D-mærket

Ordliste

Begreber fra D-mærkets kriterier beskrevet og uddybet.

Begreb	Henvisning til kriterier	Begrebet beskrevet og uddybet
Adgangsstyring	1.6.1	At styre hvilke rettigheder brugere har i et it-system, en tjeneste eller et netværk. Formålet er at have et overblik over brugeres rettigheder og være i stand til at ændre i disse, samt at sikre at brugerne kun er tildelt de nødvendige rettigheder.
Administrativ bruger/administrative rettigheder	3.3.1	En bruger med administratorrettigheder har typisk udvidede rettigheder ift. de generelle brugere. Administratorer kan fx have rettigheder til at foretage ændringer i system-indstillinger og opsætning, fx af sikkerheden i et it-system. Typisk kan administratorer også foretage ændringer af andre brugerkonti. Antallet af administratorer bør derfor begrænses.
Aggregering	1.6.1, 6.2.3	Aggregering betyder at noget samles sammen eller ophobes, fx data, enheder eller information. Persondata behandles på det højest mulige niveau af aggregering og med det mindst mulige detaljeniveau, hvor data stadig er anvendelig. Aggregering af information på tværs af grupper af kendetegn/karaktertræk og grupper af individer begrænser graden af detaljering i det resterende persondatasæt.
Aktivitet (ekstern rettet)	1.2.3.	Løsninger, produkter, tjenester e.l., som virksomheden råder over, der benyttes af brugere, kunder, samarbejdspartnere eller lignende. Kortlægningen i 1.2.3 danner grundlag for overvejelserne i Kriterie 5: transparens og kontrol med data, hvis formål er at sikre, at virksomheden lever ever op til gældende standarder, lovgivning og god praksis for databehandling i forbindelse med eksternt rettede aktiviteter, der indebærer behandling af personoplysninger.
Aktualitet	7.2.2	At noget er aktuelt eller nutidigt. Formålet er at sikre at data, som virksomheden beregner på, er ajourført og derved reducerer en eventuel skævvridning af resultaterne. Hvis

		virksomheden benytter data, der er forældet, kan det ende i resultater, der ikke er repræsentative for formålet.
Aktør (ondsindet)	6.3.3	Person eller gruppering, der med egen vinding for øje forsøger at få adgang til en virksomheds data eller enheder.
Algoritme	1.2.3, 1.7.1, 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.1.5, 7.2.1, 7.2.2, 7.2.3, 7.3.1	Algoritmer defineres som applikationer, der ofte vha. matematiske optimeringsteknikker, bruges til at udføre én eller flere opgaver såsom at indsamle, kombinere, rense, sortere, klassificere og udlede data. Dette muliggør udvælgelse, prioritering, anbefaling samt gennemførsel af beslutninger. Algoritmer skal være lovlige, overholde etiske principper og værdier (fx respekt for menneskelig autonomi, forebygge skade, være rimelige, og kunne forklares), og de skal være robuste både ud fra et teknisk og socialt perspektiv. Der sondres mellem *algoritmer* baseret på de potentielle konsekvenser de har for mennesker og mere *generel automatisering* af f.eks. industrimaskiner . Denne sondring vil følge EU-kommissionens definition af høj- og lavrisiko algoritmer.
Anerkendte krypteringsteknologier	6.2.2	Teknologier, som er opdaterede og aktuelle og som lever op til de seneste sikkerhedsforanstaltninger og ikke er mærket som ”brudt” eller ”usikker”. En virksomhed skal sørge for at anvende kryptering som er sikker. Virksomheden kan derfor stadig bruge de forskellige krypteringsformer eller hashing (se ’hashing’) som passer bedst til deres formål, så længe teknologien er anerkendt blandt forskellige aktører, eksempelvis være CFCS, ENISA eller NIST.
Angrebsflader	6.3.1	Angrebsflader er de indgangsvinkler en fjendtlig aktør vil kunne forsøge at udnytte for at tvinge sig adgang til fx et system eller en enhed.

