Afrapportering fra sprintforløb til udvikling af prototype for

Datamærkningsordning

4. september 2019

/KL.7

Danmarks nye **mærke for digital ansvarlighed** giver fordele til virksomheder og tryghed til deres kunder

Executive Summary

Flere teknologiske ekspertråd har samstemmende anbefalet, at Danmark udvikler en mærkningsordning for ansvarlig brug af data. Herved menes et mærke, som giver både forbrugere og samarbejdspartnere vished om, at virksomheder, der bærer mærket, prioriterer og har et højt niveau af it-sikkerhed og ansvarlig anvendelse af data. Ideen har været modnet og behandlet af en gruppe af myndigheder og organisationer gennem det seneste år. I forlængelse heraf bad Erhvervsstyrelsen /KL.7 om at gennemføre et designsprint for at udvikle og teste en prototype af mærket med henblik på at vurdere ideens bæredygtighed. Sprintet fandt sted fra juli til september 2019 og involverede landets førende eksperter, erhvervs- og interesseorganisationer samt virksomheder og privatpersoner blandt potentielle brugere af mærket.

Hovedkonklusionerne efter sprintet er, at:

- Stort set alle **væsentlige interessenter** støtter ideen men med varierende fokus på hhv. it-sikkerhed over for det dataetiske aspekt.
- De fleste **virksomheder** byder ideen om en mærkningsordning velkommen, bortset fra virksomheder med lille data- og organisatorisk kompleksitet (eksempelvis automekanikere og frisører). De har svært ved at se, hvad mærket gør for dem.
- Et gennemgående dilemma i mærkningsordningen er spørgsmålet om, hvad balancen skal være mellem at opnå kritisk masse af virksomheder gennem brugervenlighed over for at stille skrappe krav, som væsentligt differentierer mærkede virksomheder fra ikke-mærkede.
- **Forbrugerne** opfatter it-sikkerhed og dataetik som naturligt koblet, og de er villige til at betale ekstra for ydelser fra virksomheder, der prioriterer digital ansvarlighed.
- **Onboarding:** Der er gennemgående opbakning til en versionering af mærkningsordningen, hvor man indleder med lempeligere kriterier for at mobilisere virksomheder for så senere at skrue op for kravene.
- **Finansieringsmodel:** Betalingsvilligheden blandt virksomheder i risikogruppe 1 er tæt på nul, mens de større og mere datatunge virksomheder i risikogruppe 2 og 3 gerne vil betale for mærket. Dog afhænger deres betalingsvillighed af, at der er en autoritet bag mærket, der kan blåstemple deres digitale ansvarlighed. For de større, digitaliserede koncerner i risikogruppe 4 er prisen ikke afgørende, men de skal derimod have bedre vished om, at mærket udgør en reel differentiator for dem i markedet - nationalt som internationalt.
- **Visuel identitet:** Mærkets grafiske profil er væsentlig, men også meget vanskelig at ramme plet pga. mærkningsordningens kompleksitet. Prototypen har ikke til fulde løst formidlingsopgaven over for forbrugerne med at gøre det klart, hvad mærket dækker over og virksomhederne i brugertesten ønsker, at mærket udstråler mere 'certificering' end ansvar. Løsningen på mærkets visuelle identitet skal findes i forlængelse af en mere overordnet overvejelse af mærkets positionering, stil og tone. Hvis mærket skal efterleve virksomhedernes ønske hen imod mere certificering og autoritet, så har det konsekvenser for ordningens kontrol og tilsyn, og dermed også finansiering. Hvis mærket derimod skal opnå hurtig og kritisk masse gennem klar kommunikation og "hjælp til selvhjælp", så anbefales yderligere brugertest med virksomhederne for at afsøge mærkets værdi,funktion og differentieringspotentiale.

INDHOLDSOVERSIGT

Det indeholder rapporten

1. Baggrund

1.1 Formålet med en datamærkningsordning

Databeskyttelse har fået øget bevågenhed de senere år. Det gælder både i relation til alvorlige hackerangreb, der har lagt store virksomheder og kritisk infrastruktur ned, afsløringer af globale tech-firmaers uansvarlige brug af persondata og implementeringen af den nye europæiske persondatafordning (GDPR). Alle disse udfordringer udgør en sammenhængende dagsorden, som Danmark både har mulighed for, kompetencer til og interesse i at være førende på.

Datamærkningsordningen skal give dansk erhvervsliv et solidt sikkerhedsmæssigt løft og gøre det mere attraktivt for den enkelte virksomhed at håndtere data på en ansvarlig og sikker måde. Dette mål skal opnås ved, at mærket:

1. bygger ovenpå den eksisterende lovgivning og skaber en best practice.
2. virker som en løftestang for danske virksomheders arbejde med it-sikkerhed og ansvarlig dataanvendelse.
3. gør digital sikkerhed og ansvarlig dataanvendelse til et positivt konkurrenceparameter og en dansk styrkeposition.
4. skaber et dansk udgangspunkt for udviklingen af tilsvarende internationale tiltag.

1.2 Rammen for projektet

Erhvervsstyrelsen (ERST) ønsker at få udarbejdet en testet og godkendt prototype på datamærkningsordningen. Med det udgangspunkt har /KL.7 faciliteret et sprintforløb over fire uger fra 12. august - 6. september 2019.

Sprintforløbet skal skabe et stærkere fundament for en kommende mærkningsordning for it-sikkerhed og ansvarlig dataanvendelse ved at:

1. konkretisere de enkelte kriterier.
2. give anbefalinger til kontrol og tilsyn med de enkelte kriterier.
3. opstille et bud på en finansieringsmodel.
4. udvikle mock-up til en visualisering af mærket.
5. brugerteste prototypen på private forbrugere og virksomheder.

Det er hensigten, at en privat aktør, efter sprintets afslutning, skal arbejde videre med rammerne for mærket, og at denne aktør skal tage udgangspunkt i den brugertest og rapport som sprintet resulterer i. Erhvervsstyrelsen forventer på den baggrund ikke en helt færdig pakke, men en testet prototype.

I løbet af sprintet, har /KL.7 løbende haft møder med projektets arbejdsgruppe, hvor indholdet af prototypens delelementer er blevet diskuteret. Derudover har /KL.7 fremlagt en foreløbig version af prototypen for nogle af datamærkningsordningens interessenter på en workshop. På baggrund af workshopdeltagernes input blev prototypen yderligere gennemarbejdet, og afslutningsvist evalueret i en brugertest med virksomheder såvel som forbrugere.

1.3 Hovedspørgsmål

Datamærkningsordningen skal bidrage til et løft af både ansvarlighed og sikkerhed i danske virksomheders anvendelse data. Men samtidig skal den også sikre tilstrækkeligt uptake og virke attraktiv for både forbrugere og virksomheder. Med dette dobbelte mål for øje har /KL.7 søgt at besvare følgende hovedspørgsmål:

01 Hvem er målgruppen for mærket? Hvilke evt. undermålgrupper er der?

02 Hvilke kriterier skal mærket bestå af? Skal der være forskellige kriterier til forskellige målgrupper?

03 Hvordan skal onboarding-processen udformes?

04 Hvordan skal der føres kontrol og tilsyn med kriterierne? Skal der være forskellige kontrol- og tilsynsmekanismer til forskellige målgrupper?

05 Hvilken finansieringsmodel er ønskelig og opnåelig for mærkningsordningen?

06 Hvordan understøtter mærkets visuelle udtryk bedst muligt mærkets indhold og formål?

2. Målgruppen

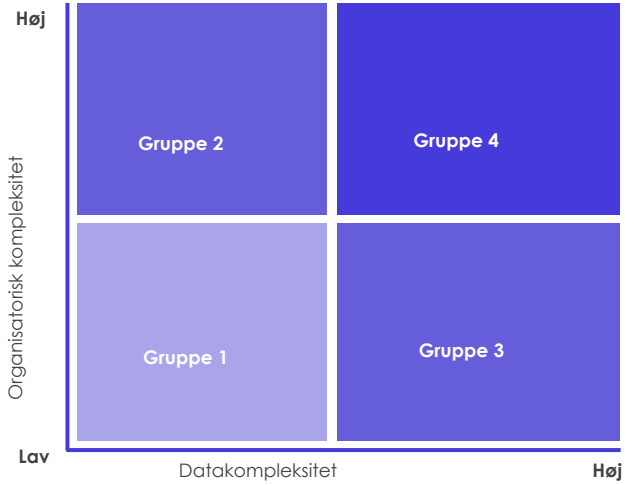
2.1 Hvem er målgruppen for datamærket?

