Bilag 5.5
Brugertest

Bilag 5.5.1: Forbrugertest

BRUGERTEST

Forbrugere

OPSUMMERING

INDSIGTER OM FORBRUGEREN

Følgende indsigter er baseret blandt andet på en brugertest, som del af sprintet og på rapporten *Et forbrugerperspektiv* (2019), udarbejdet af Konkurrence- og Forbrugerstyrelsen (en mere detaljeret gennemgang findes på side 2-5). Rapportens indsigter bygger på 1026 online-interview, mens mærket blev testet med i alt seks forbrugere. Indsigterne er indsamlet i en B2C-kontekst, hvilket betyder, at følgende ikke skal ses som en beskrivelse af mærkets relevans i en B2B-kontekst. Følgende er /KL.7's vurdering af forbrugeren på baggrund af sprintets test samt forbrugerundersøgelsen.

Det er er ikke dataetik eller it-sikkerhed, der fylder

Ifølge rapporten udarbejdet af Konkurrence- og Forbrugerstyrelsen nævnes især ordene "data" og "oplysninger" i respondenternes besvarelse af, hvad der udgør god it-sikkerhed. Her nævnes eksempelvis "*At de ikke videregiver oplysninger til tredjepart*". Besvarelserne har samme karakter i vurderingen af dataetik. Således er sondringen mellem dataetik og it-sikkerhed ikke klar for forbrugeren. Omkring halvdelen er helt enige i, at mistanke om dårlig IT-sikkerhed og dataetik har en konsekvens for deres adfærd, men samtidig fandt undersøgelsen, at langt størstedelen ikke læser om, hvordan virksomheden anvender data – primært på grund af manglende interesse eller at de ikke tænkte over det.

Det handler om tryghed

Det er, i forlængelse heraf, /KL.7's vurdering, at *tryghed* er en vigtig parameter i eksempelvis webhandel, men at forbrugerens forståelse for it-sikkerhed/dataetik ikke nødvendigvis bunder i et mærke eller en privatlivspolitik, men måske i højere grad er defineret af eksempelvis hjemmesidens design eller sidens Trustpilot-vurdering. Således er det ikke nødvendigvis begreberne it-sikkerhed og dataetik, der fylder i forbrugerens verden, men snarere *tryghed*. Begreberne er ikke velkendte for den gængse forbruger og ryger derfor sandsynligvis i samme "mentale kasse" som eksempelvis *køberbeskyttelse* eller *fup på nettet* (som E-mærket repræsenterer). En oplevet værdi på forbrugersiden forudsætter altså muligvis, at man som forbruger forstår og er opmærksom på forskellen mellem eksempelvis køberbeskyttelse og dataetik. Dén sondring er ikke nødvendigvis til stede hos forbrugeren i dag.

Vurderingen af tryghed består i meget andet end data og privatlivspolitik

Ifølge rapporten føler forbrugerne sig mindst trygge ved at afgive data på fx sociale medier og online butikker, mens de offentlige institutioner og banker opleves mere trygge. Forbrugerne vurderer især, at fx CPR-nummer, kortoplysninger og kodeord som følsomme data. Det er dog /KL.7's vurdering, at forbrugeren sjældent vil tænke på virksomhedskategorien eller specifikke typer af data i vurderingen af tryghed, men i stedet ved at spørge fx: "Har jeg handlet her før?", "Ser siden professionel ud?" eller "Hvad har andre sagt om siden?".

BAGGRUND FOR TESTEN

Mærket blev testet med i alt seks forbrugere. Forbrugerne er ligeligt fordelt mellem køn i aldersgruppen 27-55 år og handler enten dagligt eller ugentligt på nettet. Udgangspunktet for testen var handel på webshops, da denne situation er lettest at afspejle i et test-setup og samtidig formodes at være den mest gængse. Testen med forbrugere søgte at besvare tre overordnede spørgsmål:

1. Hvad har relevans for oplevet tryghed?
Mærkets relevans er stærkt afhængigt af, hvorvidt forbrugeren er opmærksom på og orienterer sig omkring mærket i eksempelvis køb på nettet via webshops eller lignende. Dette nævnes også i en forbrugerundersøgelse udarbejdet for KFST, der opfordrer til en undersøgelse af, hvor forbrugeren orienterer sig i forbindelse med køb af digitale produkter og services. Dataetik og it-sikkerhed er i denne test oversat til tryghed, da vi i /KL.7 antager, at det er dette begreb, der ligger højest i forbrugerens bevidsthed.

2. Hvad forestiller forbrugeren sig, at mærket repræsenterer?
Mærket skal hurtigt kunne kommunikere, hvad det repræsenterer og hvilken forskel virksomheder med mærket gør for forbrugeren. Derfor undersøger vi forbrugerens umiddelbare forståelse af, hvad mærket repræsenterer.

3. Hvad forventer forbrugeren af virksomheder med mærket?
Ansvarlig dataanvendelse og it-sikkerhed er ikke nødvendigvis relevante eller velkendte fænomener for forbrugeren. Derfor er det vigtigt at forstå, hvad forbrugeren selv fremhæver og forventer fra virksomheder som har mærket.