		En aktør, som er ude på at tvinge sig adgang til virksomheden, om det så er fysisk eller digitalt, vil kunne udnytte en række angrebsflader; dette kan eksempelvis være mennesker, It-systemer eller infrastruktur. Målet er at reducere den mængde angrebsflader der er, eller reducere sandsynligheden for at disse bliver udnyttet. Dette kan reduceres ved eksempelvis at træne sine medarbejdere i at gennemskue phishing og fjerne enheder fra netværket, som ikke har et formål eller segmentere sit netværk.
Anomali (i logdata)	3.7.1	Uregelmæssigheder i logdata. Anomali i logdata kan skyldes en it-sikkerhedshændelse, og logdata bør derfor overvåges.
Anonymisering	1.6.1, 6.2.1, 6.2.3	Oplysninger, der er gjort anonyme, sådan at ingen fysiske personer kan identificeres ud fra oplysningerne eller i kombination med andre oplysninger. Personoplysninger, der ikke vedrører en identificeret eller identificerbar fysisk person beskrives som anonyme oplysninger. Der er tale om anonymisering når personoplysninger, er gjort anonyme på en sådan måde, at oplysningerne ikke kan føres tilbage til en registreret person, og så den registrerede ikke kan identificeres ud fra oplysningerne eller ved at kombinere oplysninger. Det er en betingelse, at anonymiseringen er uigenkaldelig.
Antivirusprogrammer	4.1.1	Program som er designet til at detektere, fjerne og beskytte mod forskellige typer af malware (se malware). For at beskytte it-systemer og data, skal der implementeres en anti-virus løsning, der kan beskytte virksomhedens enheder. Disse skal holdes opdaterede for at anti-virus programmet også kan genkende de nyeste trusler.
Attribute based credentials (ABC)	6.2.2	En mekanisme der kan autentificere forskellige attributter om en entitet uden at afsløre informationer om denne. Det kan fx give muligheden for at fremvise alder eller lignende uden at

		fremvise andre personoplysninger, således at der anonymiseres mest muligt.
Automatisk beslutning	5.1.1, 7.1.3, 7.1.4	Beslutninger, der træffes ved/af teknologiske midler og uden menneskelig indblanding. Se evt. 'algoritmer'.
Awareness	2.2.1, 2.3.0	Awareness er at have opmærksomhed på et område, eksempelvis it-sikkerhed. Medarbejderne udgør én af de største trusler mod en virksomheds it-sikkerhed, hvilket er grunden til at man benytter awareness-træning til at uddanne medarbejderne til bedre at kunne identificere trusler og agere sikkert.
Beregningslogik (inferensmetode)	7.2.2, 7.2.3	Måden et program er indstillet til at tage beslutninger på ud fra tilgængelig data.
Bias	7.1.2, 7.1.4, 7.2.2	Forudindtagethed i beslutninger eller metodisk fejlbehæftet datagrundlag for beslutninger. Under udvikling, vedligeholdelse eller udvælgelse af data som benyttes i algoritmer eller kunstig intelligens (AI) kan der flere steder i løbet af processen opstå bias både fra personen, som udvælger datasæt, men også i selve designet af algoritmen.
Compilere	6.3.4	Programmer der oversætter et kodesprog til et andet, for at sikre en bredere funktionalitet.
Cookiedirektivet	5.1.2	Reelt EU-direktiv 2002/58/EF (revideret 2009). Et EU-direktiv om sporingsanordninger, fx cookies, som websites anvender. Mødes i praksis oftest som samtykkeanmodning, når et website besøges.
Cookie(s)	5.1.2, 5.2.1, 6.2.4	En datafil, der indsamler digitale fodspor om brugerne, når de færdes online. Der skelnes mellem nødvendige, funktionelle, statistiske og marketing cookies. Læs mere om cookies på Erhvervsstyrelsens hjemmeside.