Det er arbejdsgruppens vurdering, at målgruppen for datamærket bør være både små, mellemstore og store virksomheder og derfor virksomheder, der varierer i både organisatorisk og datamæssig kompleksitet. Datamærket skal være relevant både for de små virksomheder med få ansatte og begrænset anvendelse af data, men også for de store virksomheder, der har både mange ansatte og mange data at holde styr på. Det vil sige, at mærket skal kunne tilegnes af både den lille frisør eller automekanikeren, men også af en stor, international virksomhed. I målet om at sondre mellem de enkelte virksomhedsprofiler tages der derfor udgangspunkt i en risiko-matrix (udarbejdet af Erhvervsstyrelsen; som illustreret herunder), der gør det muligt at fordele virksomhederne ud i fire kategorier afhængig af data- og organisationskompleksitet. /KL.7 og arbejdsgruppen har givet et bud på, hvordan denne kompleksitet kan operationaliseres ved hjælp af tre simple spørgsmål.

Screening af virksomhedernes risikoprofil

1. Hvor mange ansatte er der i virksomheden?
2. Hvilke typer af data anvender virksomheden?
3. Anvender virksomheden algoritmer eller AI-teknologi?

Virksomheder får, på baggrund af de tre spørgsmål, en risikoscore for deres organisering og for deres brug af data og systemer. Alt efter deres score på de to parametre, bliver de placeret i én af fire risikogrupper. Gruppenumrene afspejler risikoen – jo større nummer, jo større risiko. De ovenstående spørgsmål er forslag til en måde at definere virksomhedsprofilens risikogruppe, men der kan vel at mærke være andre spørgsmål som også er egnet. Risikogruppen definerer de krav og kontrolparametre, som virksomheden i sidste ende skal leve op til for at tilegne sig mærket.



Forbrugere og virksomhedernes kunder

Udover virksomheder er både almindelige forbrugere og virksomhedernes kunder primære målgrupper for mærket. Disse målgrupper er afgørende for mærkets potentiale og for mærkets værdiskabelse i form af konkurrencefordele. Indsigter om forbrugere og virksomheder er samlet i bilag 5.5.1 og 5.5.2.

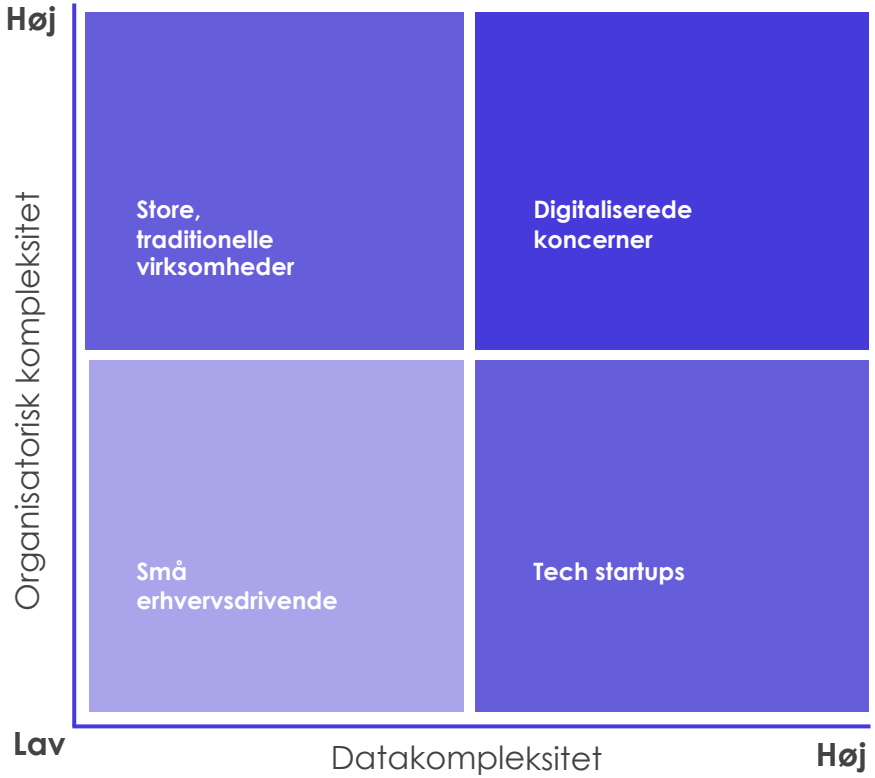
Fire arketyper af virksomheder

Lidt forsimplet kan man kategorisere virksomheder i hver af de fire risikogrupper som fire forskellige arketyper.

Virksomheder i risikogruppe 1 (lav data- og organisatorisk kompleksitet) kaldes for Små erhvervsdrivende, mens virksomheder i riskogruppe 2 (lav datakompleksitet og høj organisatiorisk kompleksitet) kaldes store, traditionelle virksomheder. Det vil typisk være klassiske produktions- og servicevirksomheder.

Virksomheder i risikogruppe 3 kaldes Tech startups, og indbefatter mindre virksomheder med høj datakompleksitet - det vil typisk være mindre virksomheder, der sælger digitale services eller software.

Virksomheder i risikogruppe 4 kaldes Digitaliserede koncerner. Det er virksomheder med høj data- og organisationskompleksitet.



Sådan placeres virksomheden i en risikogruppe

Nogle får mærket med det samme. Nogle skal gøre lidt. Andre er langt fra.

Datakompleksitet x organisatorisk kompleksitet = risikogruppe

↓ Hvilke typer af data anvender virksomheden?

Anvender virksomheden algoritmer eller AI-teknologi?

↓ Hvor mange medarbejdere er der i virksomheden?

3. Tildeling af mærket

3.1 Markedsføring

De fleste virksomheder byder ideen om en mærkningsordning velkommen, bortset fra virksomheder med lille data- og organisatorisk kompleksitet (eksempelvis automekanikere og frisører). De har svært ved at se, hvad mærket gør for dem. Virksomhederne i riskogruppe 2, 3 og 4 fremhævede særligt fordelen ved at have et mærke med brandingpotentiale, som er valideret af en ekstern og seriøs autoritet.

Hvad får man som virksomhed ud af datamærket?

Markedsføringen af datamærket skal tale ind i de behov, som virksomhederne har. De fleste virksomheder er blevet tudet ørene fulde af løftede GDPR-fingre. For mange virksomheder, har mødet med GDPR-lovgivningen været besværlig og bureaukratisk og gjort, at it-sikkerhed er blevet til et nødvendigt onde frem for en vigtig og spændende dagsorden. Samtidigt er dataetik stadig så abstrakt en størrelse, at de færreste virksomheder ved, hvordan de skal gribe den an. Set i lyset heraf, står datamærket over for den ekstraordinært svære opgave at ændre virksomhedernes opfattelse af digital ansvarlighed som noget, der oprindeligt har været et lovmæssigt krav men som nu udgør et attraktivt differentieringsparameter over for f.eks. konkurrenter. Denne ændrede opfattelse kommer også i takt med, at flere og flere forbrugere efterspørger digital ansvarlig praksis blandt virksomheder, men den kan hjælpes på vej af en stærk fortælling om, hvad virksomhederne får ud af at gøre digital ansvarlighed til deres mærkesag. I starten af sprintet, satte /KL.7 og arbejdsgruppen sig for at identificere de primære fordele ved mærket fra et virksomhedsperspektiv:

1. Datamærket tilbyder virksomhederne en ramme for at arbejde med digital ansvarlighed

Selv de mest positivt indstillede og entusiatiske virksomheder har svært ved at tage digital ansvarlighed til sig uden konkrete vejledninger til, hvordan de skal gøre det. Med datamærket får virksomheder en ramme for at arbejde med digital ansvarlighed, der tager afsæt i deres specifikke situation - hvad enten man er en online énmandsvirksomhed eller en større organisation. Datamærket viser virksomhederne, hvad de skal fokusere på, værne om og arbejde hen imod for at behandle deres kunders og samarbejdspartneres data sikkert og ansvarligt.

Denne værdiskabelse stemte delvist overens med virksomhedernes opfattelse af mærkets værdi i brugertesten. Virksomhederne var primært interesseret i at få en ekstern validering af deres digitale ansvarlighed, som de så kunne bruge i deres markedsføring over for kunder. Men de forventede også, at aktøren bag datamærket ville hjælpe dem på vej til at overholde eksisterende lovgivning og sikre, at de levede op til datamærkningsordningens kriterier.

