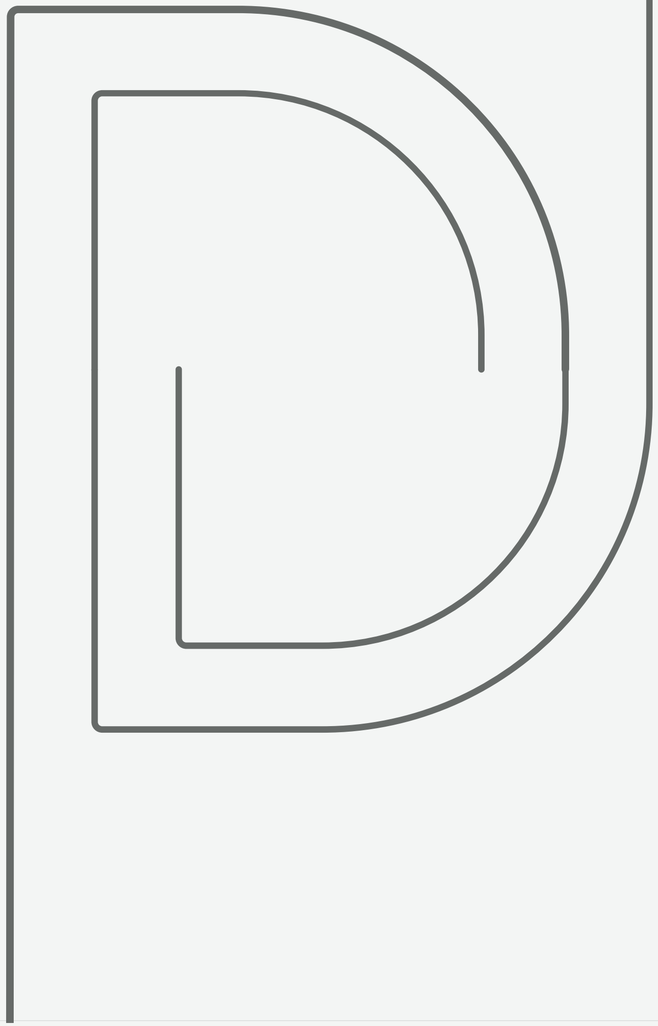
Danmarks nye mærkningsordning for it-sikkerhed og ansvarlig dataanvendelse

Mikael Jensen, D-mærket

Konference
Driving IT

Tid og sted
5. november 2021 I 15.35 – 16.00 I IDA, København



DANSK ERHVERV

SMVdanmark

Forbrugerrådet Tænk

INDUSTRIENS FOND

Agenda

1. Baggrund
2. Mærkets positionering & navn
3. Typeinddeling af virksomheder efter risikotype
4. Mærkets 8 kriterier
5. Kunderejsen og prismodel

Kapitel 1

Baggrund

D-mærket ...

- ... er en efterspørgselsdrevet og frivillig mærkningsordning for it-sikkerhed og ansvarlig dataanvendelse
- ... er mærkning af virksomheder og ikke specifikke produkter og tjenester
- ... består af 8 overordnede kriterier med fokus på it-sikkerhed, persondatabeskyttelse, kunstig intelligens og dataetik
- ... er målrettet såvel en B-2-B og en B-2-C kontekst
- ... er ét mærke, men antallet af kriterier vil afhænge af virksomhedens generiske risikoprofil
- ... er et markedsføringsredskab til virksomheder

Industriens Fond står bag D-mærket i samarbejde med Dansk Industri, Dansk Erhverv, SMVdanmark og Forbrugerrådet Tænk. D-mærket støttes af Erhvervsstyrelsen og er en uafhængig privat organisation.

Kilde: https://d-maerket.dk/om/

Det vi gerne vil med D-mærket, er at gøre digital tryghed og tillid til et positivt konkurrenceparameter og en dansk og europæisk styrkeposition.

Malene Stidsen

Programchef, Industriens Fond

Kilde: https://d-maerket.dk/events-og-artikler/verdens-forste-maerke-for-digital-ansvarlighed-er-klar-til-brug/

FORMÅL

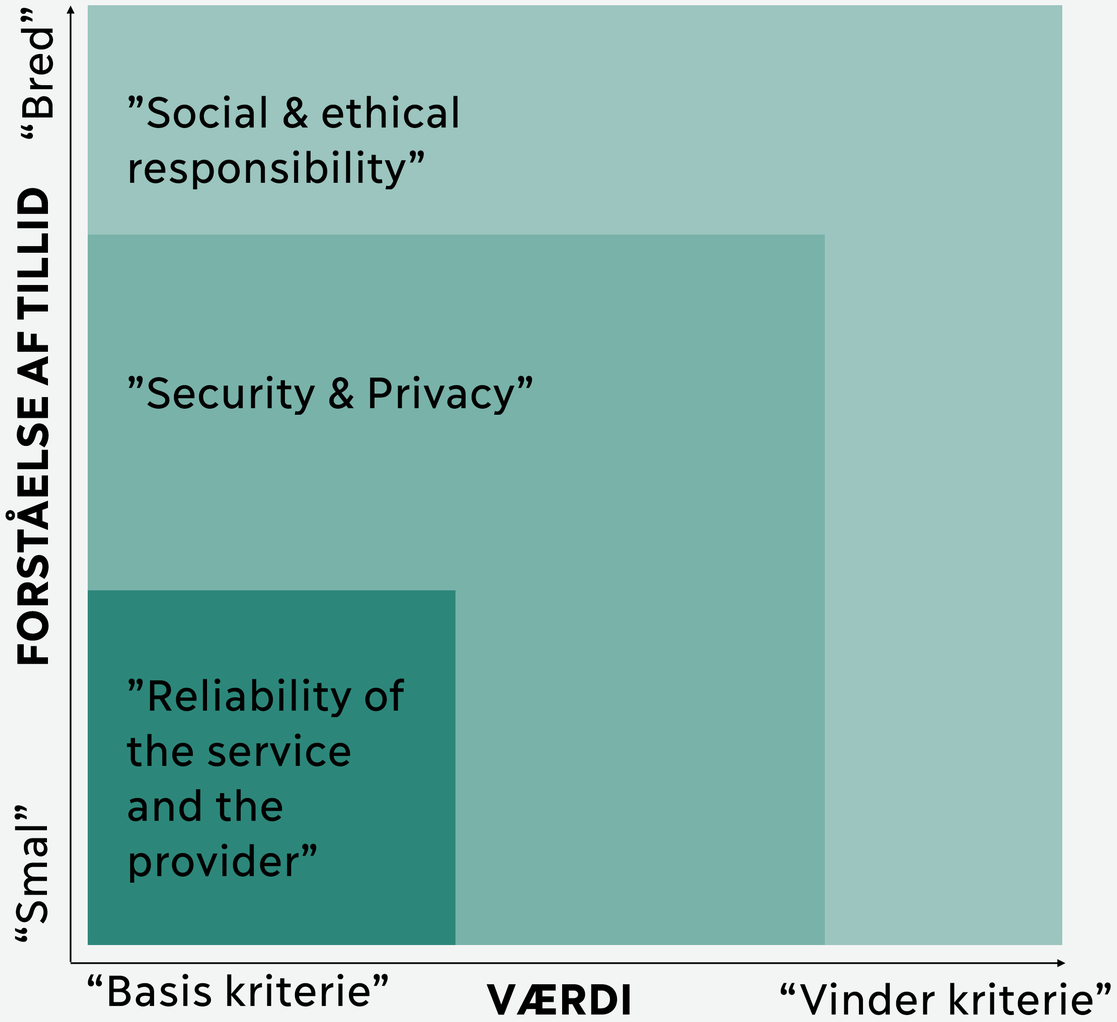
D-mærket skal skabe digital tryghed hos kunder og forbrugere og digital ansvarlighed hos virksomhederne ...