I den nylige rapport, *Et forbrugerperspektiv*, udarbejdet for Konkurrence- og Forbrugerstyrelsen (KFST) undersøges det blandt andet, i hvilken grad it-sikkerhed og dataetik påvirker forbrugernes beslutninger og forbrugernes forståelse for begreberne. Testens undersøgelsesspørgsmål ligger derfor i forlængelse af rapportens konklusioner, og tester derudover mærkets visuelle udtryk. På de næste sider præsenteres de overordnede indsigter for hvert undersøgelsesspørgsmål i forlængelse af en kort gennemgang af testformatet.

Spørgsmål 1/3: Hvad har relevans for oplevet tryghed?

Respondenterne blev i denne del af testen spurgt ind til deres vaner i forhold til at handle og færdes på nettet og herunder også, hvilke sider de foretrak, samt hvad der lå til grund for deres præferencer.

Respondenterne nævner hverken tryghed, it-sikkerhed eller relaterede fænomener i vurderingen af, hvorfor de ofte handler på specifikke, foretrukne sider. I stedet fremhæves ting som pris, gratis fragt og ekstra tilbud – herunder eksempelvis pointsystemer. Denne indsigt ligger i umiddelbar forlængelse af KFST-rapporten, der fandt, at 70 procent af de adspurgte, der ikke læste om, hvordan virksomheden anvender data, skyldtes manglende interesse eller, at de ikke tænkte over det. Samtidig viser undersøgelsen, at 83 procent af de adspurgte i nogen, høj eller i meget høj grad bekymrer sig om, at deres oplysninger misbruges.

Da respondenterne spørges ind til, hvad der potentielt kan skabe tryghed ved webhandel nævner 3 ud af 6 respondenter kvaliteten eller designet af hjemmesiden – den må ikke virke "amatør-agtig". Ingen respondenter nævner mærker eller it-sikkerhed, mens orientiering omkring, hvorvidt hjemmesiden har Trustpilot, nævnes af 5 ud af 6 respondenter. To respondenter nævner eksplicit, og uden *prompts* (opfølgende spørgsmål rettet direkte mod mærket), at de ikke kigger efter E-mærket eller andre mærker, når de handler på nettet. Slutteligt nævner 4 ud af 6 respondenter, at de foretrækker danske hjemmesider.

Forbrugerens adfærd er påvirket af mange underliggende, basale færdigheder, der styrer både opmærksomhed og beslutningsprocesser – og det er vel at mærke ikke aspekter man kan blive klogere på ved hjælp af selvrapporterede, kvalitative undersøgelsesmetoder. Dette medtages i validiteten af respondenternes tilbagemeldinger, men meget tyder på, at it-sikkerhed ikke ligger øverst i forbrugerens bevidsthed. Mens tryghed ved handel fortsat er en vigtig parameter, udgøres trygheden altså ikke nødvendigvis af mærker (såsom E-mærket), men måske i højere grad af hjemmesidens design (jf. Fogg et al., 2003) og hvorvidt hjemmesiden er dansk samt virksomhedens score på Trustpilot.

Spørgsmål 2/3: Hvad forestiller forbrugeren sig, at mærket repræsenterer?

Testen tog udgangspunkt i to primære mærker: '*Personlig tryghed*' og '*Vores fælles ansvar*'. Mærkets øvrige to mærker var, på baggrund af interessentgruppens input, fravalgt på forhånd. Alle fire mærker kan ses på side 29. De seks respondenter blev præsenteret for ét af de to mærker i en webshop-kontekst og blev bedt om at vurdere betydningen af webshoppens mærker (herunder også E-mærket og Trustpilot). Til sidst i testen blev respondenterne bedt om at vurdere alle fire mærker, med tryghed og ansvarlighed som nøgleord.

Vores fælles ansvar

Alle tre respondenter valgte i første omgang ikke at sætte ord på "Vores fælles ansvar" og undgik at svare – det var overordnet svært for respondenterne at sætte ord på mærkets betydning. Respondenterne ville først, efter flere *prompts* (opfølgende spørgsmål rettet direkte mod mærket) give udtryk for, hvad mærket repræsenterede. Her nævnte respondenterne fx "sikker nethandel", "online sikkerhed" og "sikkerhed". To respondenter giver dog udtryk for, at mærket i sig selv ikke kommunikerer dette, men i højere grad mærkets placering i bunden af hjemmesiden (sammen med fx E-mærket og Trustpilot): "*Jeg tænker kun alt det der sikkerhed, fordi det står hernede i bunden, men ellers ville jeg ikke ane hvad det var. Men jeg ville i hvert fald ikke tænke på sikkerhed.*" En anden respondent nævner: "*Det er fordi, at den står ved siden E-mærket. Derfor tænker jeg, at den kan have en relevans for sikkerhed.*" Det tyder altså på, at placeringen af mærket også har en betydning for, hvordan mærket afkodes.

Personlig tryghed

To ud af tre respondenter hverken kunne eller ville, ligesom med mærket '*Vores fælles ansvar*', sætte ord på betydningen af '*Personlig tryghed*'. Respondenterne gav udtryk for, at de ikke ville have lyst til at interagere med eller klikke på mærket: "Den dér lås har jeg aldrig set før. Så er det egentlig et sted jeg ikke har lyst til at handle, fordi når den er låst betyder det næsten, at her skal man ikke handle". Den sidste af de tre respondenter var overbevist om, at symbolet var udtryk for en krypteret forbindelse – med reference til hængelåsen, der vises i browserfeltet på Chrome-browsere.

