumenteret procedure for gendannelse af de data, som er identificerede i 3.6.1.1. Proceduren skal som minimum revideres årligt.	Inspiceret, at der foreligger en procedure for gendannelse af data. Inspiceret, at proceduren er revideret indenfor det seneste år.	Ingen væsentlige afvigelser konstateret

Kriterie 4: Krav til leverandørers it-sikkerhed og ansvarlige dataanvendelse Virksomheden skal have overblik over de leverandører, der håndterer personoplysninger og forretningskritiske data eller på anden måde kan påvirke virksomhedens it-sikkerhed. Virksomheden har formuleret passende it-sikkerhedskrav og krav til ansvarlig dataanvendelse hos leverandørerne og har implementeret kravene kontraktuelt. Større virksomheder foretager risikovurderinger af sine leverandører.			
Ref.	**Virksomhedens udvalgte krav**	**Tilsynets udførte handling**	**Resultat af test**
4.1.1.1	Virksomheden skal udarbejde og vedligeholde en kortlægning over alle leverandører og angive hvilke, der behandler og/eller kan påvirke sikkerheden af personoplysninger (1.2.1.1) og forretningskritiske data (1.2.2.2).	Inspiceret, at der forelægger en kortlægningen over alle leverandører, hvor det er angivet hvilke, der behandler eller kan påvirke sikkerheden af personoplysninger og forretningskritisk data. Inspiceret, at der foreligger en procedure for løbende og rettidig vedligeholdelse af kortlægning af leverandører.	Ingen væsentlige afvigelser konstateret
4.2.1.1	Med udgangspunkt i politik for it-sikkerhed og relaterede styringsdokumenter (1.4.1.1) skal virksomheden udarbejde en beskrivelse af virksomhedens sikkerhedskrav, som skal indgå i kontraktgrundlaget med virksomhedens leverandører kortlagt i 4.1.1.1.	Inspiceret, at der foreligger formaliserede sikkerhedskrav, der skal indgå i leverandøraftaler. Inspiceret, ved en stikprøve af leverandører, at sikkerhedskrav er medtaget i kontrakten.	Ingen væsentlige afvigelser konstateret
4.3.1.1	Med udgangspunkt i politik for behandling af personoplysninger og relaterede styringsdokumenter (1.6.1.1) skal virksomheden udarbejde en skriftlig beskrivelse af virksomhedens krav og instruks, som skal indgå i kontraktgrundlaget med virksomhedens leverandører kortlagt i 4.1.1.1, herunder databehandleraftaler.	Inspiceret, at der foreligger formaliserede krav og instrukser, der skal indgå i leverandøraftaler, herunder databehandleraftaler. Inspiceret, ved en stikprøve af leverandører, at der er indgået databehandleraftaler.	Ingen væsentlige afvigelser konstateret

Kriterie 5: Transparens & kontrol med data
Virksomheden lever op til gældende standarder, lovgivning og god praksis for databehandling i forbindelse med eksternt rettede aktiviteter, der indeholder behandling af personoplysninger.

Ref.	Virksomhedens udvalgte krav	Tilsynets udførte handling	Resultat af test
5.1.1.1	Virksomheden skal kommunikere til den registrerede, INDEN en konkret indsamling af personoplysninger eller så tidligt som muligt, hvis oplysningerne er indsamlet hos tredjepart. Der skal orienteres om: 1. Kontaktoplysninger på den dataansvarlige 2. Kontaktoplysninger på databeskyttelsesrådgiveren 3. Formål med og retsgrundlaget for behandlingen af personoplysninger 4. Kategorier af personoplysninger 5. Modtagere eller kategorier af modtagere 6. Overførsel til modtagere i tredjelande, herunder internationale organisationer 7. Hvor personoplysninger stammer fra 8. Opbevaringstiden af personoplysninger, eller kriterierne til at fastlægge disse 9. Automatiske beslutninger, herunder profilering (hvis dette benyttes) 10. Om retten til at trække samtykket tilbage, information om de legitime interesser, der forfølges eller information om hvorvidt behandlingen er lovpligtig eller et krav jf. en kontrakt. Informationen afhænger af retsgrundlaget. 11. Rettigheder (sletning, indsigelse mv.) 12. Klagevejledning til Datatilsynet	Inspiceret, at der foreligger en procedure for kommunikation til den registrerede. Inspiceret, at der foreligger krav om kommunikation til den registrerede, inden indsamling af personoplysninger finder sted. Inspiceret, at der foreligger krav om at den registrerede orienteres om følgende: 1. Kontaktoplysninger på den dataansvarlige 2. Kontaktoplysninger på databeskyttelsesrådgiveren 3. Formål med og retsgrundlaget for behandlingen af personoplysninger 4. Kategorier af personoplysninger 5. Modtagere eller kategorier af modtagere 6. Overførsel til modtagere i tredjelande, herunder internationale organisationer 7. Hvor personoplysninger stammer fra 8. Opbevaringstiden af personoplysninger, eller kriterierne til at fastlægge disse 9. Automatiske beslutninger, herunder profilering (hvis dette benyttes) 10. Om retten til at trække samtykket tilbage, information om de legitime interesser, der forfølges eller information om hvorvidt behandlingen er lovpligtig eller et krav jf. en kontrakt. Informationen afhænger af retsgrundlaget. 11. Rettigheder (sletning, indsigelse mv.) 12. Klagevejledning til Datatilsynet Inspiceret, ved en stikprøve af brud på data til tredjepart, at behandling heraf er foretaget i overensstemmelse med proceduren.	Ingen væsentlige afvigelser konstateret Vi har noteret at der ikke har været brud på data til tredjepart de seneste 12 måneder.

