Ansvarlig dataanvendelse som konkurrenceparameter

Resultater fra spørgeskemaundersøgelse

Oktober 2021

Rådet for Digital Sikkerhed

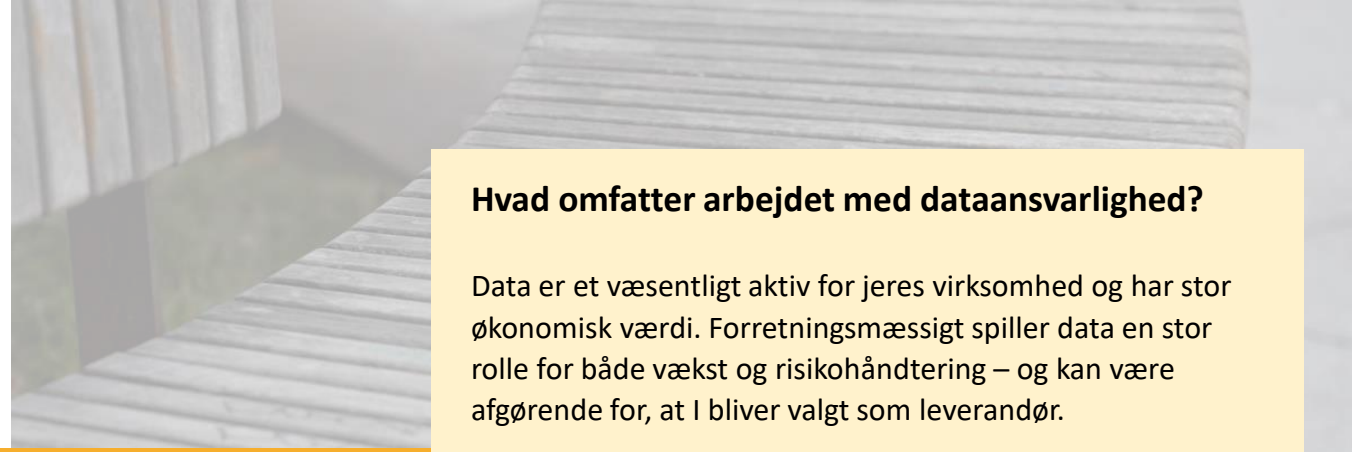
DI Digital

IT-BRANCHEN

ERHVERVSSTYRELSEN

INDUSTRIENS FOND FREMMER DANSK KONKURRENCEEVNE
The Danish Industry Foundation

Tak for jeres interesse



Kære virksomhed

Stort set alle danske virksomheder er digitale, og flere og flere arbejder i varierende grad med brugen af data til forretningsudvikling. Virksomhederne genererer, håndterer og opbevarer store mængder data, og dermed bliver behovet for databeskyttelse og ansvarlig dataanvendelse større.

Viden om ansvarlig dataanvendelse er særligt relevant for SMV'er, der typisk ikke selv har ressourcer og intern viden til at prioritere eller profilere sig på et område som ansvarlig dataanvendelse. Virksomhederne risikerer at miste kunder, få væsentlige bøder, store genetableringsomkostninger og dårlig omtale, når lovgivningen ikke overholdes, og når data behandles uansvarligt. Dataansvarlighed bidrager til at styrke virksomhedens image. Det kan bruges aktivt i markedsføring, og dermed kan det bidrage til at forbedre virksomhedens konkurrenceevne.

Rådet for Digital Sikkerhed, DI, D-mærket, IDA og IT-Branchen har i samarbejde med Erhvervsstyrelsen gennemført denne undersøgelse med fokus på danske virksomheders konkurrenceevne via ansvarlig, lovlig og sikker dataanvendelse i forretningsudviklingen. Vi håber, I bliver inspireret til at arbejde endnu mere med ansvarlig brug af data. Det er der nemlig penge i!

God læselyst

Hvad omfatter arbejdet med dataansvarlighed?

Data er et væsentligt aktiv for jeres virksomhed og har stor økonomisk værdi. Forretningsmæssigt spiller data en stor rolle for både vækst og risikohåndtering – og kan være afgørende for, at I bliver valgt som leverandør.

Arbejdet med dataansvarlighed sikrer, at jeres systemer og omgivelser samt brugen og delingen af jeres data lever op til krav og forventninger til it-sikkerhed, persondatabeskyttelse og dataetik.

Kernen i databeskyttelse er at give kunderne kontrol over, hvordan deres oplysninger bliver behandlet og skabe tillid til, at I kun behandler et minimum af oplysninger om dem. I det store billede handler det om at beskytte kundernes ret til respekt for deres privatliv og deres frihedsrettigheder.

Dataetikken inspirerer til at sætte menneskets interesser i centrum. Men dataetik handler også om at undgå diskrimination og træffe bæredygtige valg, der gavner miljøet og samfundet som helhed. Dataetikken bliver på den måde et pejlemærke for, hvad der er det rigtige at gøre i en digitaliseret verden.

Rådet for Digital Sikkerhed · DI Digital · D-mærket · IDA · IT-BRANCHEN · ERHVERVSSTYRELSEN · INDUSTRIENS FOND – Fremmer dansk konkurrenceevne – The Danish Industry Foundation

Overblik over indhold

De klareste indsigter

Metode

Hvem er respondentgruppen?

Konkurrencemæssige fordele

Er der styr på data?

Er indsatsen forankret?

It-sikkerhed – er det mere end antivirus-opdatering?

Persondatabeskyttelse – det har vi styr på?

Dataetik – hvorfor nu det?

Virksomhedernes leverandører – har de styr på det?

Kender virksomhederne de tilgængelige værktøjer?

Kontaktoplysninger

Bilag

De klareste indsigter

- 41% af de danske SMV'er i undersøgelsen vurderer, at datasikkerhedsniveauet har betydning for virksomhedens konkurrenceevne.
- 63% af de danske SMV'er i undersøgelsen vurderer, at deres virksomhed er blevet styrket af at efterleve lovgivningen om persondatabeskyttelse.
- 56 % af de danske SMV'er i undersøgelsen vurderer, at deres virksomhed bliver styrket, når de viser kunder og potentielle kunder, hvordan de arbejder med dataetik.
- 8% af virksomhederne i undersøgelsen vurderer, at arbejdet med dataansvarlighed som et konkurrenceparameter giver en øget omsætning.
- Virksomheder, der har meromsætning, har forankret og implementeret it-sikkerhed.
- Gennemsigtighed i dataanvendelsen udgør et væsentligt konkurrenceparameter.

Formålet med undersøgelsen

Rådet for Digital Sikkerhed, DI, D-mærket, IDA og IT-Branchen har i samarbejde med Erhvervsstyrelsen og med støtte fra Industriens Fond igangsat en undersøgelse, der skal gøre os og jer klogere på, hvor vi kan sætte ind for at øge it-sikkerheden og persondatabeskyttelsen for derigennem at styrke tilliden til virksomhederne.

Centralt for undersøgelsen er spørgsmålet om dataansvarlighed som et konkurrenceparameter. Vi tror på, at dét at være bedst til dataansvarlighed sikrer virksomhedernes fortsatte vækst.

Rådet for Digital Sikkerhed · DI Digital · D-mærket · IDA · IT-Branchen · Erhvervsstyrelsen · Industriens Fond – Fremmer dansk konkurrenceevne – The Danish Industry Foundation

Metode

Spørgeskemaets opbygning

FAKTA
Spørgeskemaet består af 32 spørgsmål inden for tre temaer. Spørgsmålene giver ny viden om arbejdet med dataansvarlighed som konkurrenceparameter hos de danske SMV'er.

It-sikkerhed

Virksomhedens etablering af tekniske og organisatoriske foranstaltninger til at opnå sikkerhed på netværk, systemer, udstyr og fysiske omgivelser samt styring af, hvem der har adgang hertil. Det handler også om forståelse for risiko- og trusselsbilledet, så sikkerheden kan tilpasses til det aktuelle sårbarhedsniveau for interne og eksterne sikkerhedshændelser.

Persondatabeskyttelse

Virksomhedens implementering af kravene i persondataforordningen (GDPR) til gennemsigtighed, formålsbestemthed, dataminimering, lovligt grundlag, indlejret databeskyttelse og datarettigheder. Centralt er også forståelsen for forordningens krav til risikohåndtering og ansvarlighed gennem organisatoriske foranstaltninger, fx interne politikker, procedurer og vejledninger.

Dataetik

Virksomhedens forståelse for effekten af deres databehandling i forhold til adfærdspåvirkning, kundens kontrol med egne data og gavn af gevinsterne af databehandlingen, bias ved indhentning og behandling af data samt utilsigtede sociale, miljømæssige og etiske konsekvenser. En dataetisk strategi er et pejlemærke for virksomhedens ansvarlige brug af data.

Konkurrenceparameter

Virksomhedens oplevelse af dataansvarlighed som barrierenedbrydende og værdiskabende, fordi den dataansvarlige profil giver adgang til nye markeder og nye kundesegmenter.

Fakta om undersøgelsen

Antal adspurgte

7.700 virksomheder har modtaget invitation til undersøgelsen via mail. Mailadresser er trukket via CVR-registeret. Spørgeskemaet er sendt til virksomhedstyperne: Aktieselskaber, anpartsselskaber, andelsselskaber med begrænset ansvar og enkeltmandsvirksomheder med mere end fem medarbejdere.

Antal besvarelser og svarprocent

772 besvarelser hen over en periode på 14 dage. Dette tal svarer til en svarprocent på 10%.

Anonymitet

Fuldstændig anonymitet betyder, at vi ikke kan sige, hvem det er, der har deltaget i undersøgelsen.

Data

Data fra undersøgelsen bliver tilgængelig i en visualiseret udgave i forbindelse med den endelige rapport.

Tidslinje

29. oktober 2021: præsentation af den kvantitative del af undersøgelse

1. kvartal 2022: præsentation af den samlede undersøgelse inklusive case-beskrivelser på roadshows i hele landet

Validitet

Intern validitet (undersøgelsens konklusioner)

Overordnet vurderes den interne validitet af undersøgelsen at være relativt høj.

Undersøgelsens interne validitet er blandt andet blevet højnet ved at sikre respondenterne fulde anonymitet. Anonymitet medfører større gyldighed i form af mere sandfærdige svar, da respondenten ikke efterfølgende kan identificeres på baggrund heraf. Eftersom undersøgelsen beskæftiger sig med forretningskritiske områder, vurderes anonymitet som en forudsætning for sandfærdige svar.

Svarmuligheder, der ikke har en naturlig rækkefølge, blev randomiseret for at undgå, at rækkefølgen havde en effekt på respondenternes svar, hvilket er god praksis inden for spørgeskemaundersøgelser.

Til gengæld er det en kendt effekt i spørgeskemaundersøgelser, at respondenter forsøger at svare ud fra deres opfattelse af, hvad de tror forfatterne ønsker at finde ud af. Af den grund kan der være en risiko for, at respondenterne har haft en systematisk positiv bias mod pro dataansvarlige handlinger, da det ikke var muligt at maskere spørgeskemaets formål.

Ekstern validitet (generalisérbarhed)

Undersøgelsens stikprøve vurderes relativt repræsentativ for danske SMV'er som helhed, blandt andet fordi stikprøvens branchefordeling i store træk modsvarer populationens.
Endvidere vurderes undersøgelsens svarprocent på 10% som relativt tilfredsstillende givet målgruppen, undersøgelsens længde og kompleksitet, samt det faktum at der er tale om en internetundersøgelse, der blev foretaget over en kort periode (20. september til 6. oktober 2021).

Undersøgelsens stikprøvestørrelse anses som tilfredsstillende, men den eksterne validitet for meromsætningsgruppen vurderes som middelmådig på grund af delstikprøvens størrelse på 40 respondenter, svarende til 8% af besvarelserne på det pågældende tidspunkt i spørgeskemaundersøgelsen.

Det bemærkes, at de sidste 150 respondenter ikke havde nogen nævneværdig effekt på undersøgelsens konklusioner. Dette kunne indikere, at mere dataindsamling ikke ville have bidraget med yderligere viden.

Reliabilitet

Reliabilitet er et udtryk for undersøgelsens pålidelighed.
Overordnet vurderes undersøgelsens reliabilitet at være høj. Eksempelvis højner det undersøgelsens pålidelighed, at respondenter deltager i eksperimentet gennem et internetlink, da det øger sandsynligheden for, at resultaterne kan reproduceres af andre, der udfører samme eksperiment.

Hvem står bag undersøgelsen?
… Og hvad skal den bruges til?

FAKTA
Der er ca. 300.000 SMV'er i Danmark, hvilket udgør ca. 99% af alle virksomheder i Danmark. Tilsammen står SMV'erne for omkring halvdelen af den samlede beskæftigelse.
Kilde DST.dk

Analysemetoden

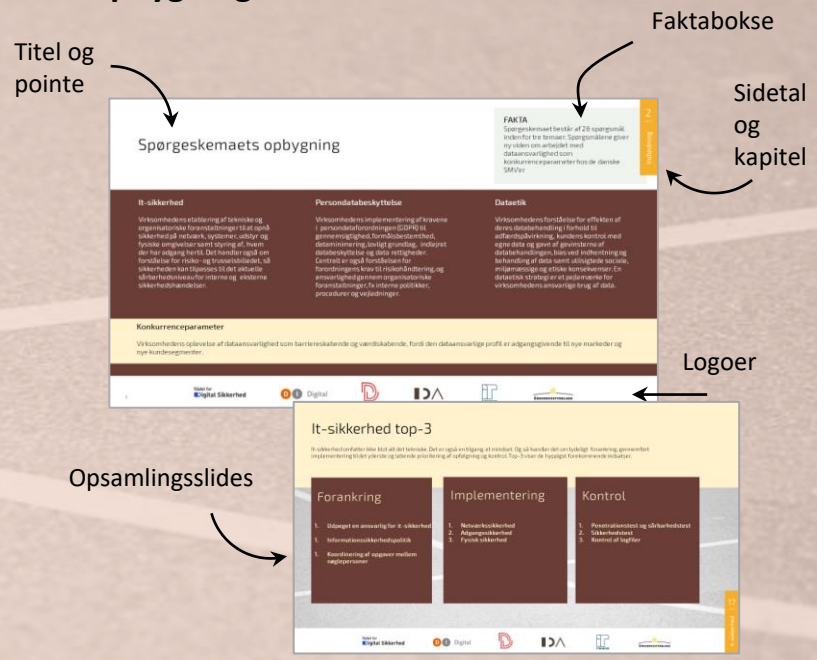
Data er blevet analyseret ved hjælp af simpel og avanceret statistik, herunder klyngeanalyser, hvilket muliggør opdagelsen af bagvedliggende mønstre i data og tendenser på tværs af grupper.

Resultaterne

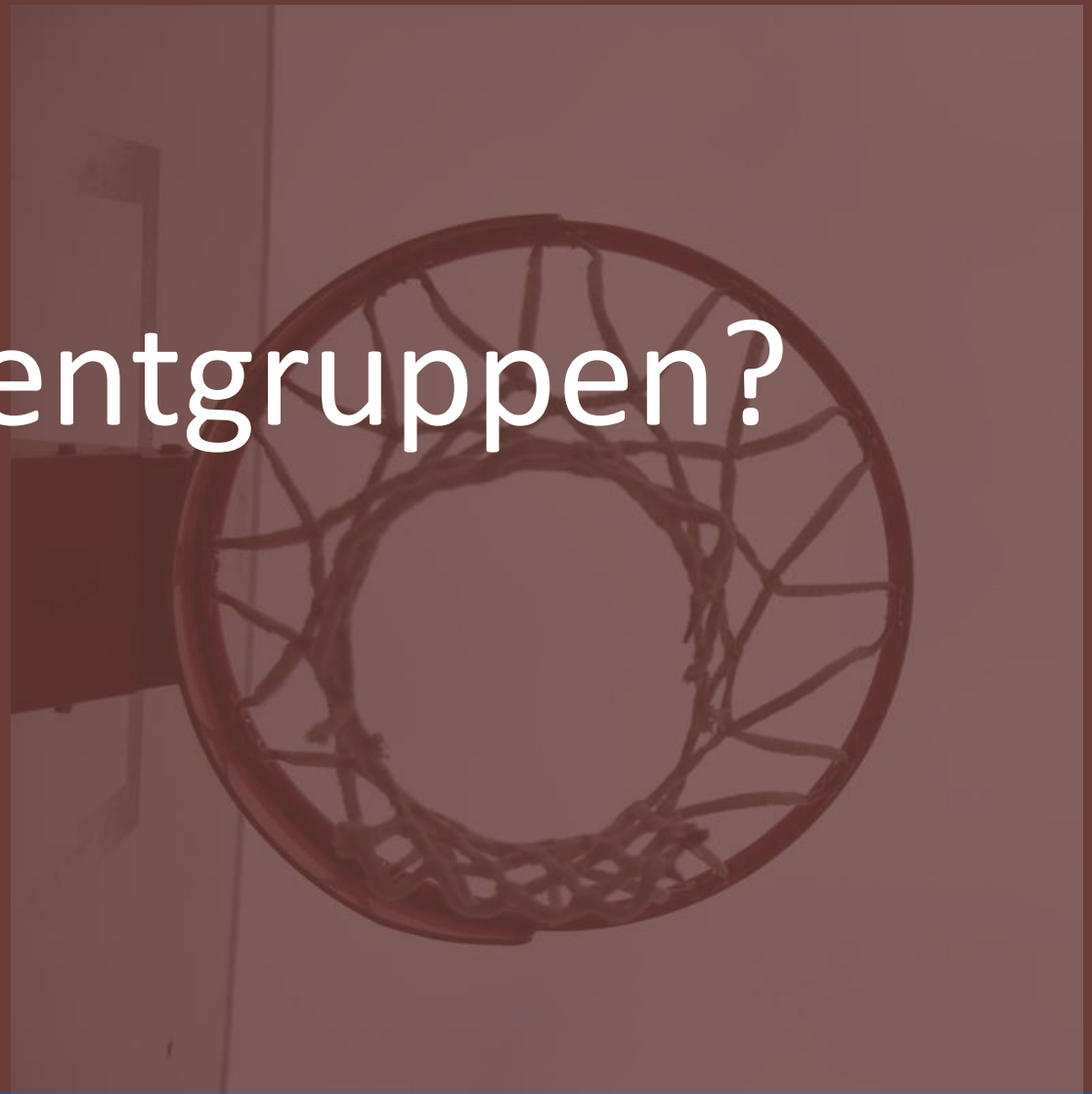
Undersøgelsens resultater præsenteres i det følgende. Der er fokus på, hvordan arbejdet med ansvarlig dataanvendelse har skabt forretningsmæssig værdi for virksomheder, men også på de udfordringer, der er forbundet med indsatsen.

Resultaterne vil blive fulgt op af case-beskrivelser med gode eksempler på, hvordan arbejdet med dataansvarlighed kan gribes an. Input fra undersøgelsen vil også blive brugt til tilretning af eksisterende digitale værktøjer. Det samlede resultat vil blive præsenteret på roadshows i hele landet.

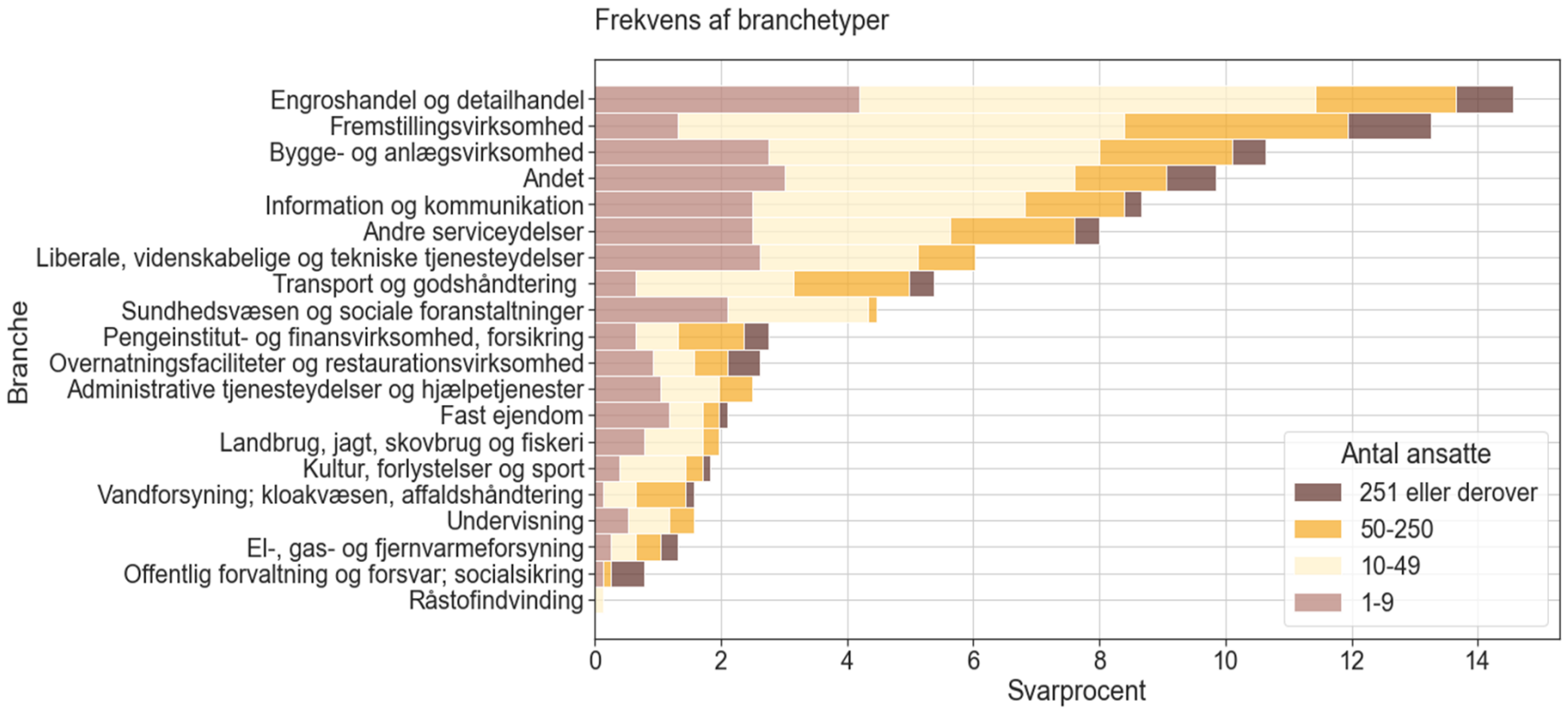
Sideopbygning



Hvem er respondentgruppen?