CVSS (Common Vulnerability Scoring System)	3.5.1	CVSS er et open-source rammeværk til at kategorisere og bedømme trusler og sårbarheder mod software eller IT-systemer.
Dashboard	5.3.1	Overblik over indstillinger evt. med mulighed for ændringer af samme indstillinger. Dette kan fx være et dashboard over en hjemmesides indsamling af cookies og med mulighed for ændring af denne.
Databeskyttelsesrådgiver	5.1.1	En databeskyttelsesrådgiver (ofte betegnet som en DPO – data protection officer) er en rådgiverfunktion i en organisation, der skal inddrages i alle spørgsmål om databeskyttelse og rådgive om de databeskyttelsesretlige regler. Alle virksomheder med mere end 250 ansatte skal som følge af Databeskyttelsesloven have en databeskyttelsesrådgiver.
Databroker	5.1.2	Tredjepart (virksomhed) der sælger/køber data indsamlet bl.a. via hjemmesider.
Dataetik	1.2.3, 1.6.2, 2.1.1, 2.3.2, 4.3.2, 8.0.0	At drage nytte af data, men med forståelse for og efterlevelse af menneskets ret til privatlivsbeskyttelse samt generelle etiske principper.
Datas proveniens	7.2.2	Datas oprindelse og oprindelige sammenhæng. At være bevidst om datas proveniens er i denne sammenhæng at være vidende om, hvordan data er indsamlet og hvad et dataset består af, for at kunne vurdere dets gyldighed til det pågældende formål.
Dataanvendelse	1.1.1, 1.6.0, 2.1.1, 2.3.0, 4.0.0, 4.3.0, 5.4.1	Anvendelse af data som grundlag for andre formål. Det kan fx være at indsamle data om en forbruger for senere at anvende dem til målrettet markedsføring.
Designmønster	6.2.1, 6.2.2, 6.2.3,	En beskrivelse af, hvordan en it-løsning tænkes udarbejdet. I forbindelse med Kriterie 6 er det dermed, hvordan de forskellige Privacy by design & default-hensyn tænkes implementeret og designet.
Differential privacy	6.2.3	Metode til at kunne bearbejde data anonymt baseret på mønsteret i datasættet. Med andre ord kan virksomheden indsamle informationer om

		forbrugsmønstre, men ændre data inden indsamling og lagring, og derved forhindre muligheden for at genskabe den oprindelige data.
Enheder	1.2.3, 2.2.1, 3.1.1, 3.1.2, 3.2.1, 3.3.1, 3.4.1, 3.5.1, 3.6.1, 3.7.1, 4.2.1,	Virksomhedens slutbruger-enheder, herunder bærbare og mobile enheder, Internet of Things (IoT)-enheder og -servere), der er forbundet til netværket fysisk, virtuelt, eksternt eller i cloud-miljøer. Skal kendes for at få et præcist kendskab til alle de aktiver, der skal overvåges og beskyttes i virksomheden. Dette vil også støtte identifikation af uautoriserede og uadministrerede aktiver, der skal fjernes eller afhjælpes.
Etablere	1.3.1, 1.7.1, 2.2.1, 2.3.1, 2.3.2, 3.1.2, 3.2.1, 3.7.1, 6.1.1, 6.2.5, 7.1.2, 7.1.3, 7.1.4, 7.2.1, 8.1.1	Oprette/anlægge/installere kravsmål i virksomheden.
Firewall	3.1.1, 4.1.1	Software eller hardware der scanner indkommende trafik til dine enheder. Sortlistet trafik formenes adgang, hvorfor opdateringer af firewalls er nødvendige, da disse vedligeholder sortlisten.
Flerfaktorautentifikation	3.1.1, 3.1.2, 3.3.1	Adgang til virksomhedens enheder, software, mm. kræver mere end én autentifikation. Fx password og mobilkode, password og biometrisk genkendelse, og nøglekort, etc.
Forretningskritiske data	1.2.2, 1.5.1, 3.1.1, 3.2.1, 3.6.1, 3.7.1, 4.0.0, 4.1.1, 4.2.0	Data som en virksomhed vil lide stor overlast af at miste, få offentliggjort, eller som kun kan generhverves ved betydelige omkostninger.
Grænseflader	3.1.1	Også kendt som *interfaces*. Den præsentation eller fremstilling af et program, der stilles til rådighed for brugere. Fx oplever kunden på en webshop en anden grænseflade end udvikleren af webshoppen.
Hashing	6.2.2	Hashing er en algoritmisk funktion, der udregner en kort værdi ud fra en fils indhold. Værdien kan anvendes til forskellige formål, som fx en maskering af det egentlige indhold.
Homomorf kryptering	6.2.2	Dette er en type kryptering som gør det muligt at foretage operationer på krypteret tekst, uden at dekryptere det til klartekst.