Kriterie 5: Transparens & kontrol med data Virksomheden lever op til gældende standarder, lovgivning og god praksis for databehandling i forbindelse med eksternt rettede aktiviteter, der indeholder behandling af personoplysninger.			
Ref.	**Virksomhedens udvalgte krav**	**Tilsynets udførte handling**	**Resultat af test**
5.3.1.1	Den registrerede skal have mulighed for at udøve sine rettigheder på en enkel måde.	Inspiceret, at der foreligger en privatlivspolitik. Inspiceret, at privatlivspolitikken indeholder information om: - Hvordan den registrerede kan få indsigt i eller rette oplysninger - Hvordan den registrerede har adgang til at trække samtykke tilbage. - Hvordan den registrerede kan ændre indstillinger for en given behandling. Vurderet, at ovenstående er tilstrækkeligt nemt for den registrerede.	Ingen væsentlige afvigelser konstateret
5.3.1.2	Den registrerede skal kunne administrere sine valg omkring virksomhedens brug af den registreredes personoplysninger i et brugervenligt dashboard.	Inspiceret, at den registrerede kan administrere sine valg omkring brugen af cookies i et brugervenligt dashboard. Inspiceret, at der foreligger en politik vedrørende cookies. Inspiceret, at den registreredes valg og eventuelle ændring af cookies gennemføres.	Ingen væsentlige afvigelser konstateret

Kriterie 8: Dataetik
Virksomheder skal kunne drage nytte af data. Dette skal altid ske på baggrund af menneskets ret til privatlivsbeskyttelse samt ud fra en række etiske principper. Virksomheder, der forholder sig til dataetik, arbejder med at identificere de mest kritiske risici som brugen af data kan medføre på kort sigt og på langt sigt. Virksomheden udvikler produkter og tjenester med udgangspunkt i disse indsigter.

Ref.	Virksomhedens udvalgte krav	Tilsynets udførte handling	Resultat af test
8.1.1.1	Virksomheden skal udfylde skemaet med dataetiske overvejelser med udgangspunkt i virksomhedens eksternt rettede aktiviteter kortlagt i 1.2.3.3. For hvert spørgsmål skal virksomheden give status ved at svare ét af følgende: • Ikke relevant • Ingen overvejelser • Nogle overvejelser • Foranstaltninger planlagt • Foranstaltninger implementeret • Kontinuerlig proces etableret Udover status skal der for hvert spørgsmål i fritekst beskrives, hvilke overvejelser virksomheden har gjort eller gør.	Inspiceret at, alle dataetiske overvejelser i D-mærkets skema er blevet udfyldt og besvaret. Inspiceret, at der for hvert spørgsmål hvor relevant, er angivet hvilke overvejelser virksomheden har gjort eller gør.	Ingen væsentlige afvigelser konstateret

7. Forløb af audit

Virksomheden anmodede om tilsyn den 27.02.2024

Virksomheden fik tilsendt Mærkningsordningens udvalgte kontrolmål og krav den 05.03.2024

Virksomheden og Mærkningsordningen afholdt workshop den 17.04.2024

Virksomheden og Mærkningsordningen afholdt opfølgende workshop den 01.05.2024

Mærkningsordningen modtog det sidste efterspurgte dokumentation 15.05.2024

Mærkningsordningen afsluttede tilsynet med Virksomheden den 28.05.2024

8. Konklusion

Virksomheden har på generel tilfredsstillende måde, uden væsentlige mangler, dokumenteret efterlevelse af Mærkningsordningens udvalgte kontrolmål og krav.

Mærkningsordningens tilsyn konkluderer på baggrund af ovenstående, at D-mærket tildeles Virksomheden. Tildelingen gælder for perioden 01.06.2024 til 01.07.2025. Virksomheden kan genansøge om D-mærket, som beskrevet i D-mærkets vilkår.

Lead Auditor	Jetmir Asani	**Dato**	28.06.2024
Underskrift			
Auditor	Stine Randklev Nissen	**Dato**	28.06.2024
Underskrift			
D-mærketildeling	**D-mærket er blevet tildelt**	**D-mærket er *ikke* blevet tildelt**	
	☒	☐	

Type af kontrol	☒ Point in time	☐ Over time