Spørgsmål 2/3: Hvad forestiller forbrugeren sig, at mærket repræsenterer?

Forbrugernes samlede vurdering af mærkernes visuelle udtryk

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: *"Men generelt forstår jeg ikke, hvorfor det skal være så kluntet. Det ligner ikke noget, der er blevet brugt tid på."*. Dette kunne også observeres på respondenternes adfærd omkring spørgsmål til mærket – samtlige respondenter havde svært at svare på eller forstå meningen med mærket i en webshop-kontekst.

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.

Spørgsmål 3/3: Hvad forventer forbrugeren af virksomheder med mærket?

I denne del af testen blev respondenterne bedt om at vurdere, hvad de tænker, at virksomheder med mærket gør for digital ansvarlighed og tryghed. Samtlige respondenter nævner tryghed, trygge data, sikker data eller oplysninger. Her er der dog en risiko for, at respondenterne er farvet af interviewets ramme op til dette spørgsmål og blot nævner de nøgleord, som er blevet introduceret i spørgerammen. Indsigten stemmer dog overens med en konklusion fra KFST's rapport, hvor ordet data nævnes 127 gange, mens kvalitative udtræk fra rapporten lyder eksempelvis: *"At data er sikkert gemt, og ikke bliver videregivet"* eller *"At de gemmer ens personlige data betryggende"*.

Generelt kunne vi observere, at respondenterne har svært ved at svare præcist eller konkret på, hvad de forventer, eller foretrækker, at virksomheden gør anderledes, hvis de har mærket. En respondent refererer eksempelvis tilbage til købs- eller handelsret: "… det kunne måske også betyde noget med "retur" og "fortrydelsesret". En anden respondent nævner, at det ville være smartere, hvis alle de ting, der har at gøre med it-sikkerhed og data blot samles i ét mærke: "Det er smartere end, at jeg skal forholde mig til et helt nyt mærke – ellers bliver det alt for forvirrende. Umiddelbart ville jeg tro, at de ville gøre det samme – altså giver mig en form for tryghed". Det kan tyde på, at forbrugerne ikke har gjort sig klare tanker omkring, hvad der ligger bag "sikker" eller "tryg" databehandling, men blot samler alt, der berører emnet i én kategori. Dette underbygges yderligere af KFST's rapport, der indikerer, at forbrugere har en svag idé om forskellen mellem it-sikkerhed og dataetik.

Bilag 5.5.2: Virksomhedstest

OPSUMMERING

På side 8-10 gennemgås de mest centrale indsigter fra interviews med virksomheder (på side 11-20 ses en mere detaljeret gennemgang). Gennemgangen vil primært lægge vægt på de steder, hvor virksomhederne fremhævede potentielle barrierer forbundet med implementering, kontrol eller værdi. Efter denne gennemgang gives et overordnet indblik i, hvad virksomhederne vægter højest ifm. Datamærkningsordningen. Virksomhederne er i interviewene blevet præsenteret for konceptet omkring mærket, de 8 udvalgte kriterier, onboarding, bud på kontrol og tilsyn samt bud på mærkningsordningens visuelle identitet.

RISIKOGRUPPE 1

Virksomheden i risikogruppe 1 kunne gennemgående ikke genkende værdien i datamærkningsordningen; herunder hverken kriterier eller bud på værdiskabelse. Virksomheden har et overordnet ønske om at drive sin forretning (i dette tilfælde et auto-mekaniker værksted) og mener blot, at kravene til digital sikkerhed (jf. GDPR) bebyrder ham. Han har ikke et ønske om at modtage yderligere rådgivning, da brancheforeningen, i hans optik, varetager de behov, der er nødvendige for en virksomhed som hans. Respondenten understreger, at han ikke oplever, at risikoen ligger hos ham: "*Vi har en adressebog, som jo ikke skal ligge fremme, men altså hvem skulle gå ind og snage i vores ting?*".

Hvad er vigtigst for virksomheden i risikogruppe 1?

Virksomheden i risikogruppe 1 kan ikke se værdien i datamærkningsordningen, primært fordi mærket ikke ville tjene som en konkurrencefordel, men tværtimod vurderes til at bebyrde virksomhedens primære formål i at drive forretningen.

RISIKOGRUPPE 2

Respondenten i risikogruppe 2 kan se en værdi i langt de fleste kriterier og mener, at de er både relevante og meningsfulde – selvom kun få kriterier lader til at blive efterlevet i virksomheden. Eksempelvis er hverken it-sikkerhedsmæssige eller dataetiske retningslinjer pt forankret i virksomhedens ledelse. Dog nævner respondenten, at afpersonalisering af data ikke har en relevans for dem som B2B-virksomhed; de behandler kun meget få personfølsomme data.

Hvad er vigtigst for virksomheden i risikogruppe 2?

Det er vigtigt for virksomheden at kunne være en ansvarlig partner også på det amerikanske marked og vise, at man overholder både nationale og internationale standarder for digital ansvarlighed. Derudover er især en guide til implementering fordelagtig for virksomheden i denne risikogruppe.

