01. oktober 2025

D-mærket

Virksomhedsrapport

D-mærkets kontrol af PERSPEKTIVA IT ApS

1. Formål og tiltænkte brugere

Denne attest er udarbejdet til PERSPEKTIVA IT ApS (”**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 attesten.

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 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	PERSPEKTIVA IT ApS				
Virksomhedsadresse	Højvang 5				
Postnummer	4300	**By**	Holbæk		
Telefonnummer	8853 0200	**CVR**	29616892		
URL	https://www.perspektiva-it.dk/				
Branche	Andre IT- og computerserviceaktiviteter				
Branchekode	629000				
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	Claus Daugaard Hansen				
Titel	Systemarkitekt	**E-mail**	cdh@perspektiva-it.dk		

5. Omfang for audit

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

Tilsynet er udført som et "*over time*" tilsyn, hvorfor Virksomheden har dokumenteret den operationelle effektivitet af de udvalgte krav, hvor perioden fra seneste tildeling af D-mærket til genanmodning om D-mærket (12 måneder) er afdækket.

Mærkningsordningens Auditors har udtaget stikprøver dækkende for perioden på relevante krav.

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
1.2.1.2	Kortlægningen af alle typer personoplysninger (1.2.1.1) skal som minimum revideres årligt og opdateres ved ændringer af de typer af personoplysninger, der behandles.	Forespurgt, om processen for vedligeholdelse af kortlægningen. Inspiceret, at en procedure for vedligeholdelse af kortlægning er udarbejdet og revideres. Inspiceret, at proceduren er er revideret indenfor det seneste år.	Ingen væsentlige afvigelser
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
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
1.2.3.5	Kortlægningerne (1.2.3.1, 1.2.3.2, 1.2.3.3, 1.2.3.4) skal som minimum revideres årligt og opdateres i forbindelse med væsentlige ændringer, som påvirker dem.	Inspiceret, at procedure for vedligeholdelse af kortlægningerne er udarbejdet. Inspiceret, at der er krav om årlig revidering af kortlægningerne.	Ingen væsentlige afvigelser

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
		Inspiceret, at kortlægningerne er revideret inden-for det seneste år.	
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 afsluttende accept af restrisiko. Inspiceret, at identificerede risici er vurderet og tildelt en vægtning ud fra sandsynlighed og konsekvens. Inspiceret, at processen indeholder definition af risikoappetitten.	Ingen væsentlige afvigelser
1.3.1.4	Virksomhedens øverste ledelse skal definere og minimum årligt revidere virksomhedens risikoappetit, og denne skal indgå i risikovurderingsprocessen (1.3.1.2).	Inspiceret, at risikoappetit er defineret af den øverste ledelse. Inspiceret, at procedure for vedligeholdelse af definitionen er udarbejdet.	Ingen væsentlige afvigelser

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
		Inspiceret, at definition af risikoappetit er foretaget indenfor det seneste år.	
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 relaterede handlingsplaner er revideret indenfor det seneste år.	Ingen væsentlige afvigelser
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

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
1.6.1.2	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
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
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

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
2.2.1.1	Virksomheden skal have et træningsprogram om it-sikkerhed for alle ansatte og brugere, som benytter it.	Inspiceret, at der foreligger et træningsprogram om it-sikkerhed. Inspiceret, at der foreligger en procedure for træning af ansatte og eksterne.	Ingen væsentlige afvigelser
2.3.1.3	Træningsprogram om ansvarlig behandling af personoplysninger (2.3.1.1) skal som minimum dække; 1. Virksomhedens politik for behandling af personoplysninger (1.6.1.1) og den ansattes/brugerens ansvar (kun gældende for virksomhedsgruppe III og IV) 2. Viden om ansvarlig behandling af personoplysninger, og hvordan dette efterleves 3. Hvordan man skal forholde sig, hvis man opdager eller mistænker et databrud	Inspiceret, at træningsprogram dækker: 1. Virksomhedens politik for behandling af personoplysninger og den ansattes/brugerens ansvar 2. Viden om ansvarlig behandling af personoplysninger og hvordan dette efterleves 3. Hvordan man skal forholde sig, hvis man opdager eller mistænker et databrud	Ingen væsentlige afvigelser

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
2.3.2.1	Virksomheden skal etablere et træningsprogram om dataetik for alle ansatte, som arbejder med eksternt rettede aktiviteter (1.2.3.3).	Inspiceret, at der foreligger et træningsprogram om dataetik.	Ingen væsentlige afvigelser