		I tilfælde af arbejde med eksempelvis personoplysninger i en database, kan det være en fordel hvis man kan bearbejde de data uden at skulle dekryptere dem til klartekst og derved udsætte informationen for fare i form af et datalæk. Homomorf kryptering er ikke en meget benyttet metode, men kan være relevant for nogle virksomheder, og i forbindelse med AI kan det udgøre en stor fordel at virksomheden kan processere data baseret på krypterede data.
Hændelse	1.3.1, 1.5.1, 2.2.1, 2.3.1, 3.4.1, 3.7.1, 4.1.1, 4.2.1, 6.2.1, 6.3.3	Situationer hvor data eller adgang til data er blevet kompromitteret ubevidst eller bevidst af ondsindede aktører.
Implementere	1.3.1, 1.4.1, 1.5.1, 1.6.1, 1.6.2, 1.7.1, 3.1.1, 3.2.1, 3.3.1, 3.4.2, 3.5.1, 4.0.0 6.2.4, 6.3.1, 6.3.2, 6.4.1, 7.2.2, 7.3.1, 8.1.1	Sætte i kraft/føre ud i livet/iværksætte. Krav er omsat til konkret handling eller procedure i virksomheden
Interessent	7.1.1, 7.1.2	Individ, gruppe eller organisation, der kan påvirke, bliver påvirket af, eller opfatter sig selv som påvirket af en beslutning eller en aktivitet, herunder udvikling af algoritmer. I majoriteten af tilfælde vil det være relevant, at få indblik og feedback fra de interessenter som bliver berørt af en algoritmisk beslutning eller aktivitet.
IOT	3.1.1, 4.1.1	*Internet of Things*. Dækker over at stadig flere dagligdags-apparater, som fx termostater og køleskabe, får internetforbindelse. Disse IOT-apparater er til tider dårligt sikrede mod malware eller hackerangreb, der kan sprede sig til andre enheder via fælles netværk.
It-beredskabsplan	1.5.1, 4.1.1	En plan for reetablering af it-systemer og it-infrastruktur. I en it-beredskabsplan beskriver man hvordan rette vedkommende skal agere, hvis der opstår en hændelse med virksomhedens it (fx hackerangreb, malware, brand, tyveri, mm.),