1. **... ved at give dansk erhvervsliv et solidt løft for it-sikkerhed og ansvarlig dataanvendelse**
2. **... ved at give forretningsværdi for den enkelte virksomhed**
3. **... ved at skabe tryghed hos virksomhedernes kunder og samarbejdspartnere**
4. **... ved at gøre it-sikkerhed og ansvarlig dataanvendelse til en dansk styrkeposition**

Kapitel 2

Mærkets positionering & navn

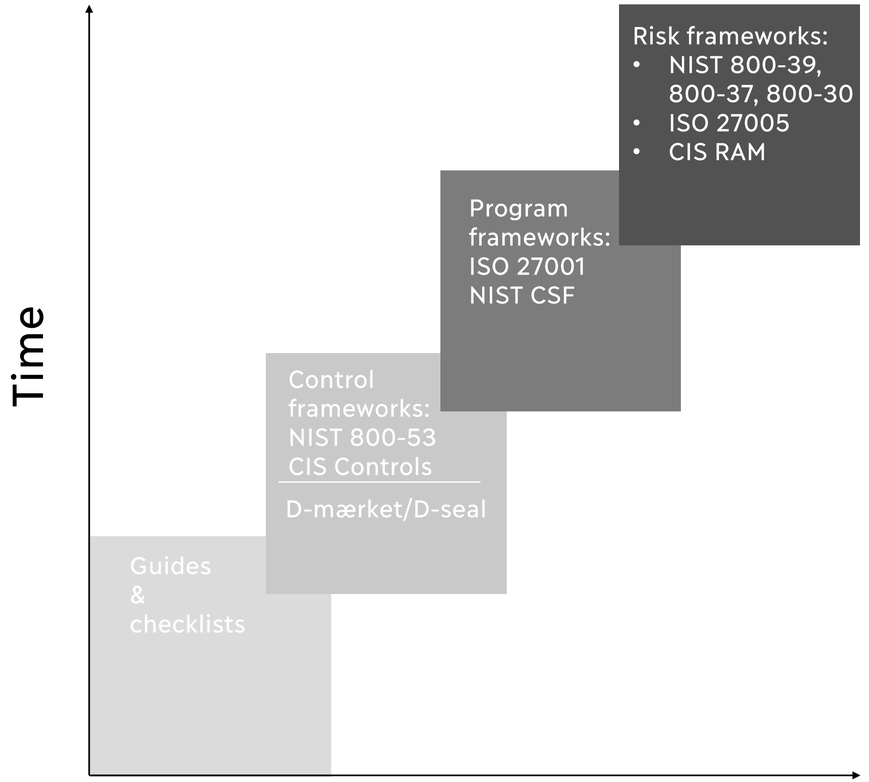
Digital tillid set fra brugerens synsvinkel



Kilde: Digital trust from the customer’s perspective A qualitative study in Switzerland, January 2020

Mærkets rolle set fra et virksomhedsperspektiv

Complexity in IT security work methods in relation to the maturity of an SME



Inspired by: ”Anbefaling: En mærkningsordning for it-sikkerhed”, Virksomhedsrådet for IT-sikkerhed (December 2018) & CIS Controls V7 poster https://www.cisecurity.org/white-papers/cis-controls-v7-poster/

D-mærkets differentiator/USP og ESSENS

FORBRUGERE

D-mærket giver mig tillid til (deling og anvendelse af) data, og gør det nemt for mig at vælge virksomheder og tjenester, der behandler data sikkert og ansvarligt.

“Skaber digital tryghed for mig!”

VIRKSOMHEDER

D-mærket er en enkel og tillidsfuld guide, der gør det nemt at håndtere data sikkert og ansvarligt og derefter skilte med det.

“Skaber værdi for min forretning!”

SAMFUNDET

D-mærket gør digital sikkerhed og ansvarlig dataanvendelse til et positivt konkurrenceparameter og en dansk styrkeposition.

“Skaber et stærkere digitalt Danmark”