RISIKOGRUPPE 3

Indsigterne i det følgende er fordelt ud på de kriterier, hvor virksomhederne havde flest opmærksomhedspunkter.

Forankring i ledelsen

Virksomhederne i risikogruppe 3 har gennemgående svært ved at se værdien i '*Forankring i ledelsen*', da det har et overlap med GDPR og derfor ikke vurderes til at bidrage ekstra. Med yderligere forankring i ledelsen er en enkelt virksomhed bekymret for, at den ledelsesansvarlige vil skulle bruge uhensigtsmæssigt meget tid på at varetage opgaven. Alle virksomheder anerkender dog vigtigheden i kravet.

Fair og fordomsfri algoritmer

Èn virksomhed fremhæver, at deres AI-teknologi er købt af tredjepart og at de derfor ikke selv vil kunne vurdere teknologiens "fairness". En virksomhed (hvis kerneydelse består i udviklingen af AI-teknologi) mener ikke, at kravet til fordomsfri algoritmer er relevant, da det aldrig er en ambition for en AI-virksomhed at udvikle fordoms*fulde* algoritmer. I stedet foreslår virksomheden, at man fokuserer energien på underrepræsenterede datapopulationer i algoritmer og på en tydeliggørelse af, hvad man har tænkt sig at gøre som virksomhed for at skabe repræsentative datagrundlag – og tydeliggøre, hvor datagrundlaget er begrænset.

Krav til leverandørers behandling

Mens samtlige virksomheder i risikogruppe 3 anerkender værdien af kravet, understreger en virksomhed, at kontrollen ikke bør bestå i en ekspertvurdering men i en intern vurdering, da dette ellers vil blive for omstændigt for små- og mellemstore virksomheder – både tids- og prismæssigt.

Awareness og sikker adfærd

Virksomhederne anerkender værdien i kravet og er positivt afstemte overfor eksempelvis at benytte app'en 'Sikker Kollega'. Virksomhedernes opmærksomhedspunkter består i, at indholdet i så fald også skal udbydes på engelsk og at de, som virksomhedsledere, skal kunne stå inde for værdien i læringsforløbet.

Hvad er vigtigst for virksomheden i risikogruppe 3?

For virksomhederne i risikogruppe 3 handler det i høj grad om at signalere over for omverdenen, at man tager digital ansvarlighed seriøst. Lige nu er der ingen synlighed i forhold til, hvilke virksomheder, der efterlever GDPR – og hvem der ikke gør. Virksomhederne oplever, at flere af kriterierne har et overlap med GDPR, så mens den brugervenlige indføring i digital ansvarlighed er et fint supplement, har virksomheder i denne gruppe højst sandsynligt allerede godt styr på data- og it-sikkerhed og mangler primært en instans, der kan *kvalificere* virksomhedens digitale ansvarlighed: "*Vi har brug for officielle instanser, som der, qua en revision, kan blåstemple at en given virksomhed følger reglementerne inden for sikker og rettidig brug af data. Vi har ikke brug for flere instanser, som kun kan yde rådgivning*".

RISIKOGRUPPE 4

Indsigterne i det følgende er fordelt ud på de kriterier, hvor virksomhederne havde flest opmærksomhedspunkter.

Forankring i ledelsen

Virksomhederne i risikogruppe 4 mener, ligesom i risikogruppe 3, at kravet til '*Forankring i ledelsen*' er redundant, da dette i forvejen efterleves i kraft af GDPR-lovgivningen.

Fair og fordomsfri algoritmer

Virksomhederne mener, i forhold til kriteriet *'Fair og fordomsfri algoritmer'*, at ambitionen bør ligge i at *efterstræbe* fordomsfri algoritmer, og herunder at skabe en gennemsigtighed i et repræsentativt datagrundlag, men at der aldrig vil kunne opnås fuldstændig repræsentativitet eller fordomsfrihed.

Krav til leverandørers behandling

Mens virksomhederne i risikogruppe 4 anerkender værdien i kriteriet understreges det, at det vil blive svært at efterleve kriteriet med antallet af underleverandører. Specifikt lægger respondenten vægt på, at der vil skulle oprettes specifikke retningslinjer eller kontrakter tilpasset den enkelte underleverandør, da én ikke vil kunne passe på tværs af leverandører. Yderligere nævner en virksomhed, at der ofte er områder med kun en håndfuld leverandører på markedet og at det derfor bliver svært at fravælge enkelte leverandører som følge af eventuelle dataetiske retningslinjer.

Kontrol over egne data

Èn virksomhed nævner, at visse data ikke er forretningskritiske, men alligevel udgør en vigtig komponent i forhold til serviceydelsen – herunder eksempelvis netværksdata. Respondenten nævner, at hvis forbrugeren fik mulighed for at fravælge netværksdata ville det have en konsekvens for netværksydelsen generelt. Den anden virksomhed i risikogruppe 4 fremhæver, at de som B2B-virksomhed, ikke kan se meget værdi i at efterleve kriteriet.

Hvad er vigtigst for virksomheden i risikogruppe 4?