2. Datamærket er en brugervenlig guide til implementering af digital ansvarlig praksis

Den amerikanske forfatter, Derek Sivers, har sagt: "Hvis information var løsningen på vores problemer, ville vi alle rende rundt som milliardærer med perfekte sixpacks". Med andre ord, så kræver det mere end blot informationer og oplysningskampagner at få virksomheder til at praktisere digital ansvarlighed. Virksomhederne skal have brugervenlige guides, der tager udgangspunkt i deres virkelighed - dvs. det skal være operationelt og forståeligt for dem.

Denne værdiskabelse blev især fremhævet af virksomhederne i gruppe 2, som ikke nødvendigvis har ressourcerne eller tilstrækkelig viden til at overholde og implementere retningslinjerne for digital ansvarlighed.

3. Datamærket giver virksomheder en mulighed for at differentiere sig over for konkurrenter og dermed en øget konkurrencefordel

Virksomhederne i risikogruppe 3 arbejder ofte med digitale kerneydelser, hvis teknologiske afsæt forudsætter en høj grad af it-sikkerhed eller dataetik. I brugertesten var det yderligere gennemgående, at virksomhederne i risikogruppe 3 i forvejen er godt på vej med den digitale ansvarlighed. Derfor vil virksomheder i risikogruppe 3 potentielt opleve konkurrencefordelen i mærket som ekstra værdifuld, hvilket bør afspejles i markedsføring og kommunikation.

4. Datamærket giver virksomheder et forspring til hurtigt at opnå internationalt mærke og dermed øget international konkurrencefordel

Virksomhederne i risikogruppe 4 stiller sig kritiske over for ideen om, at mærket giver et forspring til at opnå internationalt mærke i dets nuværende form. Dels henvender det sig til danske marked, dels er det ikke synligt, at det trumfer internationale standarder. Hvis denne fordel ved mærket skal realiseres, vil det højst sandsynligt kræve tid og en række cases, der evaluerer på mærkets effekt i en international kontekst.

Datamærket skal kunne markedsføres til alle slags virksomheder

Jo tættere vi kommer på dét behov, som den enkelte virksomhed har, jo større sandsynlighed for at få virksomheden ind i mærkningsordningen. Med andre ord skal hver virksomhedstype kunne se sig selv i datamærket.

En konkret del af markedsføringen bør derfor bestå i at tydeliggøre problemet via cases, hvor begrænset it-sikkerhed og/eller dataetiske retningslinjer fx har ført til datalæk eller mistet værdi i en kontekst, som hver virksomhed genkender. Dette efterspørges direkte af en virksomhed på risikogruppe 3, der mener, at dette mangler i det offentlige billede og kan være en årsag til den manglende opmærksomhed omkring emnet. Samtidig er det vigtigt at demonstrere forbrugernes fokus på, at virksomheder anvender deres data ansvarligt. Her er forbrugerne ikke ønskværdigt tydelige endnu, men indtil digital ansvarlighed bliver et tydeligere pejlemærke for de fleste forbrugere, kan cases med progressive kunder anvendes. Hvad der ikke ligger i volumen kan troværdigt ligge i udsagn fra 'first-movers' og meningsdannere være fin erstatning i udrulning.

Datamærket kan med fordel markedsføres af interesseorganisationerne

Brugertesten pegede på, at flere virksomheder gerne vil have en offentlig instans' ord for, at deres digitale ansvarlighed lever op til højeste standarder. Eftersom mærket vil blive varetaget af en privat aktør, er det derfor oplagt at udnytte den høje grad af troværdighed til virksomhedernes interesseorganisationer til at blåstemple datamærket som led i en markedsføringsstrategi.

Helt konkret vil arbejdsgruppens respektive interesseorganisationer med fordel kunne koordinere, hvordan de i fællesskab markedsfører datamærket til deres medlemmer med udgangspunkt i virksomhedernes risikoprofil.

VIRKSOMHEDERNE I BRUGERTESTEN KUNNE DELVIST GENKENDE FORDELENE VED MÆRKNINGSORDNINGEN

Virksomhedstype	*"Virksomheden får en ramme og brugervenlig guide til at arbejde med digital ansvarlighed"*	*"Virksomheden får mulighed for at differentiere sig over for konkurrenter og opnår dermed konkurrencefordel (nationalt og internationalt)"*
Risikogruppe 1 Lav org. kompleksitet Lav datakompleksitet *Eksempel: Automekaniker, frisør.*	Virksomheden mener ikke, at der er brug for yderligere rådgivning – dette ydes af virksomhedens brancheforening.	Virksomheden i denne gruppe oplever ikke mærket som en potentiel konkurrencefordel over for deres kundesegment.
Risikogruppe 2 Høj org. kompleksitet Lav datakompleksitet *Eksempel: Produktionsvirksomhed*	Denne indsigt fremhæves især af virksomheden – virksomheden har interessen, men ikke nødvendigvis ressourcer/viden til at overholde retningslinjer.	Virksomheden slår sig, som følge af deres datakompleksitet, ikke nødvendigvis på it-sikkerhedsmæssige eller dataetiske retningslinjer, men ser en potentiel merværdi i at overholde lovgivning vha. guide.
Risikogruppe 3 Lav org. kompleksitet Høj datakompleksitet *Eksempel: AI startup*	Mens guiden er et fint supplement, har virksomheder i denne gruppe godt styr på data- og it-sikkerhed og mangler primært en instans, der kan kvalificere virksomhedens digitale ansvarlighed.	Denne værdiskabelse er især relevant for virksomheder i risikogruppe 3, da deres forretning vil være tæt forbundet med at have styr på digital ansvarlighed. Ifølge virksomhederne er det dog både synligheden omkring deres indsats, men også vigtigt at have en instans i ryggen, der kan blåstemple indsatsen.
Risikogruppe 4 Høj org. kompleksitet Høj datakompleksitet *Eksempel: Teleselskab, medicinalvirksomhed, retail.*	Ligesom virksomheder i risikogruppe 3 er virksomheder på dette niveau ofte opmærksomme på dataetiske/it-sikkerhedsmæssige retningslinjer, men mangler en officiel instans, der kan give dem en konkurrencefordel på et internationalt marked	Ligesom virksomheder i risikogruppe 3 er både synlighed og en officiel instans vigtig for virksomhederne i risikogruppe 4. Dog tvivler virksomhederne på den internationale konkurrencefordel med mærket i sin nuværende form, da mærket ikke trumfer internationale standarder og primært henvender sig det danske marked

3.2 Prissætning

Følgende indsigter er indsamlet på baggrund af interviews med virksomheder i forbindelse med sprintet.

Risikogruppe 2 og 3
Virksomheder i henholdsvis risikogruppe 2 og 3 anslår at ville give mellem 5.000-20.000 kr. for en mærkningsordning med udgangspunkt i de kriterier og den værdiskabelse, der er foreslået. Samtidig er prisen for virksomhederne i risikogruppe 3 tæt knyttet sammen med to ting:
1. Om virksomheden kan læne sig op ad mærkets instans (hvilken grad af sikkerhed vil organisationen bag mærket give virksomhederne),
2. Typen af kontrol.

Virksomhederne ser gerne, at mærket giver en ansvarlig instans at læne sig op ad over for kunder og foretrækker i den forbindelse også en vis grad af officielle audits – for meget egenkontrol underbygger blot virksomhedernes i forvejen store eget-ansvar for den digitale sikkerhed. En virksomhed i risikogruppe 3 foretrækker dog nogle redskaber, der gør det muligt at udføre en intern kontrol. For respondenten hér ligger forskellen i prissætningen i, hvorvidt mærket ville betyde, at man ikke samtidig skal vise, at man lever op til fx ISO-27001 standarder, men at mærket kan stå alene som et udtryk for sikkerhed, også over for internationale kunder. Hvis sidstnævnte er tilfældet vil virksomheden give mellem 30.000-50.000 kr. Pointen afspejles også i en anden virksomhed i risikogruppe 3, hvis prissætning afhænger af, hvor meget risiko mærkningsordningen mitigerer – altså hvor meget virksomheden kan læne sig op ad organisationen bag.

Risikogruppe 4
Ligeledes fremhæver en virksomhed i risikogruppe 4, at købsvilligheden afhænger af, hvor stor en differentiator mærkningsordning vil give dem på markedet. Det handler for virksomheden om tydeligt at kunne synliggøre de ressourcer de lægger i digital ansvarlighed og på den måde styrke kunderelationen. Hvis mærket kan garantere en sikkerhed for, at virksomhedens services lever op til og tager højde for dataetiske/it-sikkerhedsmæssige problemstillinger, er betalingsvilligheden større. Antaget at mærkningsordningen giver en reel konkurrencefordel, er prisen for virksomheder i risikogruppe 4 ikke nødvendigvis en barriere.