digital tryghed

digital tryghed

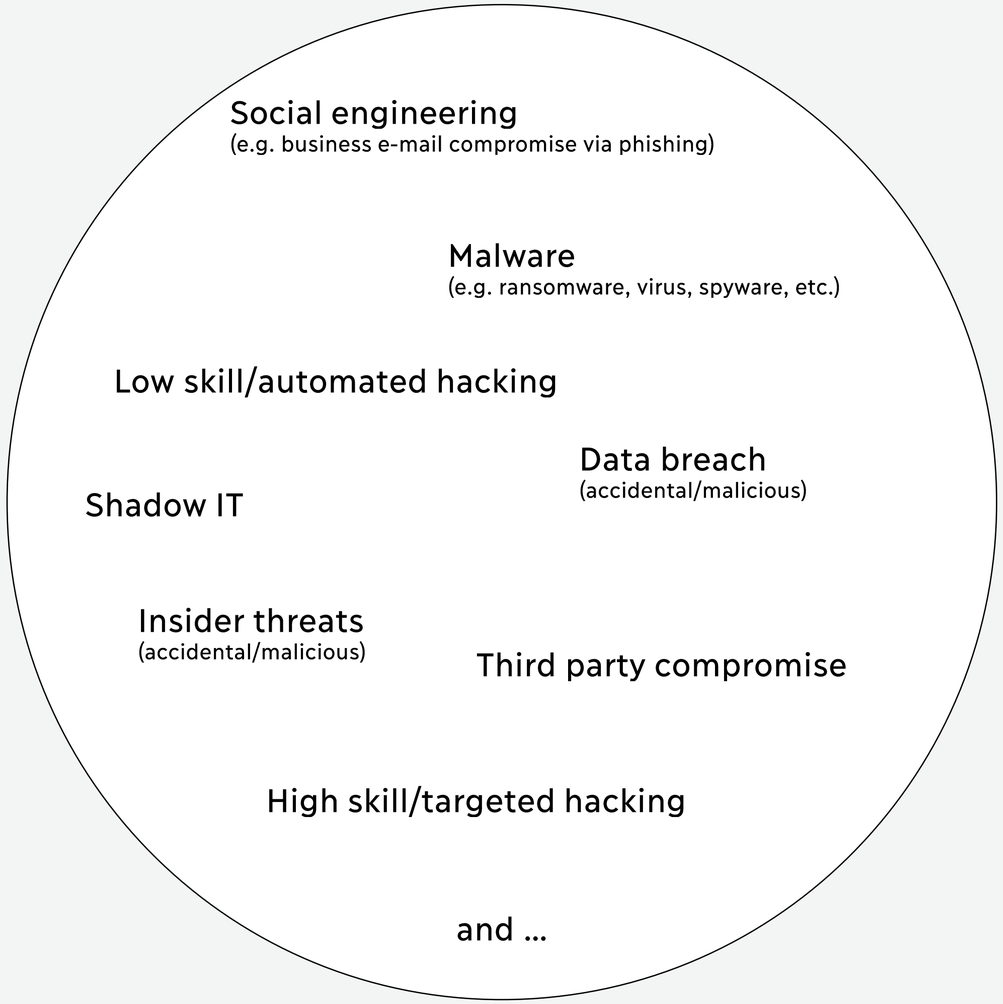
digital trust

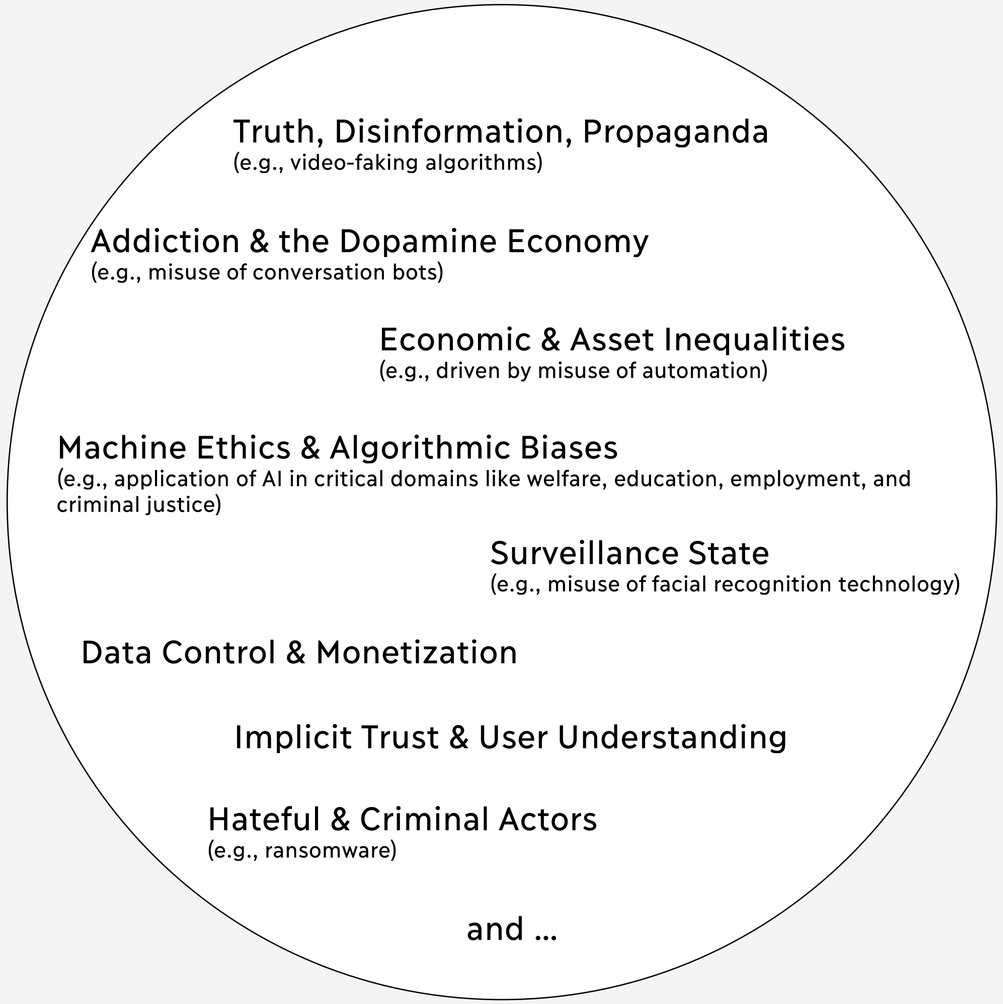
digital trust

Kapitel 3

Typeinddeling af virksomheder efter risikotype

Trusselsbillede: it-sikkerhed og dataetik





Hvilken gruppe tilhører din virksomhed?

Antallet af kriterier og krav som virksomheden skal leve op til afhænger af virksomhedsgruppen, men alle virksomheder skal som minimum leve op til kriterie 1, 2, 3 og 5.

Kriterier for indplacering i gruppe	Gruppe I	Gruppe II	Gruppe III	Gruppe IV
Antal ansatte	0-9	10-49	50-249	250+
Nettoomsætning (mio. DKK)	0-7,9	8-155,9	156-313	≥ 313
Leverandør af software eller it-tjenester	Nej	Nej	Ja	Ja
Behandler særlige kategorier af personoplysninger (fx helbredsoplysninger, race, sexualitet)	Nej	Ja	Ja	Ja

Kilde: https://d-maerket.dk/virksomhedsgrupper/

Kapitel 4

Mærkets 8 kriterier

Mærkets kriterier i værdikæden

Kilde: https://d-maerket.dk/kriterier/

Eksempel på udmøntning af kriterier til krav

Kriterie: Niveau 1 (fx 3.0) Overordnede kriterier indenfor it-sikkerhed, privatliv og etik	**Fx 3.0 Teknisk it-sikkerhed**			
Kriterie: Niveau 2 (fx 3.1 – 3.7) Opdeling af overordnede niveau 1 kriterier til håndterbare kriterier på lavere niveau	Fx 3.1 Netværkssikkerhed og kryptering		Fx 3.4 Beskyttelse mod malware	
Kriterie: Niveau 3 (fx 3.1.1 – 3.7.1) Opdeling af niveau 2 kriterier i operationelle kriterier	3.1.1 Beskyttelse af administrative grænseflader, netværk og enheder	3.1.2 Kryptering af ekstern netværksadgang	3.4.1 Implementering af beskyttelsesmekanismer mod malware	3.4.2 Beskyttelse mod uønskede e-mails
Krav til praktisk implementering (fx 3.1.1.1 – 3.7.1.6) Konkrete handlingskrav til praktisk implementering for at opfylde niveau 3-kriterier	3.1.1.1 – 3.1.1.3 Konkrete og handlingsorienterede krav	3.1.2.1 – 3.1.2.3 Konkrete og handlingsorienterede krav	3.4.1.1 – 3.4.1.10 Konkrete og handlingsorienterede krav	3.4.2.1 – 3.4.2.3 Konkrete og handlingsorienterede krav
Tilsyn og kontrol Tilsyns- og kontrolprocesser	Beskrivelse af, hvordan det er bevist, at kravene eller indikatorerne er opfyldt og / eller mængden eller kvaliteten i, hvor langt krav eller indikatorer er opfyldt	Beskrivelse af, hvordan det er bevist, at kravene eller indikatorerne er opfyldt og / eller mængden eller kvaliteten i, hvor langt krav eller indikatorer er opfyldt	Beskrivelse af, hvordan det er bevist, at kravene eller indikatorerne er opfyldt og / eller mængden eller kvaliteten i, hvor langt krav eller indikatorer er opfyldt	Beskrivelse af, hvordan det er bevist, at kravene eller indikatorerne er opfyldt og / eller mængden eller kvaliteten i, hvor langt krav eller indikatorer er opfyldt

Oversigt over D-mærkets kriterier på niveau 1 og 2 samt relation til rammeværker

KRITERIE 1 Styring og forankring i ledelsen	KRITERIE 2 Awareness og sikker adfærd	KRITERIE 3 Teknisk it-sikkerhed	KRITERIE 4 Krav til leverandørers it-sikkerhed og ansvarlige dataanvendelse	KRITERIE 5 Transparens & kontrol med data	KRITERIE 6 Privacy & security by design & default	KRITERIE 7 Pålidelige algoritmer & AI	KRITERIE 8 Dataetik
NIVEAU 2 KRITERIER 1.1 Roller og ansvar i forhold til it-sikkerhed og ansvarlig dataanvendelse 1.2 Overblik over data og systemer 1.3 Risikostyring 1.4 Politik for it-sikkerhed 1.5 It-beredskabsplan 1.6 Politikker for ansvarlig dataanvendelse 1.7 Udviklingsproces	NIVEAU 2 KRITERIER 2.1 Træn bestyrelsen og den øverste ledelse i sikkerhed, databeskyttelse og dataetik 2.2 Awareness om og træning i it-sikkerhed 2.3 Awareness om og træning i ansvarlig dataanvendelse	NIVEAU 2 KRITERIER 3.1 Netværkssikkerhed og kryptering 3.2 Korrekt konfiguration 3.3 Beskyttelse af administrative brugerkonti 3.4 Beskyttelse mod malware 3.5 Kontinuerlig opdatering af software og styresystemer 3.6 Beskyttelse mod tab af vigtige og fortrolige data 3.7 Overvågning af systemaktivitet gennem logning	NIVEAU 2 KRITERIER 4.1 Leverandørlivscyklus og risikovurdering 4.2 Krav til it-sikkerhed hos leverandører 4.3 Krav til ansvarlig databehandling hos leverandører	NIVEAU 2 KRITERIER 5.1 Information i relation til personoplysninger 5.2 Cookies 5.3 Kontrol over egne personoplysninger 5.4 Lettilgængelig klagevejledning	NIVEAU 2 KRITERIER 6.1 Vurdering 6.2 Privacy by design & default 6.3 Security by design & default 6.4 Implementering igennem udviklingsproces	NIVEAU 2 KRITERIER 7.1 Menneskeligt tilsyn og mellemkomst/indgriben og transparens 7.2 Data- og modelkvalitet 7.3 Implementering igennem udviklingsproces	NIVEAU 2 KRITERIER 8.1 Dataetik
EUROPÆISKE KILDER • GDPR	EUROPÆISKE KILDER • GDPR • Europarådet*	EUROPÆISKE KILDER • GDPR • High-Level Expert Group on AI (EU)	EUROPÆISKE KILDER • GDPR	EUROPÆISKE KILDER • GDPR • Datatilsynet (NO) • Datatilsynet (DK) • ENISA**	EUROPÆISKE KILDER • GDPR • Norwegian Data Protection Authority • ENISA**	EUROPÆISKE KILDER • GDPR • Europarådet* • High-Level Expert Group on AI (EU) • AIEI Group (DE) • German Data Ethics Commission (DE) • French Data Protection Authority (CNIL) • DS/PAS 2500 – 1.2020 (DK) • DS/PAS 25000-2.2020 (DK)	EUROPÆISKE KILDER • Den Europæiske Unions charter om grundlæggende rettigheder • Rådet for Digital Sikkerhed (DK) • Dataethics.eu (DK) • Ekspertgruppen om dataetik (DK) • Dataetisk Råd (DK) • UK GOV, Data Ethics Framework (UK) • ICO: Age Appropriate Design Code (UK)
INTERNATIONALE KILDER • ISO/IEC 27001:2013 • ISO/IEC 27701:2019 • NIST-CSF • CIS20	INTERNATIONALE KILDER • ISO/IEC 27001:2013 • ISO/IEC 27701:2019 • NIST-CSF • CIS20	INTERNATIONALE KILDER • ISO/IEC 27001:2013 • ISO/IEC 27701:2019 • NIST-CSF • CIS20 • OECD recommendations on AI	INTERNATIONALE KILDER • ISO/IEC 27001:2013 • ISO/IEC 27701:2019 • NIST-CSF • CIS20	INTERNATIONALE KILDER • ISO/IEC 27001:2013 • ISO/IEC 27701:2019	INTERNATIONALE KILDER • ISO/IEC 27001:2013 • ISO/IEC 27701:2019	INTERNATIONALE KILDER • OECD recommendations on AI • ISO/IEC TR 24028:2020 (Overview of trustworthiness in artificial intelligence)	INTERNATIONALE KILDER • Ethical OS (US)

* Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems
** Privacy and Data Protection by Design–from policy to engineering

Kriterie 1 - 3

#	Kriterier: niveau 1	Kriterier: niveau 2
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.	1.1 Roller og ansvar i forhold til it-sikkerhed og ansvarlig dataanvendelse 1.2 Overblik over data og systemer 1.3 Risikostyring 1.4 Politik for it-sikkerhed 1.5 It-beredskabsplan 1.6 Politikker for ansvarlig dataanvendelse 1.7 Udviklingsproces
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.	2.1 Træn bestyrelsen og den øverste ledelse i sikkerhed, databeskyttelse og dataetik 2.2 Awareness om og træning i it-sikkerhed 2.3 Awareness om og træning i ansvarlig dataanvendelse
3	**Teknisk it-sikkerhed** Virksomhedens systemer og enheder skal være sikret, så virksomheden reducerer sandsynligheden for hændelser 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 bruddet eller angrebet sker.	3.1 Netværkssikkerhed og kryptering 3.2 Korrekt konfiguration 3.3 Beskyttelse af administrative brugeradgange 3.4 Beskyttelse mod malware 3.5 Kontinuerlig opdatering af software og styresystemer 3.6 Beskyttelse mod tab af vigtige og fortrolige data 3.7 Overvågning af systemaktivitet gennem logning

Kilde: https://d-maerket.dk/kriterier/

Kriterie 4 - 5

#	Kriterier: niveau 1	Kriterier: niveau 2
4	**Krav til leverandørers it-sikkerhed og ansvarlige dataanvendelse** Virksomheden skal have overblik over sine 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.	4.1 Leverandørlivscyklus og risikovurdering 4.2 Krav til it-sikkerhed hos leverandører 4.3 Krav til ansvarlig databehandling hos leverandører
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.	5.1 Information i relation til personoplysninger 5.2 Cookies 5.3 Kontrol over egne personoplysninger 5.4 Lettilgængelig klagevejledning

Kilde: https://d-maerket.dk/kriterier/

Kriterie 6 - 8

#	Kriterier: niveau 1	Kriterier: niveau 2
6	**Privacy & security by design & default** I forbindelse med udviklingen af produkter og tjenester har det stor betydning for tiltroen til virksomheden, at der strukturelt arbejdes med privacy & security by design & default (PbD & SbD). Målet er at skabe sikre produkter og tjenester og beskytte brugernes privatliv og personoplysninger bedst muligt.	6.1 Vurdering 6.2 Privacy by design & default 6.3 Security by design & default 6.4 Implementering igennem udviklingsproces
7	**Pålidelige algoritmer & AI** Virksomheden skal sikre pålidelige algoritmer og AI, som man kan have tillid til, hvor der er menneskeligt tilsyn og mellemkomst, og hvor der tages ansvar for løbende at sikre kvaliteten. Derved sikres, at algoritmerne og AI virker til gavn for den enkelte og fællesskabet og kan accepteres af dem, de berører.	7.1 Menneskeligt tilsyn og mellemkomst/indgriben og transparens 7.2 Data- og modelkvalitet 7.3 Implementering igennem udviklingsproces
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.	8.1 Dataetik

Kilde: https://d-maerket.dk/kriterier/

Kriterie 6: Operationalisering af Privacy-by-Design

STEP 1: MAPPING

Hvis virksomheden udvikler software …

… så skal virksomheden **udarbejde og vedligeholde en kortlægning af virksomhedens nyudviklede produkter og tjenester,** som en del af kriterie 1.2.3

Del af den indledende typeinddeling samt mapping i kriterie 1.2.3 ” Overblik over it-systemer, tjenester, netværkskomponenter, enheder, software og aktivitetsbaserede algoritme/AI use cases”

STEP 2: RISIKOVURDERING

Virksomheden risikovurderer sine nyudviklede produkter og tjenester med udgangspunkt i risici for de registrerede og for virksomheden.

Del af kriterie 6.1.1 ”Risikovurdering”

STEP 3: SPECIFICERING AF KRAV

På baggrund af risikovurderingen dokumenterer virksomheden, hvilket niveau af persondatabeskyttelse og sikkerhed, som er nødvendigt i hvert nyudviklede produkt og tjeneste.

Del af kriterie 6.1.2 ”Tag stilling til persondatabeskyttelses- og sikkerhedsniveau”

STEP 4: VÆLG PBD STRATEGI(ER)

Med udgangspunkt i de specificerede krav skal virksomheden vælge minimum én af de tre PbD-strategier til hver af de nyudviklede produkter og tjenester.

- **Minimering og begrænsning** (kriterie 6.2.1)
- **Separering og skjul** (kriterie 6.2.2)
- **Aggregering** (kriterie 6.2.3)

Del af kriterie 6.2.1 – 6.2.3

Kilde: https://d-maerket.dk/kriterier/

Kriterie 7: Operationalisering af algoritmer & AI

STEP 1: ANVENDELSESOMRÅDE

Hvis virksomheden anvender algoritmer & AI så …

Del af den indledende typeinddeling

STEP 2: MAPPING

…skal virksomheden **identificere algoritme- og AI-baserede "use-cases"** som en del af kriterie 1.2.3

Del af Kriterie 1.2 "Overblik over data og systemer"

STEP 3: RISIKOVURDERING

…for hver "use-case" skal der udføres en **risikovurdering**, der anvender følgende klassifikation:

- **Meget høj** (out of scope)
  (meget store ulemper for mennesker)
- **Høj**
- **Lav**
  (mindre ulemper for mennesker)
- **Meget lav** (out of scope)

Del af Kriterie 7.1 "Menneskeligt tilsyn og mellemkomst/indgriben og transparens"

STEP 4: KRITERIER OG KRAV

Hvis "use-case" falder indenfor **"lav"** og **"høj"**, så skal kravene i kriterie 7 efterleves.