Brancher – hvem er med?



9%

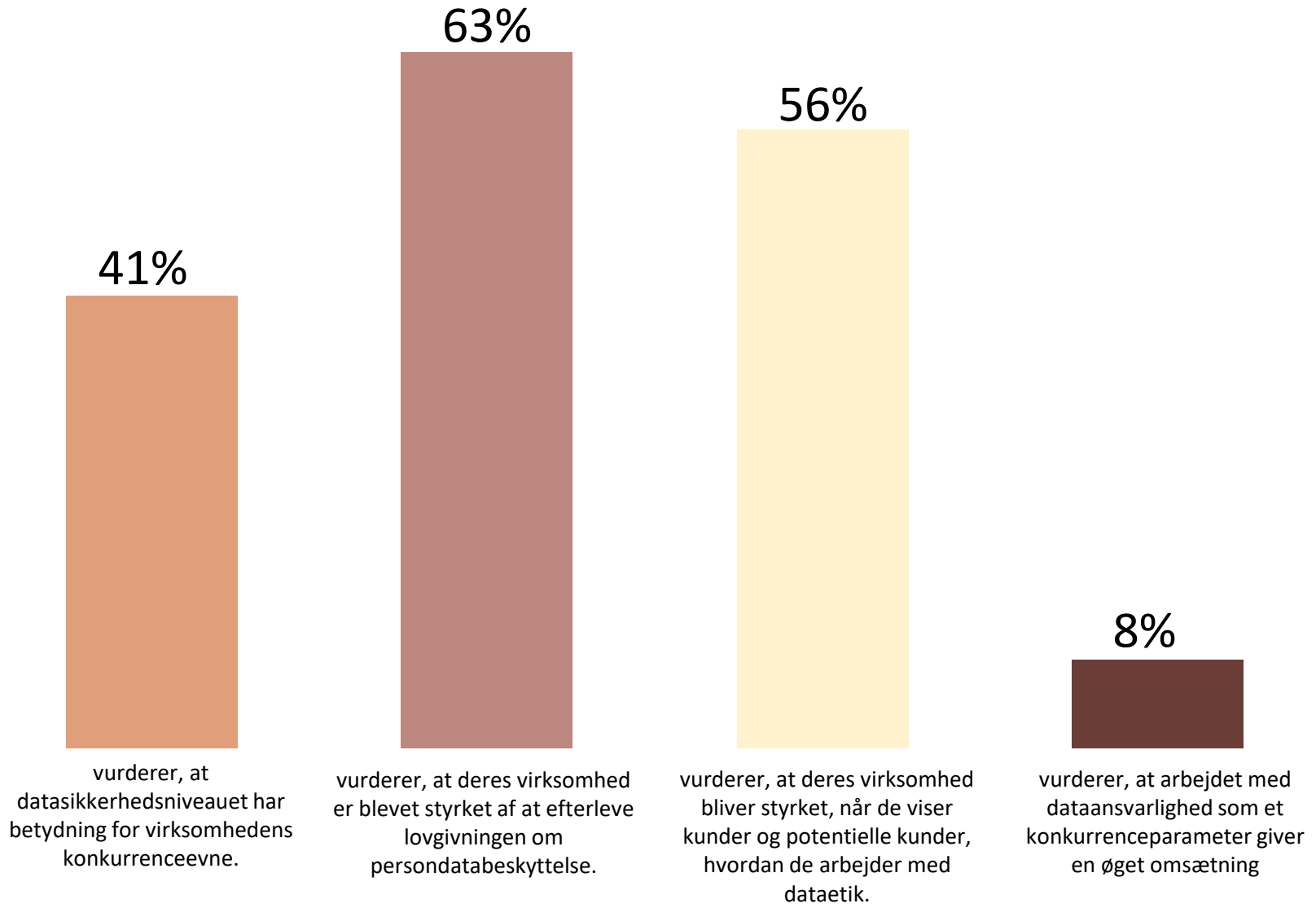
Undersøgelsen peger på, at kategorien ”Andet” omfatter en række it-relaterede virksomheder.

- Virksomheder med 10-49 ansatte repræsenterer 47% af virksomhederne i undersøgelsen.
- 9% af deltagerne i undersøgelsen svarer, at de tilhører branchen ”Andet”.
- I ”Andet” fylder særligt it, software og systemudvikling.

- Brancherne engros- og detailhandel, fremstillingsvirksomheder og bygge- og anlægsvirksomheder repræsenterer 42% i undersøgelsen.
- Hos Danmarks Statistik repræsenterer de samme tre brancher 48 %.

Konkurrencemæssige fordele

Effekten af arbejdet med dataansvarlighed for konkurrenceevne og meromsætning



Mere end halvdelen af virksomhederne i undersøgelsen peger på, at arbejdet med dataansvarlighed har betydning for deres konkurrenceevne.

Effekten kommer især af arbejdet med at forankre og implementere persondatabeskyttelse i virksomhederne, men også ved at vise kunderne, hvordan de arbejder med dataetik.

Effekten af virksomhedernes datasikkerhedsniveau ligger lidt lavere, når de vurderer betydningen heraf for deres konkurrenceevne.

Det er kun en forholdsvis lille del af virksomhederne, der vurderer, at arbejdet med dataansvarlighed giver meromsætning. Effekten er imidlertid ikke set tidligere, og det er derfor interessant at se nærmere på, hvad der adskiller disse virksomheders indsatser fra de øvrige deltagende virksomheder i undersøgelsen.

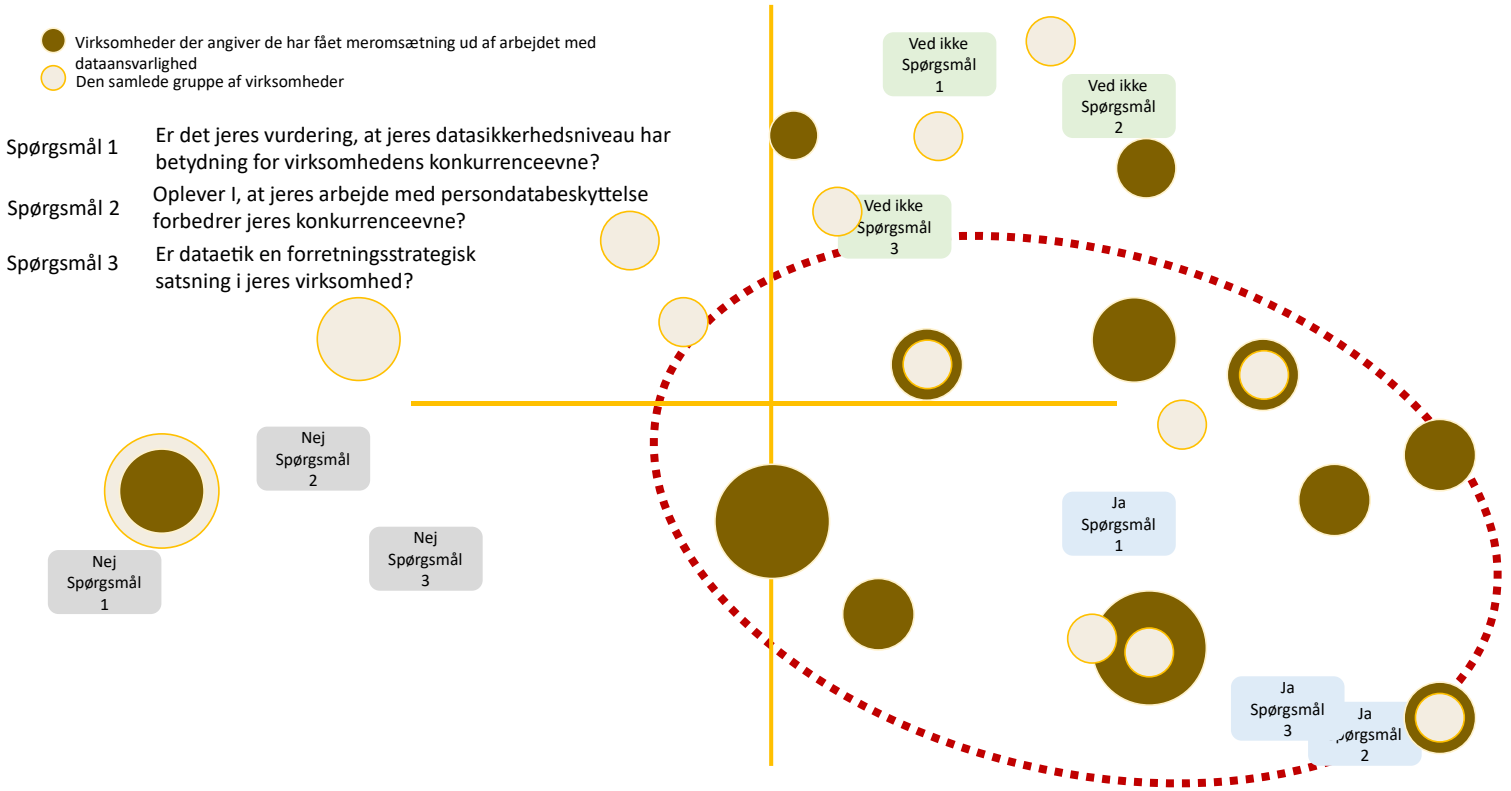
Sammenhæng mellem et dedikeret fokus og virksomhedernes meromsætning

Klyngeanalyse

I undersøgelsen er der fokus på danske SMV'ers ansvarlige brug af data som konkurrenceparameter. Ud af de 32 spørgsmål er der tre, der specifikt omhandler konkurrenceevne. To spørgsmål afdækker, hvorvidt arbejdet med it-sikkerhed og persondatabeskyttelse har givet en konkurrencefordel (1 og 2). Ét spørgsmål fokuserer på det forretningsstrategiske i arbejdet med dataetik (3).

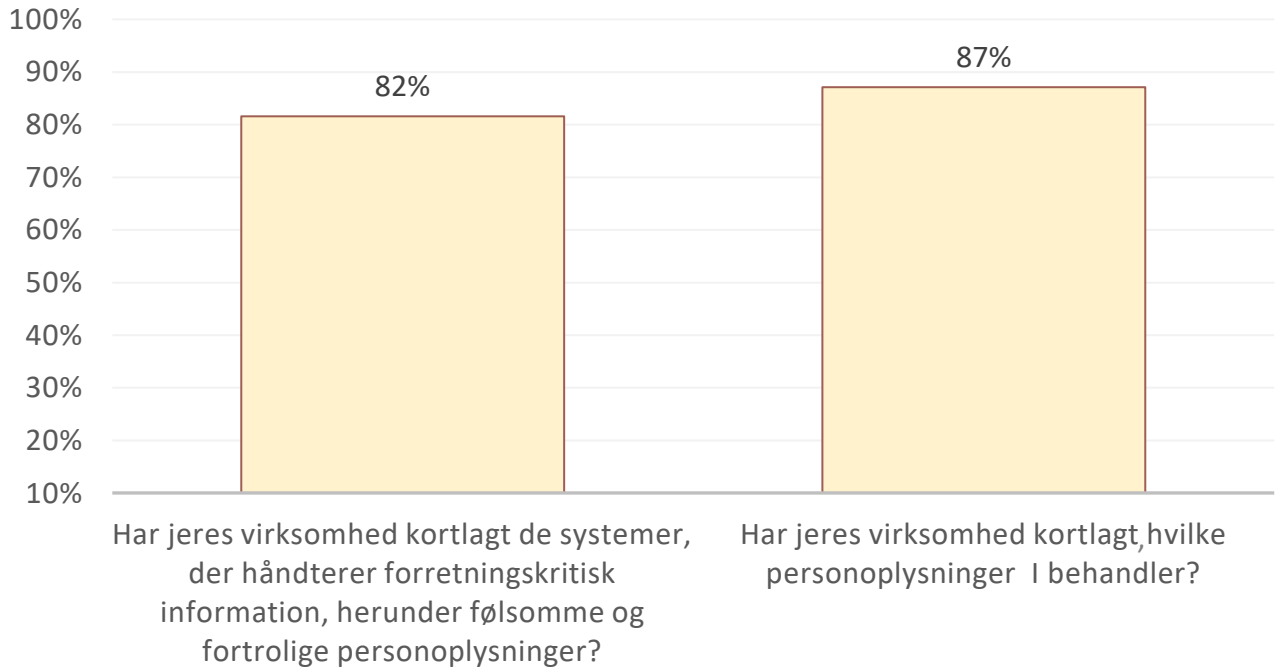
På denne baggrund er der udarbejdet en klyngeanalyse. Klyngeanalysen viser en tendens til, at svarmuligheden "ja" i de tre spørgsmål i overvejende grad bliver brugt af de virksomheder, der også angiver, at de har fået meromsætning ud af arbejdet med ansvarlig databehandling. Klyngen er markeret med en rød cirkel.

Gruppen af virksomheder, der angiver, at de har fået meromsætning, er derfor blevet isoleret i en del af de øvrige analyser. Dette med henblik på at finde viden og handlinger, der kan anbefales til andre virksomheder, som ønsker at styrke deres konkurrenceevne gennem øget fokus på dataansvarlighed.



Er der styr på data?

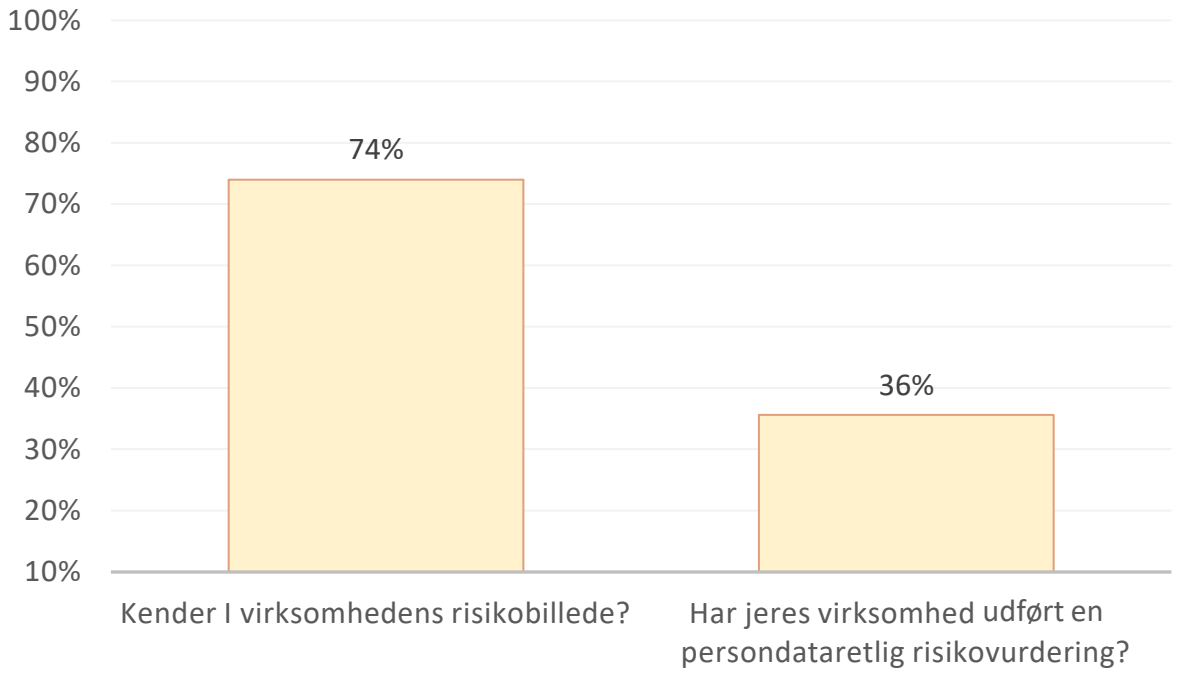
Mange virksomheder har kortlagt deres systemer og behandling af forretningskritisk information og persondata



Hovedparten har kortlagt de systemer, der håndterer forretningskritisk information

Hovedparten har kortlagt de personoplysninger, der arbejdes med i virksomheden

…men der er stor forskel på virksomhedernes indsigt i deres it-sikkerhedsrisiko og deres persondataretlige risiko



En stor andel af virksomhederne kender deres risikobillede i forhold til eksterne trusler og sikkerhedsmæssige sårbarheder.

Kun 36% kender risikoen for at påvirke kundernes friheder og rettigheder negativt.

Er indsatsen forankret?

Virksomhederne er gode til at forankre indsatsen for persondatabeskyttelse gennem en intern persondatapolitik, mens en mindre del har en politik om informationssikkerhed. Og dataetikken er overraskende godt med.

80%

har udformet en

Politik for persondatabeskyttelse

GDPR's specifikke krav til organisatoriske foranstaltninger og til dokumentation betyder, at virksomhederne skal overveje, hvordan de forankrer databeskyttelsen i den daglige drift.
Det kan opfyldes gennem politikker eller andre former for intern regulering i virksomheden, der instruerer medarbejderne i, hvordan de skal beskytte persondata som led i behandlingen af dem.

50%

har udformet en

Informations-sikkerhedspolitik

Lovgivning om sikkerhed i net- og informationssystemer (NIS) er kun relevant for et fåtal af undersøgelsens respondenter. Men et krav om en ledelsesgodkendt net- og informationssikkerhedspolitik slår ofte igennem på virksomheder, der leverer ydelser til organisationer omfattet af reglerne. En informationssikkerhedspolitik er derudover et væsentligt element i den type ledelsessystemer, der anbefales i ISO27001.

22%

har udformet en

Politik eller retningslinjer for dataetik

Kravet om en årlig dataetisk redegørelse i årsregnskabslovens § 99d gælder kun for virksomheder med mere end 250 ansatte, en nettoomsætning på 313 mio. og en balancesum på 156 mio. Blandt respondenterne er der 30 virksomheder med mere end 250 ansatte, hvoraf 40% har oplyst, at de har formuleret en dataetisk politik eller retningslinjer. Da emnet er forholdsvist nyt, er det positivt, at en femtedel af alle respondenter allerede nu knytter dataetik til deres dataanvendelse.

Forankring af indsatserne sker også gennem udpegning af en ansvarlig for det enkelte område, procedurer, koordinering og etablering af klageadgang

It-sikkerhed

67%

Har udpeget en ansvarlig for it-sikkerhed

- **28%** Beredskabsplan
- **37%** Nedskrevne procedurer eller processer for test og evaluering af sikkerhedsforanstaltninger
- **49%** Koordinering af opgaver mellem nøglepersoner

Persondatabeskyttelse

66%

Har udpeget en ansvarlig for GDPR-indsatsen

- **61%** Procedurer for sletning og anmodninger om brug af datarettigheder samt håndtering af databrud

Dataetik

17%

Har udpeget en ansvarlig for dataetik

- **12%** Klageadgang

Rådet for Digital Sikkerhed · DI Digital · IDA · IT-BRANCHEN · Erhvervsstyrelsen · Industriens Fond – fremmer dansk konkurrenceevne – The Danish Industry Foundation

It-sikkerhed – er det mere end antivirus-opdatering ?

It-sikkerhed top-3

It-sikkerhed omfatter ikke blot etablering af tekniske sikkerhedsforanstaltninger, men også om at placere roller og ansvar i organisationen.
På de områder er virksomhederne godt med. Men det halter lidt med at få test og kontroller på plads.

Forankring

1. Udpeget en ansvarlig for it-sikkerhed (67%)
2. Informationssikkerhedspolitik (50%)
3. Koordinering af opgaver mellem nøglepersoner (49%)

Implementering

1. Netværkssikkerhed (89%)
2. Adgangssikkerhed (68%)
3. Sikker affaldshåndtering (71%)

Kontrol

1. Penetrationstest og sårbarhedstest (19%)
2. Systemsikkerhedstest (43%)
3. Kontrol af logfiler (14%)

It-sikkerheden – fokus er på det forebyggende

It-sikkerheden er forretningskritisk, og ingen har lyst til at miste kunder eller indtjening som følge af datatyveri og sletning. De danske SMV'er er gode til at sikre deres netværk og til at styre, hvem der har adgang til data. Men opdatering af software er kun halvdelen af de danske SMV'er med på, og endnu færre gennemfører regelmæssig test af deres netværk.

Netværkssikkerhed

89%

Bruger firewalls og antivirusprogrammer

Adgangssikkerhed

68%

Tildeler adgangsrettigheder

Systemsikkerhed

43%

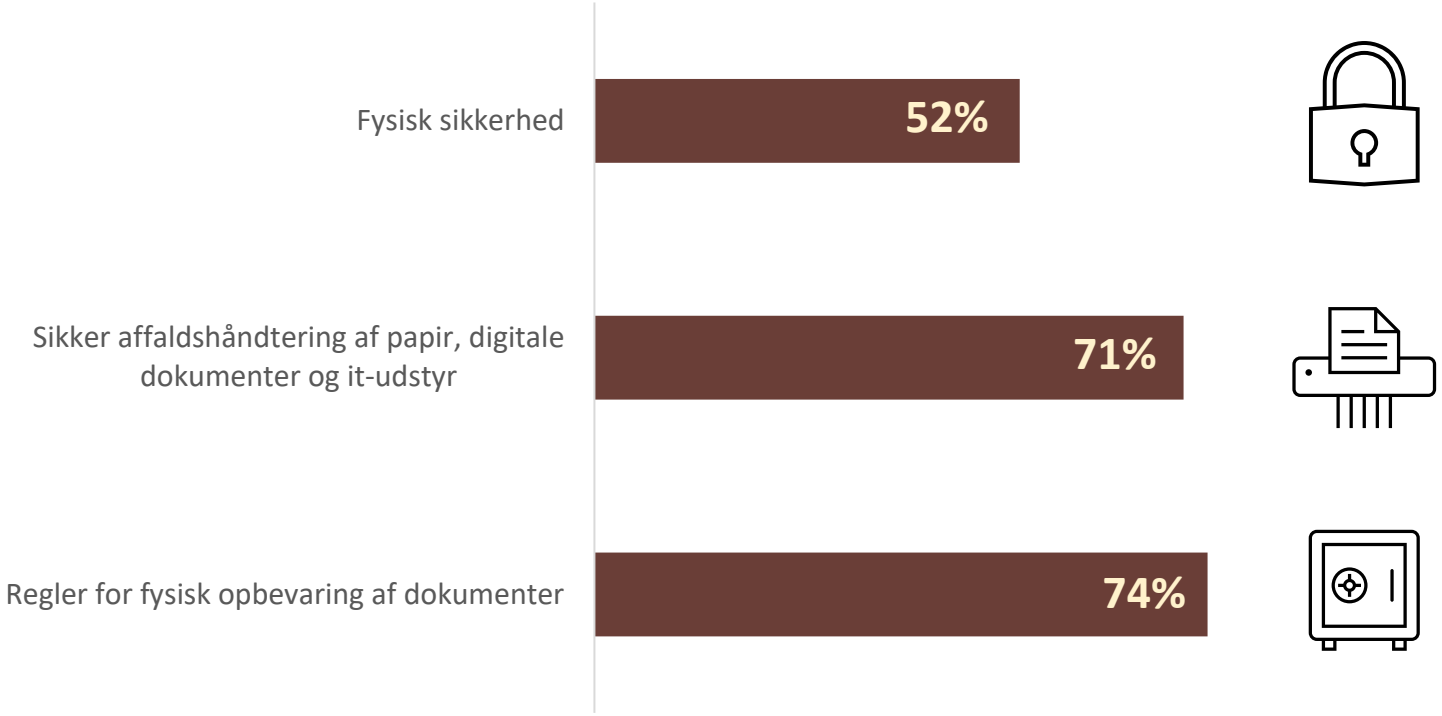
Bruger patching

Kontrolmekanisme

19%

Gennemfører regelmæssig penetrations- eller sårbarhedstest

Virksomhederne har generelt godt styr på den fysiske sikkerhed



Den fysiske sikkerhed i de bygninger og arealer, hvor virksomheden udfører sine aktiviteter, har betydning for en sikker opbevaring af data. Både de data, der indgår i fysiske dokumenter, og dem, der opbevares på elektronisk udstyr. Det omfatter f.eks. sikker affaldshåndtering af papir, digitale dokumenter og it-udstyr. 71% af virksomhederne oplyser, at de har styr på den del.