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
3.1.1.1	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 tekniske krav om brug af flerfaktorautentifikation for administrative grænseflader. Inspiceret, ved en stikprøve af identificerede enheder, at der er etableret flerfaktorautentifikation.	Ingen væsentlige afvigelser
3.2.1.1	For at sikre ensartet konfiguration af funktionalitet og sikkerhed, skal der etableres konfigurationstandarder. De skal som minimum indeholde følgende: 1) Fjerne og deaktivere unødvendige brugerkonti 2) Ændre eventuelle standard eller usikre kontoadgangskoder til stærke adgangskoder 3) Fjerne eller deaktivere unødvendig software og funktionalitet (fx applikationer, systemværktøjer, scripts og netværkstjenester) 4) Deaktivere enhver "auto-run" tjeneste, der tillader filudførelse uden brugertilladelse (fx når filerne downloades fra internettet) 5) Slå relevant logning til og som minimum sikre, at alle handlinger som udføres af administratorer og superbrugere logges 6) Som udgangspunkt slå alt sikkerhedsfunktionalitet til med mindre at dette forhindrer ønsket funktionalitet	Forespurgt, hvorledes der etableres konfigurationsstandarder på nye systemer. Inspiceret, ved en stikprøve af identificerede enheder, at konfigurationsstandarder er etableret.	Ingen væsentlige afvigelser

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
3.3.1.5	Virksomheden skal kun tildele administrative rettigheder til et minimum af brugere. Der skal kun tildeles de rettigheder, der er nødvendige for at brugeren kan udføre sit arbejde. Virksomheden skal vedligeholde en kortlægning over brugere, som har fået tildelt en administrativ brugerkonti og forklare, hvorfor denne er tildelt.	Inspiceret, at udelukkende brugere med et arbejdsbetinget behov har en administrativ brugerkonto. Inspiceret, at der foreligger en kortlægning over brugere med administrative rettigheder.	Ingen væsentlige afvigelser
3.3.1.7	Alle brugerkonti med tildelte administrative adgangsrettigheder (3.3.1.5) skal revideres hvert kvartal. Unødvendige brugerkonti med administrative rettigheder fjernes eller deaktiveres.	Inspiceret, at brugere med administrative adgangsrettigheder revideres kvartalsvist Inspiceret, at unødvendige brugerkonti fjernes eller deaktiveres rettidigt.	Ingen væsentlige afvigelser
3.3.1.8	Administrative brugerkonti (3.3.1.5) skal fjernes eller deaktiveres, når de ikke længere er nødvendige.	Inspiceret, at der er formaliseret en procedure, der beskriver vedligeholdelse af brugerkonti, herunder at burgerkonti fjernes når de ikke længere er nødvendige. Inspiceret, at unødvendige brugerkonti fjernes eller deaktiveres rettidigt.	Ingen væsentlige afvigelser
3.4.1.4	Anti-malwaresoftwaren (3.4.1.1) skal konfigureres til at scanne filer og eksterne enheder (fx USB-nøgler) automatisk, når de hentes, åbnes eller indsættes.	Inspiceret, at anti-malwaresoftware er konfigureret til at scanne filer når de downloades. Inspiceret, at anti-malwaresoftware automatisk scanner eksterne enheder, når de tilsluttes.	Ingen væsentlige afvigelser

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
3.4.2.1	Virksomheden skal have installeret og konfigureret et spamfilter og en anti-malware-løsning til scanning af e-mails.	Inspiceret, at spamfilter er installeret og konfigureret. Inspiceret, at anti-malwaresoftware er konfigureret til scanning af e-mails.	Ingen væsentlige afvigelser
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
3.6.1.2	Virksomheden skal dokumentere; • Hvilken type backup der tages • Hvor ofte der tages backup • Hvor lang tid backup'en gemmes	Inspiceret, at der forefindes dokumentation for: • Hvilken type backup der tages • Hvor ofte der tages backup • Hvor lang tid backup'en gemmes	Ingen væsentlige afvigelser
3.6.1.3	Backupdata (3.6.1.1) skal krypteres under transport og opbevaring.	Inspiceret, ved en stikprøve af backupdata, at det krypteres under transport og opbevaring.	Ingen væsentlige afvigelser
3.6.1.5	Backupdata (3.6.1.1) skal opbevares på en måde, så infektion af virksomhedens net ikke påvirker backuppen	Inspiceret, at backupdata opbevares således at det ikke påvirkes ved infektion af virksomhedens net.	Ingen væsentlige afvigelser
3.6.1.7	Procedure for gendannelse af data (3.6.1.6) skal testes jævnligt, minimum årligt. Hvis fejl eller mangler identificeres som en del af testen, skal disse udbedres.	Inspiceret, at der foreligger en procedure for test af data gendannelse. Inspiceret, at den seneste test af data gendannelse er foretaget indenfor det seneste år. Inspiceret, at fejl identificeret med testen er udbedret rettidigt.	Ingen væsentlige afvigelser