Anbefalinger til
Prissætning

Risikogruppe	Minimumspris	Maximumspris	Betalingsvillighed afhænger af
1	0 kr.	10.000 kr.	Må ikke føles som spildte penge.
2	5.000 kr.	20.000 kr.	Mærket skal udgøre en reel konkurrencefordel og gøre det muligt at implementere foranstaltninger.
3	30.000 kr.	50.000 kr.	Organisationen bag mærket skal give virksomheden sikkerhed, og graden af kontrol og tilsyn (skal ikke bare baseres på egenkontrol).
4	? kr.	? kr.	Hvor stor en differentiator bliver mærkningsordningen på markedet?

3.3 Onboarding

Ud over markedsføringen af datamærkningsordningen, er en brugervenlig onboarding også vigtig for virksomhedernes tilslutning til data mærket. Datamærkningsordningens kriterier vil for mange virksomheder eksempelvis være helt nye. Derfor er en gradvis kommunikation af mærkets kontrol og krav afgørende. /KL.7 foreslår, at onboardingen følger en *progressive disclosure model*, hvilket betyder, at virksomhederne kun præsenteres for den information, der er nødvendig på de rigtige tidspunkter i løbet af brugerrejsen. I praksis betyder det, at man ikke beder virksomhederne forholde sig til samtlige kriterier, kontrol og krav på én gang, men i stedet giver mulighed for gradvist og sekventielt at blive introduceret for de forskellige kriterier i mærkningsordningen. Det betyder, at virksomhederne først opnår mærket når de indfrier samtlige kriterier, men at kommunikationen i onboardingen bedst muligt understøtter virksomhederne i at tilegne sig mærket ét kriterie ad gangen.

Et par overordnede tommelfingerregler for onboardingen er:

Reducér kompleksiteten
Mængden af information og valgmuligheder har en stor betydning for, hvor nemt vi har ved at træffe en beslutning. Derfor bør mængden af information og valgmuligheder reduceres ved kun at fremhæve de kriterier, virksomheden skal forholde sig til lige nu.

Gør det nemt at komme i gang
De skridt, der er lette og hurtige at udføre, skal placeres i starten – det øger sandsynligheden for 100 pct. færdiggørelse.

Giv feedback undervejs
Bryd brugerrejsen ned i overskuelige del-elementer, som kan 'afkrydses' undervejs, for at give en en løbende oplevelse af progression.

På de næste sider ses forslag til et muligt onboarding-flow, der søger at implementere ovenstående tommelfingerregler: Virksomheden placeres i en risikogruppe ved at besvare tre spørgsmål delt op i tre steps. På baggrund af onboardingen præsenteres virksomheden for de kriterier, der matcher risikogruppen – med vægt på de to kriterier, der er mest oplagte for virksomheden at starte med.

I målet om at give virksomhederne en følelse af hurtig progression, kan man yderligere spørge ind til, hvor virksomhederne ligger i forhold til kriterierne i dag. På den måde kan det tydeliggøres, at virksomhederne allerede er på vej mod at kunne tilegne sig mærket – og derigennem forstærke virksomhedens oplevelse af hurtig progression.

1 HVOR MANGE ANSATTE ER I?

2 HVILKE TYPER DATA ANVENDER I?

3 BENYTTER I AI ELLER ALGORITMER?

Hvor mange medarbejdere er der i virksomheden?

- [x] Mindre end 50 medarbejdere
- [ ] Mellem 50 og 250 medarbejdere
- [ ] Flere end 250 medarbejdere

Digitalt Ansvar

← Tilbage

Næste →

1 — 2 — 3

HVOR MANGE ANSATTE ER I? | HVILKE TYPER DATA ANVENDER I? | BENYTTER I AI ELLER ALGORITMER?

Hvilke typer data anvender I?

- [x] CPR-numre
- [x] Kort-oplysninger
- [ ] GPS/IP
- [x] Sundhedsdata

Digitalt Ansvar

← Tilbage

Næste →

1 HVOR MANGE ANSATTE ER I?

2 HVILKE TYPER DATA ANVENDER I?

3 BENYTTER I AI ELLER ALGORITMER?

Anvender I algoritmer eller AI-teknologier?

- [x] Ja
- [ ] Nej

Digitalt Ansvar

← Tilbage

Næste →

4 HVAD SKAL I GØRE FOR AT TILEGNE JER MÆRKET?

5 HVOR BØR I STARTE?

Kriterier

Digitalt Ansvar

← Tilbage

Vi hjælper jer godt i gang

Med jeres type virksomhed anbefaler vi, at i starter med at have fokus på *Forankring i ledelsen* og *Krav til leverandører*.

Herunder kan du se præcis, hvad det vil kræve af jer at møde kriterierne og hvordan der føres kontrol med kriterierne løbende. På næste side viser vi dig, hvordan du kommer i gang.

KRITERIE

Forankring i ledelsen

Krav

Virksomhedens øverste ledelse tager ansvar for arbejdet for øget sikkerhed og ansvarlighed i databehandlingen

Kontrol

Årlige stikprøver, hvor virksomhedens ledelse bliver ringet op og bedt om at dokumentere it-sikkerhed

KRITERIE

Krav til leverandørers databehandling

Krav

Virksomheden har et overblik over leverandører og har foretaget en risikovurdering af dem hver især.

Kontrol

It-leverandører har skrevet under på virksomhedens politik for it-sikkerhed og ansvarlig databehandling.

Næste →

3.4 Tildelingskriterier

Datamærkningsordningen skal give dansk erhvervsliv et solidt sikkerhedsmæssigt løft og gøre det mere attraktivt for den enkelte virksomhed at håndtere data på en ansvarlig og sikker måde. Kernen i mærkningsordningen er de kriterier, man som virksomhed skal leve op til for at blive tildelt mærket. Kriterierne skal kommunikere til virksomhederne, at mærket kræver mere end blot compliance med eksisterende lovgivning og gældende standarder. Men samtidig skal kriterierne også være overskuelige og realistiske for virksomheder med meget forskellige niveauer af kompleksitet i både organisation og i databeholdning. Først beskrives processen for udvælgelsen af kriterierne, og derefter gennemgås de udvalgte kriterier.

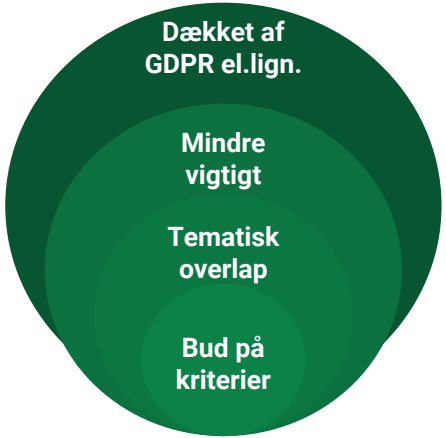
3.4.1 Udvælgelsesprocessen

Udvælgelsen af kriterierne blev foretaget i en række trin, som blev fremlagt på to workshops undervejs i sprintforløbet. /KL.7's proces omkring udvælgelsen af kriterierne op til de to workshops er illustreret i figuren nederst t.h. og er forklaret i teksten umiddelbart herunder.

Først blev kriterier med kraftigt overlap med eksisterende lovgivning (især GDPR) fjernet. Det var nødvendigt, fordi mærkningsordningen skal bygge ovenpå den eksisterende lovgivning og skabe en best practice. Samtidig skulle lovgivningsmæssige kriterier ikke skrives helt ud af tildelingskriterierne, fordi mærkningsordningen også skal virke som en løftestang for danske virksomheders arbejde med it-sikkerhed og ansvarlig dataanvendelse.

Derefter konsulterede /KL.7 eksperternes vurdering af kriteriernes vigtighed, som blev tilkendegivet i en online survey udsendt til 36 eksperter i ansvarlig dataanvendelse og 20 eksperter i it-sikkerhed. Kriterierne blev vurderet af eksperterne som "Meget vigtigt", "Vigtigt", "Mindre vigtigt" eller "Ikke vigtigt". Kriterier med en gennemsnitlig score i surveyen på mindre end "Vigtigt" blev fjernet. Afslutningsvist lagde /KL.7 de kriterier sammen, som havde større eller mindre grad af tematisk overlap med hinanden.