Det styrker beskyttelsen, når virksomheden har vedtaget interne regler om, hvordan den fysiske opbevaring af dokumenter skal indrettes. Det svarer 74% af virksomheder, at de har gjort.

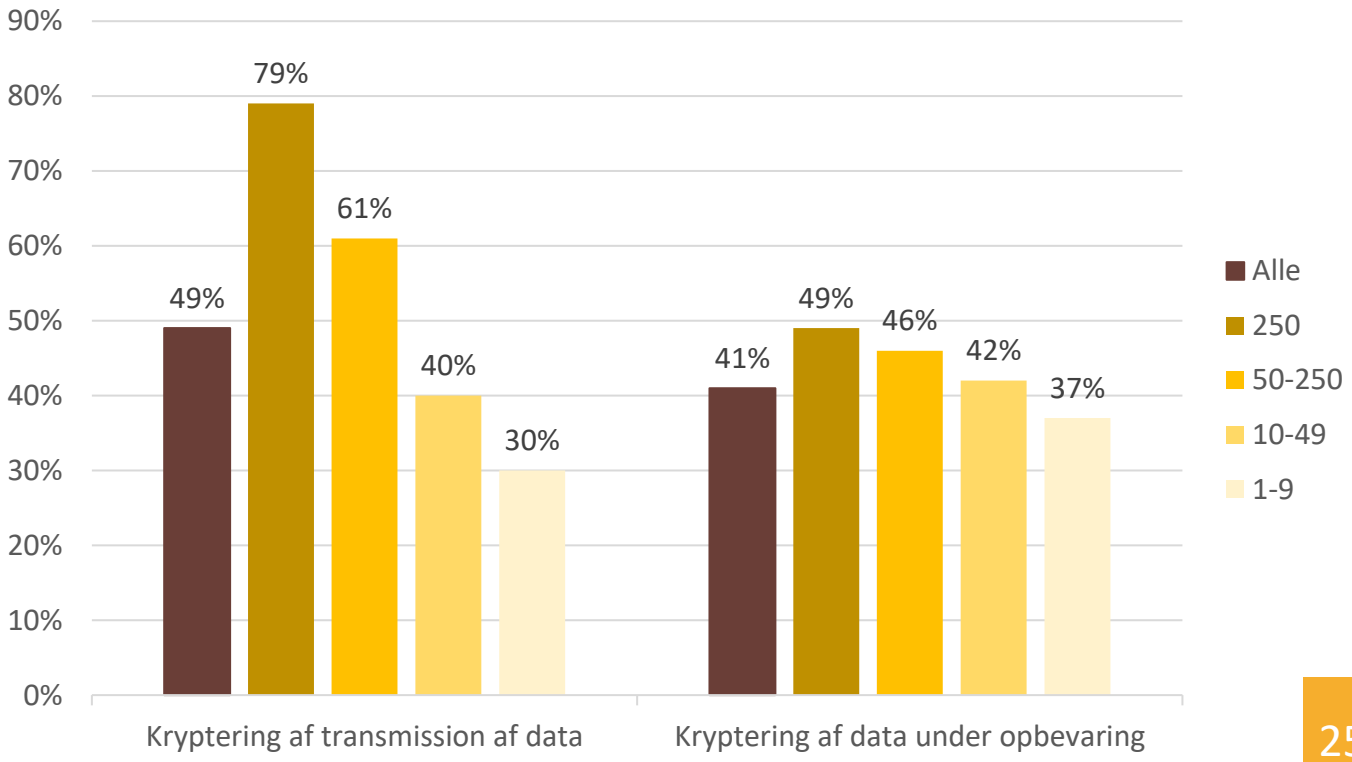
Den fysiske beskyttelse forebygger tyveri og ødelæggelse af data og beskytter mod uvedkommendes indsigt i data. Den omfatter derfor også kontrol af adgang til virksomhedens bygninger. Halvdelen af virksomhederne oplyser, at de har etableret fysisk sikkerhed.

Kryptering er et godt redskab til at sikre fortrolighed og beskytte data mod hacking og kriminalitet

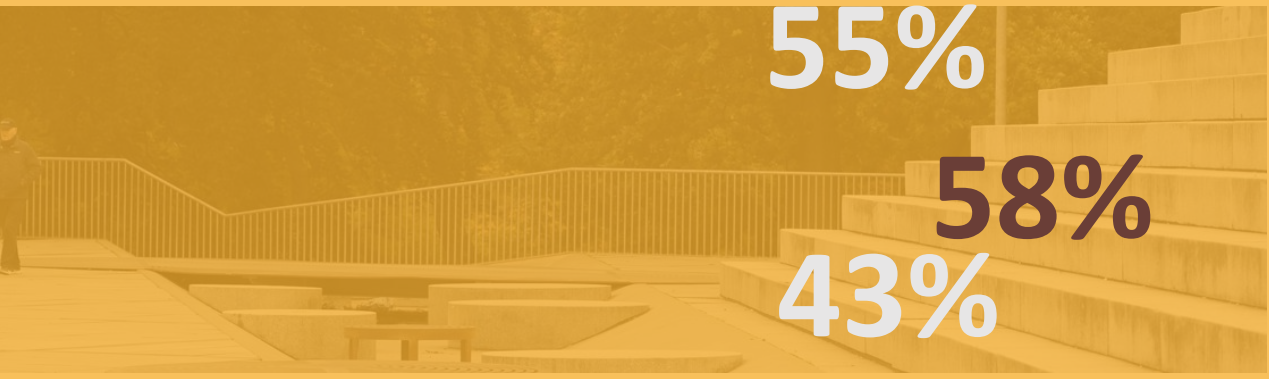
Opmærksomheden på at beskytte data mod indsigt fra uvedkommende aktører og mod ændringer eller sletning, når data transmitteres og opbevares, er forholdsvis begrænset.

Hensynet til fortrolighed og integritet slår tydeligst igennem hos de største virksomheder, hvor 79% krypterer deres transmissioner. Alle virksomhederne ligger derimod en del lavere med et gennemsnit på 49%.
Brugen af kryptering under opbevaring af data ligger gennemsnitligt lavere for alle virksomhederne, nemlig på 41%.

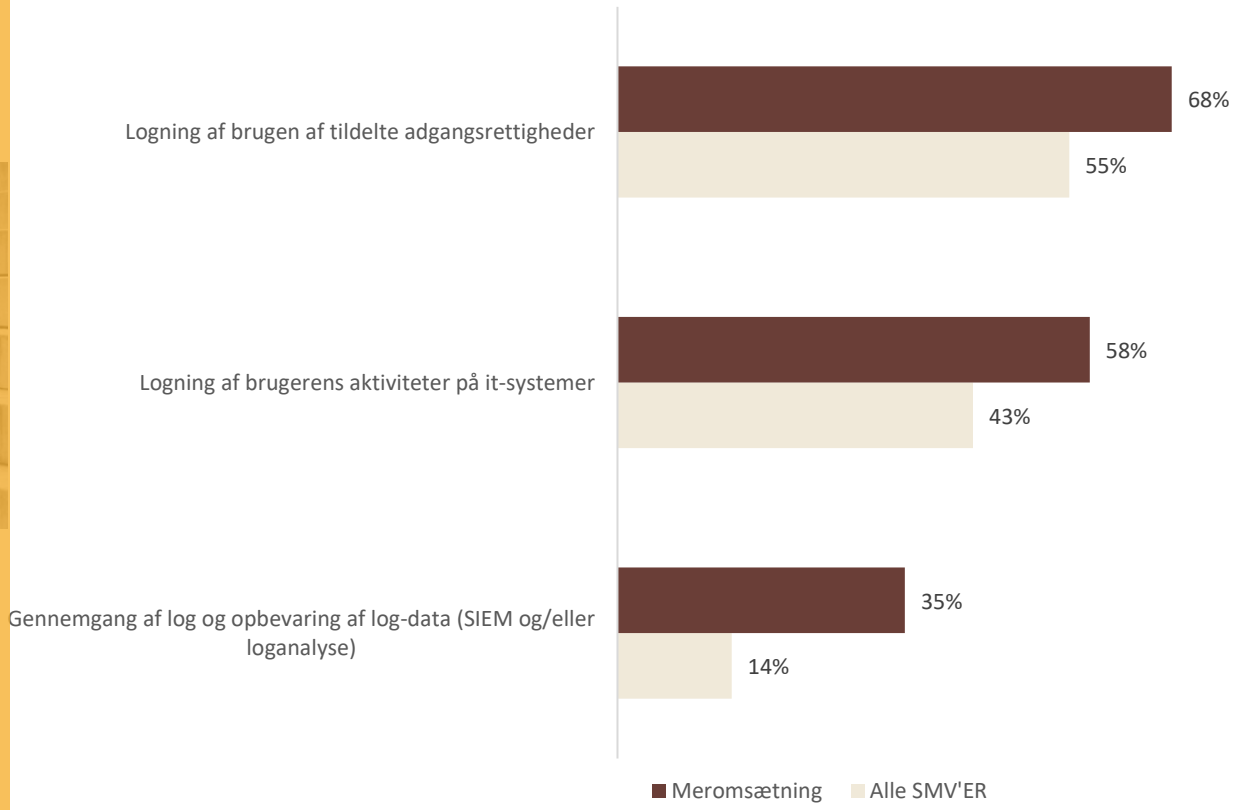
I forhold til den meget høje risiko for cyberkriminalitet og cyberspionage, der kan aflæses af det generelle trusselsbillede (CFCS 2021), men også i lyset af, at kryptering er blevet lettere tilgængeligt i mailsystemer, på devices og i cloud-løsninger, er niveauet overraskende lavt.



Virksomhederne er generelt gode til at logge adgang og aktiviteter, men loggen kontrolleres ikke meget



68%
55%
58%
43%
35%
14%



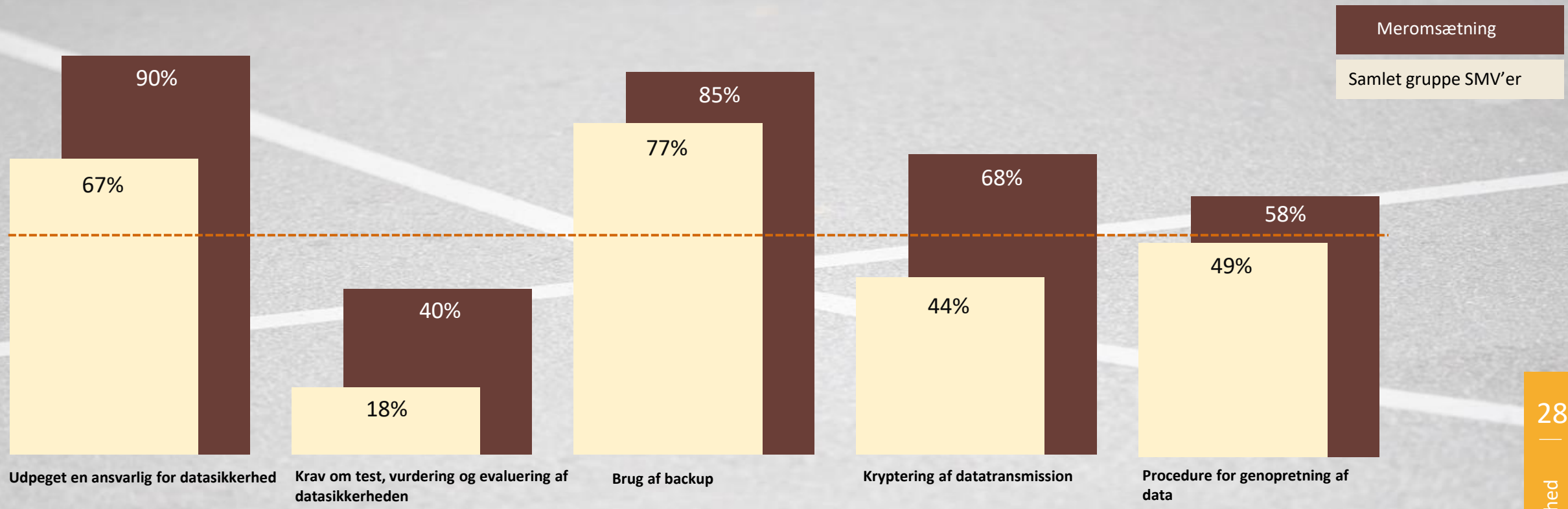
Der indføres sikkerhed, men det halter med test og kontroller – dog har størrelsen på virksomheden en betydning

		Test og kontroller i virksomheder +250
Beskyttelse af dataintegritet og fortrolighed		
Implementerede tiltag	55%	59%
Test og kontroller	20%	
Beskyttelse mod eksterne angreb		
Implementerede tiltag	64%	56%
Test og kontroller	19%	
Adgang til systemer og bygninger		
Implementerede tiltag	52%	49%
Test og kontroller	14%	

Rådet for Digital Sikkerhed · Digital · IT-BRANCHEN · ERHVERVSSTYRELSEN · INDUSTRIENS FOND The Danish Industry Foundation

Virksomheder, der opnår gevinster i arbejdet med dataansvarlighed, arbejder målrettet med it-sikkerhed

FAKTA
Virksomhederne er i undersøgelsen blevet bedt om, at svare på, om de har fået meromsætning ud af arbejdet med dataansvarlighed. Vi holder gruppen op mod den samlede gruppe af SMV'er.



Persondatabeskyttelse – det har vi styr på?

Persondatabeskyttelse – top 3

Effektiv persondatabeskyttelse opnås gennem interne regler og placering af roller og ansvar i organisationen. Basale elementer er også viden om de data, virksomheden råder over, både internt og hos leverandører, og gennemsigtighed i dataanvendelsen. Det har virksomhederne styr på. Men de oplever også, at lovkravene skaber også udfordringer for forretningsudvikling.

Forankring

1. Intern persondatapolitik (80%)
2. Udpegning af en ansvarlig for GDPR-indsatsen (66%)
3. Procedurer for virksomhedens sletning af data, håndtering af anmodninger om brug af datarettigheder og responsplan for databrud (61%)

Implementering

1. Kortlægning af persondata (87%)
2. Databehandleraftaler (61%)
3. Gennemsigtighed (48%)

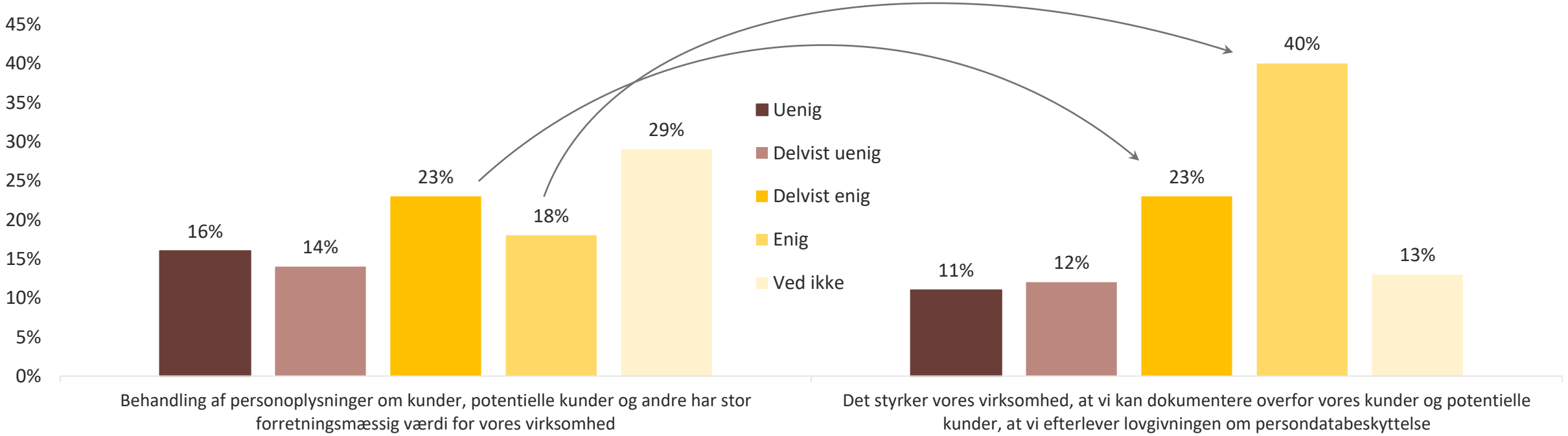
Udfordringer

1. Indsamling af personoplysninger (34%)
2. Brug af persondata til forretningsudvikling (19%)
3. Berigelser af personoplysninger med data fra sociale medier, registre eller andre datasæt (15%)

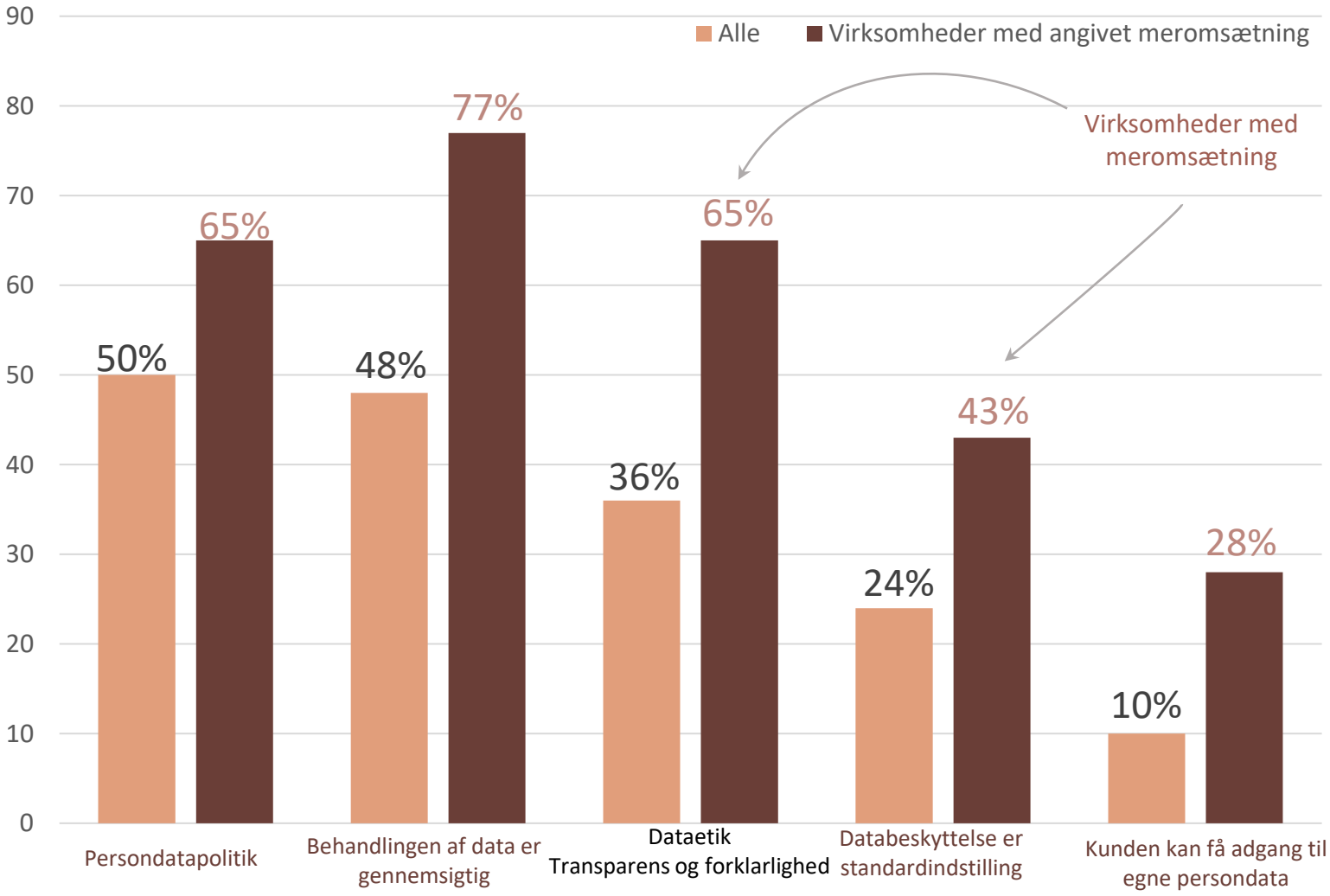
Compliance betaler sig – opfyldelse af lovkrav til persondatabeskyttelse styrker virksomhederne

41% af de danske SMV'er i undersøgelsen vurderer, at det har en stor forretningsmæssig værdi for deres virksomhed at arbejde med data om kunder og potentielle kunder.