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
4.1.1.2	I forbindelse med udvælgelse af mulige leverandører skal det afklares, hvorvidt leverandører kan leve op til de krav, som virksomheden selv skal leve op til for at kunne efterleve D-mærkets kriterier.	Inspiceret, at der foreligger en procedure for leverandørstyring. Inspiceret, at det afklares, hvorvidt leverandører kan efterleve samme krav som virksomheden skal efterleve.	Ingen væsentlige afvigelser
4.1.1.3	Inden virksomheden indgår en aftale med en leverandør, og leverandøren kommer til at håndtere eller kunne påvirke sikkerheden af personoplysninger (1.2.1.1) eller forretningskritiske data (1.2.2.2), skal der laves en risikovurdering -og håndtering som defineret i 1.3.1.2. Her skal der også tages højde for eventuelle krav, som leverandøren ikke kan efterleve.	Inspiceret, at der udarbejdes en risikovurdering på leverandører inden en aftaleindgåelse.	Ingen væsentlige afvigelser
4.2.1.2	De it-sikkerhedskrav som virksomheden stiller til sine leverandører skal som minimum indeholde de it-sikkerhedskrav, som D-mærket stiller til virksomheden.	Inspiceret, at der stilles krav til leverandører, som minimum indeholder de it-sikkerhedskrav virksomheden selv skal efterleve.	Ingen væsentlige afvigelser

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

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
5.1.2.1	For hver dataindsamling af personoplysninger og tilhørende samtykke, bør der inden samtykke blive fremvist en liste over, hvordan data videregives og anvendes, grupperet efter overskrifterne: • Forskning • Markedsføring • Videresalg, • Lagring udenfor EU	Inspiceret, at en liste af hvordan data videregives og anvendes bliver fremvist inden der gives samtykke. Inspiceret, at listen er grupperet efter overskrifterne: • Forskning • Markedsføring • Videresalg, • Lagring udenfor EU	Ingen væsentlige afvigelser
5.2.1.1	Den registrerede skal give samtykke til brug af cookies udover de strengt nødvendige, før cookies bliver placeret.	Inspiceret, at der skal gives samtykke før cookies bliver placeret.	Ingen væsentlige afvigelser
5.2.1.2	Den registrerede skal modtage nøjagtige og specifikke oplysninger om de data, som hver cookie lagrer, og formålet hermed. Oplysningerne skal være på et almindeligt sprog, og gives før cookies placeres.	Inspiceret, at der foreligger en cookiepolitik. Inspiceret, at specifikke oplysninger herunder formål med cookie er beskrevet i et let forståeligt sprog før samtykke gives.	Ingen væsentlige afvigelser
5.2.1.3	Den registrerede skal kunne få adgang til basal funktionalitet af virksomhedens service, selvom brugen af visse cookies nægtes.	Inspiceret, at det er muligt og nemt at afvise eller afgive samtykke til cookies. Inspiceret, at der som minimum er adgang til basal funktionalitet ved afvisning af cookies.	Ingen væsentlige afvigelser
5.2.1.4	Den registrerede skal kunne trække sit samtykke tilbage lige så let, som det var at give samtykke i første omgang.	Inspiceret, at den registrerede på let vis kan trække sit samtykke tilbage. Inspiceret, at tilbagetrækning af samtykke effektivt gennemføres på hjemmesiden.	Ingen væsentlige afvigelser

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
5.4.1.1	Der skal være en enkel og lettilgængelig klagevejledning om, hvordan den registrerede kan indsende spørgsmål eller klage vedrørende dataanvendelsen og it-sikkerheden, samt hvordan den registrerede kan gøre indsigelse mod virksomhedens anvendelse af den registreredes personoplysninger.	Inspiceret, at der forefindes en lettilgængelig vejledning på hjemmesiden. Inspiceret, at klagevejledningen er beskrevet på et let og forstået sprog. Inspiceret, at processen for behandlingen er beskrevet. Inspiceret, ved en stikprøve af klager eller indsigelse mod anvendelse af persondata, at de efterleves effektivt	Ingen væsentlige afvigelser

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 udfyldt og besvaret. Inspiceret, at der for hvert spørgsmål i fritekst, er angivet hvilke overvejelser virksomheden har gjort eller gør.	Ingen væsentlige afvigelser
8.1.1.4	Virksomheden skal opdatere skemaet med dataetiske overvejelser (8.1.1.1) minimum årligt, eller ved væsentlige ændringer.	Inspiceret, at skema med dataetiske overvejelser er blevet opdateret indenfor de seneste 12 måneder.	Ingen væsentlige afvigelser

7. Forløb af audit

Virksomheden anmodede om tilsyn den 04.07.2025.

Virksomheden og Mærkningsordningen afholdt opstartsmøde den 07.08.2025.

Virksomheden fik tilsendt Mærkningsordningens udvalgte kontrolmål den 07.08.2025.

Mærkningsordningen afsluttede tilsynet med Virksomheden den 23.09.2025.

8. Konklusion

PERSPEKTIVA IT ApS 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 01.09.2025 til 01.10.2026. Virksomheden kan genansøge om D-mærket, som beskrevet i D-mærkets vilkår.

Lead Auditor	Emil Zeiler Alfsen	**Dato**	01.10.2025
Underskrift			
Auditor	Jetmir Asani	**Dato**	01.10.2025
Underskrift			
D-mærketildeling	**D-mærket er blevet tildelt**	**D-mærket er *ikke* blevet tildelt**	
	☒	☐	

Type af kontrol	☐ Point in time	☒ Over time