Det handler for virksomhederne i risikogruppe 4 om tydeligt at kunne synliggøre de ressourcer, der er blevet lagt i digital ansvarlighed og på den måde styrke relationen til deres kunder – dette gør sig gældende især for B2C-virksomheder i risikogruppe 4. Hvis mærket kan garantere en sikkerhed for, at virksomhedens services lever op til og tager højde for dataetiske/it-sikkerhedsmæssige problemstillinger, er betalingsvilligheden større. I den forbindelse nævner virksomhederne, at mærket formentlig ikke vil lede til en international konkurrencefordel, dels fordi mærket vurderes til primært at henvende sig til det danske marked, dels fordi kriterierne i deres nuværende form ikke lever op til internationale standarder

BAGGRUND FOR TESTEN

Prototypen på datamærkningsordningen er drøftet med i alt syv virksomheder. Virksomhederne er fordelt ud på risiko-matrixens fire risikogrupper og repræsenterer altså virksomheder af henholdsvis lav og høj datamæssig/organisatorisk kompleksitet. Overordnet søgte brugertesten at få svar på tre spørgsmål:

1. Giver kriteriets krav og kontrol mening for virksomhederne?
Det er vigtigt både for kommunikationen omkring kriterierne og for modtagelsen hos virksomhederne, at virksomheden kan forstå og se idéen med kriteriets indhold.

2. Hvordan matcher implementeringen af kriterier virksomhederne?
Det er afgørende for mærkets optag, at virksomhederne oplever, at de realistisk kan leve op til mærkets kriterier, herunder krav og kontrol. Derfor undersøges det, hvordan kriteriernes krav matcher virkeligheden ude i virksomhederne.

3. Kan virksomhederne spejle sig i mærkets værdiskabelse og hvad er virksomhederne villige til at give for mærket?
Balancen mellem mærkets værdiskabelse og pris er afgørende for det potentielle optag af mærket. Derfor undersøges det, hvorvidt virksomheden kan spejle sig i mærkets værdiskabelse og hvad virksomhederne vil prissætte mærket til. Herunder ligger også, hvad virksomhederne vurderer til at være den vigtigste værdiskabelse ifm. en ny datamærkningsordning.

Det bør noteres, at særligt virksomhederne, der er rekrutteret i risikogruppe 3 og 4, i forvejen tager it-sikkerhed og dataetiske processer seriøst – og derfor allerede lever op til flere af kriterierne. Derfor italesætter virksomhederne muligvis andre problemstillinger end virksomheder på samme niveau, som arbejder mindre seriøst med dataetik/it-sikkerhed.

På næste side ses en oversigt over, hvilke virksomheder, der har bidraget til undersøgelsen. Kriterierne vil herefter blive gennemgået med udgangspunkt i undersøgelsesspørgsmålene og de fire risikogrupper. Gennemgangen vil primært lægge vægt på de steder, hvor virksomhederne fremhævede potentielle barrierer forbundet med implementering, kontrol eller værdi. Slutteligt gives et overordnet indblik i, hvad virksomhederne vægter højest ifm. mærkningsordningen.

BAGGRUND FOR TESTEN

De syv virksomheder er fordelt ud på risiko-matrixens fire risikogrupper.

RISIKOGRUPPE 1

- **Henrik Petersen, J. A. Auto Aps**
  Virksomheden er et auto-mekaniker værksted, hvor respondenten varetager bl.a. kundehåndtering, fakturering og ledelse.

RISIKOGRUPPE 2

- **Susanne Andersen Bækgaard, Bifodan A/S**
  Virksomheden er en B2B-virksomhed, der producerer og leverer pro-biotiske piller til relevante kæder, herunder fx apotekskæder. Respondenten er marketingsansvarlig i virksomheden.

RISIKOGRUPPE 3

- **Kevin Rebsdorf, Compan Young**
  CompanYoung er en full-service virksomhed der hjælper hhv. virksomheder, uddannelsesinstitutioner og brancheorganisationer med at tiltrække og rekruttere unge. Respondenten er CEO og Co-Founder.
- **Lars Maaløe, Corti**
  Virksomheden laver decision support systemer med AI-teknologi, der lytter med og hjælper bl.a. sundhedsfagligt med at træffe bedre beslutninger på baggrund af patientopkald. Respondenten er CTO i virksomheden.
- **Jakob Lose, Webitall**
  Webitall er et webbureau og IT-foretagende. Jakob er CEO i virksomheden.

RISIKOGRUPPE 4

- **Jesper Packert Pedersen, TDC Group**
  Virksomheden udbyder netværk og digitale ydelser til den danske befolkning. Jesper Packert er Public Affairs Manager i virksomheden
- **Morten Pors Simonsen, Danfoss**
  Danfoss udvikler teknologier til kunder i både stor og lille skala – alt fra ventiler til drift af transportbånd. Morten er it-ansvarlig i virksomheden.

KRITERIE

Forankring i ledelsen

Risikogruppe 1 (J. A. Auto ApS)
Virksomheden giver udtryk for godt at kunne varetage en forankring i ledelsen, men kan ikke se nogen værdi i at leve op til kriteriet.

Risikogruppe 2 (Bifodan A/S):
Virksomheden kan sagtens se en værdi i, og har mulighed for at implementere kriteriet. Ledelsen har pt. ikke nogen forankring i ledelsen.