/KL.7 forelagde udvælgelsesprocessen og de udvalgte kriterier for deltagerne på et arbejdsmøde og en workshop undervejs i sprintforløbet. På den baggrund blev enkelte kriterier fjernet og lagt til samt kvalificeret med henblik på endelig operationalisering og segmentering i kontrol og tilsyn.



3.4.2 Udvalgte tildelingskriterier

1

Forankring i ledelsen

Virksomhedens øverste ledelse tager ansvar for arbejdet for øget sikkerhed og ansvarlighed i databehandlingen

2

Krav til leverandørers databehandling

Virksomheden har et overblik over leverandører og har foretaget en risikovurdering af dem hver især. I tilfælde af en kritisk risikovurdering skal der foreligge en handlingsplan.

3

Awareness og sikker adfærd

Virksomhedens medarbejdere bliver løbende og med jævne mellemrum trænet, testet og evalueret i awareness og handlingskompetencer i relation til databehandling og -beskyttelse.

4

Klar kommunikation

Virksomhedens privatlivspolitik og er let at finde og forstå for lægmænd, og beslutninger truffet pba. profilering og automatiserede processer er transparente og formidlet i et forståeligt sprog.

5

Teknisk it-sikkerhed

Virksomheden lever op til gældende standarder for teknisk it-sikkerhed, især hvad angår antivirus-/firewall, kontobeskyttelse og opdatering af software.

6

Kontrol over egne data

Virksomheden gør det nemt for forbrugere og samarbejdspartnere at forstå, hvilke data der er nødvendige for virksomhedens service, og at slå behandlingen af ikke-nødvendige data til og fra.

7

Fair og fordomsfri algoritmer

Virksomheden træner sine algoritmer på et datagrundlag, der er repræsentativt for den gruppe mennesker, der serviceres, og har proces for at de-biase alle automatiserede beslutninger.

8

Afpersonalisering af persondata

Virksomheden har et erklæret mål om og en konkret strategi for at anonymisere og pseudnoymisere alle persondata, den behandler.

Gruppe 1

1 Forankring i ledelsen

Virksomhed skal uploade dokument, der viser, at ledelsen har en forpligtende målsætning for arbejdet med it-sikkerhed og for at bruge data ansvarligt.

1. Sekretariatet gennemgår af det uploadede dokument og formelt godkendelse.
2. Sekretariatet foretager årlige stikprøver, hvor virksomhedens ledelse bliver ringet op og bedt om at dokumentere, at it-sikkerhed og ansvarlig databehandling er en del af ledelsens fokus.

2 Krav til leverandører

Virksomheden uploader en **liste over leverandører** i tekstformat og angiver, at den har foretaget **risikovurdering** af disse leverandører. I tilfælde af høj risiko angives det, at der foreligger en **handleplan.**

1. Sekretariatet gennemgår listen og vurderer, om der pba. af virksomhedsnavnene er grund til at betvivle risikovurdering.
2. Sekretariatet foretager årlige stikprøver, hvor virksomheden bliver kontaktet og bedt om at fremvise risikovurdering af de angivne leverandører og evt. handleplan.

3 Awareness om sikker adfærd

Virksomheden erklærer, at den har dokumentation for, at alle medarbejdere har opnået masterdiplom i app'en SikkerKollega, og uploader onboarding-plan, der viser, at alle nye medarbejdere bliver introduceret til app'en.

1. Sekretariatet gennemgår onboarding-planen og godkender formelt.
2. Sekretariatet foretager årlige stikprøver, hvor virksomheden bliver kontaktet og bedt om at fremvise dokumentation for medarbejdernes masterdiplomer.

4 Klar kommunikation

VIrksomheden uploader sin privatlivspolitik i tekstformat eller indtaster hjemmesidestien og erklærer, at privatlivspolitkkken er lettilgængelig og -forståelig for lægmænd.

1. Sekretariatet gennemgår privatlivspolitikken i tekstformat eller på hjemmesidestien og godkender, at den er letforståelig.
2. Sekretariatet nedsætter et borgerpanel, som iværksættes til årlige stikprøver, hvor medlemmerne uhjulpet skal finde, læse og forstå virksomhedens privatlivspolitik på virksomhedens egen hjemmeside.

5 Teknisk it-sikkerhed

Virksomheden erklærer, at den har en it-sikkerhedsansvarlig medarbejder, og angiver, at der anvendes antivirus/firewall, og uddyber i fritekstsvar, hvordan det sikres, at virksomheden foretager jævnlige backup og sørger for tilstrækkelig kontobeskyttelse og automatisk opdatering af software.

1. Sekretariatet gennemgår fritekstsvaret og godkender, at det lever op til tilstrækkelige og nødvendige forudsætninger for teknisk it-sikkerhed.

8 Afpersonalisering af data

Virksomheden angiver i fritekstfelt, hvordan den sikrer, at persondata bliver pseudonymiseret eller anonymiseret.

1. Sekretariatet gennemgår besvarelsen og godkender formelt
2. Sekretariatet foretager årlige stikprøver, hvor virksomheden bliver bedt om at dokumentere afpersonalisering af data.

Gruppe 2

1 Forankring i ledelsen

Virksomheden uploader dokument, der viser, at man har en it-sikkerhedsstyrekomité eller en it-sikkerhedsansvarlig i ledelsen og KPI'er/målsætninger for arbejdet.

1. Sekretariatet gennemgår det uploadede dokument og godkender, at arbejdet er forankret i ledelsen.
2. Sekretariatet foretager årlige stikprøver, hvor virksomhedens ledelse bliver ringet op og bedt om at dokumentere arbejdet for at nå de angivne KPI'er/målsætninger for arbejdet.

2 Krav til leverandører

Virksomheden uploader en **liste over leverandører** i tekstformat og angiver, at den har foretaget **risikovurdering** af disse leverandører. I tilfælde af høj risiko angives det, at der foreligger en **handleplan.**

1. Sekretariatet gennemgår listen og vurderer, om der pba. af virksomhedsnavnene er grund til at betvivle risikovurdering.
2. Sekretariatet foretager årlige stikprøver, hvor virksomheden bliver kontaktet og bedt om at fremvise risikovurdering af de angivne leverandører og evt. handleplan.

3 Awareness om sikker adfærd

Virksomheden erklærer, at den har dokumentation for, at alle medarbejdere har opnået masterdiplom i app'en SikkerKollega, og uploader onboarding-plan, der viser, at alle nye medarbejdere bliver introduceret til app'en.

1. Sekretariatet gennemgår onboarding-planen og godkender formelt.
2. Sekretariatet foretager årlige stikprøver, hvor virksomheden bliver kontaktet og bedt om at fremvise dokumentation for medarbejdernes masterdiplomer.

4 Klar kommunikation

VIrksomheden uploader sin privatlivspolitik i tekstformat eller indtaster hjemmesidestien og erklærer, at privatlivspolitkkken er lettilgængelig og -forståelig for lægmænd.

1. Sekretariatet gennemgår privatlivspolitikken i tekstformat eller på hjemmesidestien og godkender, at den er letforståelig.
2. Sekretariatet nedsætter et borgerpanel, som iværksættes til årlige stikprøver, hvor medlemmerne uhjulpet skal finde, læse og forstå virksomhedens privatlivspolitik på virksomhedens egen hjemmeside.

5 Teknisk it-sikkerhed

Virksomheden erklærer, at den har en it-sikkerhedsansvarlig medarbejder, og uddyber i fritekstsvar, hvilken antivirus/firewall der anvendes, samt hvordan det sikres, at virksomheden foretager jævnlige backup og sørger for tilstrækkelig kontobeskyttelse og automatisk opdatering af software.

1. Sekretariatet gennemgår fritekstsvaret og godkender, at det lever op til tilstrækkelige og nødvendige forudsætninger for teknisk it-sikkerhed.

6 Kontrol over egne data

Virksomheden tilkendegiver, at den har en liste over indsamlede persondata (inkl. formål og opdeling af nødvendige/ikke-nødvendige), og sletter efter antal t./d.. 1-3 screendumps el. links med eks. på, hvordan kunder/samarb.part. gøres opmærksom på dette og deres rettigheder til at slå ikke-nødvendige til/fra.

1. Sekretariatet gennemgår screendumps og godkender formelt
2. Sekretariatet foretager årlige stikprøver, hvor borgerpanel gennemgår screendumps og ser, om informationen er forståelig og overskuelig eller ej.

8 Afpersonalisering af data

Virksomheden angiver, at den har procedurer for systematisk afpersonalisering af persondata, og uddyber i fritekstfelt, hvad denne systematiske afpersonalisering består i.