63% af de danske SMV'er i undersøgelsen vurderer, at deres virksomhed er blevet styrket af at efterleve lovgivningen om persondatabeskyttelse.



Gennemsigtighed er et væsentligt konkurrenceparameter



Gennemsigtighed i behandlingen af persondata giver kunden mulighed for at forestille sig, hvad deres data bliver brugt til. Det giver også kunden en følelse af kontrol med egne data. For virksomheden ligger værdien i, at kundernes forventninger til virksomhedens databehandling bliver afstemt. Det giver også mindre administration, når kunden selv kan få adgang til sine data.

Virksomheder med rapporteret meromsætning i undersøgelsen ligger da også væsentligt højere på de gennemsigtighedsparametre, undersøgelsen har spurgt ind til:

- En tilgængelig persondatapolitik på hjemmesiden
- Sikring af, at databehandlingen er gennemsigtig
- Processer, der sikrer gennemsigtighed og forklarlighed
- Brug af databeskyttelse som standardindstilling
- Direkte adgang til egne persondata, f.eks. gennem et dedikeret område på en hjemmeside.

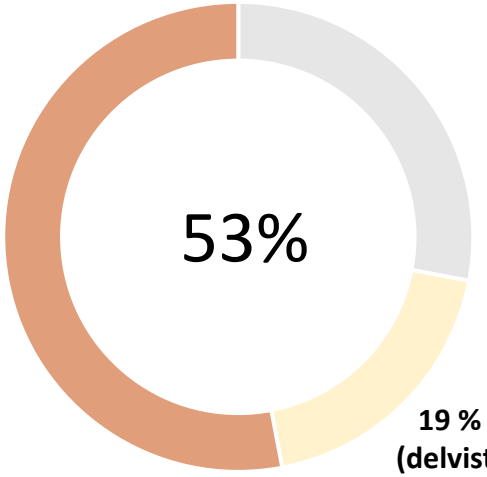
Mange virksomheder arbejder med princippet om dataminimering for at sikre, at kun nødvendige persondata behandles til et specifikt formål

Dataminimering er et grundprincip i GDPR og sikrer, at både indsamling, behandling og opbevaring af persondata er begrænset til det nødvendige for at opfylde det samlede behandlingsformål.

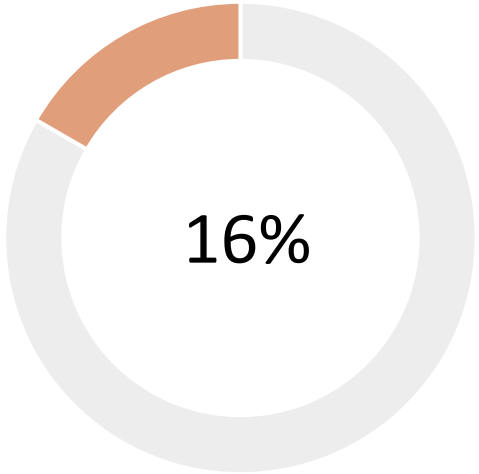
Dataminimering anvendes af lidt over halvdelen af virksomhederne, når de vurderer, hvilke data de har brug for at indsamle eller behandle til et bestemt formål. 19% har derudover oplyst, at de delvist arbejder med dataminimering.

Pseudonymisering er en anden måde at minimere mængden eller typen af persondata på. Et CPR-nummer kan f.eks. erstattes af et kundenummer. Det giver en mindre sårbar datamængde og mindsker risikoen for datasubjektet.
Det er en metode, der er slået igennem hos 41% af virksomhederne med mere end 250 medarbejdere, mens det kun gælder for 16% af de øvrige virksomheder.

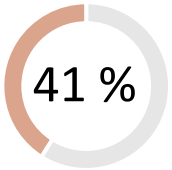
Dataminimering



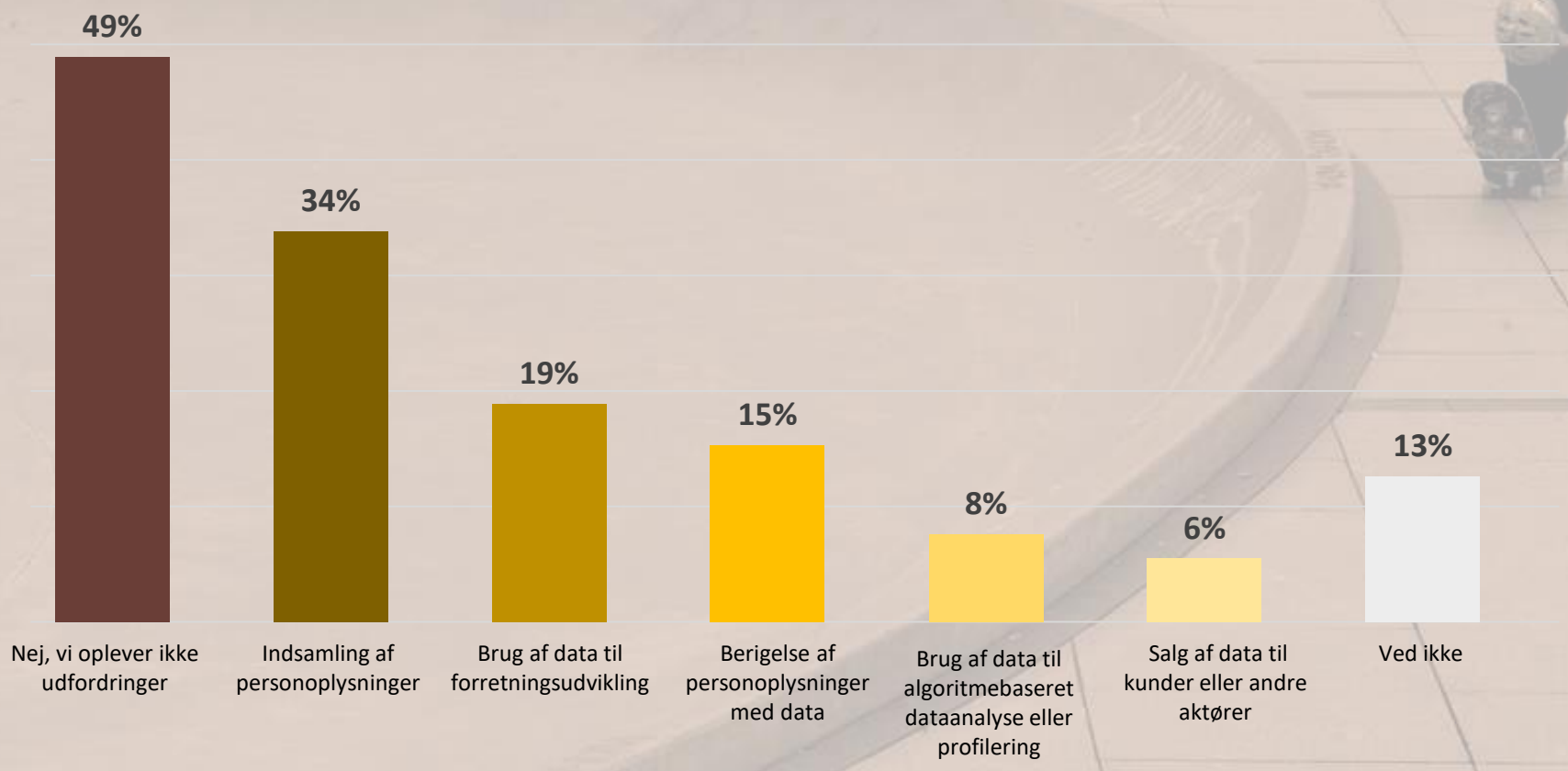
Pseudonymisering



For virksomheder med +250 medarbejdere



Halvdelen af virksomhederne bliver (ikke) udfordret af lovkravene til persondatabeskyttelse



Brancherne oplever forskellige udfordringer, men de samler sig om indsamling og berigelse af persondata

De hyppigst oplevede udfordringer fordelt på brancher

Indsamling af personoplysninger

- Overnatningsfaciliteter og restaurationsvirksomhed (73%)
- Vandforsyning, kloakvæsen mv. (50%)
- Administrative tjenesteydelser og hjælpetjenester (50%)
- Information og kommunikation (42%)

Berigelse af data til forretningsudvikling

- Information og kommunikation (28%)
- Liberale, videnskabelige og tekniske tjenesteydelser (34%)
- Administrative tjenesteydelser og hjælpetjenester (40%)
- Sundhedsvæsen og sociale foranstaltninger (38%)
- Kultur, forlystelser og sport (29%)

Brug af data til algoritmebaseret dataanalyse eller profilering

- Information og kommunikation (16%)
- Sundhedsvæsen og sociale foranstaltninger (13%)
- Kultur, forlystelser og sport (14%)
- Andet (bl.a. it-virksomheder) (14%)

Dataetik – hvorfor nu det?

Dataetik – top-3

Dataetik er ikke bare et spørgsmål om GDPR og it-sikkerhed, men handler om at sætte mennesket i centrum, og behandle deres data med respekt, gennemsigtighed og blik for bæredygtig anvendelse af data. Arbejdet med dataetik indeholder både forankring, konkrete initiativer og overvejelser. Virksomhedernes har her taget de første skridt.

Forankring

1. Politik eller retningslinjer for dataetik (22%)
2. Udpegning af en ansvarlig for dataetik (17%)
3. Processer for at sikre gennemsigtighed og forklarlighed for kunder (36%)

Initiativer

1. Krav om sporbarhed i dataanvendelsen (13%)
2. Klageadgang (12%)
3. Vurdering af miljømæssige konsekvenser af teknologi eller databehandling (6%)

Overvejelser

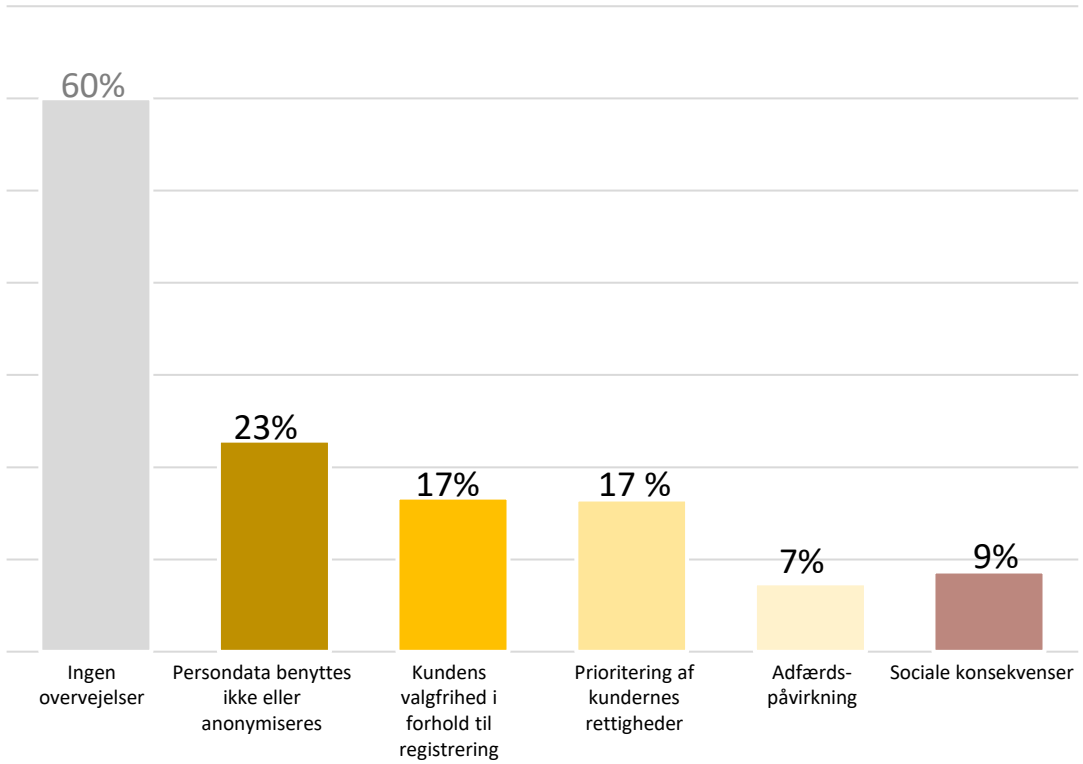
1. Dataminimering og anonymisering (23%)
2. Valgfrihed for kunden i forhold til at blive registreret (17%)
3. Prioritering af kundens rettigheder fremfor kommercielle eller organisatoriske interesser (17%)

Virksomhederne er så småt i gang med dataetiske overvejelser

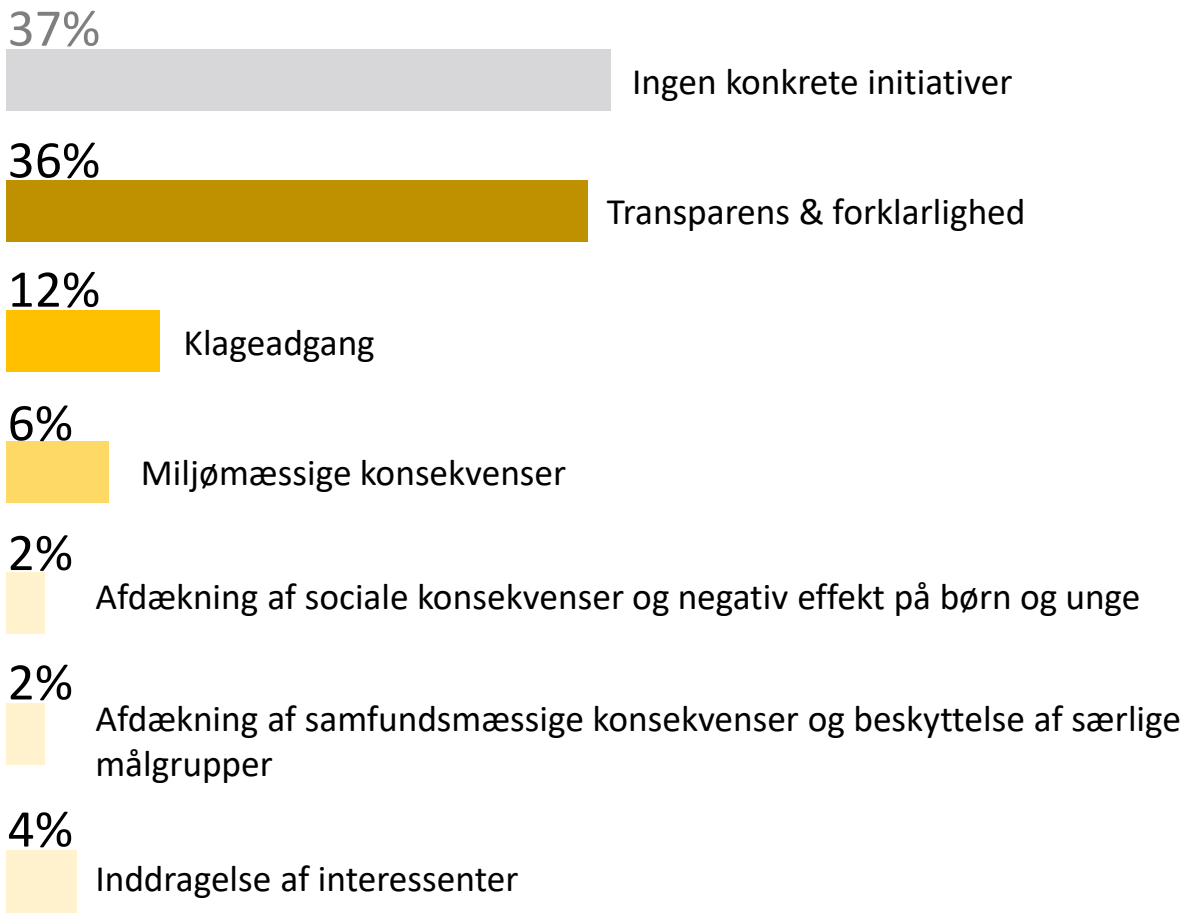
Virksomhedernes dataetiske overvejelser har især fokus på at skjule kundens identitet ved at undlade at bruge persondata eller gennem anonymisering.

Omkring en femtedel af virksomhederne sætter mennesket i centrum ved at overveje, hvordan de kan prioritere kundernes rettigheder fremfor kommercielle eller organisatoriske interesser. Mere konkret overvejer de, om de kan give kunden valgfrihed i forhold til at blive registreret, f.eks. i kundeanalyser eller cookie-opsætning.

Færre virksomheder overvejer, hvordan de påvirker kundernes adfærd gennem deres databehandling, f.eks. til overbrug eller afhængighed. Et tilsvarende lavt niveau ses angående sociale konsekvenser som følge af forskelsbehandling eller stigmatisering.



Virksomhedernes dataetiske initiativer er på vej, men stadig begrænsede



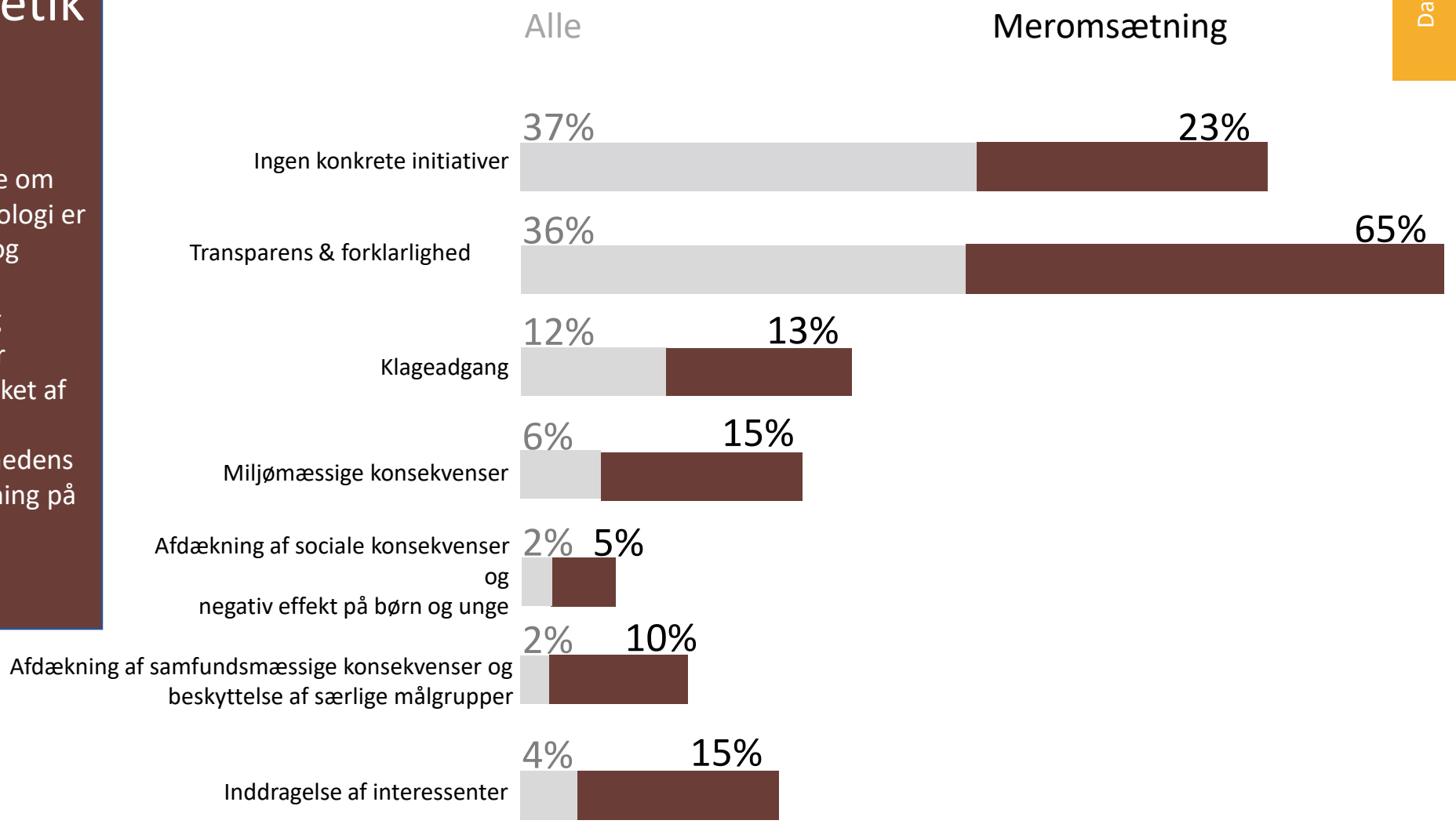
De virksomheder, der arbejder med dataetik, har især fokus på, at deres databehandling er gennemsigtig og kan nemt forklares for kunderne. Profilering, stigmatisering og anden påvirkning samt ulighed er samfundsmæssige konsekvenser af databehandlingen, som kan minimeres gennem et fokuseret arbejde. Bias og fordomme i databehandlingen kan have sociale konsekvenser for kunderne, når de afspejles i produkter og services. Et fåtal af virksomheder arbejder med dette, men med øget fokus på området kan det forventes at blive et af nøgleområderne i arbejdet med dataansvarlighed.

Virksomhederne har et lidt større fokus på de miljømæssige konsekvenser af databehandlingen. Dette kan afspejle, at den offentlige debat om grøn omstilling bl.a. har omhandlet energiforbruget fra driften af cloud-servere.

Undersøgelsen viser, at det kun er få virksomheder, der arbejder med dataetik eller inddrager interessenter for at få mere viden om konsekvenserne af deres databehandling.
En lille andel af de deltagende virksomheder har svaret, at de har etableret en klageadgang, der kan håndtere klager om dataetiske spørgsmål.

Virksomhederne med meromsætning gør mere inden for dataetik

Omgivelsernes fokus på dataetik og en generelt øget bevidsthed hos kunderne om konsekvenserne af at anvende ny teknologi er et incitament til at skabe transparens og forklarlighed.
Sammenkædningen af digitalisering og klimapåvirkning gør det også oplagt for virksomheder at se på f.eks. CO_2-aftrykket af teknologianvendelsen.
Inddragelse af interessenter i virksomhedens indsatser kan også have positiv påvirkning på virksomhedens profil.