Risikogruppe 3 (Webitall, Corti, Compan Young):
Webitall vil, på dette niveau, som en mindre organisation, ikke have et problem med at indsætte en it-sikkerheds- og dataetisk ansvarlig i ledelsen. Compan Young er dog betænkelig ved, at person(erne) i ledelsen vil kunne komme til at bruge for meget tid på it-sikkerhedsmæssige opgaver. Webitall fremhæver, at kravet overlapper med GDPR-lovgivningen – og at spørgsmålet i virkeligheden ligger i, hvorvidt medarbejderne efterlever ledelsens retningslinjer.

Virksomheden Corti kan heller ikke se, hvordan dette kriterie giver ekstra værdi i forhold til GDPR-lovgivningen og efterspørger i stedet nogle foranstaltninger, der kan godkende om de er GDPR-compliant: *"Vi har brug for officielle instanser, som der, qua en revision, kan blåstemple at en given virksomhed følger reglementerne inden for sikker og rettidig brug af data. Vi har ikke brug for flere instanser, som kun kan yde rådgivning"*.

Risikogruppe 4 (TDC Group, Danfoss):
Ligesom virksomhederne på Risikogruppe 3 oplever både Danfoss eller TDC Group, at kriteriet er redundant – det er allerede noget virksomheden "står på mål for dagligt". Virksomhederne kan altså nemt implementere og føre kontrol med kriteriet.

KRITERIE

Krav til leverandørers databehandling

Risikogruppe 1 (J. A. Auto ApS)
Virksomheden mener ikke at kunne definere, hvilke krav virksomheden skal overholde: "Det ville være helt urealistisk". Respondenten mener ikke at kunne få indblik i, hvordan leverandører behandler data.

Risikogruppe 2 (Bifodan A/S):
Virksomheden mener allerede at efterleve dette kriterie og lægger især vægt på værdien: Hvis ikke man man stiller krav til leverandører kan det "annullere" værdien af de andre parametre (de andre kriterier).

Risikogruppe 3 (Webitall, Corti, Compan Young):
Samtlige virksomheder kan se værdien i at få overblik over leverandører og indblik i potentiel redundans. Der lægges dog samtidig vægt på, at ekspertvurderingen som kontrol ikke er realistisk, da en sådan i praksis vil blive for dyr for SMV'er (ifølge Webitall). Derfor bør kontrollen bestå i en intern vurdering og ikke i en ekspertvurdering på dette niveau.

Virksomheden, Corti, kan ikke se, hvilken værdi kriteriet giver, da man i forvejen skal kunne efterleve dette på baggrund af proces- og ejerregler i GDPR.

Risikogruppe 4 (TDC, Danfoss):
TDC Group kan forstå både kriteriet og værdien: Især fremhæver respondenten, at leverandørers dataetiske retningslinjer, eller mangel på samme, kan smitte af på dem som virksomhed. Samtidig understreger respondenten, at det for deres virksomhedsprofil vil blive svært at efterleve kriteriet med antallet af underleverandører. Specifikt lægger respondenten vægt på, at der vil skulle oprettes specifikke retningslinjer eller kontrakter tilpasset den enkelte underleverandør, da én ikke vil kunne passe på tværs af leverandører. Yderligere nævner virksomheden, at der ofte er områder med kun en håndfuld leverandører på markedet og at det derfor bliver meget svært at fravælge enkelte leverandører som følge af eventuelle dataetiske retningslinjer. Danfoss kan spejle sig i værdien og betegner det som en fundamental kontrol; dog mener respondenten, at kontrollen kan udføres mere effektivt – lige nu facilitere virksomheden en kontrol ved at bede leverandører om at præsentere en rapport, der dokumentere ansvarlig behandling af data.

KRITERIE

Awareness og sikker adfærd

Risikogruppe 1 (J. A. Auto ApS)
Virksomheden forstår kravet, men kan ikke se, hvilken værdi det tilfører virksomheden. Respondenten forklarer, at hans kunder ikke er bekymrede for it-sikkerheden, men "*om mekanikeren har lavet fejl på bilen*".

Risikogruppe 2 (Bifodan A/S):
Virksomheden har ikke før arbejdet med awareness og sikker adfærd, men er positivt stemt især overfor at få konkret hjælp til implementeringen af træningsforløb.

Risikogruppe 3 (Webitall, Corti, Compan Young):
Kravet giver absolut mening for virksomhederne. Webitall fremhæver samtidig vigtigheden i, at træningen i awareness og sikker adfærd skal kunne dokumenteres eksempelvis over for Datatilsynet. Her lægger respondenten vægt på betydningen af, at der også ses en sikker adfærd i virksomheden (som afspejler træningen i awareness). Samtidig fremhæver virksomheden, at træningen skal være kontinuerlig og ikke en "engangsting".

Både Compan Young og Corti fremhæver, at et app'en Sikker Kollega ville være en god tilføjelse til virksomhedens awareness-træning, men at man som virksomhedsleder også skal kunne stå inde for, at træningsforløbet rent faktisk har en virkning. Yderligere lægger Corti, som international virksomhed, vægt på, at indholdet skal kunne være tilgængeligt på engelsk.