Hvis "use-casen" vurderes til **"meget lav"**, så skal virksomheden ikke leve op til kravene i kriterie 7

Hvis "use-casen" vurderes til **"meget høj"**, så kan og vil D-mærket ikke vurdere virksomheden og dermed kan virksomheden ikke tildeles D-mærket

Kriterie 7.1 – 7.3

Kilde: https://d-maerket.dk/kriterier/

Kriterie 8: Dataetik

#	Dataetiske spørgsmål
1	Har virksomheden overvejet **løsninger til at forbedre arbejdet med dataetik**? Fx nedsættelse af dataetisk arbejdsgruppe, awareness-skabende aktiviteter, åbenhedskultur
2	Har virksomheden overvejet **løbende inddragelse af relevante interessenter**? Fx for at undgå utilsigtet bias
3	Har virksomheden gjort sig overvejelser om **konsekvenserne forbundet med at påvirke brugerens adfærd**? Fx modvirke afhængighed, overforbrug, mobning
4	Hvis virksomheden **påvirker brugerens adfærd**, har virksomheden i så fald gjort sig overvejelser om, hvordan det kan **gøres mere transparent**, og **give brugeren mere kontrol**?
5	Har virksomheden gjort sig overvejelser om, **hvordan brugerens rettigheder bliver prioriteret** frem for kommercielle eller institutionelle interesser?
6	Har virksomheden gjort sig overvejelser om, hvordan **brugeren får mest mulig værdi ud af de data, der indsamles**?
7	Har virksomheden overvejet, hvordan de **undgår utilsigtede konsekvenser**? Fx overvågning, misbrug, spredning af misinformation eller lignende
8	Har virksomheden gjort sig overvejelser om, hvordan virksomheden kan **beskytte særlige målgrupper**? Fx børn og unge eller samfundsgrupper med særlige udfordringer
9	Har virksomheden gjort sig overvejelser om, **hvorvidt dataindsamling** og løsninger/produkter kan **begrænse borgernes rettigheder**?
10	Har virksomheden overvejet, om de kan **undgå at forstærke sociale og etiske problemstillinger**? Fx ulighed, udstilling af befolkningsgrupper og segmenter eller at en løsning kun kan bruges af bestemte brugere
11	**Kommunikerer** virksomheden sine **privacy-by-design strategier** til sine brugere?

Ikke relevant	Ingen overvejelser	Nogle overvejelser	Foranstaltninger planlagt	Foranstaltninger implementeret	Kontinuerlig proces etableret
☐	☐	☐	☐	☐	☐

Kilde: https://d-maerket.dk/kriterier/

Har virksomheden overvejet løsninger til at forbedre arbejdet med dataetik?

Fx nedsættelse af dataetisk arbejdsgruppe, awareness-skabende aktiviteter, åbenhedskultur

Dataetisk spørgsmål 1

Har virksomheden gjort sig overvejelser om konsekvenserne forbundet med at påvirke brugerens adfærd?

Fx modvirke afhængighed, overforbrug, mobning

Dataetisk spørgsmål 3

Har virksomheden gjort sig overvejelser om, hvordan brugerens rettigheder bliver prioriteret frem for kommercielle eller institutionelle interesser?

Dataetisk spørgsmål 5

Har virksomheden overvejet, hvordan de undgår utilsigtede konsekvenser?

Fx overvågning, misbrug, spredning af misinformation eller lignende

Dataetisk spørgsmål 7

Niveau 3 kriterier: virksomhedstype I (minimum)

Kriterie: niveau 1	Kriterie: 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
	1.5.1	It-beredskabsplan
2 Awareness og sikker adfærd	2.2.1	Træn alle ansattes og brugers viden om it-sikkerhed kontinuerligt
	2.3.1	Træn alle ansatte og brugeres viden om ansvarlig behandling af personoplysninger kontinuerligt
3 Teknisk it-sikkerhed	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
4 Krav til leverandørers it-sikkerhed og ansvarlige dataanvendelse		Afhænger af scope
5 Transparens og 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
	5.4.1	Lettilgængelig klagevejledning vedrørende ansvarlig dataanvendelse og it-sikkerhed
6 Privacy & security by design & default		Afhænger af scope
7 Pålidelige algoritmer & AI		Afhænger af scope
8 Dataetik		Afhænger af scope

Kapitel 5

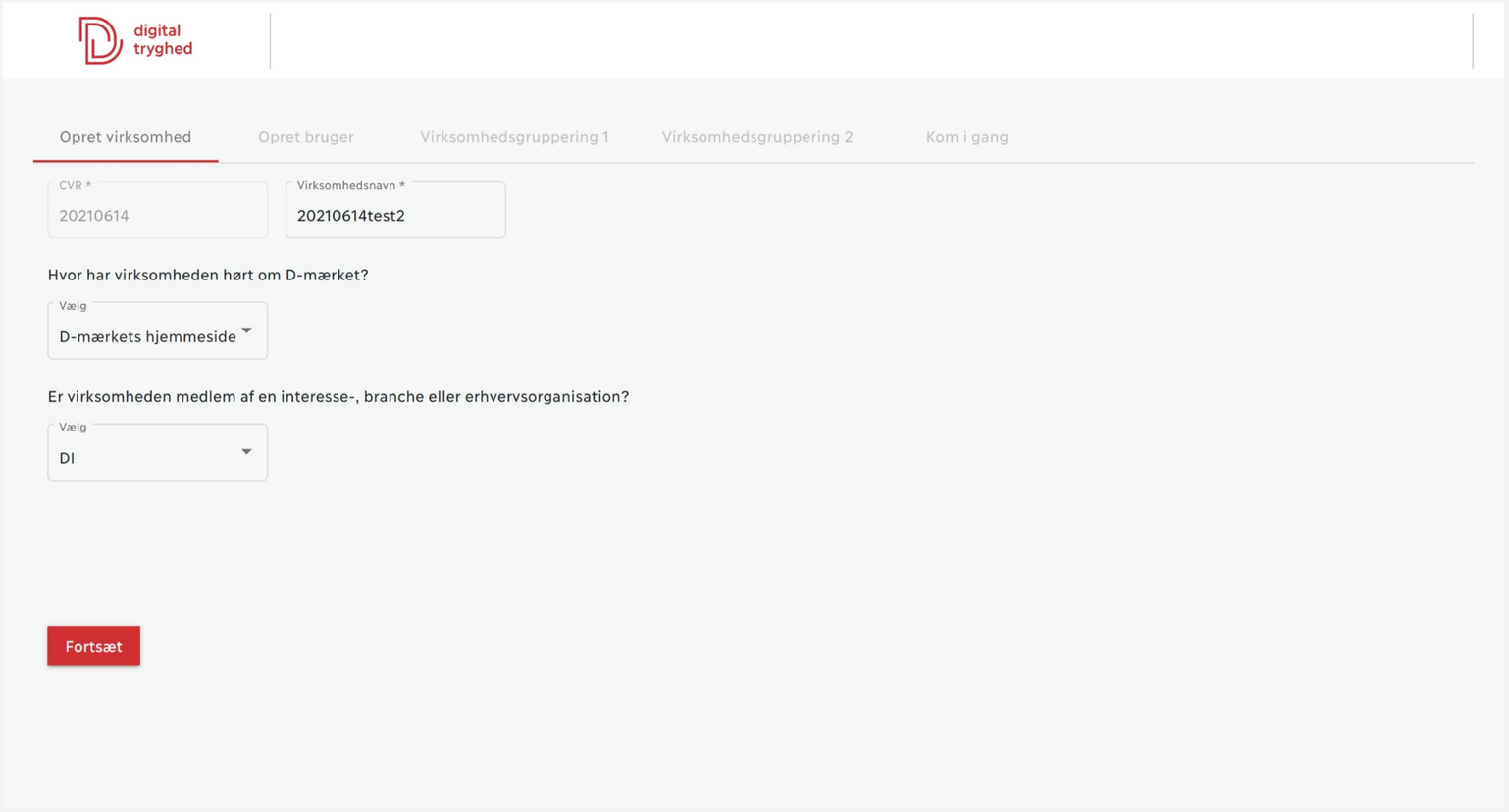
Kunderejsen og prismodel

Proces for virksomheder

1. **Anmodning**
2. **Inplacering og kriterier**
3. **Selvevaluering**
4. **Ansøgning og betaling**
5. **Tilsyn og kontrol**
6. **Tildeling af D-mærke**