Træning og oplysning skaber bedre databeskyttelse og en kultur med fokus på sikkerhed – der er gode takter, men kun en mindre del indtænker dataetik

46%

It-sikkerhed

Medarbejderne har modtaget uddannelse og oplysning om datasikkerhed

48%

Persondatabeskyttelse

Medarbejderne har modtaget undervisning eller oplysning om politik og procedurer

Dataetik

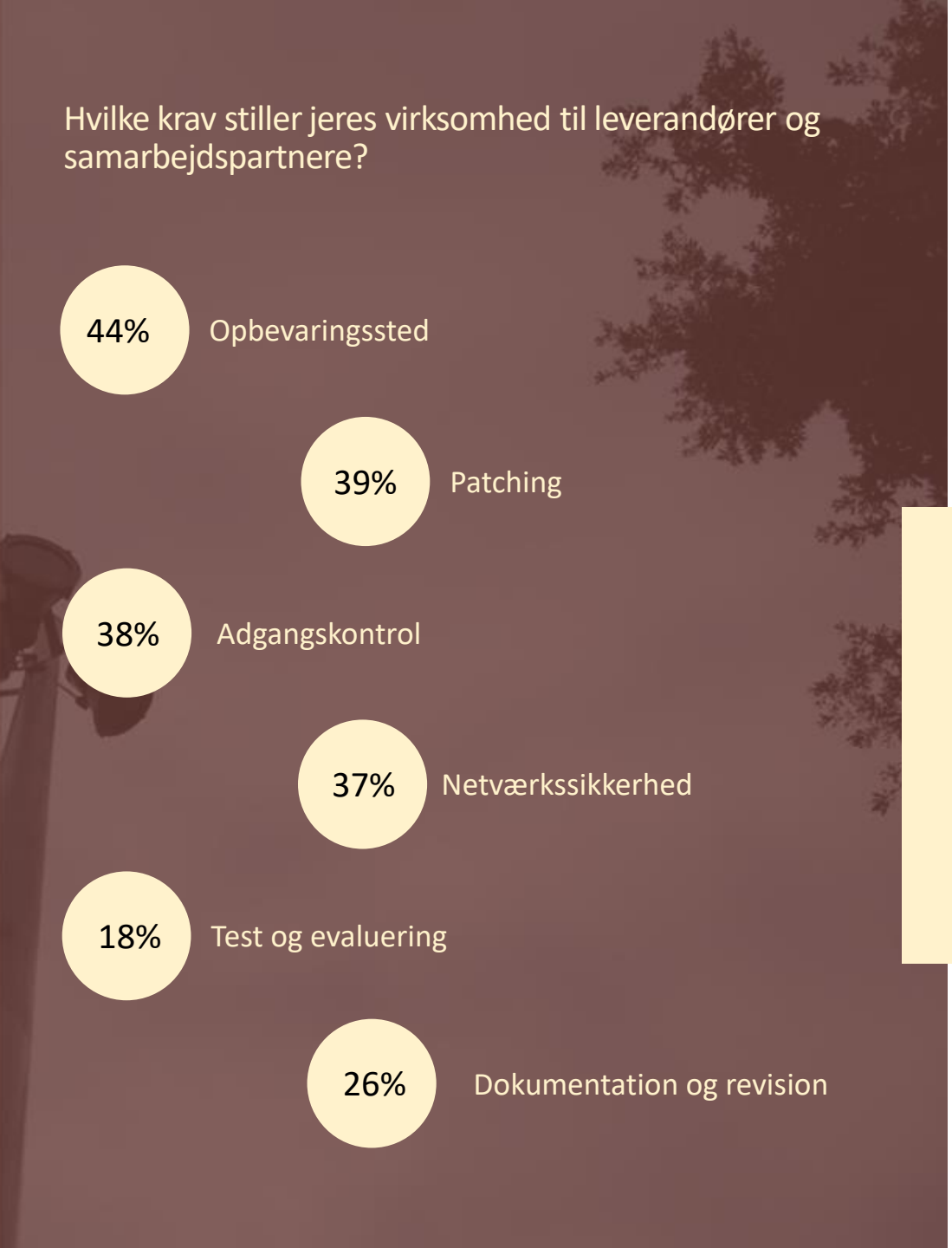
61%
ved ikke

8%	Workshops
15%	Infomateriale
12%	Løbende skriftlig påmindelse på intranet
8%	Tjeklister til udviklere, indkøbere, compliance, revision

Rådet for Digital Sikkerhed · Digital · IT-BRANCHEN · Erhvervsstyrelsen · Industriens Fond – The Danish Industry Foundation

Virksomhedernes leverandører – har de styr på det?

Sårbarheder hos leverandører udgør en it-sikkerhedsrisiko, men under halvdelen af virksomhederne stiller krav til leverandørerne



Virksomhedernes leverandørkrav til it-sikkerhed afspejler mange af de indsatser, virksomhederne selv har indført.
Men svarene viser, at under halvdelen ved, hvor deres leverandører opbevarer data. Lidt færre stiller krav om netværkssikkerhed, patching og adgangskontrol.
En mindre andel stiller krav om, at leverandøren udfører test og evaluering af deres sikkerhedsforanstaltninger. Det samme gælder krav om, at leverandøren kan dokumentere eller vise revisionserklæringer for deres it-sikkerhed.

Persondatabeskyttelse er også relevant hos leverandører og databehandlere – det har omkring halvdelen styr på

Leverandørers behandling af persondata og overførsel til tredjelande udgør en særlig risiko for kunderne på grund af spredningen af deres data udenfor EU. Risikoen er øget efter EU-Domstolens afgørelse i Schrems II-sagen, som erklærer USA for et usikkert tredjeland.

En større andel af virksomhederne har indgået databehandleraftaler, mens mindre end en tredjedel ved, om leverandører overfører data til lande udenfor EU. I det lys er det bemærkelsesværdigt, at 35% har svaret, at de har udarbejdet en analyse af beskyttelsesniveauet i usikre modtagerlande.

Har jeres virksomhed kortlagt, om jeres leverandører overfører personoplysninger til lande udenfor EU?

61% Har indgået databehandleraftaler

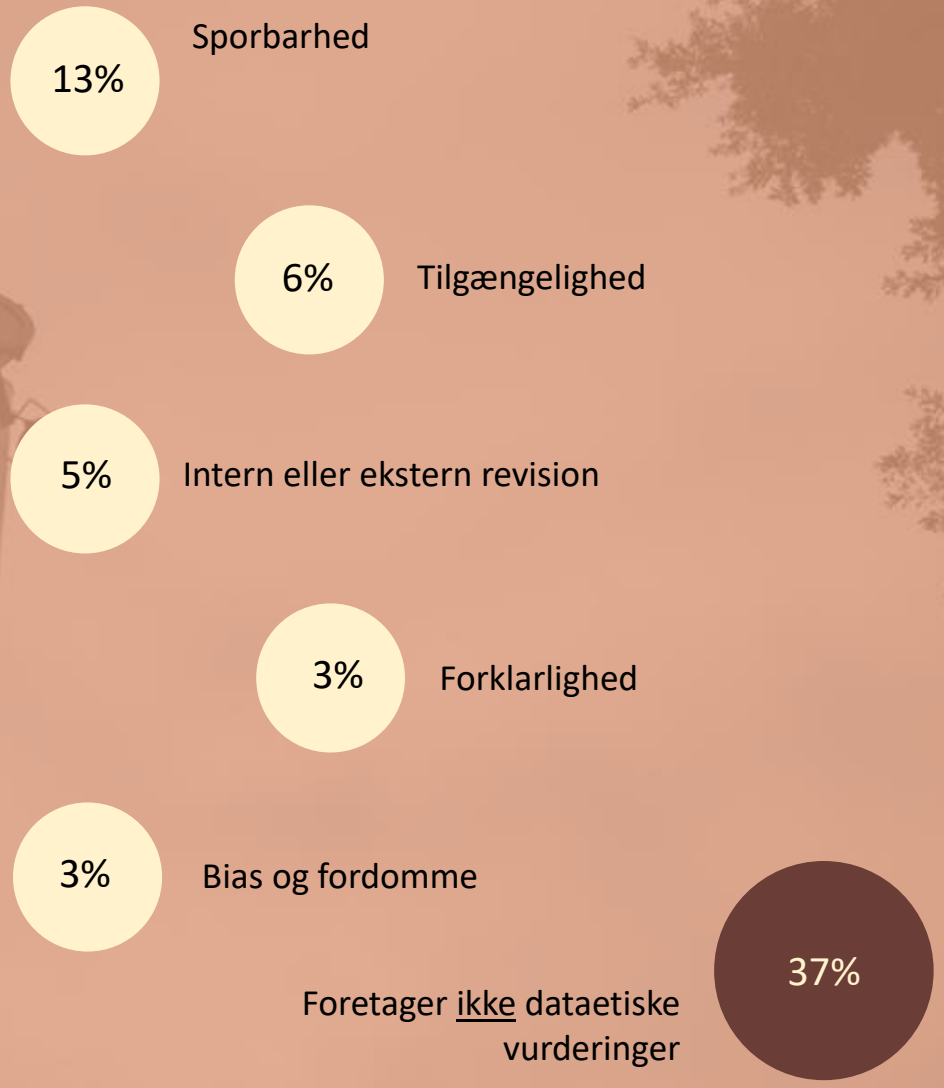
35% Har udarbejdet en analyse af overførsler til tredjelande

30% Har kortlagt, om leverandører overfører personoplysninger til lande udenfor EU

Har ikke eller kun delvist kortlagt, om leverandører overfører personoplysninger til lande udenfor EU 43%

Sporbarhed har en lille betydning for leverandørvalget – men ellers er dataetiske vurderinger ikke udbredt

Hvilke dataetiske vurderinger foretager jeres virksomhed af leverandører af teknologi eller databehandling?

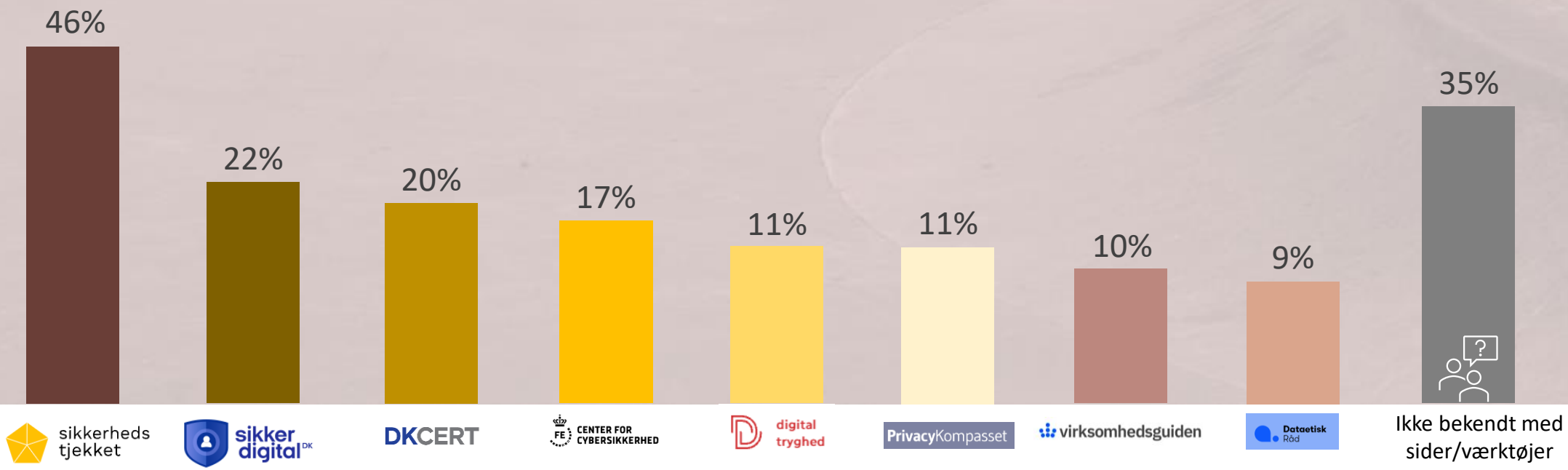


Virksomhederne er ikke rigtig kommet i gang med at stille dataetiske krav til deres leverandører. Leverandørkrav om afdækning af bias og fordomme, der kan føre til diskrimination, benyttes kun af en meget begrænset andel af virksomhederne. Det samme gælder krav om, at leverandørerne kan forklare deres algoritmers variabler og det output, de giver.

Krav om intern eller ekstern revision og vurdering af tilgængelighed til software, der benyttes til kundekontakt, stilles også kun i ringe omfang. Lidt flere virksomheder vurderer, om anvendte datakilder og datasæt er sporbare.

Kender virksomhederne de tilgængelige værktøjer?

Virksomhederne har et sparsomt kendskab til mange af de relevante hjemmesider og værktøjer, der er tilgængelige



Kontaktoplysninger

Partnerne bag projektet og kontaktoplysninger

Undersøgelsen er udarbejdet af Carve Consulting for
Rådet for Digital Sikkerhed, DI, D-mærket, IDA og IT-Branchen i samarbejde med Erhvervsstyrelsen fra september til oktober 2021

Projektet er støttet af:
INDUSTRIENS FOND FREMMER DANSK KONKURRENCEEVNE
The Danish Industry Foundation

Fotoakkreditering
Forsidebillede af Pedro José Borges
Øvrige billeder af Ernst Tobisch

Spørgsmål til projektet og undersøgelsens resultater rettes til:

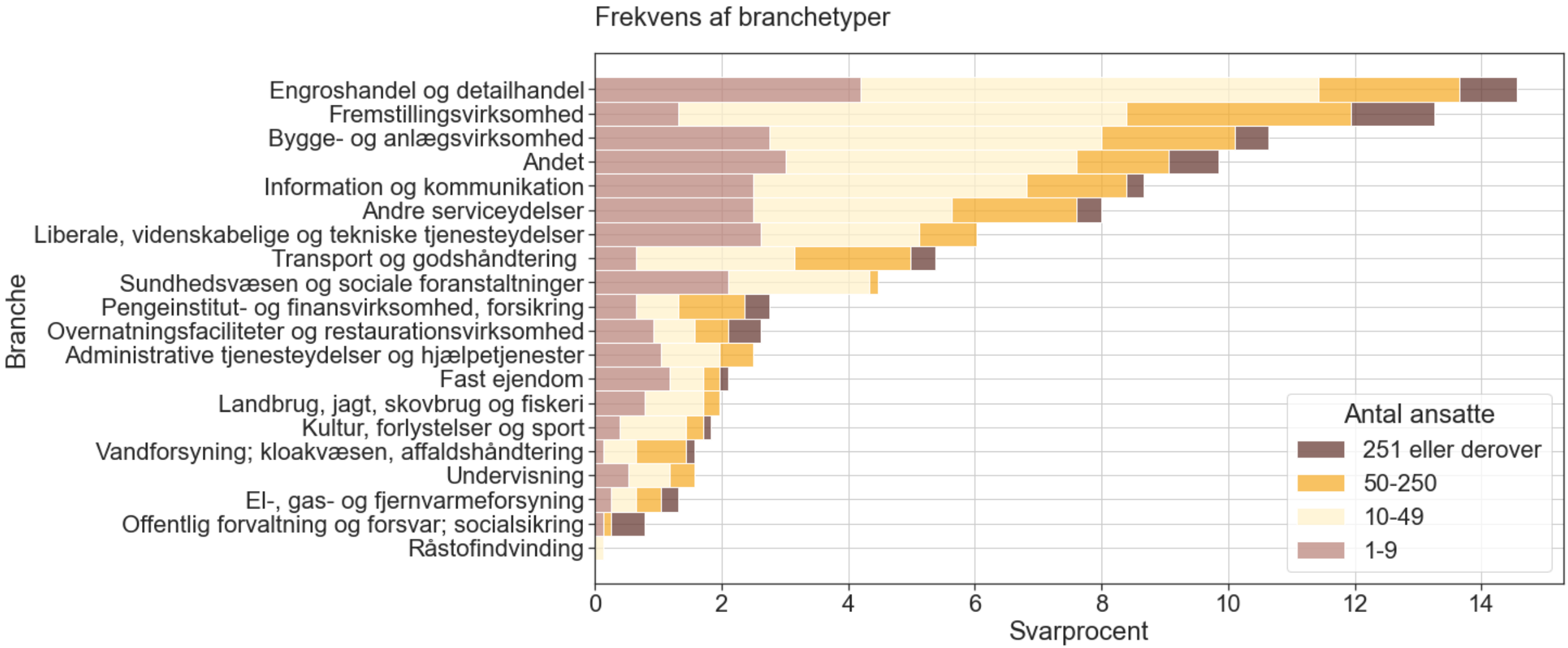
Henning Mortensen, Formand for Rådet for Digital Sikkerhed

Anna Bay Damholt, Sekretariatschef for Rådet for Digital Sikkerhed

Birgitte Kofod Olsen, Partner, ph.d., Carve Consulting

Bilag

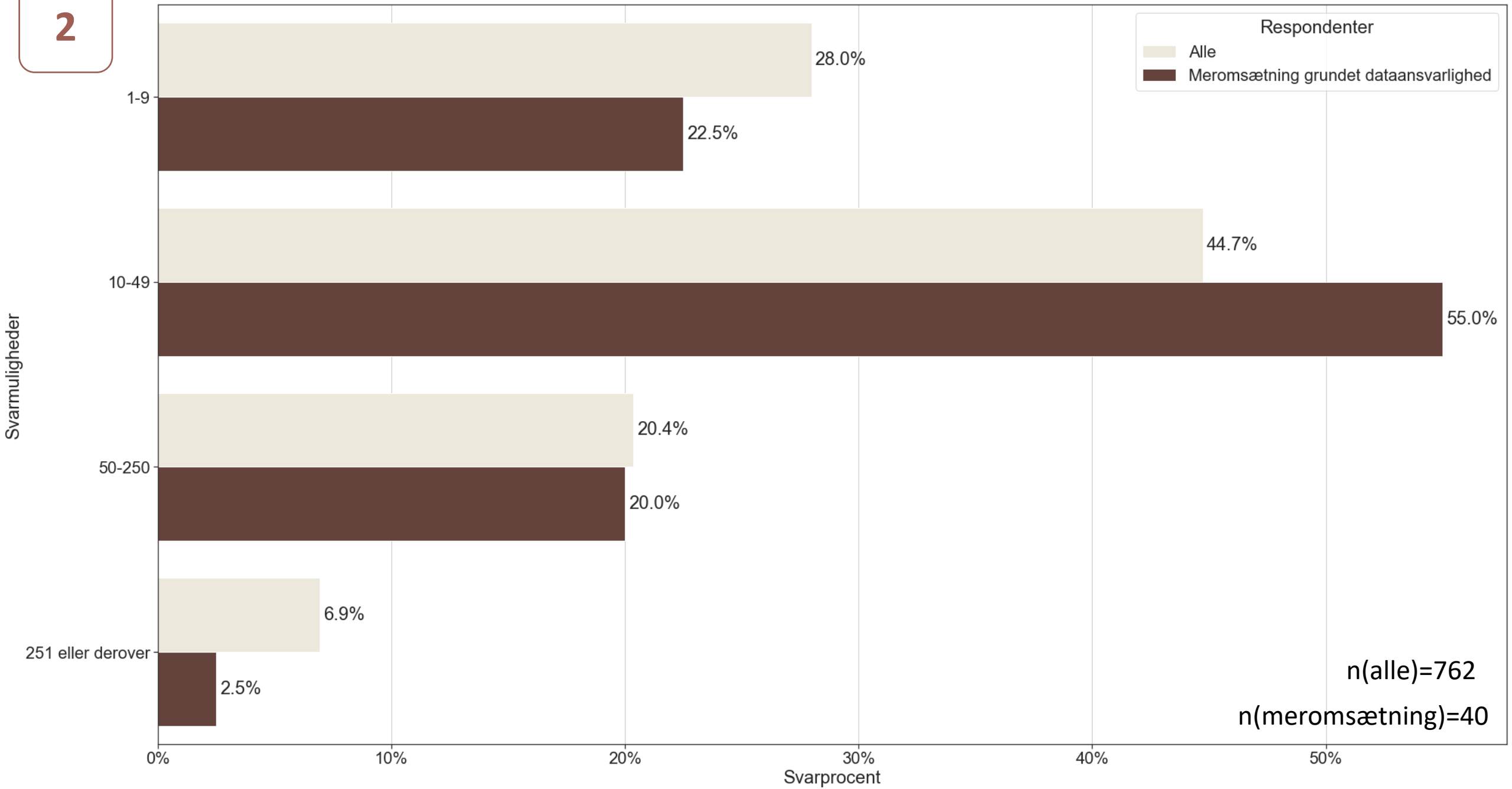
1


Frekvens af branchetyper
Branche
Engroshandel og detailhandel
Fremstillingsvirksomhed
Bygge- og anlægsvirksomhed
Andet
Information og kommunikation
Andre serviceydelser
Liberale, videnskabelige og tekniske tjenesteydelser
Transport og godshåndtering
Sundhedsvæsen og sociale foranstaltninger
Pengeinstitut- og finansvirksomhed, forsikring
Overnatningsfaciliteter og restaurationsvirksomhed
Administrative tjenesteydelser og hjælpetjenester
Fast ejendom
Landbrug, jagt, skovbrug og fiskeri
Kultur, forlystelser og sport
Vandforsyning; kloakvæsen, affaldshåndtering
Undervisning
El-, gas- og fjernvarmeforsyning
Offentlig forvaltning og forsvar; socialsikring
Råstofindvinding
0
2
4
6
8
10
12
14
Svarprocent
Antal ansatte
251 eller derover
50-250
10-49
1-9

n=771

2

Hvor mange ansatte er der i jeres virksomhed?