Risikogruppe 4 (TDC, Danfoss):
TDC Group har selv faciliteret compliance-kurser i forbindelse med GDPR-lovgivningen og er derfor meget enige i vigtigheden af kriteriet. Dog fremhæver respondenten, at det ikke er realistisk for en organisation med flere tusinde medarbejdere, at få alle til at benytte en applikation som "Sikker Kollega" eller anden teknologi – dog vil kontrolkravet kunne imødegås i enkelte teams eller projekter, hvor dataetiske/it-sikkerhedsmæssige problemstillinger er særligt relevante. Danfoss mener ligesom TDC Group, at det ikke er realistisk at implementere på tværs af landegrænser og ansatte og at man derfor bør gøre det muligt for virksomhederne at efterleve kravet på anden vis – men anerkender vigtigheden i generel awareness og sikker adfærd.

KRITERIE

Klar kommunikation

Risikogruppe 1 (J. A. Auto ApS):
Virksomheden forstår kravet, men refererer til den standardformulering som brancheforeningen har udarbejdet. Respondenten vil ikke bruge tid på selv at formulere noget yderligere. Kriteriet har, for respondenten, udelukkende en værdi i det, at det sikrer, at man ikke får en bøde (jf. GDPR).

Risikogruppe 2 (Bifodan A/S):
Virksomheden kan tydeligt spejle sig i kriteriets værdi med vægt på især forståeligheden og mener at kriteriet kan implementeres: Respondenten refererer til, at hun ikke selv er helt med på virksomhedens privatlivspolitik – og at der derfor er brug for en implementering af kravet.

Risikogruppe 3 (Webitall, Corti, Compan Young):
Virksomhederne har ingen opmærksomhedspunkter til dette kriterie og er blot enig i vigtigheden af klar og gennemsigtig kommunikation. Især virksomheden Compan Young lægger vægt på værdien i, at gøre det eksplicit og gennemsigtigt, hvordan virksomhedens bagvedliggende processer afvikles. Corti, der arbejder med AI-teknologi, pointerer dog, at det ikke vil være muligt for dem at gøre alle processer tydelige: Hvis modellerne er tilstrækkeligt komplekse er det ikke muligt at afgøre et kausalitetsforhold. Derfor er *kontrolkravet* ifølge Corti urealistisk.

Risikogruppe 4 (TDC Group, Danfoss):
TDC Group mener allerede at leve op til dette kriterie både ift. tilgængelighed/forståelighed og kan derfor både forstå og se værdien i kriteriet. Ligeledes mener Danfoss allerede at leve op til kriteriet og mener primært, at det giver slutbrugeren en værdi – respondenten nævner dog, at deres privatlivspolitik ikke nødvendigvis er forståelig for lægmand og derfor kunne have brug for en revision.

KRITERIE

Teknisk it-sikkerhed

Risikogruppe 1 (J. A. Auto ApS)
Virksomheden refererer til udbyderen af deres økonomistyringssystem og at de, i deres ydelse, har styr på basal it-sikkerhed. Respondenten mener at kunne efterleve kriteriet, men mener ikke at det kan tilføre en ekstra værdi, da "de fleste ville tage det som en selvfølge".

Risikogruppe 2 (Bifodan A/S):
Respondenten er ikke teknisk ansvarlig og kan derfor ikke svare på dette kriterie.

Risikogruppe 3 (Webitall, Corti, Compan Young):
Virksomhederne kan spejle sig i kriteriets værdi og fremhæver, at det kan give et grundlæggende niveau af sikkerhed og samtidig give et overblik over, hvilke systemer man anvender. Virksomhederne efterlever allerede kriteriet med deres nuværende niveau af sikkerhed. Dog sondrer Webitall igen mellem it-sikkerhed og organisatorisk sikkerhed og lægger vægt på, at også de ansatte skal agere sikkert. Først dér bliver det effektivt, ifølge respondenten.

Risikogruppe 4 (TDC, Danfoss):
TDC Group har allerede implementeret den krævne it-sikkerhedspakke og det er derfor ikke noget problem for virksomheden at leve op til kriteriet. Danfoss lever ligeledes op til samtlige krav, men kommenterer på, at automatiske opdateringer er svære at implementere, da opdateringerne er noget der udføres manuelt i virksomheden.

KRITERIE

Kontrol over egne data

Risikogruppe 1 (J. A. Auto ApS)
Virksomheden vil godt kunne fjerne de persondata de har liggende, men har svært ved at se værdien, da de ikke opbevarer andre data, end dem der er nødvendige for at køre virksomheden (kontakt-information mv.)

Risikogruppe 2 (Bifodan A/S):
Virksomheden er enig i værdiskabelsen ved dette kriterie og mener at kriteriet kan implementeres.

Risikogruppe 3 (Webitall, Corti, Compan Young):
Compan Young forstår kravet og værdien, men er i tvivl om, hvorvidt kravet kan efterleves – det vil ikke være muligt for virksomheden at fremskaffe al data med det samme. Dette underbygges af virksomheden, Webitall, der nævner, at det ville enormt komplekst at skulle leve op til kriteriet, hvis brugeren skal kunne krydse "fra og til med flueben", hvad virksomheden ved om dem. I stedet foreslår virksomheden, at man stiller krav til tidsaspektet: At man kan forvente, at det tager x antal timer/dage før data er slettet.