1. Sekretariatet gennemgår besvarelsen og godkender formelt
2. Sekretariatet foretager årlige stikprøver, hvor virksomheden bliver bedt om at dokumentere den systematiske afpersonalisering af persondata.

1 Forankring i ledelsen

Virksomhed skal uploade dokument, der dokumenterer, at man har en it-sikkerhedsstyrekomité, en it-sikkerhedsansvarlig i ledelsen, KPI'er/målsætninger for arbejdet eller lignende).

1. Sekretariatet gennemgår det uploadede dokument og godkender, at arbejdet er forankret i ledelsen.
2. Sekretariatet foretager årlige stikprøver, hvor virksomhedens ledelse bliver ringet op og bedt om at dokumentere arbejdet for at nå de angivne KPI'er/målsætninger for arbejdet.

2 Krav til leverandører

Virksomheden uploader en **liste over leverandører** i tekstformat og angiver, at den har foretaget **risikovurdering** af disse leverandører. I tilfælde af høj risiko angives det, at der foreligger en **handleplan.**

1. Sekretariatet gennemgår listen og vurderer, om der pba. af virksomhedsnavnene er grund til at betvivle risikovurdering.
2. Sekretariatet foretager årlige stikprøver, hvor virksomheden bliver kontaktet og bedt om at fremvise risikovurdering af de angivne leverandører og evt. handleplan.

3 Awareness om sikker adfærd

Virksomheden erklærer, at den har dokumentation for, at alle medarbejdere har opnået masterdiplom i app'en SikkerKollega, og uploader onboarding-plan, der viser, at alle nye medarbejdere bliver introduceret til app'en.

1. Sekretariatet gennemgår onboarding-planen og godkender formelt.
2. Sekretariatet foretager årlige stikprøver, hvor virksomheden bliver kontaktet og bedt om at fremvise dokumentation for medarbejdernes masterdiplomer.

4 Klar kommunikation

Virksomheden angiver, at dens privatlivspolitik forefindes i en udgave, der er lettilgængelig og -forståelig for lægmænd, og hvilken procedure man anvender for at undgå 'black box'-algoritmer.

1. Sekretariatet gennemgår privatlivspolitikken i tekstformat eller på hjemmesidestien og godkender, at den er letforståelig.
2. Sekretariatet gennemgår proceduren for undgå 'black box'-algoritmer og godkender.
3. Sekretariatet nedsætter et borgerpanel, som iværksættes til årlige stikprøver, hvor medlemmerne uhjulpet skal finde, læse og forstå virksomhedens privatlivspolitik på virksomhedens egen hjemmeside.

5 Teknisk it-sikkerhed

Virksomheden uploader dok. fra ekstern auditør på, at virksomheden lever op til gældende ledelsesstandard for databeskyttelse (DS/ISO/ISF). Alternativt uddybning i fritekst af, hvordan man lever op til tilsv. krav for ansvars-/rollefordeling og interne processer samt antivirus/firewall, kontobeskyttelse, procedure for backup og automatisk opdatering af software.

1. Sekretariatet stiller liste til rådighed over de tilsvarende krav fra gældende ledelsesstandard, så virksomheder uden disse standarder
2. Sekretariatet gennemgår det uploadede dokument eller fritekst-svaret og godkender formelt.

6 Kontrol over egne data

Virksomheden tilkendegiver, at den har en liste over indsamlede persondata (inkl. formål og opdeling af nødvendige/ikke-nødvendige), og sletter efter antal t./d.. 1-3 screendumps el. links med eks. på, hvordan kunder/samarb.part. gøres opmærksom på dette og deres rettigheder til at slå ikke-nødvendige til/fra.

1. Sekretariatet gennemgår screendumps og godkender formelt
2. Sekretariatet foretager årlige stikprøver, hvor borgerpanel gennemgår screendumps og ser, om informationen er forståelig og overskuelig eller ej.

7 Fair og fordomsfri algoritmer

Virksomheden angiver hvilken procedure, der anvendes for 1) at imødegå bias i automatiserede beslutninger foretaget af algoritmer, for at 2) optimere repræsentativiteten i datagrundlaget for algoritmernes træning og 3) identificere og udbedre lav repræsentativitet i datagrundlaget.

1. Sekretariatet gennemgår besvarelsen og godkender formelt.
2. Sekretariatet foretager årlige stikprøver, hvor virksomheden med faresignaler (f.eks. lav repræsentativitet) kontaktes og bedes dokumentere resultaterne af arbejdet med at udbedre problemet.

8 Afpersonalisering af data

Virksomheden angiver, at den har en strategi for at arbejde for indbygget databeskyttelse (privacy-by-design), og forklarer i fritekstfelt strategiens indhold og tidsplan eller uploader strategien.

1. Sekretariatet gennemgår strategien og tidsplanen og godkender.
2. Sekretariatet foretager årlige stikprøver, hvor virksomheden bliver bedt om at dokumentere arbejdet med den angivne strategi.

1 Forankring i ledelsen

Virksomhed skal uploade dokument, der dokumenterer, at man har en it-sikkerhedsstyrekomité, en it-sikkerhedsansvarlig i ledelsen, KPI'er/målsætninger for arbejdet eller lignende).

1. Sekretariatet gennemgår det uploadede dokument og godkender, at arbejdet er forankret i ledelsen.
2. Sekretariatet foretager årlige stikprøver, hvor virksomhedens ledelse bliver ringet op og bedt om at dokumentere arbejdet for at nå de angivne KPI'er/målsætninger for arbejdet.

2 Krav til leverandører

Virksomheden uploader en **liste over leverandører** i tekstformat og angiver, at den har foretaget **risikovurdering** af disse leverandører. I tilfælde af høj risiko angives det, at der foreligger en **handleplan.**

1. Sekretariatet gennemgår listen og vurderer, om der pba. af virksomhedsnavnene er grund til at betvivle risikovurdering.
2. Sekretariatet foretager årlige stikprøver, hvor virksomheden bliver kontaktet og bedt om at fremvise risikovurdering af de angivne leverandører og evt. handleplan.

3 Awareness om sikker adfærd

Virksomheden angiver dokumentation for, at alle medarb. har gennemgået en systematisk awareness- og videnstræning, og uploader onboarding-plan, der viser, at alle nye medarb. gennemfører tilsvarende, samt tidsplan for at fastholde og forbedre awareness og adfærd.

1. Sekretariatet gennemgår onboarding-planen og godkender formelt.
2. Sekretariatet foretager årlige stikprøver, hvor virksomheden bliver kontaktet og bedt om at fremvise dokumentation for resultater af awareness- og vidensindsatsen.

4 Klar kommunikation

Virksomheden angiver, at dens privatlivspolitik forefindes i en udgave, der er lettilgængelig og -forståelig for lægmænd, og hvilken procedure man anvender for at undgå 'black box'-algoritmer.

1. Sekretariatet gennemgår privatlivspolitikken i tekstformat eller på hjemmesidestien og godkender, at den er letforståelig.
2. Sekretariatet gennemgår proceduren for undgå 'black box'-algoritmer og godkender.
3. Sekretariatet nedsætter et borgerpanel, som iværksættes til årlige stikprøver, hvor medlemmerne uhjulpet skal finde, læse og forstå virksomhedens privatlivspolitik på virksomhedens egen hjemmeside.

5 Teknisk it-sikkerhed

Virksomheden uploader dok. fra ekstern auditør på, at virksomheden lever op til gældende ledelsesstandard for databeskyttelse (DS/ISO/ISF).

1. Sekretariatet gennemgår det uploadede dokument og godkender formelt.

6 Kontrol over egne data

Virksomheden tilkendegiver, at den har en liste over indsamlede persondata (inkl. formål og opdeling af nødvendige/ikke-nødvendige), og sletter efter antal t./d.. 1-3 screendumps el. links med eks. på, hvordan kunder/samarb.part. gøres opmærksom på dette og deres rettigheder til at slå ikke-nødvendige til/fra.

1. Sekretariatet gennemgår screendumps og godkender formelt
2. Sekretariatet foretager årlige stikprøver, hvor borgerpanel gennemgår screendumps og ser, om informationen er forståelig og overskuelig eller ej.

7 Fair og fordomsfri algoritmer

Virksomheden angiver hvilken procedure, der anvendes for 1) at imødegå bias i automatiserede beslutninger foretaget af algoritmer, for at 2) optimere repræsentativiteten i datagrundlaget for algoritmernes træning og 3) identificere og udbedre lav repræsentativitet i datagrundlaget.