		hvem der skal kontaktes (fx leverandør, myndigheder, mm.), og hvordan man reetablerer systemer og data.
It-sikkerheds-hændelser	4.2.1	En hændelse hvor data eller et it-system er blevet kompromitteret.
It-system	1.2.1-3, 1.3.1, 1.5.1, 2.2.1, 3.1.1, 3.2.1, 3.3.1, 3.4.1, 3.4.2, 3.5.1, 3.6.1, 3.7.1, 4.1.1, 4.2.1, 6.3.1, 6.3.3, 7.1.1	Et it-system er en sammenhængende helhed af hardware og software som bruges til databehandling. Informationssystemer binder flere komponenter eller enheder sammen, og data kan sendes fra enhed til enhed via netværk. Ser vi alene på systemer til indsamling, organisering, lagring og kommunikation af information, har vi at gøre med informationssystemer, og når computer-teknologi anvendes til at behandle disse informationer eller data, har vi at gøre med it-systemer.
K-anonymitet	6.2.3	En metode til at praktisk anvende data uden at afsløre hvilke entiteter data kommer fra.
Konfiguration	3.2.1, 3.4.1, 6.2.4, 6.3.2	Indstilling. At man kan indstille graden af noget. Fx at man aktivt indstiller sikkerhedsniveauet i et stykke software. Konfigurations*standarder* er bevidsthed- og stillingtagen til, hvordan fx software er indstillet.
Kortlægning	1.2.1, 1.2.2, 1.2.3, 3.3.1, 3.4.1, 3.5.1, 3.6.1, 4.1.1, 4.3.1, 6.3.1,	En detaljeret fortegnelse, der danner overblik over virksomhedens anvendte it-systemer, tjenester, netværkskomponenter, enheder og software samt de persondata og forretningskritisk data, der indgår i disse. For nogle virksomheder vil det ligeledes være nødvendigt at inddrage evt. algoritme/AI "use cases", eksternt rettede aktiviteter og nyudviklede produkter og tjenester.
Kryptering	1.6.1, 3.1.2, 3.6.1, 6.2.2	Kryptering er en teknik, der får information til at fremstå uforståeligt og på den måde hemmeligholdt. Kryptering bruges ofte til at sikre information, der skal sendes via ikke-sikre kommunikationskanaler som f.eks. internettet. Kryptering gør, at budskabet ikke kan blive forstået af uvedkommende.

Logning	1.6.1, 3.2.1, 3.7.1, 4.1.1	Automatisk nedfældning af aktivitet (handling og tidspunkt) i et it-system.
Malware	3.3.1, 3.4.1, 3.4.2	Malware betyder malicious software og er en betegnelse for computerprogrammer, der gør ondsindede, skadelige eller uønskede ting der, hvor de er installeret. Begrebet dækker over alle kategorier af skadelige programmer herunder virus og orme.
Meddelelseseffekt	5.1.2	Hvor markant en meddelelse kommunikeres. I dette tilfælde er det, at muligheden for at afvise et valg kommunikeres tilsvarende med muligheden for at træffe et valg. Fx at en knap til at godkende ikke er grøn og stor, hvor knappen til at afvise er gråned ud og lille.
Middleware	6.3.3	En type software der leverer tjenester til andre softwareapplikationer. Middleware gør det nemmere for udviklere at implementere kommunikation samt input/output, så de kan fokusere på deres softwareapplikation.
Minimering	1.5.1, 6.2.1	Ifm. 'minimering og begrænsning'. Privacy by design-strategi, hvor der i udarbejdelsen af nye produkter og/eller tjenester implementeres en minimal indsamling af personoplysninger.
Netværkskomponenter	1.2.3, 3.1.1, 3.2.1, 3.3.1, 3.5.1, 3.6.1, 3.7.1	Netværkskomponenter beskriver hvilke fysiske komponenter der er til stede for at opstille f.eks. LAN (Local Area Network) eller WLAN (Wireless Local Area Network). Dette kan fx være routere, switches, gateways etc.
Passende	4.0.0, 6.1.1	Rimeligt og fornuftigt valg i en bestemt sammenhæng eller situation. Ordet angiver, at virksomheden har mulighed for at argumentere for til- og fravalg.
Phishing	2.2.1, 3.3.1, 3.4.2	Phishing er et forsøg på at narre e-mailmodtagere til i god tro at videregive personlige eller andre værdifulde oplysninger eller give uretmæssig adgang til bl.a. it-systemer. Ofte vil angriberen forsøge at få modtageren til at klikke på links til falske hjemmesider, åbne