Risikogruppe 4 (TDC, Danfoss):
Virksomheden stiller gerne alle data til rådighed til til- og fravælgelse, hvis de ikke er afgørende for at udbyde servicen. Dog er virksomheden bekymret for, at en gennemsigtighed og kontrol over, hvilke data der samles og bruges vil have en negativ følgevirkning, da det er respondentens opfattelse, at der er en dårlig forståelse for *nødvendigheden* af mange data. Virksomheden nævner eksempelvis netværksdata, der ikke er afgørende for at yde en teleservice, men dog er vigtige ift. at holde netværket stabilt – hvis mange forbrugere valgte at slå netværksdata fra ville det have en effekt på dækningen og derfor på kundeoplevelsen. Virksomheden kan derfor se værdien i form af transparens, men er også bekymret for kriteriets følgevirkninger. Danfoss mener at blive udfordret på implementeringen af kriteriet da virksomheden arbejder med mange forskellige use cases/forretningsområder. Samtidig nævner respondenten, at han ikke kan komme i tanke om en use case, hvor det her vil give ekstra værdi hverken internt/eksternt.

Fair og fordomsfri algoritmer

Risikogruppe 1 (J. A. Auto ApS)
Virksomheden arbejder ikke med algoritmer eller AI-teknologier.

Risikogruppe 2 (Bifodan A/S):
Virksomheden arbejder ikke med algoritmer eller AI-teknologier.

Risikogruppe 3 (Webitall, Corti, Compan Young):
Webitall giver udtryk for ikke at kunne møde kravet om et repræsentativt grundlag, da deres algoritmesoftware er købt af tredjepart. I forlængelse heraf mener virksomheden ikke at kunne se nogen værdi i kriteriet – respondenten kan ikke se, hvordan kriteriet skal kunne imødegås. Virksomheden Corti, som udvikler AI-teknologi, mener ikke at kriteriet giver mening, da det aldrig er en ambition for en AI-virksomhed at udvikle fordomsfulde algoritmer: "*En biased algoritme er det værste du kan lave. Det er ikke godt for din forretningsmodel og det er ikke godt for nogen*". I stedet foreslår virksomheden, at man fokuserer energien på underrepræsenterede datapopulationer i algoritmer og en tydeliggørelse af, hvad man har tænkt sig at gøre som virksomhed for at skabe repræsentative datagrundlag – og hvor datagrundlaget er begrænset. Virksomheder bør altså gøre det gennemsigtigt, hvad deres modeller er trænet på – og hvor de er dårligt trænet.

Risikogruppe 4 (TDC, Danfoss):
Ligesom virksomheder i Risikogruppe 3 lægger TDC Group vægt på, at virksomheden meget gerne stiller deres datagrundlag til rådighed og vil gøre deres for at sikre transparens i algoritme- og model-datasættet, men at fuldstændig fordomsfri algoritmer ikke er opnåeligt. Derfor foreslår virksomheden, at kontrollen i stedet består i, at en auditør eksempelvis reviderer datagrundlaget. Danfoss arbejder pt ikke med algoritmer, men udtrykker en villighed til at leve op til kriteriet, når eller hvis det bliver aktuelt. Respondenten kan se en ekstern værdi i kriteriet, overfor kunden – men mener ikke nødvendigvis, at det vil give en værdi internt i virksomheden.

KRITERIE

Afpersonalisering af data

Risikogruppe 1 (J. A. Auto ApS)
Virksomheden har svært ved at forstå, hvad kravet går ud på og mener ikke, at det tilfører ekstra værdi, men blot gøre det mere besværligt at drive virksomhed.

Risikogruppe 2 (Bifodan A/S):
Virksomheden har svært ved at se meningen og værdien i kriteriet; virksomheden arbejder B2B og arbejder derfor med et begrænset antal persondata.

Risikogruppe 3 (Webitall, Corti, Compan Young):
Virksomhederne kan spejle sig i kriteriets værdi i form af bedre sikkerhed i tilfælde af et brud, men nævner samtidig, at det afhænger af graden af afpersonalisering. Eksempelvis er der stor forskel på, om man skal afpersonalisere data på indsamlet via handel på webshop eller om det er samtlige persondata på tværs af virksomhedens processer. Hvis det er samtlige data, der skal afpersonaliseres, så snart de ikke er i brug, introducerer det en urealistisk kompleksitet for virksomhederne og derfor vil kriteriet ikke kunne efterleves. Virksomheden Corti understreger, at 100 procent afpersonalisering aldrig vil være muligt og at det i stedet ville give værdi, at sige, hvilken grad af afpersonalisering, der efterspørges – er det 95 eller 100 procent?

Virksomheden Compan Young nævner en ubalance mellem arbejde og værdi: Afpersonaliseringen er et kæmpe arbejde og gør det samtidig svært at bruge data effektivt – derfor ville virksomheden foretrække at slette data i stedet, hvis kontrollen betød en fuldstændig afpersonalisering.

Risikogruppe 4 (TDC, Danfoss):
TDC Group er villige til at arbejde på et Privacy by Design-koncept, der som udgangspunkt afpersonaliserer de nødvendige data. De kan se en værdi i at få "blåstemplet" eksempelvis Machine Learning-projekter, der ellers ville kunne opfattes uetiske. Danfoss mener ikke at kriteriet er vildt relevant, da virksomheden ikke behandler mange af den type data (personhenførbare data). Derudover foreslår respondenten andre, mindre omfattende metoder, som fx kryptering af data eller sletning af data.