1. Sekretariatet gennemgår besvarelsen og godkender formelt.
2. Sekretariatet foretager årlige stikprøver, hvor virksomheden med faresignaler (f.eks. lav repræsentativitet) kontaktes og bedes dokumentere resultaterne af arbejdet med at udbedre problemet.

8 Afpersonalisering af data

Virksomheden angiver, at den har en strategi for at arbejde for indbygget databeskyttelse (privacy-by-design), og forklarer i fritekstfelt strategiens indhold og tidsplan eller uploader strategien.

1. Sekretariatet gennemgår strategien og tidsplanen og godkender.
2. Sekretariatet foretager årlige stikprøver, hvor virksomheden bliver bedt om at dokumentere arbejdet med den angivne strategi.

3.5 Kontrol og tilsyn

I dette afsnit uddyber vi forslag til, hvordan hver af de otte tildelingskriterier kan operationaliseres og dokumenteres. Forslagene for dokumentation er udarbejdet af /KL.7 på baggrund af research, brugertest, arbejdsmøder og en workshop undervejs i sprintforløbet. På den baggrund blev enkelte kriterier fjernet og lagt til samt kvalificeret med henblik på endelig operationalisering. Herunder gives bud på, hvordan sekretariatet godkender og fører kontrol og tilsyn med efterlevelsen af de otte kriterier for tildelingen.

1. Forankring i ledelsen

Virksomheden uploader årligt et dokument fra indeværende kalenderår, som enten viser, at virksomheden har nedsat en it-sikkerhedsstyrekomité, har en it-sikkerhedsansvarlig med foretræde for ledelsen, har erklærede KPI'er/målsætninger for arbejdet med sikkerhed og ansvarlighed i databehandlingen eller lignende.

Dokumentet kan være mødereferater, organisationsdiagram eller lignende, men skal være anonymiseret og med overstregning af evt. fortrolig information. Sekretariatets juridiske medarbejder gennemgår det uploadede dokument og godkender formelt. Dokumentationen skal uploades én gang årligt (dvs.at uploaden må være maks 365 dage gammel).

Sekretariatet foretager årlige stikprøver, hvor virksomhedens ledelse bliver ringet op og bedt om at redegøre eller henvise til dokumentation for, hvordan it-sikkerhed og ansvarlig databehandling er en del af ledelsens arbejde.

2. Krav til leverandørers databehandling

Virksomheden skal årligt uploade en liste over leverandører i tekstformat og angive, at den har foretaget en risikovurdering af disse leverandører. Hvis virksomheden i risikovurderingen konkluderer, at enkelte leverandørers databehandling er indebærer høj risiko, skal virksomheden forklare i fritekst, hvilken handlingsplan der foreligger med henblik på at udskifte pågældende leverandør eller stille krav til leverandøren om at imøde disse risici. Brugertesten viste dog en mulig faldgrube her, idet virksomhederne i nogle tilfælde vil have meget få leverandører at vælge imellem, og at 'red-flagging' af én potentielt er kritisk for virksomhedens mulighed for at vælge leverandører.

Sekretariatet gennemgår og godkender, at fritekstsvaret står mål med kriteriet om at stille krav til leverandørers databehandling.

Sekretariatet foretager årlige stikprøver, hvor virksomhederne bliver bedt om at fremvise risikovurderingen af de angivne leverandører.

3. Awareness og sikker adfærd

Små og mellemstore virksomheder: Virksomheden angiver, at alle medarbejdere inden for det seneste år har opnået et masterdiplom i app'en SikkerKollega el.lign. Alle råd og anbefalinger følger nationale råd og opdateres løbende i overensstemmelse hermed. Virksomheden bliver bedt om at besvare dette spørgsmål på ny én gang årligt. Desuden uploades onboarding-plan for, hvordan og hvornår nye medarbejdere bliver introduceret til app'en SikkerKollega eller lignende.

Store virksomheder: Denne type virksomheder har i mange tilfælde deres egne interne indsatser, og derfor giver det ikke mening at afkræve anvendelse af app'en SikkerKollega el.lign.. I stedet skal disse virksomheder angive, at alle medarbejdere har gennemgået awareness- og videnstræning inden for det seneste år, hvad denne træning overordnet har bestået i, og hvad planen er for at vedligeholde og forbedre awareness, viden og handlingskompetencer blandt nuværende og nye medarbejdere.

Sekretariatet gennemgår og godkender de små og mellemstore virksomheders onboarding-planer og de store virksomheders planer for vedligeholdelse og forbedring af awareness, viden og handlingskompetencer blandt medarbejderstaben.

Sekretariatet foretager stikprøver, hvor de små og mellemstore virksomheder skal fremvise dokumentation for, at deres medarbejdere har masterdiplom fra SikkerKollega. For de store virksomheder, som har deres egne interne indsatser til fremme af awareness og sikker adfærd, efterspørger sekretariatet i stikprøven dokumentation for gennemført awareness- og videnstræning og planer for fremtidige indsatser og målsætninger for dem.

4. Klar kommunikation

Virksomheden angiver, at dens privatlivspolitik kan findes, læses og forstås af en person uden juridisk eller teknisk viden.
Hvis virksomheden anvender automatiserede beslutninger, redegør den for i fritekst, hvilke procedurer der anvendes for at holde transparensen i automatiserede beslutningsprocesser så høj som muligt. Dvs. hvordan virksomheden sikrer, at den kan forklare, hvilke input algoritmerne baserer beslutninger på.

Sekretariatet gennemgår fritekstsvar og godkender formelt, om procedurer står mål med kriteriet om transparens.

Sekretariatet nedsætter et borgerpanel, som iværksættes til årlige stikprøveundersøgelser, hvor medlemmerne af panelet som lægmænd uhjulpet forsøger at finde, læse og forstå virksomhedens privatlivspolitik.

5. Teknisk it-sikkerhed

Som udgangspunkt antages det, at virksomhederne ikke har købt en gældende standard. Derfor vil sekretariatet administrere en opdateret liste over tekniske krav fra gældende standarder (DS/ISO og ISF's Standard of Good Practise) i forhold til antivirus-/firewall, kontobeskyttelse, procedure for backup og automatisk opdatering af software. Listen kan tilgås af de virksomheder, som ønsker at opnå mærket, men som hverken har købt eller agter at købe en af disse gældende standarder. De pågældende virksomheder skal krydse af, at de lever op til hvert af kravene på listen, samt beskrive i et fritekstfelt, hvordan de mere præcist lever op til dem.

Sekretariatets medarbejdere gennemgår beskrivelserne og godkender, at fritekstsvaret står mål med efterlevelse af de oplistede krav.

De virksomheder, som har købt en gældende ledelsesstandard for informationssikkerhed, uploader certifikat eller lign. gældende dokumentation fra ekstern auditør på, at den lever op til gældende ledelsesstandarder for informationssikkerhed (DS/ISO og ISF's Standard of Good Practise).

Sekretariatets medarbejdere gennemgår i dette tilfælde dokumentationen og godkender.

6. Kontrol over egne persondata

Virksomheden gør det nemt for dens brugere at forstå, hvilke data der er nødvendige for virksomhedens service, og hjælper med at slå behandlingen af de ikke-nødvendige data til og fra.

Virksomheden tilkendegiver, at den har en liste over, hvilke persondata der indsamles, til hvilke formål, og hvilke af dem, der er hhv. nødvendige og ikke-nødvendige for virksomhedens service/ydelse. Dertil uploader virksomheden 1-3 screendump med eksempler på, hvordan den gør kunder/samarbejdspartnere opmærksom på indsamling af nødvendige og ikke-nødvendige persondata, og hvordan den hjælper kunder/samarbejdspartnere med at slå de ikke-nødvendige persondata til og fra.

Sekretariatet gennemgår og godkender, at de uploadede screendumps viser en tilstrækkeligt overskuelig og forståelig oversigt over indsamling af nødvendige og ikke-nødvendige persondata, og at kunden/samarbejdspartneren bliver hjulpet tilstrækkeligt med at slå ikke-nødvendige persondata til og fra.

Sekretariatet foretaget desuden årlige stikprøver, hvor borgerpanel gennemgår virksomhedens screendumps og ser, om informationen er forståelig og overskuelig eller ej.

7. Fair og fordomsfri algoritmer

Hvis virksomheden anvender algoritmer, angiver den

- hvilken procedure der anvendes for at imødegå bias i automatiserede beslutninger foretaget af algoritmer.
- hvad der gøres for at optimere repræsentativiteten i datagrundlaget for algoritmernes træning.
- hvor der evt. er lav repræsentativitet i datagrundlaget for algoritmerne, og hvad der gøres for at imødegå dette.