		inficerede filer eller afgive personlige oplysninger
Politik	1.4.1, 1.6.1, 1.6.2, 2.2.1, 2.3.1, 2.3.2, 3.4.2, 4.2.1, 4.3.1, 4.3.2	En politik er et styringsdokument for ét eller flere områder i en virksomhed. Politikken kan derfor opsætte en ramme for, hvordan virksomheden og dens ansatte skal operere. Politikkens indhold kan være defineret ud fra fx forretningskrav, lovgivning, kontrakter, risikovurderinger eller standarder, så det sikres, at virksomheden opererer i henhold til disse.
Privacy	1.2.3, 1.7.0, 6.1.1, 6.1.2, 6.2.1, 6.2.2, 6.2.3, 6.2.5, 6.4.1	I forbindelse med D-mærket særligt retten til- og muligheden for at værne mod misbrug af egne eller andres persondata.
Procedure	2.2.1, 2.3.1, 2.3.2, 3.4.2, 3.6.1, 7.1.5	En fastlagt fremgangsmåde for udførsel af en opgave eller handling, ofte reguleret ved hjælp af formelle regler.
Proces	1.3.1, 1.6.1, 1.7.1, 2.1.1, 3.3.1, 3.4.1, 3.5.1, 4.1.1, 4.2.1, 4.3.1, 4.3.2, 5.4.1, 6.1.2, 6.2.5, 6.4.1, 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.1.5, 7.2.1, 7.3.1, 8.1.1	En nedskrevet arbejdsgang, der beskriver en bestemt måde en opgave eller handling skal udføres på. En proces har til hensigt at sikre en ensartet udførsel af arbejdsopgaven gennem en række forbundne handlinger eller trin.
Profilering	5.1.1, 6.2.4, 7.1.3	Enhver form for automatisk behandling af personoplysninger, der består i at anvende personoplysninger til at evaluere bestemte personlige forhold vedrørende en fysisk person. Navnlig for at analysere eller forudsige forhold vedrørende den fysiske persons arbejdsindsats, økonomiske situation, helbred, personlige præferencer, interesser, pålidelighed, adfærd, geografisk position eller bevægelser.
Ransomware	1.5.1, 3.6.1	Ved ransomware-angreb bliver data og systemer gjort utilgængelige for offeret, ofte ved kryptering. Angriberen kræver en løsesum, for at give offeret adgang til sine data igen.
Reproducerbarhed	7.2.3	At et pålideligt resultat kan udføres eller opnås på samme måde fra gang til gang.

		I forhold til kunstig intelligens og algoritmer er det nødvendigt at kunne genskabe et resultat, hvilket kan hjælpe med at definere præcis hvad systemets egenskaber er. Dette kan også bruges til at teste og genskabe tidligere opførsel.
Residualrisici	4.2.1, 4.3.2	De tilbageværende risici. Fx at der er risici, som en bestemt indsats ikke har modvirket, men man har forholdt sig til og evt. accepteret.
Risikoappetit	1.3.1	En formel stillingtagen til hvilket risikoniveau en virksomhed kan acceptere at eksponeres for. Risikoappetit kan eksempelvis defineres ud fra det maksimale tålelige niveau for økonomisk tab, maksimalt antal hændelser eller største konsekvens for virksomhedens omdømme.
Signaturfiler	3.4.1	Filer der indeholder lister over kendte vira. I anti-virus og anti-malware programmer ofte koblet med programmer til at eliminere disse vira.
Software	1.2.3, 3.1.1, 3.2.1, 3.4.1, 3.5.1, 3.6.1, 3.7.1, 6.2.4, 6.3.1, 6.3.4, 8.1.0	Operativsystemer og applikationer specialiserede i behandling af data eller udførelse af funktioner. Funktionaliteten af software er meget alsidig, og kan fx dække over billedredigeringsprogrammer, antivirusprogrammer, egenudviklet software, lagerstyring, CRM-systemer, etc.
Subsymbolske	7.2.1	Simulerer de fundamentale fysiske processer i den menneskelige hjerne. F.eks. Neurale netværk.
Styringsdokument	1.4.1, 1.6.1, 1.6.2, 4.2.1, 4.3.1, 4.3.2	Et retningsvisende eller rammesættende dokument for et emne, fx en politik eller et sæt interne retningslinjer om håndtering af personoplysninger.
Tjenester	1.2.1-3, 1.5.1, 1.6.2, 2.1.1, 2.2.1, 3.3.1, 3.2.1, 3.3.1, 3.6.1, 3.7.1, 4.2.1, 5.1.2, 5.3.1, 6.1.1, 6.1.2, 6.2.1, 6.2.2, 6.2.3, 6.2.4, 6.2.5, 6.3.1,	En tjeneste indenfor it er typisk kendetegnet ved at være software, der er tilgængeligt for virksomheden, men ikke bliver lagret inden for virksomhedens grænser. Det er i de senere år blevet kendt som Software as a Service (SaaS). En tjeneste kan f.eks. være Outlook, som er en