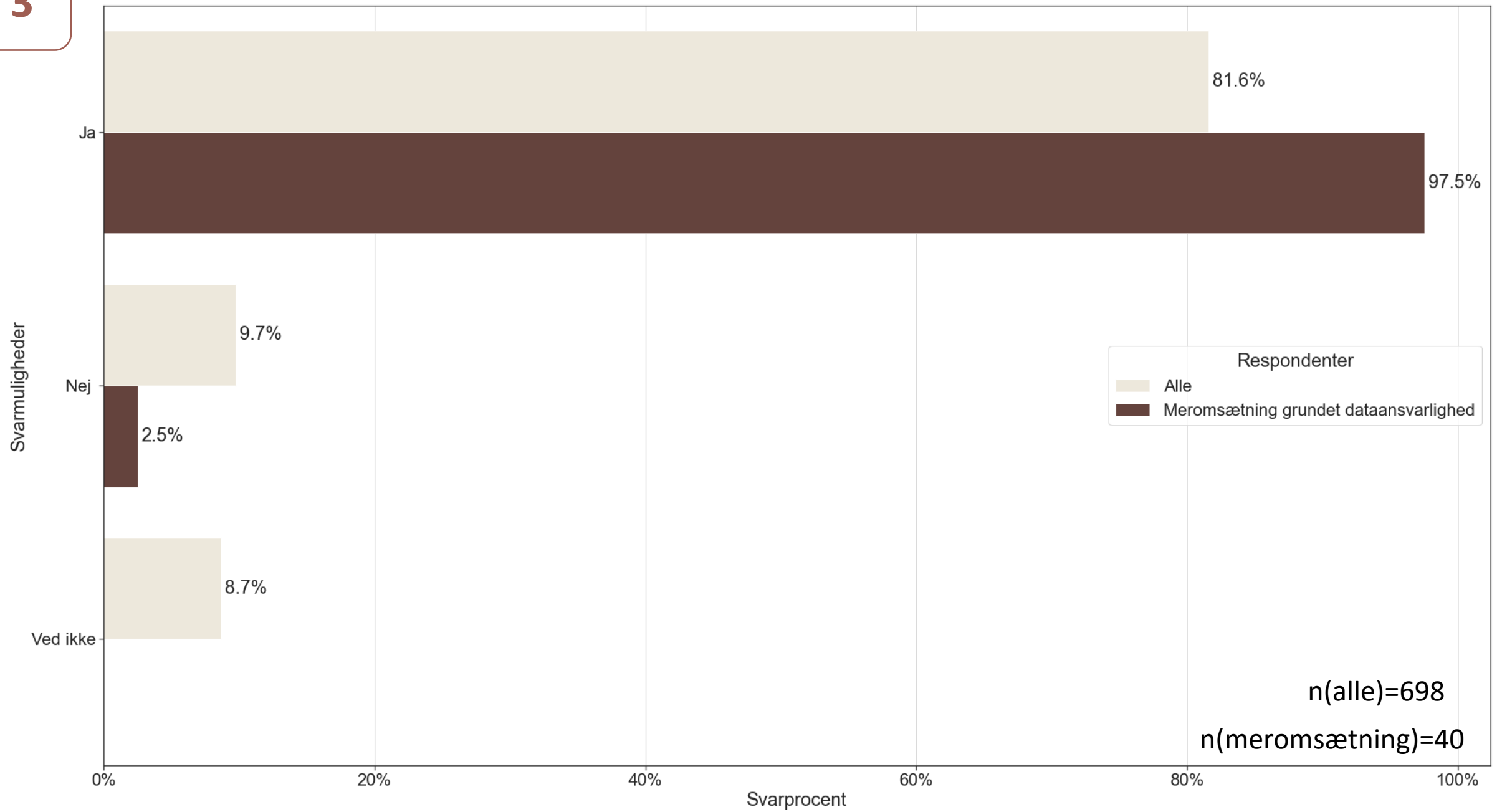


n(alle)=762

n(meromsætning)=40

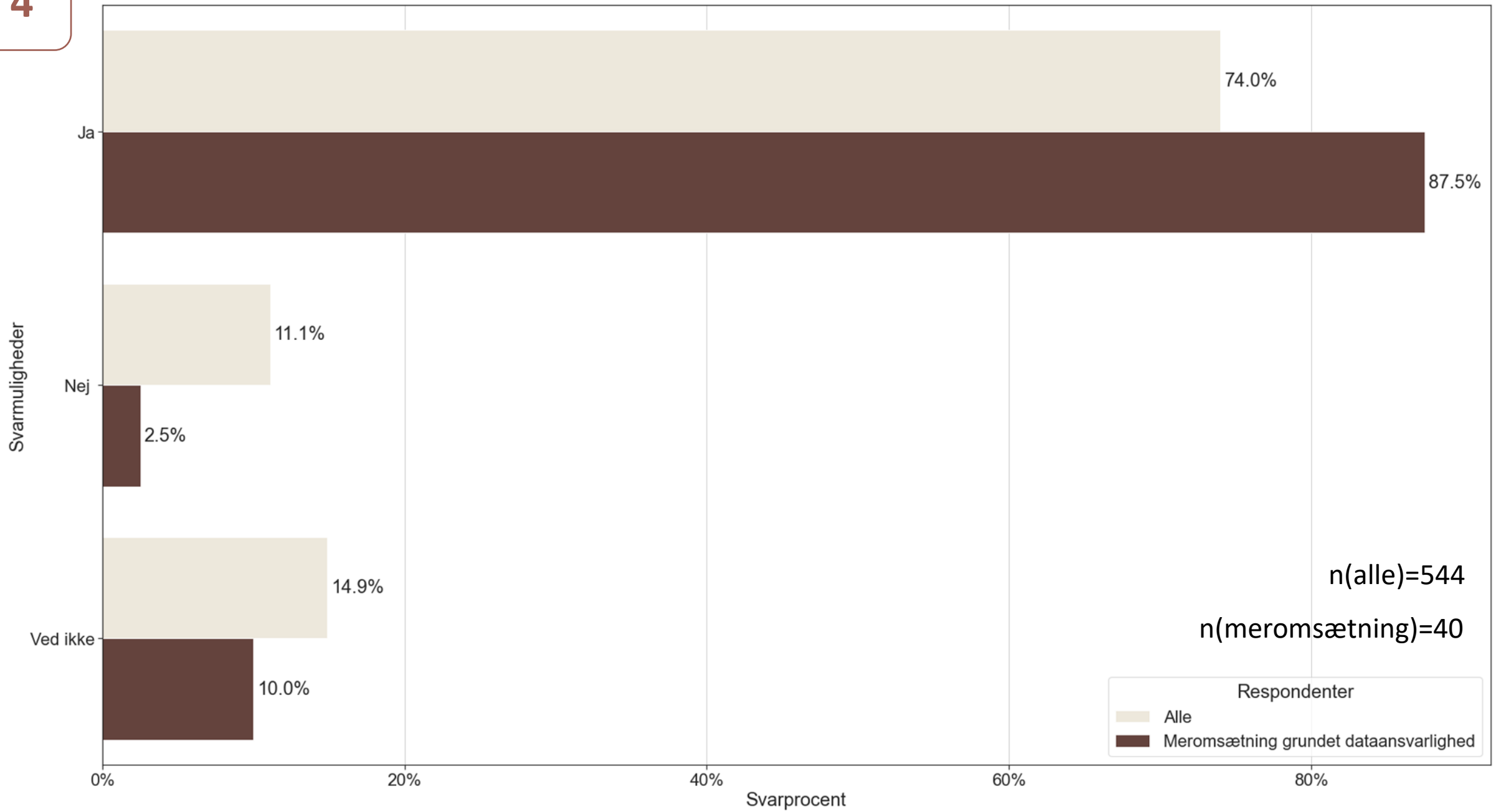
3

Har jeres virksomhed kortlagt de systemer, der håndterer forretningskritisk information, herunder følsomme og fortrolige personoplysninger?



4

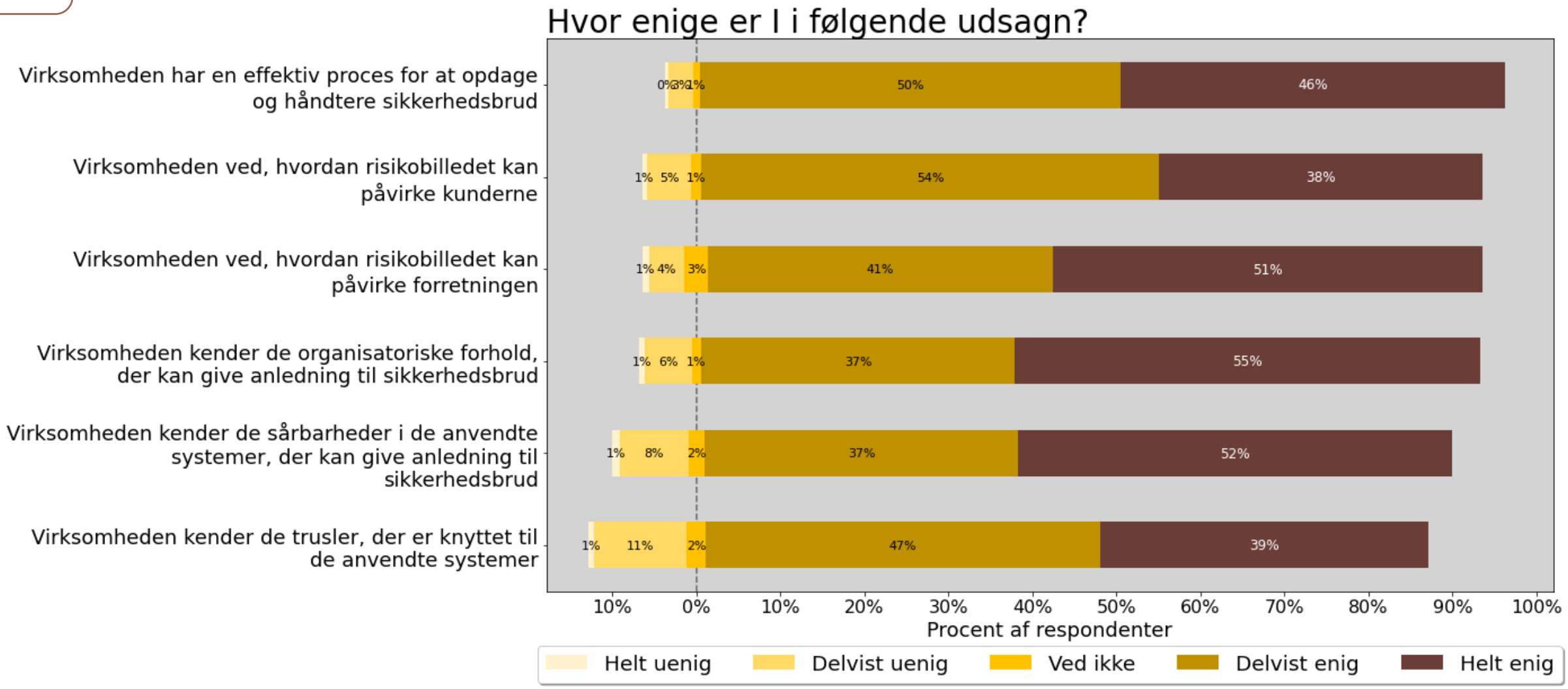
Kender I virksomhedens risikobillede? Dvs. de trusler, sårbarheder og forhold, der kan udgøre en risiko for it-sikkerheden



n(alle)=544

n(meromsætning)=40

5

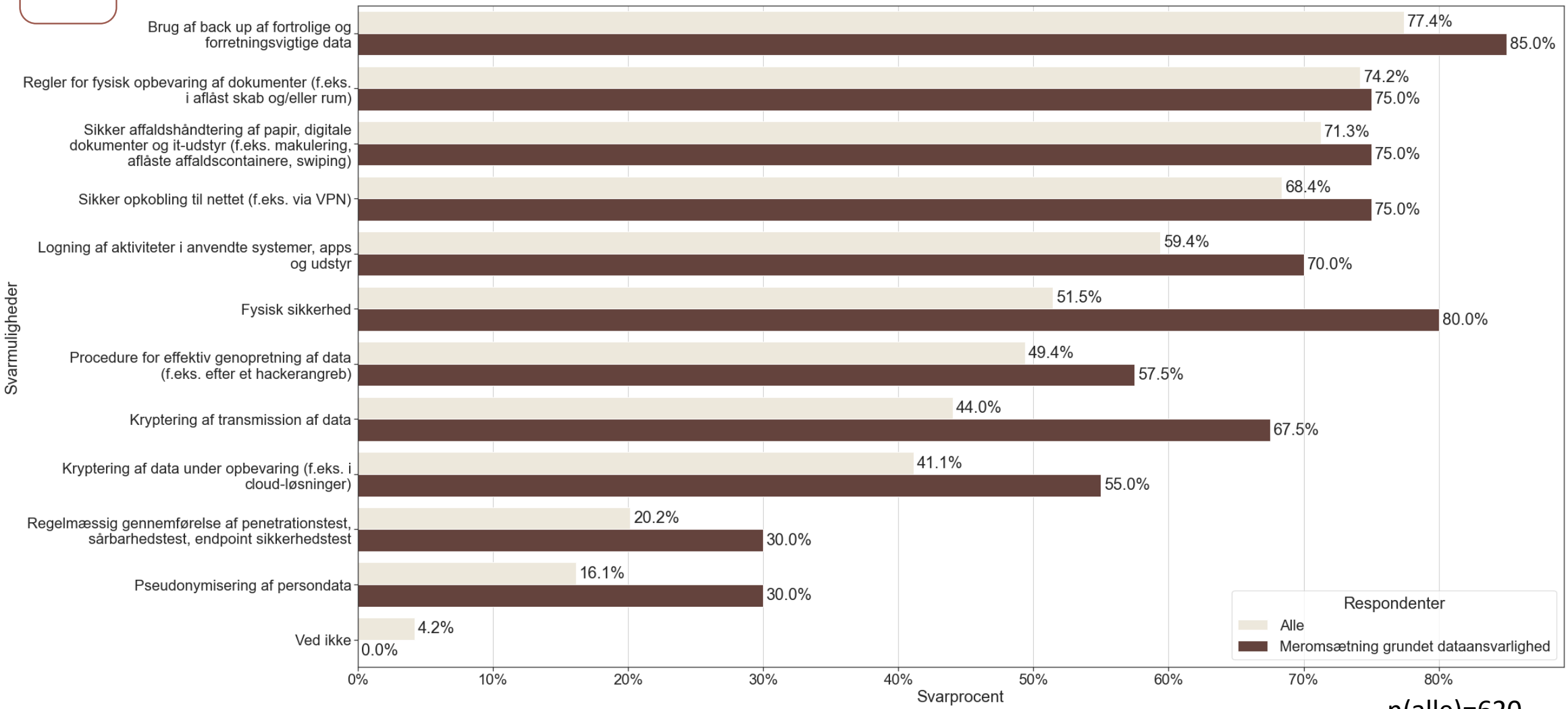


n=481

n(meromsætning)=40

6

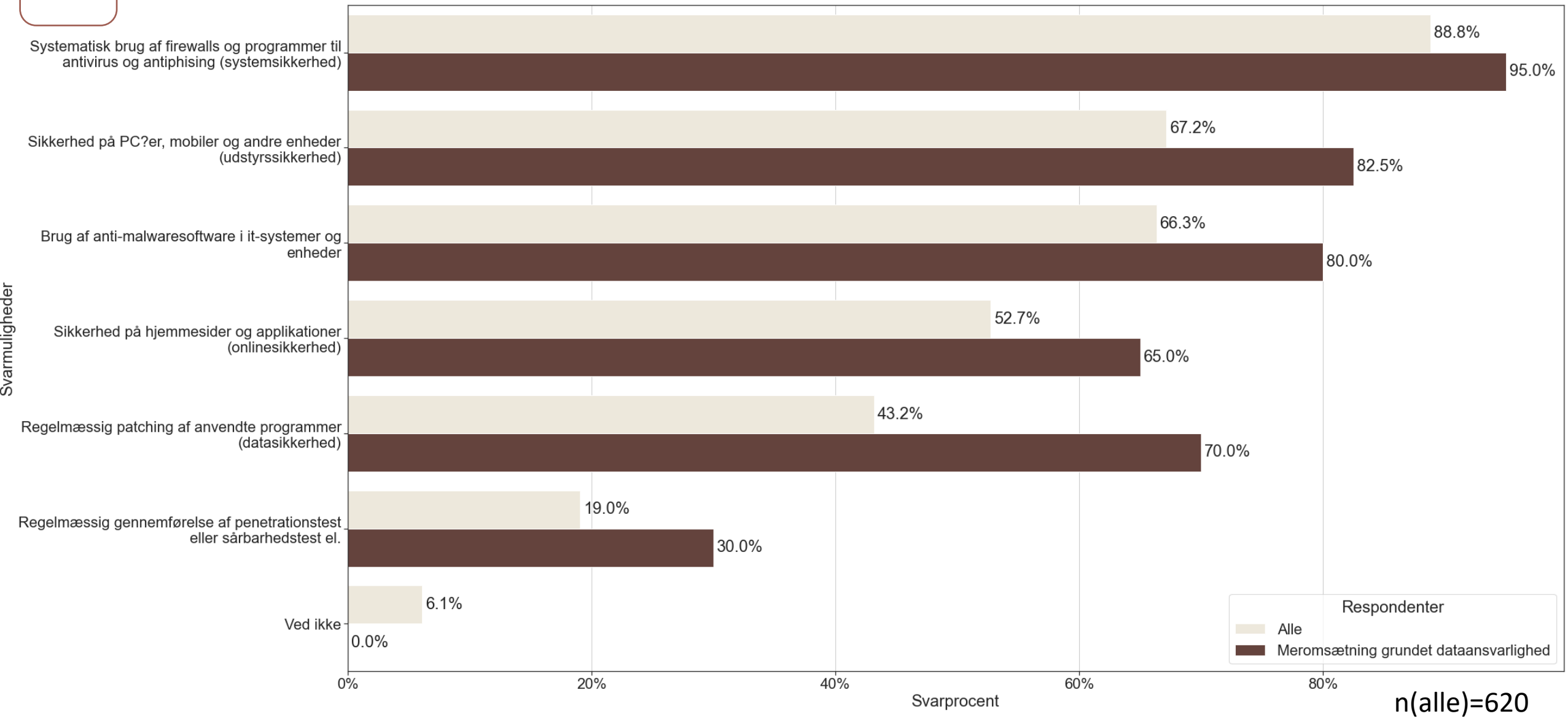
Hvilke sikkerhedsforanstaltninger har I implementeret i virksomheden? (Markér gerne flere)



n(alle)=620
n(meromsætning)=40

7

Hvordan sikrer jeres virksomhed, at jeres it-systemerne er svære at angribe? (Markér gerne flere)

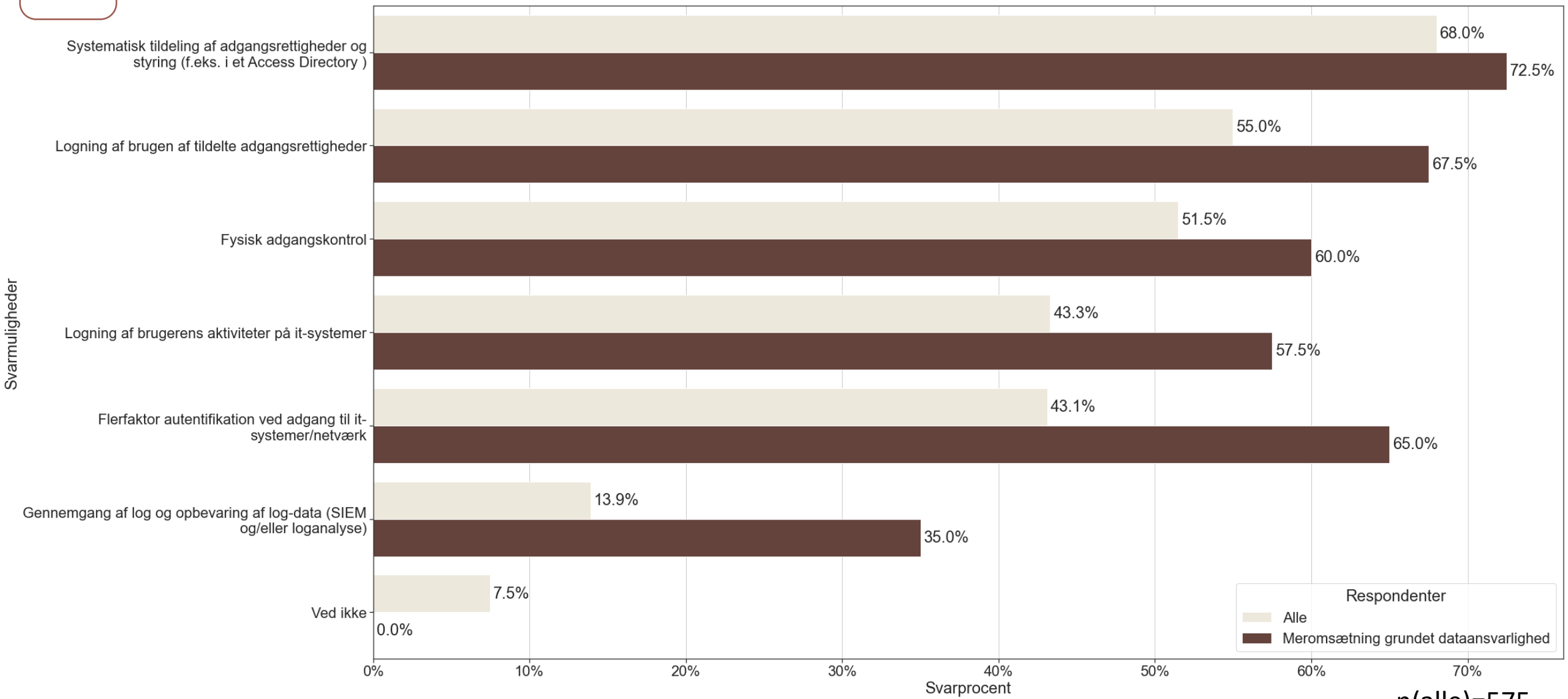


n(alle)=620

n(meromsætning)=40

8

Hvordan styrer I, hvem der har adgang til it-systemer og bygninger? (Markér gerne flere)