Sekretariatets tekniske og juridiske medarbejdere gennemgår besvarelsen og vurderer, hvorvidt den lever op til kravet om processer, der understøtter fair og fordomsfri algoritmer.

Sekretariatet foretager årlige stikprøver, hvor virksomheden med faresignaler (f.eks. lav repræsentativitet) kontaktes og bedes dokumentere resultaterne af udbedringen.

7. Afpersonalisering af persondata

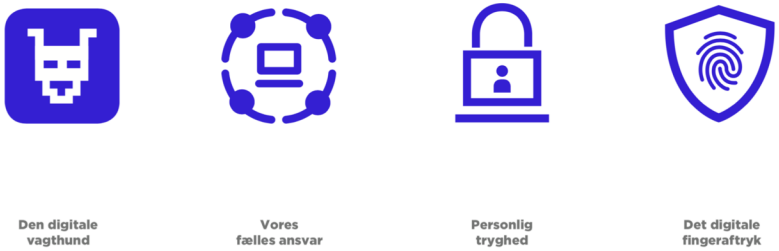
Virksomheden angiver, at den har en strategi for at arbejde for indbygget databeskyttelse (privacy-by-design) eller procedurer for systematisk afpersonalisering af persondata. Desuden forklarer virksomheden strategiens indhold og tidsplan i fritekst.

Sekretariatet gennemgår besvarelsen og godkender formelt, at strategien understøtter arbejdet for privacy-by-design eller tilsvarende inden for en overskuelig tidshorisont.

Sekretariatet foretager årlige stikprøver, hvor virksomheden bliver bedt om at dokumentere arbejdet med og efterlevelsen af den angivne strategi.

3.6 Visuel identitet

/KL.7 har udarbejdet fire bud på mærkets visuelle udtryk. Som udgangspunkt blev arbejdsgruppen præsenteret for forskellige visuelle udtryk, som vist herunder:



På baggrund af arbejdsgruppens input blev 'Det digitale fingeraftryk' og 'Den digitale vagthund' fravalgt inden brugertest med henholdsvis forbrugere og virksomheder. Derfor er mærkerne ***'Vores fælles ansvar'*** og ***'Personlig tryghed'*** drøftet i brugertests med virksomheder. I forbrugertesten blev respondenterne også bedt om at vurdere alle fire mærker ved siden af hinanden.

Indsigter fra virksomheds- og forbrugertest

Tre ud af seks forbrugere fremhævede mærket 'Personlig tryghed' i deres vurdering, mens to foretrak mærket 'Det digitale fingeraftryk'. Blandt respondenterne var der dog bred enighed om, at mærkerne overordnet ikke kommunikerede budskabet særlig effektivt, eksempelvis nævner en respondent: "*Men generelt forstår jeg ikke, hvorfor det skal være så kluntet*". Dette kunne yderligere observeres på respondenternes adfærd omkring spørgsmål til mærket, da **alle havde svært at svare på eller forstå meningen med mærket** i en webshop-kontekst. De respondenter som nævnte 'sikkerhed' i deres besvarelse gjorde det først efter lang tid – og refererede i deres begrundelse ikke til mærkets visuelle udtryk, men til placeringen på hjemmesiden (mærket var placeret ved siden af fx E-mærket/Trustpilot).

Ift. virksomheder foretrak respondenterne gennemgående 'Personlig tryghed' over 'Vores fælles ansvar', men flere syntes også, at mærkerne var for simple – i stedet efterspurgte flere virksomheder et mærke med en mere **autoritær signalværdi, der også kan bruges til at profilere sig overfor internationale kunder.**

Anbefalinger

Mærkets visuelle udtryk og signalværdi er vigtigt for forbrugerens forståelse af datamærkningsordningen – og for virksomhedernes villighed til at benytte mærket på kanaler og platforme. Derfor bør mærkets visuelle identitet, på baggrund af indsigterne fra brugertest, gentænkes og evt. videreudvikles i et separat sprint. Konkret anbefaler /KL.7, at mærket adskiller sig fra øvrige mærker (herunder fx E-mærket og Trustpilot) i form og farve og lægger vægt på tryghed i det visuelle udtryk. Yderligere bør mærkets signalværdi også kunne vise, hvilken indsats virksomheder i især risikogruppe 3 og 4 gør – også i et internationalt perspektiv. Konkret efterspørger en virksomhed i risikogruppe 3 eksempelvis et "statsligt emblem", der udtrykker den danske kvalitet og myndighed.

Klarhed

- Mærket rummer stor kompleksitet, og brugertesten dokumenterede, at uden markedsføring og vedholdende kommunikation om mærket, vil det forblive uklart for mange brugere, hvad mærket dækker over.
- Mærket kan i sig selv ikke visualisere de mange aspekter af digital ansvarlighed med et så begrænset grafisk felt.

Myndighed

- Mærket bør repræsentere en autoritet for at belønne og sanktionere virksomheder, der gør en ekstra indsats.
- Hvis signalværdien overgøres, kan det sætte mærket over styr. Dels fordi ordningen er frivillig og ikke lovbaseret. Dels fordi meget autoritet i ordningen vil kræve flere ressourcer til kontrol for at understøtte signalværdien.

Ethvert valg om mærkets visuelle udtryk har konsekvenser for hele kommunikationen

- Mærket skal designes ud fra en konsekvent strategi for kommunikation, målgrupper, organisering og forretningsmodel.
- Et autoritativt mærke kræver stærkere kriterier og mere tilsyn. Et klart kommunikerende mærke vil få mindre opmærksomhed, men måske kræve mindre forklaring. Et unikt mærke vil kræve meget understøttende kommunikation, men forventeligt skabe mere opmærksomhed og have større brandingeffekt.

4. Next steps og fokus inden lancering

Inden lancering af mærket, er der en række dele af mærkningsordningen, der skal helt på plads. Vi har opsummeret de væsentligste opfølgningspunkter her.

Visuel identitet og kommunikationsstrategi

Tilbagemeldingerne fra brugertesten peger på, at der er behov for en ny visuel identitet. De nuværende udtryk er enten for kedelige eller for useriøse, og de indfrier ikke virksomhedernes ønsker til en mere officiel mærkningsordning. Hvis mærket skal efterleve virksomhedernes forventning om, at mærket skal signalere autoritet og seriøsitet, så kræver det en ny plan for, hvordan mærket skal kommunikeres og markedsføres. /KL.7 anbefaler at virksomheden bag mærkningsordningen skal give den visuelle identitet, herunder stil og tone for mærkningsordningen, et nyt skud baseret på indsigterne fra sprintets brugertest.

Få brugerrejsen på plads

For at ramme alle fire virksomhedssegmenter og appellere til deres individuelle behov og kontekst, anbefales det at lave fire forskellige use cases, der giver svar på:

- Hvilke problemer kan mærkningsordningen løse for de fire segmenter?
- Hvilken markedsføringsvinkel ræsonnerer bedst med de fire forskellige segmenter?
- Hvad skal der helt konkret til for at indfri kriterierne i hvert virksomhedssegment?
- Hvilke guides, vejledninger og værktøjer skal mærket tilbyde virksomhederne?

Flere virksomheder i brugertesten efterspurgte konkrete eksempler på, at mærket er værdiskabende og udgør en differentieringsparameter. Det kunne derfor være en god ide at lave en blød lancering af mærket i samarbejde med en række testvirksomheder fra hver af de fire risikogrupper med henblik på at måle effekten af mærkningsordningen på virksomhedernes konkurrencedygtighed, oplevede tilfredshed og bundlinje. Resultaterne af denne effektmåling vil kunne bruges i markedsføringen til de øvrige virksomheder i et senere og mere aggressivt markedsføringsfremstød.

Kontrol og tilsyn

Når vi ved, hvad det vil kræve for hvert virksomhedssegment at indfri kriterierne (og dermed har fået bekræftet, at det er muligt for dem), anbefales det at lave en standardiseret drejebog til kontrol og tilsyn for hver virksomhedstype.

Budget og finansieringsmodel

Den endelige finansieringsmodel skal på plads. Baseret på et estimat af det forventede optag af mærket blandt hvert virksomhedssegment og differentieret prissætning, skal der lægges en plan for mærkningsordningens finansiering af de væsentligste aktiviteter i ordningen - fordelt over sekretariat, kontrol og tilsyn, markedsføring og udvikling af guides og vejledninger.