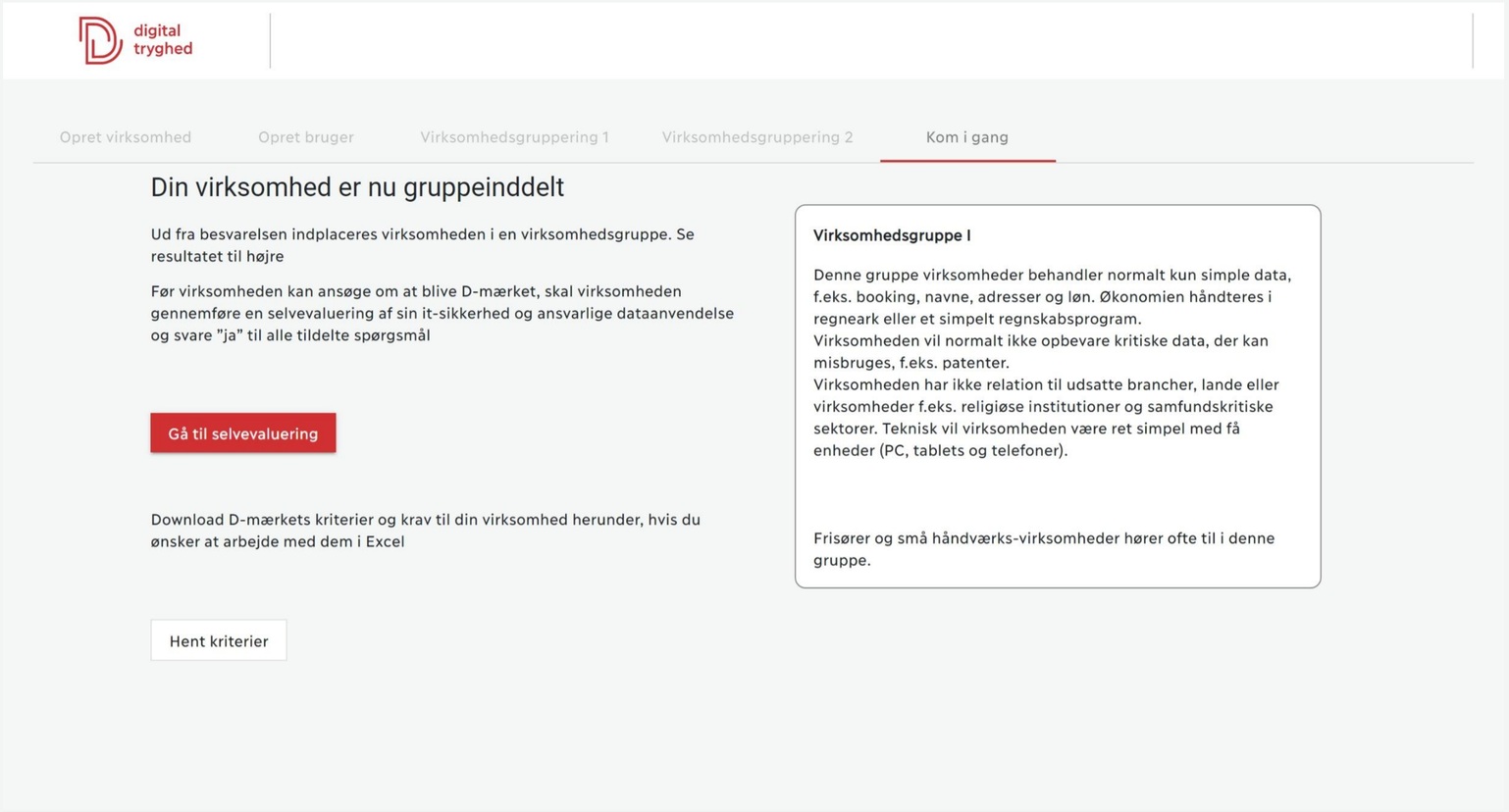
Kilde: https://d-maerket.dk/proces/

D-mærkets selvevalueringsværktøj



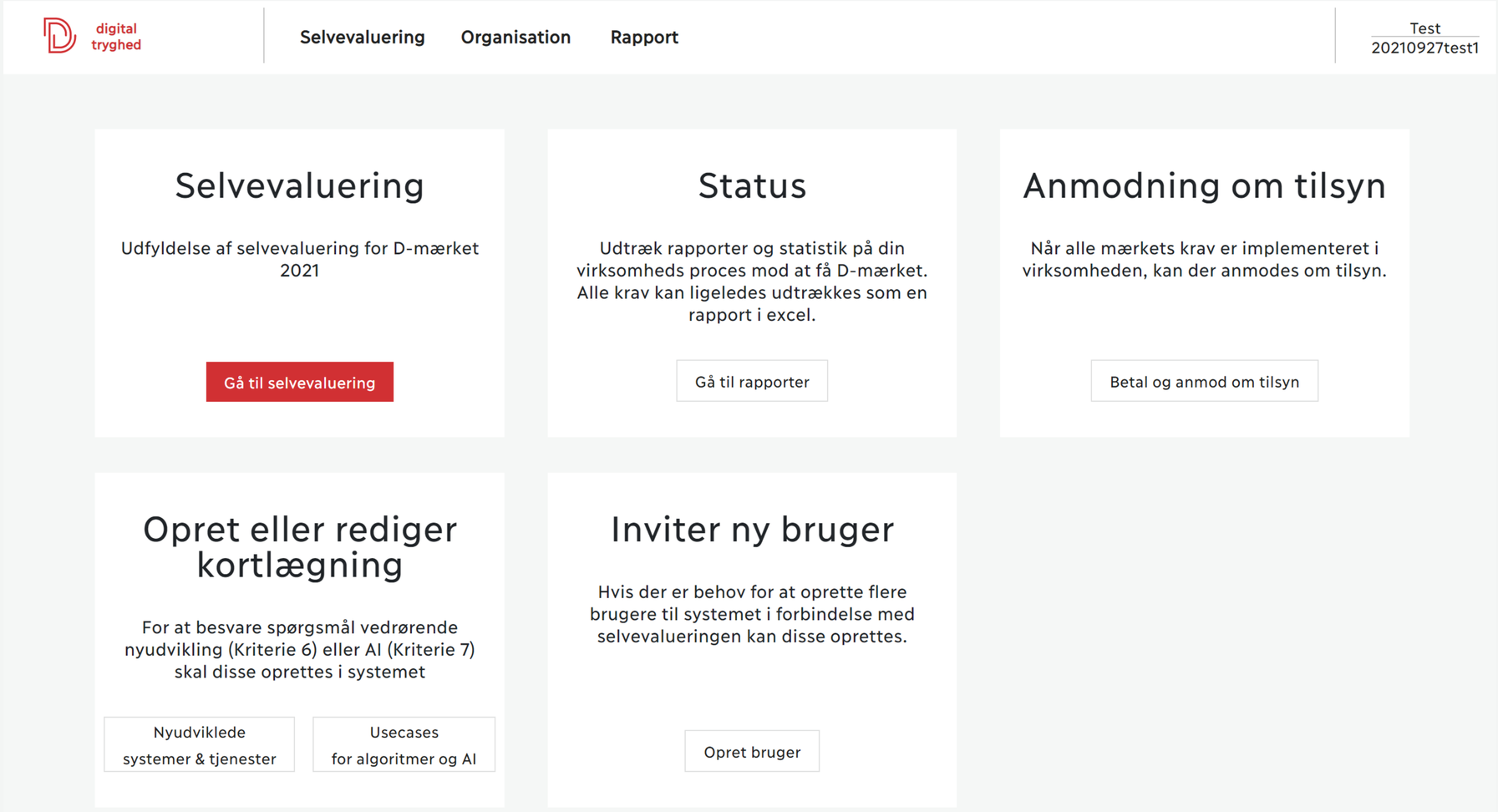
Kilde: https://d-maerket.dk/proces/

D-mærkets selvevalueringsværktøj



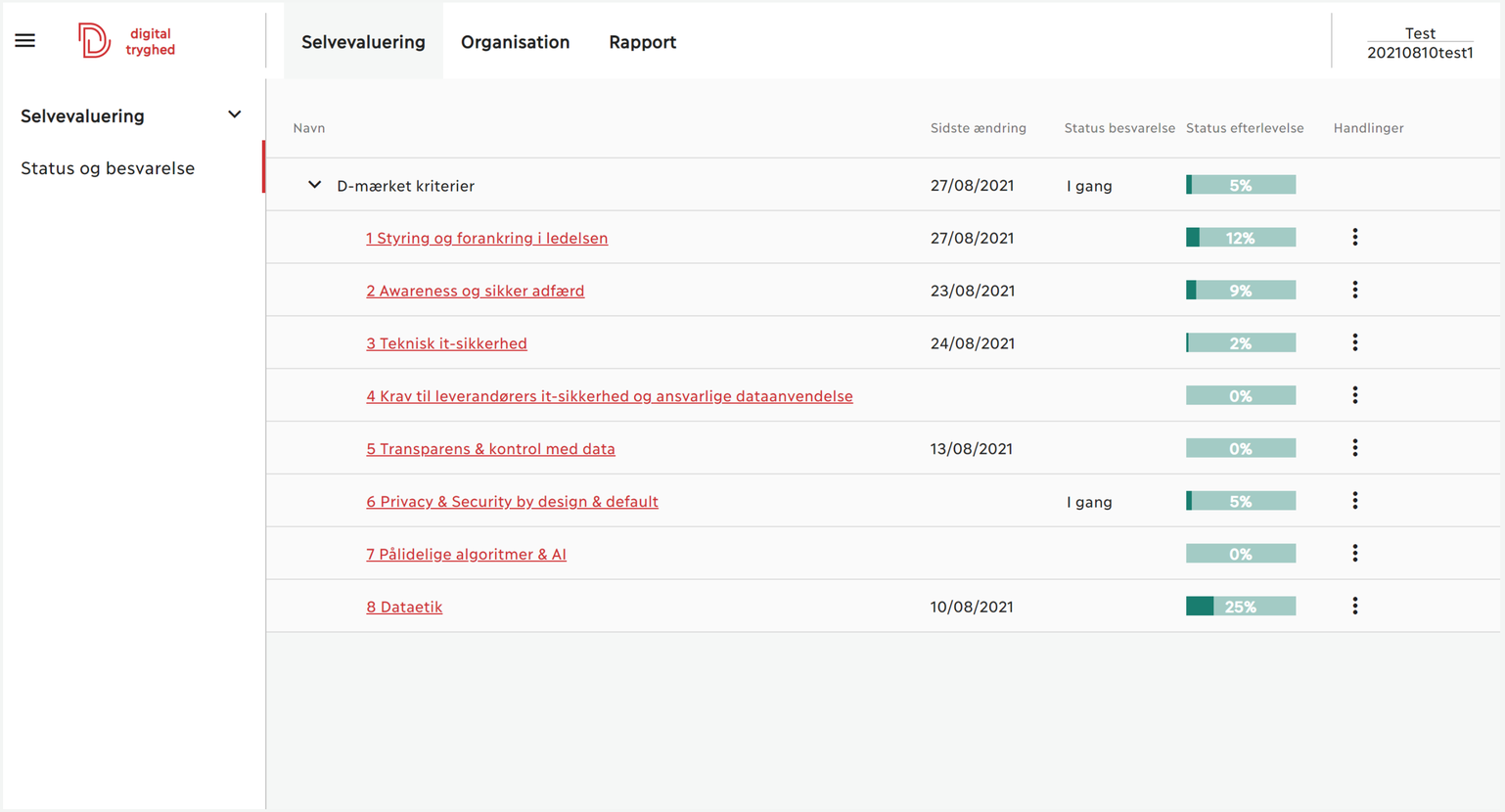
Kilde: https://digital.d-maerket.dk/

D-mærkets selvevalueringsværktøj



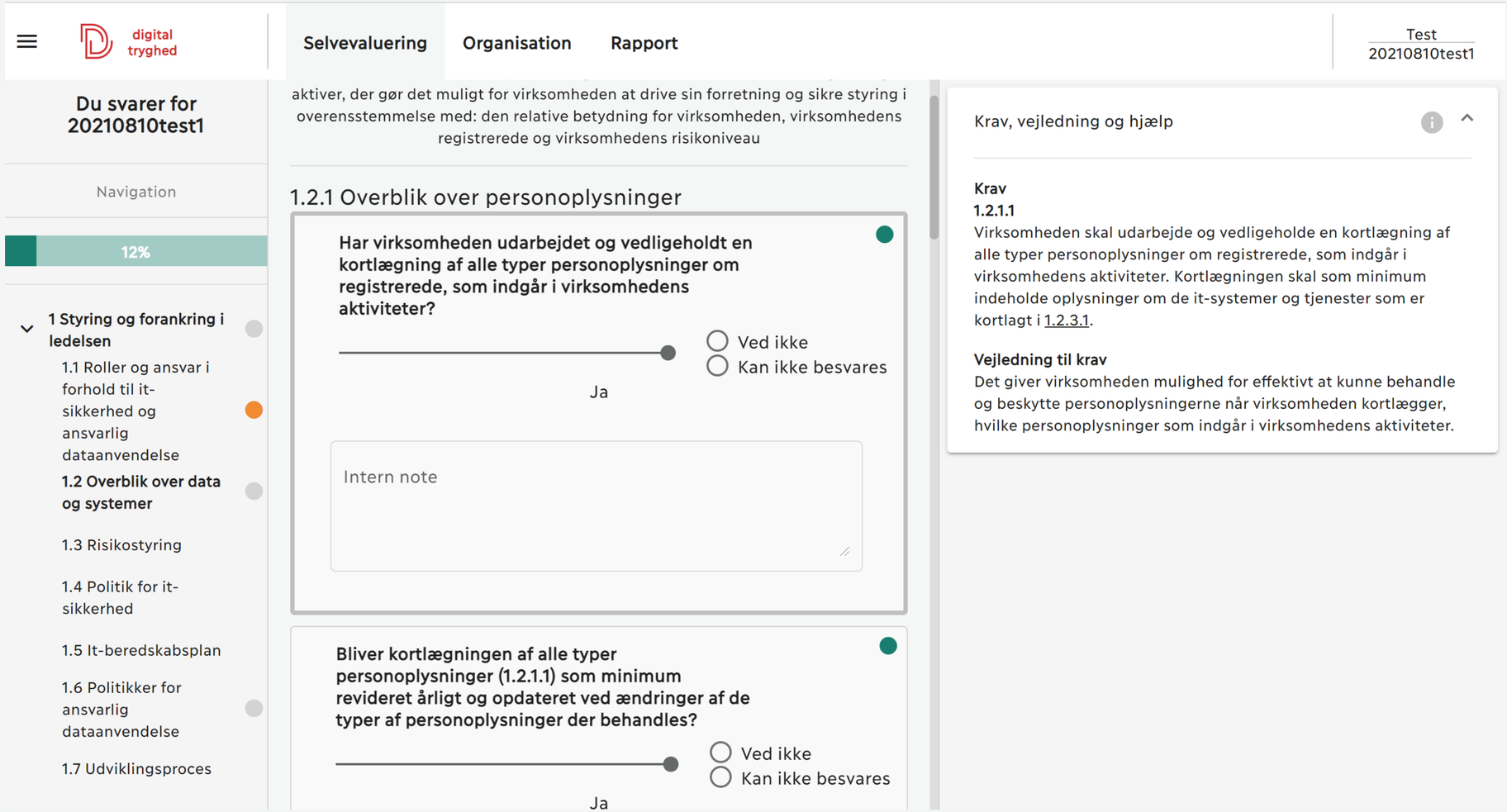
Kilde: https://digital.d-maerket.dk/

D-mærkets selvevalueringsværktøj



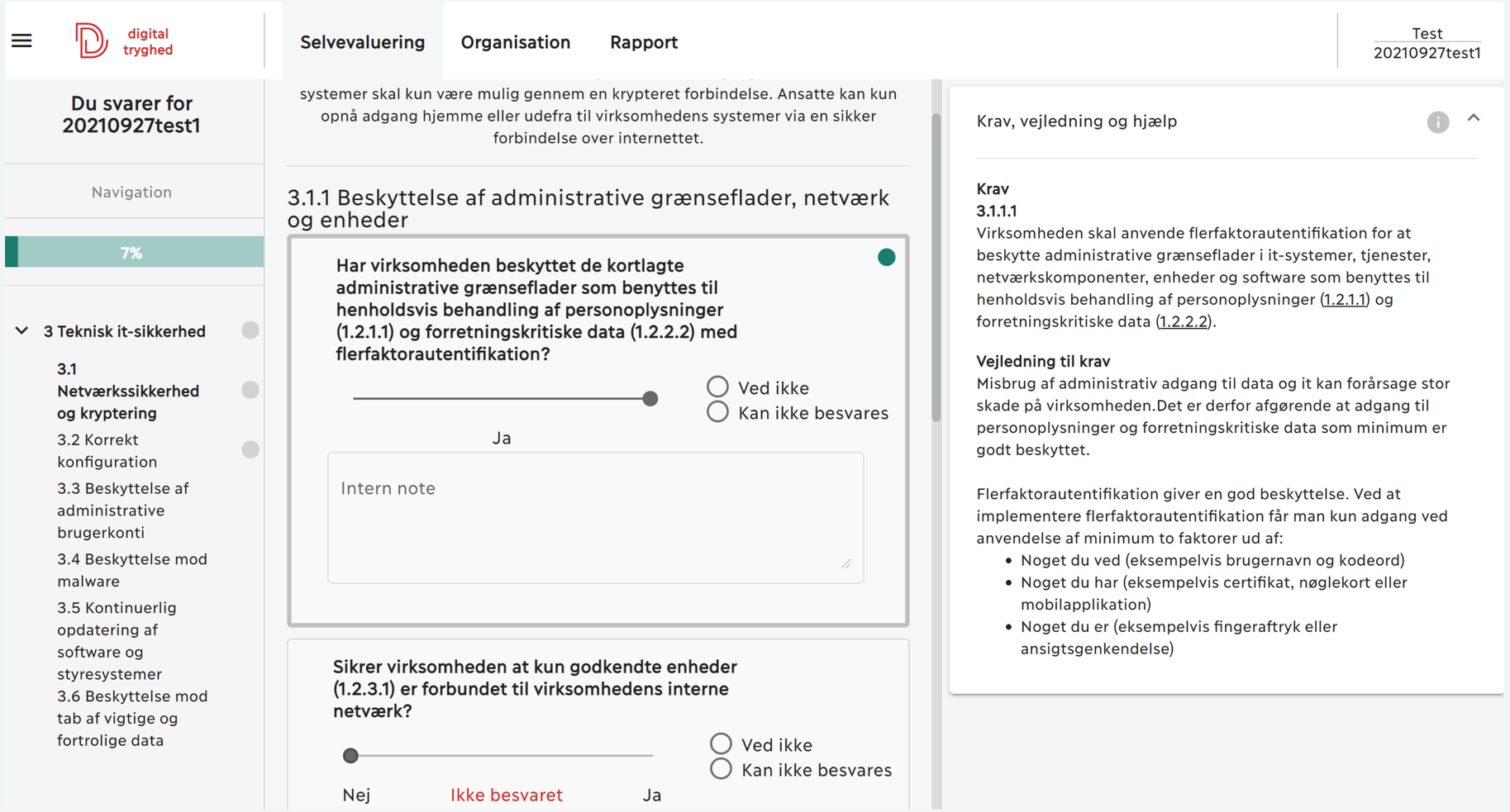
Kilde: https://digital.d-maerket.dk/

D-mærkets selvevalueringsværktøj



Kilde: https://digital.d-maerket.dk/

D-mærkets selvevalueringsværktøj



Kilde: https://digital.d-maerket.dk/

Prismodel

	Gruppe I	Gruppe II	Gruppe III	Gruppe IV	Gruppe IV+
	0-9 ansatte	10-49 ansatte	50-249 ansatte	250-999 ansatte	>1000 ansatte
Pris for tilsyn	**DKK 2.800**	**DKK 8.400**	**DKK 21.000**	**DKK 52.250**	**Afhænger af størrelse**

Undtagelser	**Max pris**	**Rabat**
Hvis under 10 ansatte, men tilhører virksomhedsgruppe III	DKK 8.400	-60%
Under 50 ansatte, men tilhører virksomhedsgruppe III	DKK 12.600	-40%

Kilde: https://d-maerket.dk/priser/

Hvordan skaber D-mærket forretningsværdi?

- Det er hurtigt at komme i gang - og selvevaluering er gratis
- Virksomheden betaler først, når og hvis tilsyns-og kontrolprocessen igangsættes