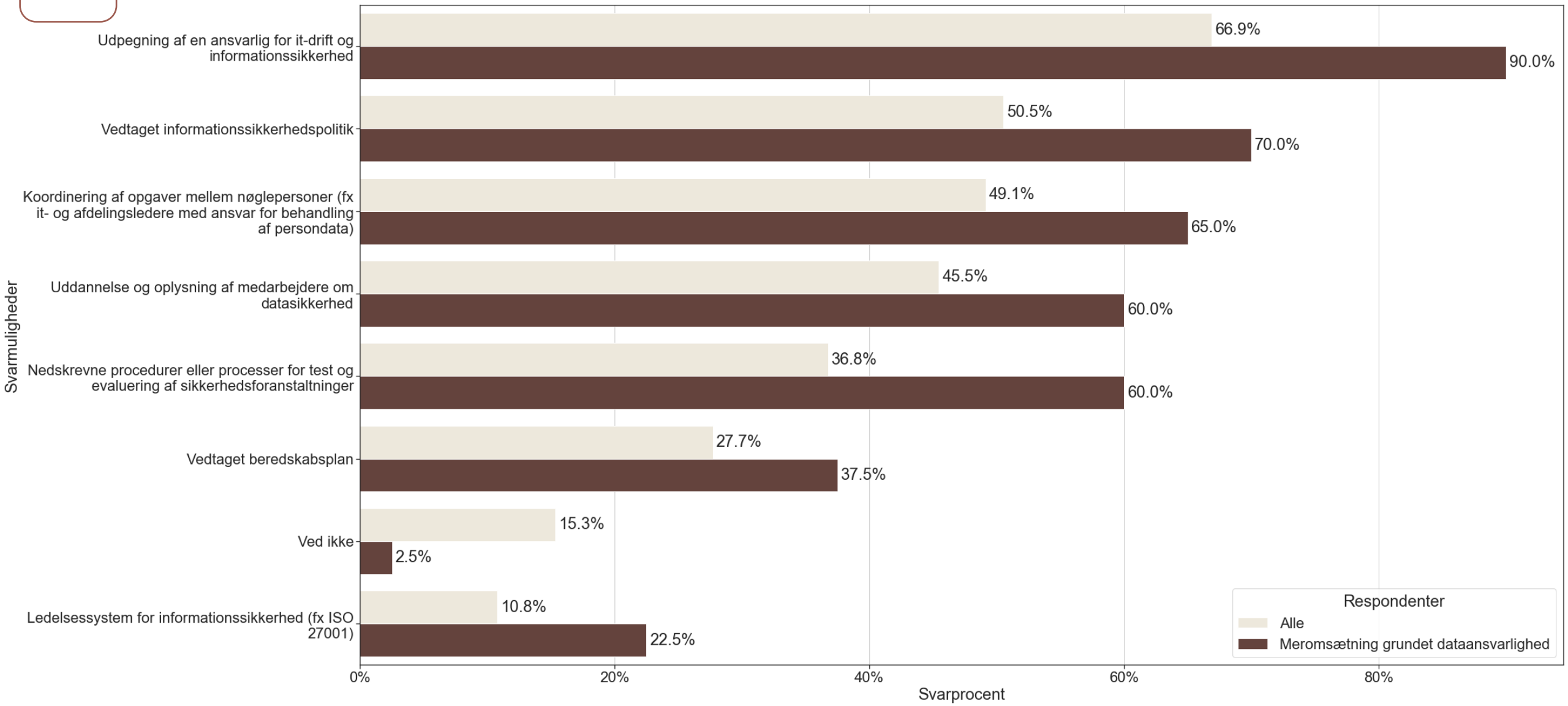


n(alle)=575

n(meromsætning)=40

9

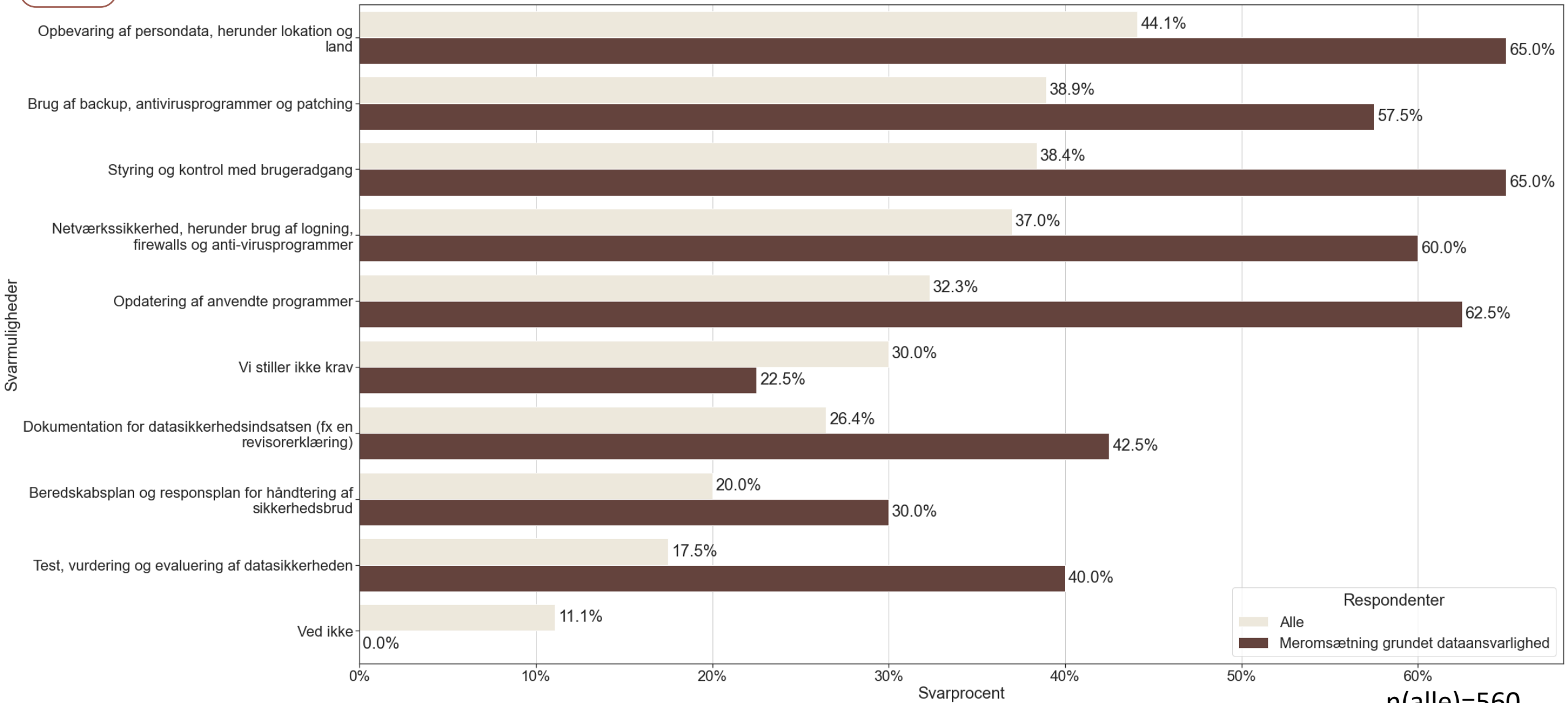
Hvordan er datasikkerhedsindsatsen forankret? (Markér gerne flere)



n(alle)=574
n(meromsætning)=40

10

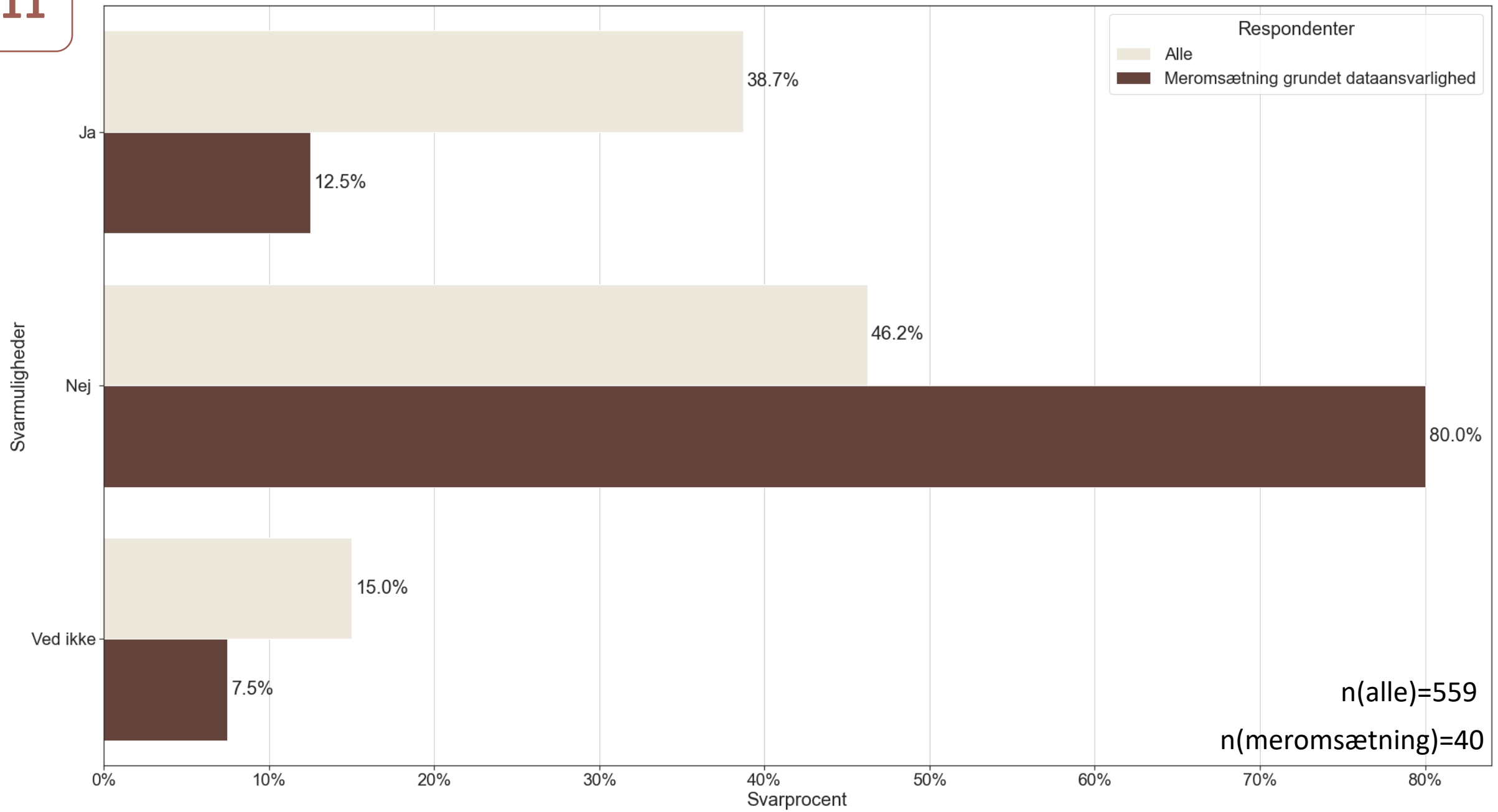
Hvilke krav stiller jeres virksomhed til leverandører og samarbejdspartnere? (Markér gerne flere)



n(alle)=560
n(meromsætning)=40

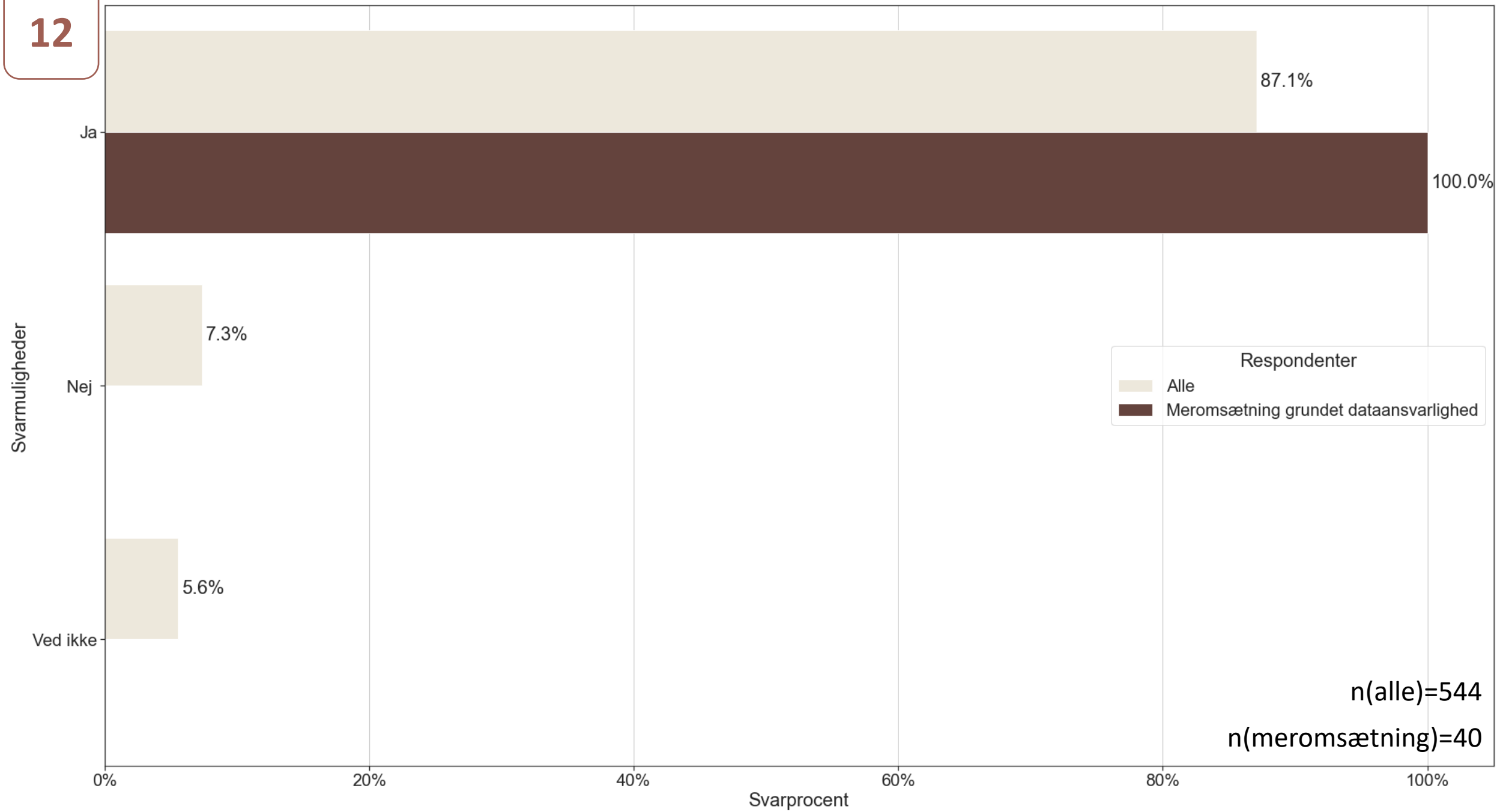
11

Er det jeres vurdering, at jeres datasikkerhedsniveau har betydning for virksomhedens konkurrenceevne?



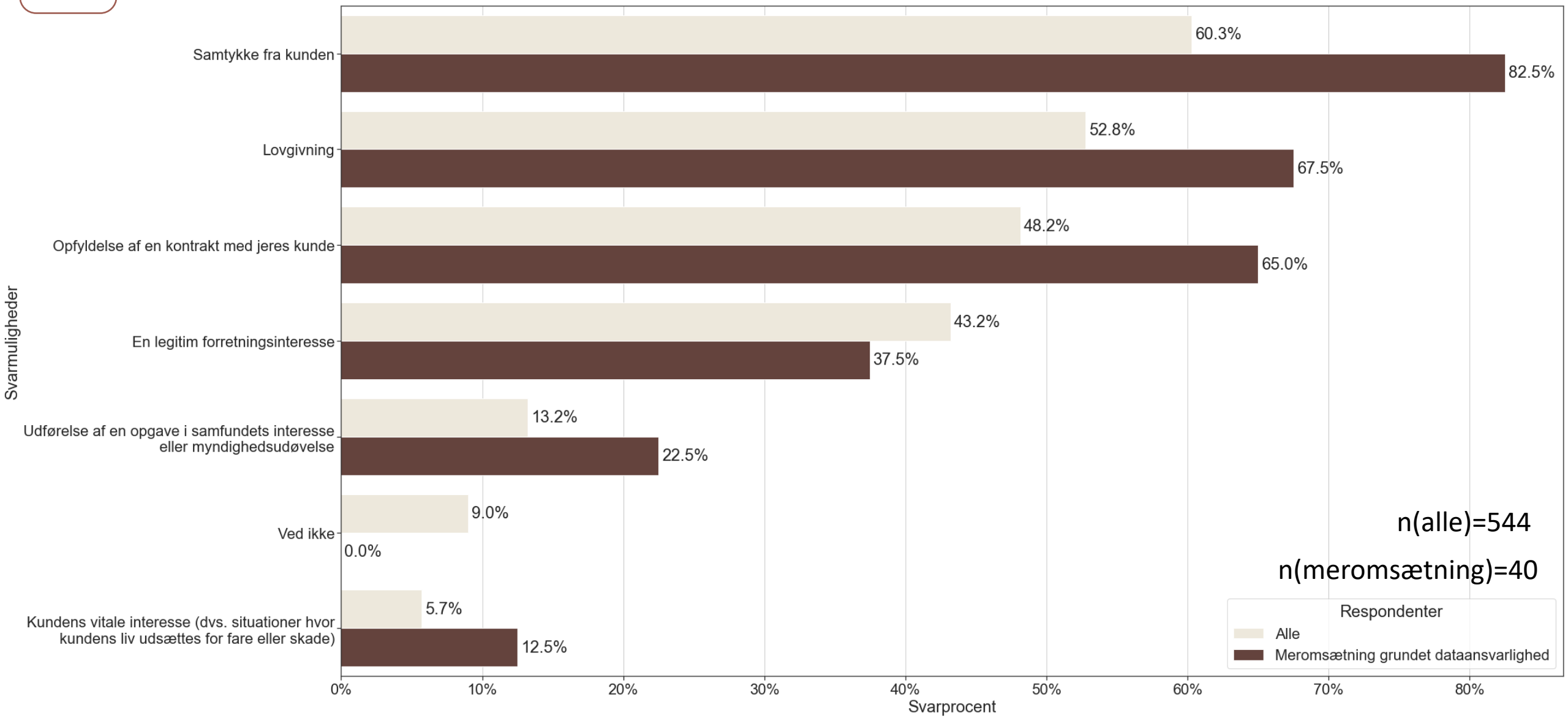
12

Har din virksomhed kortlagt hvilke personoplysninger, I behandler?