	6.3.2, 6.3.3, 6.4.0, 7.3.0, 8.1.1	mailklient, her logger brugeren på eksempelvis via. en browser for at tilgå mails, som ligger på udbyderens servere – også kaldet ”skyen”. Online tjenester sparer brugeren for at installere software og skulle vedligeholde samt bruge plads på sin lokale enhed. Andre kendte eksempler er f.eks. Dropbox, iCloud samt Office365.
Træningsprogram	2.2.1, 2.3.1, 2.3.2	En planlagt og målrettet udvikling af visse færdigheder.
Unlinkability	6.2.2	Målet er at adskille personoplysninger og dermed mindske risikoen for databrud samt at personoplysninger benyttes til nye formål. Det hænger sammen med princippet vedrørende dataminimering samt at behandlingen skal være proportional med formålet.
Use case	1.2.3, 2.2.1, 2.2.1, 2.3.1, 2.3.2, 7.1.1, 7.2.1	En overordnet beskrivelse af hvordan en algoritme eller kunstig intelligens agerer og hvilken påvirkning den har på mennesker. Målet for use casen er at afdække om den har nogle konsekvenser for mennesker, hvilket blandt andet gøres for effektivt at kunne risikovurdere.
Validitet	7.2.2	Sikkerhed for at et videnskabeligt undersøgelsesresultat er gyldigt, dvs. dækkende for det man har ønsket at undersøge. Formålet med have validitet er at sikre at dataene som virksomheden benytter, er repræsentative – hvilket bl.a. dækker over aktualitet og integritet af data.
Væsentlige ændringer	1.2.2, 1.2.3, 1.4.1, 1.6.1, 1.6.2, 6.1.1, 7.1.1. 7.1.2, 8.1.1	Ændringer som påvirker det fundamentale indhold, stadie eller opbygningen af det pågældende element. Følgende er eksempler på væsentlige ændringer, men listen er ikke udtømmende, og der kan derfor være andre eksempler.

		Væsentlige ændringer kan resultere i ændring af virksomhedens gruppetype, f.eks. hvis virksomheden bliver opkøbt. Et andet eksempel kan være at virksomhedens it-tjenester, produkter eller lignende øger/ændrer opsamling af personoplysninger. Hvis virksomhedens risikobillede ændrer sig, kan det være på baggrund af en væsentlig ændring eller medføre en væsentlig ændring.
Åbenhedskultur	D-mærkets skema til dataetiske overvejelser (Jf. 8.1.1)	En etableret kultur i en organisation, hvor der aktivt arbejdes med- og efterleves principper omkring gennemsigtighed i beslutningsprocesser, italesættelse af fejl og uhensigtsmæssigheder, samt en anerkendelse af at organisationens handlinger påvirker både dens ansatte, dens stakeholders samt organisationens omverden.