- Kravene er tilpasset til virksomheden - og er til at forstå
- D-mærket kommer hele vejen rundt om virksomheden
- Virksomheden bestemmer selv farten - og kan få vejledning undervejs
- Godt sted at starte, hvis virksomheden på sigt vil fx ISO/IEC 27001 og ISO/IEC 27701 certificeres
- D-mærket er fremtidssikret – da mærket indeholder krav til PbD/SbD, algoritmer/AI og dataetik
- D-mærket er starten på en digital ansvarlig modenhedsrejse – og virksomheden kan skilte med det

I forhold til den proces vi har været igennem, kan vi i høj grad se os selv i de kriterier, der er fastsat til en lille virksomhed som vores og det har været positivt og lærerigt på den måde, at vi har igangsat mindre tekniske foranstaltninger for at leve op til de stillede krav

Per U. Nielsen

Partner, sure'it

Kilde: https://d-maerket.dk/events-og-artikler/verdens-forste-maerke-for-digital-ansvarlighed-er-klar-til-brug/

Generelt bruger vi vores forskellige certificeringer aktivt til at understøtte vores forretning og være med til at dokumentere sikkerheden omkring vores services, og forventer også at D-mærket vil bidrage positivt og være med til at differentiere Dubex fra vores konkurrenter

Jacob Herbst

Partner & CTO, Dubex

Kilde: https://d-maerket.dk/events-og-artikler/verdens-forste-maerke-for-digital-ansvarlighed-er-klar-til-brug/

Vi har hele tiden ment, at god dataetik skal ses som et konkurrenceparameter, bl.a. i forbindelse med at man som virksomhed har styr på de persondata man opbevarer og behandler. Det kan D-mærket være med til at signalere og underbygge endnu mere

Jacob Overby

Partner & CIO, Lexoforms

Kilde: https://d-maerket.dk/events-og-artikler/verdens-forste-maerke-for-digital-ansvarlighed-er-klar-til-brug/

Det er min overbevisning, at mange virksomheder ikke har nok fokus på området og som derfor kan lære af denne proces og få en øget opmærksomhed på datasikkerhed

Karsten Noel Poulsen

Direktør, ViSSEVASSE

Kilde: https://d-maerket.dk/events-og-artikler/verdens-forste-maerke-for-digital-ansvarlighed-er-klar-til-brug/

Se D-mærkets lanceringsevent

Onsdag d. 22. sep. 2021

Lanceringsevent hos Digital Hub Denmark, foto af Sebastian Stigsby

Se eller gense D-mærkets lancering d. 22. september 2021. Eftermiddagen bød på oplæg og ekspertpanel, interviews med virksomheder som har testet mærket og ikke mindst officiel lancering.

Kilde: https://d-maerket.dk/events-og-artikler/verdens-forste-maerke-for-digital-ansvarlighed-er-klar-til-brug/

digital tryghed

www.d-mærket.dk

D-mærket/D-seal

@Dmaerket

DANSK ERHVERV

DI

SMVdanmark

Forbrugerrådet Tænk

INDUSTRIENS FOND

H. C. Andersens Boulevard 18, 1553 København V • Telefon: +45 33 77 33 77 • kontakt@d-maerket.dk