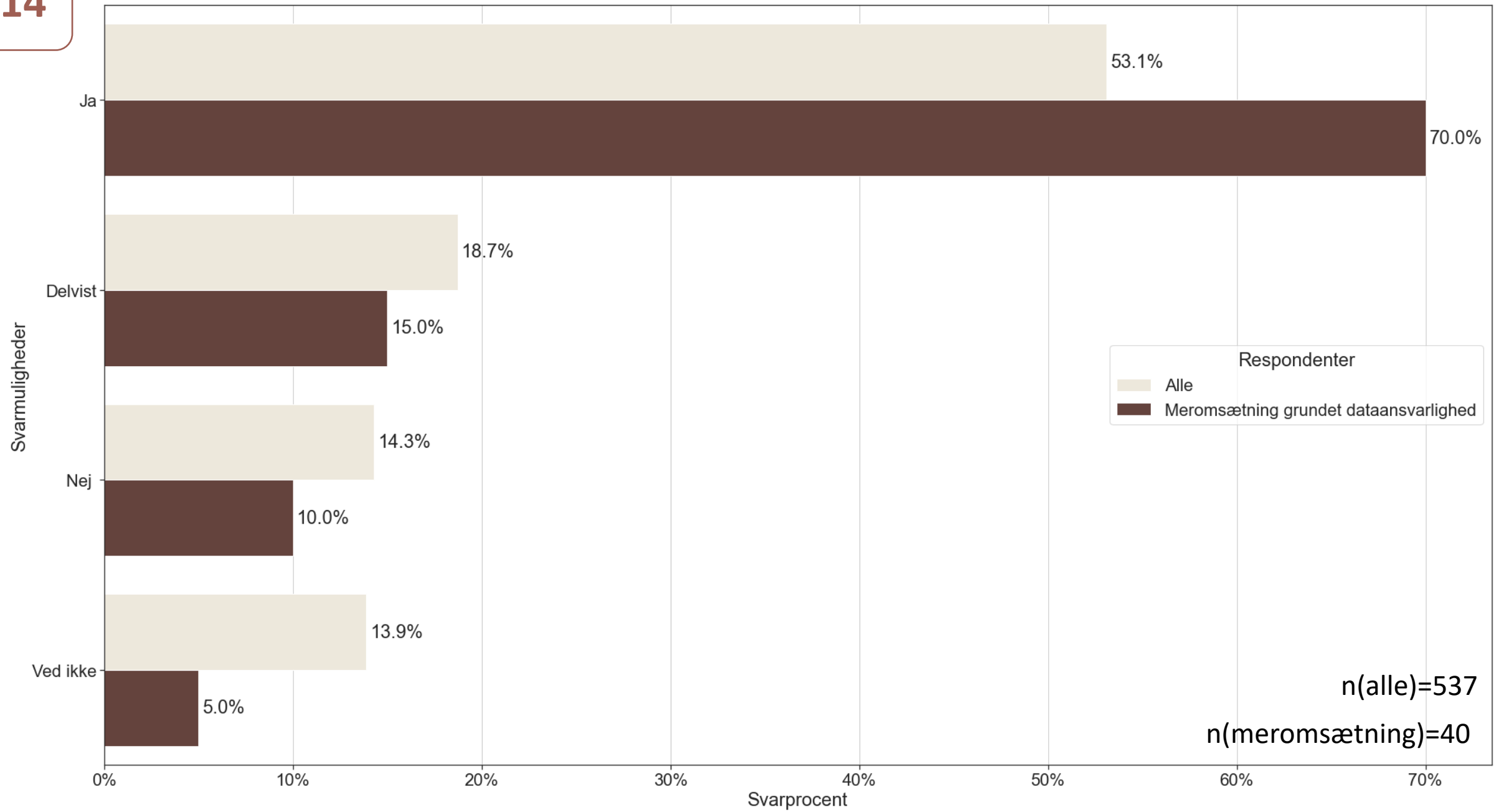


13

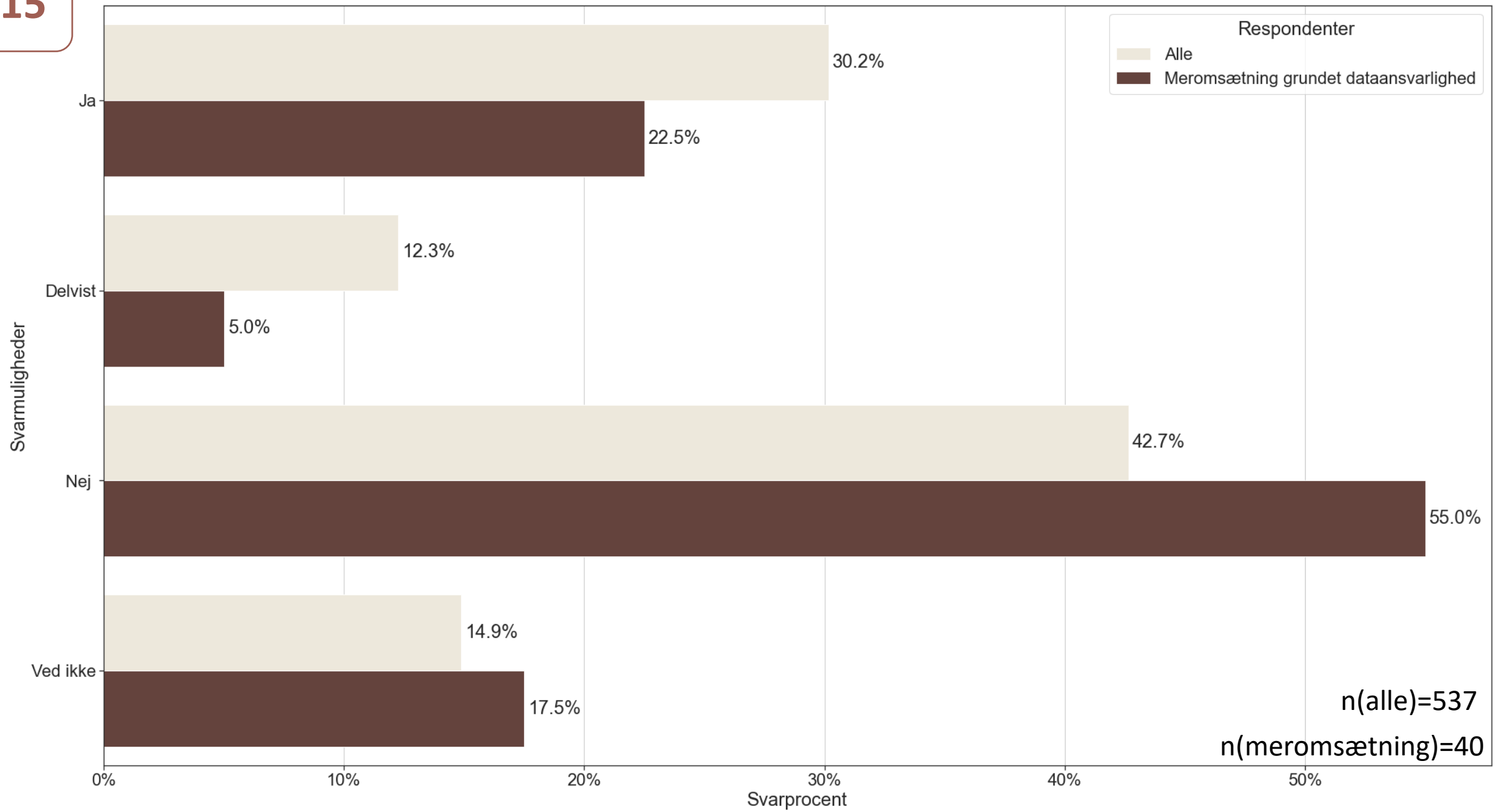
Hvilket lovligt grundlag er behandlingen af personoplysninger baseret på? (Markér gerne flere)



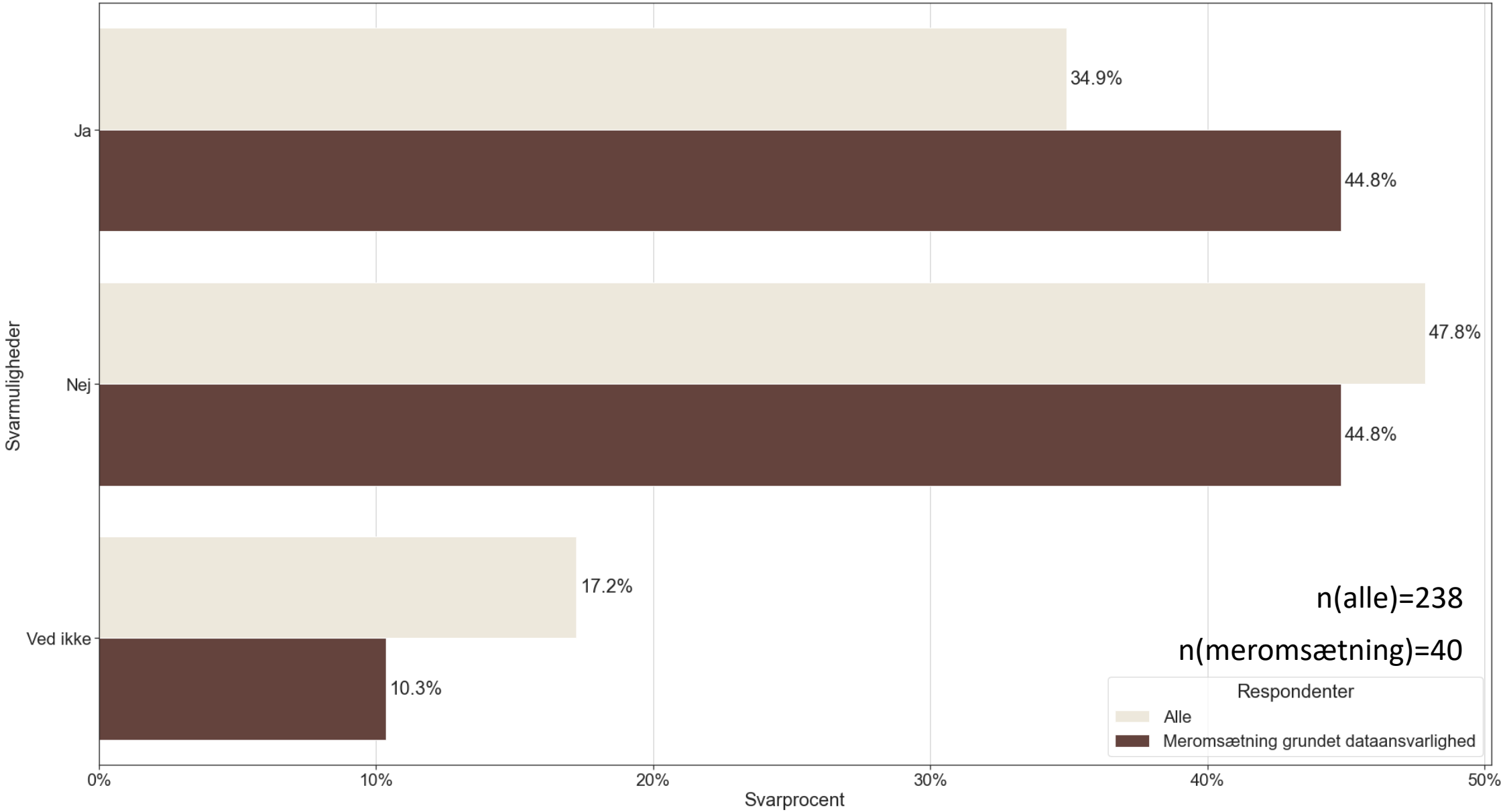
Anvender I princippet om dataminimering, når I vurderer hvilke data, I har brug for at indsamle eller behandle til et bestemt formål?



Har jeres virksomhed kortlagt om jeres leverandører overfører personoplysninger til lande udenfor EU?

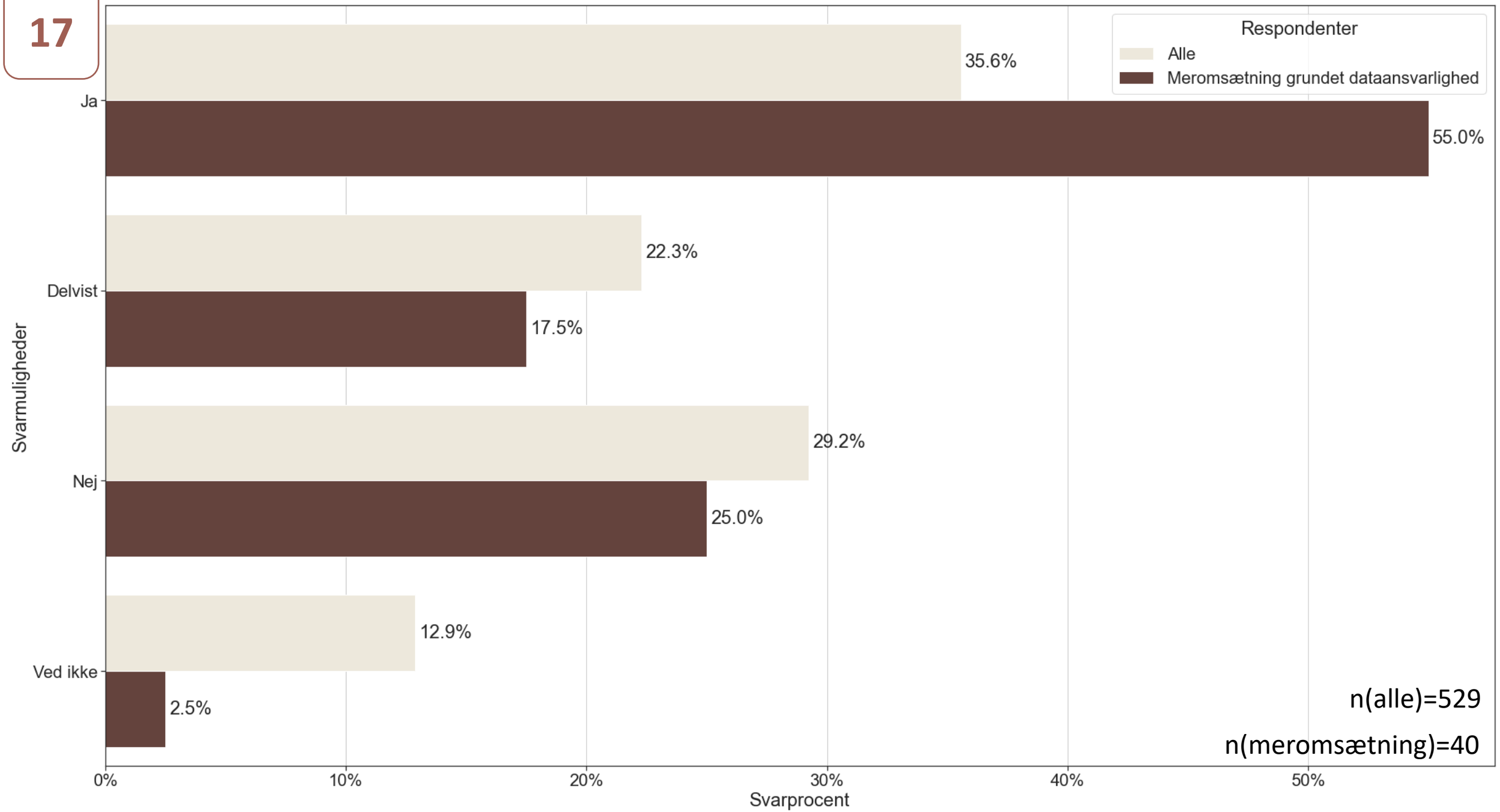


Har I udarbejdet en analyse af overførsler til usikre tredjelande (transfer impact assessment) (Usikre tredjelande er lande udenfor EU, der ikke er optaget på EU-Kommissionens liste over sikre tredjelande. Usikre tredjelande omfatter bl.a. Indien, Kina, Filippinerne, Rusland, Ukraine og USA)



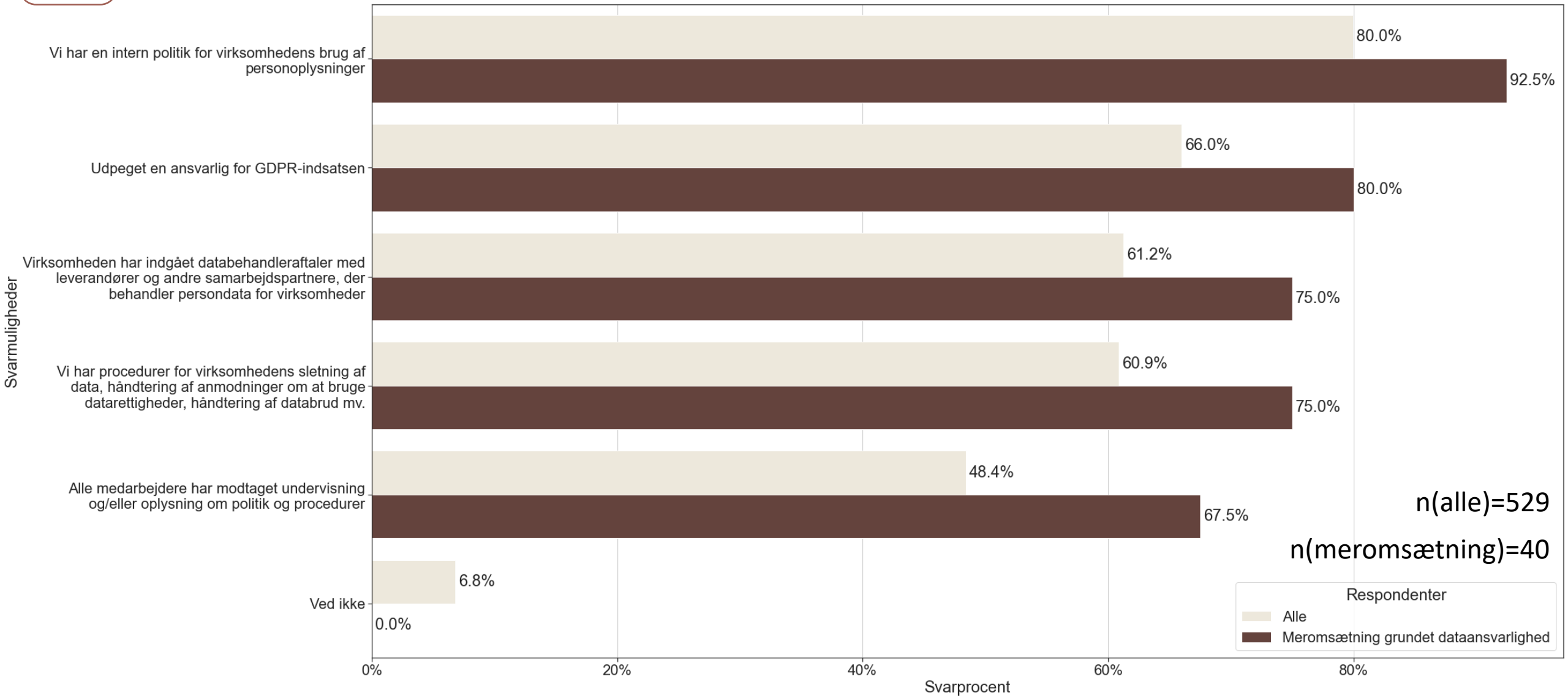
17

Har jeres virksomhed udført en persondataretlig risikovurdering?

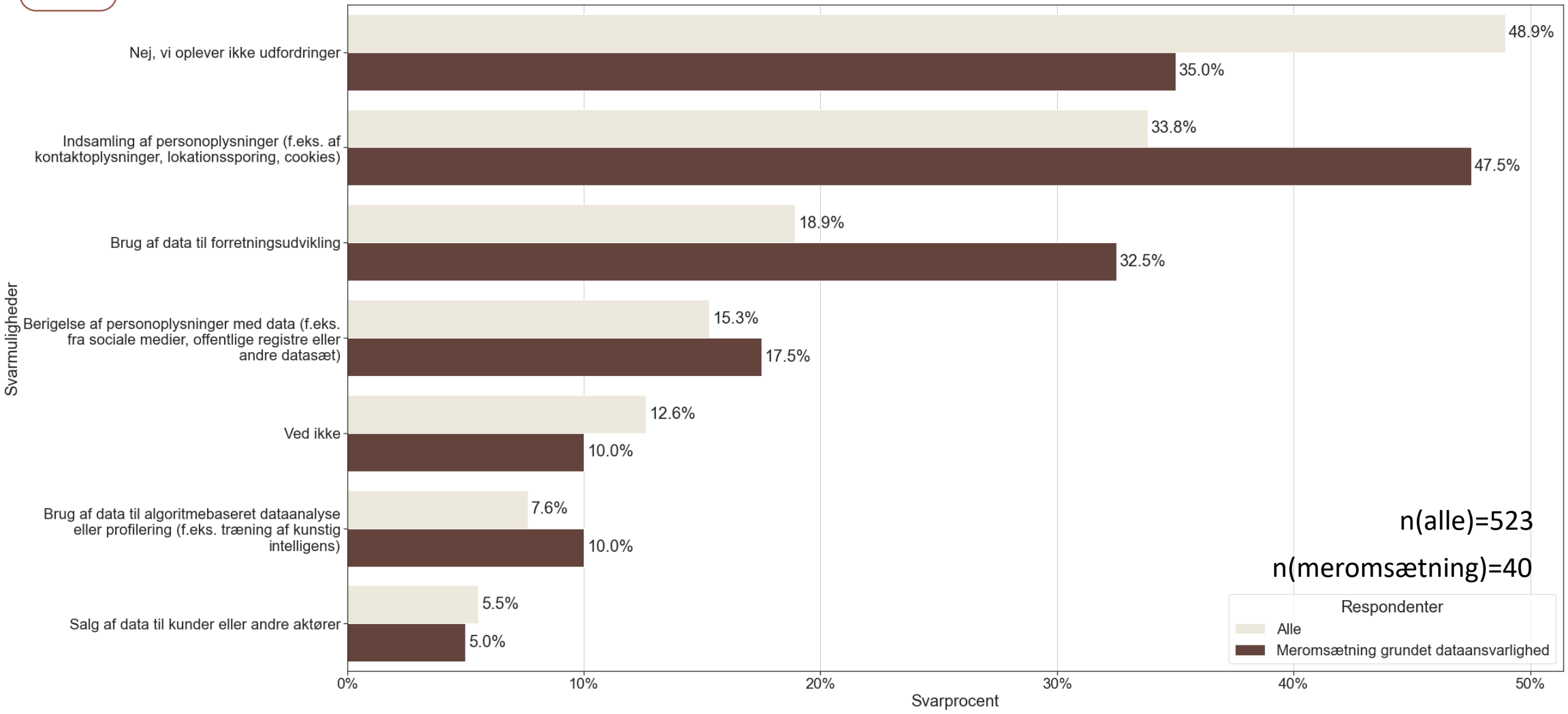


18

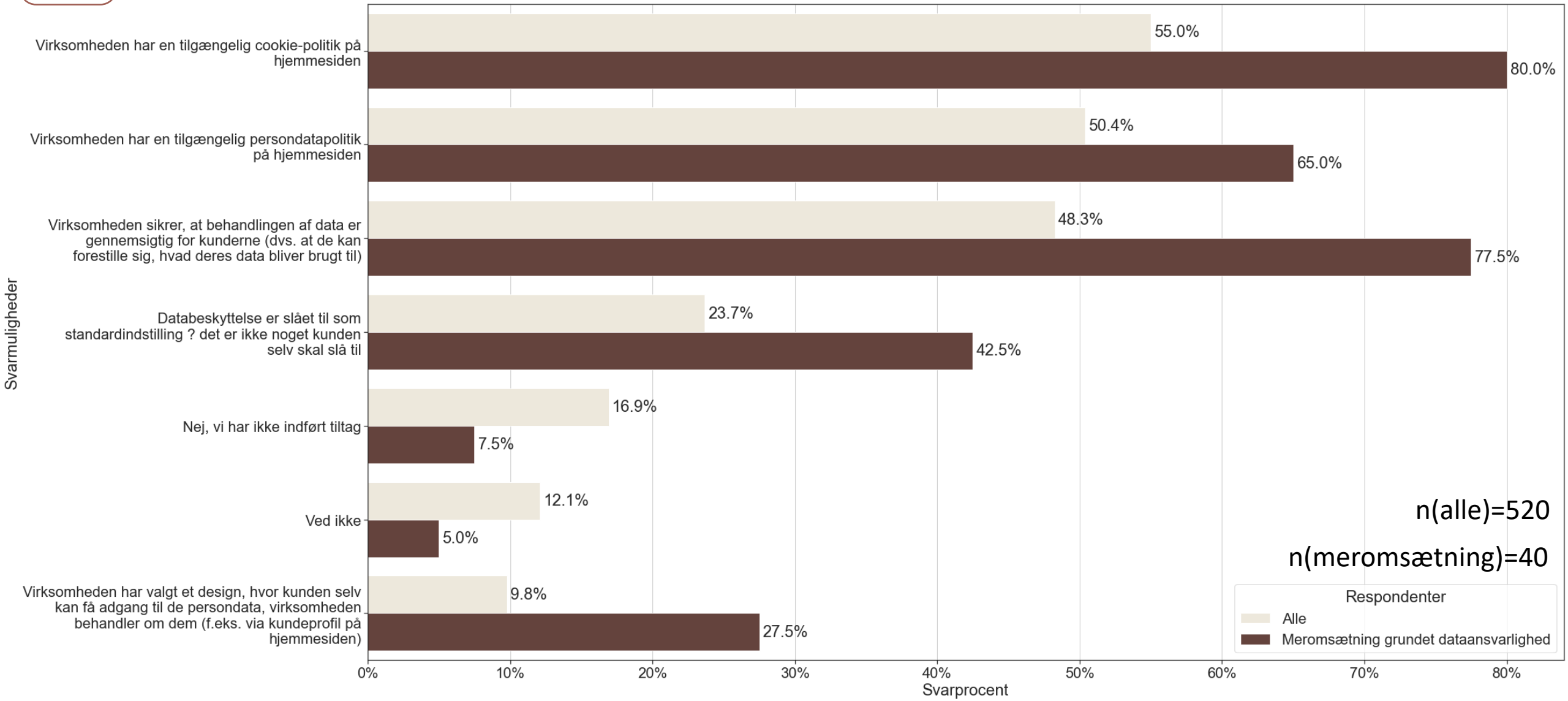
Hvordan har jeres virksomhed forankret arbejdet med persondatabeskyttelse? (Markér gerne flere)



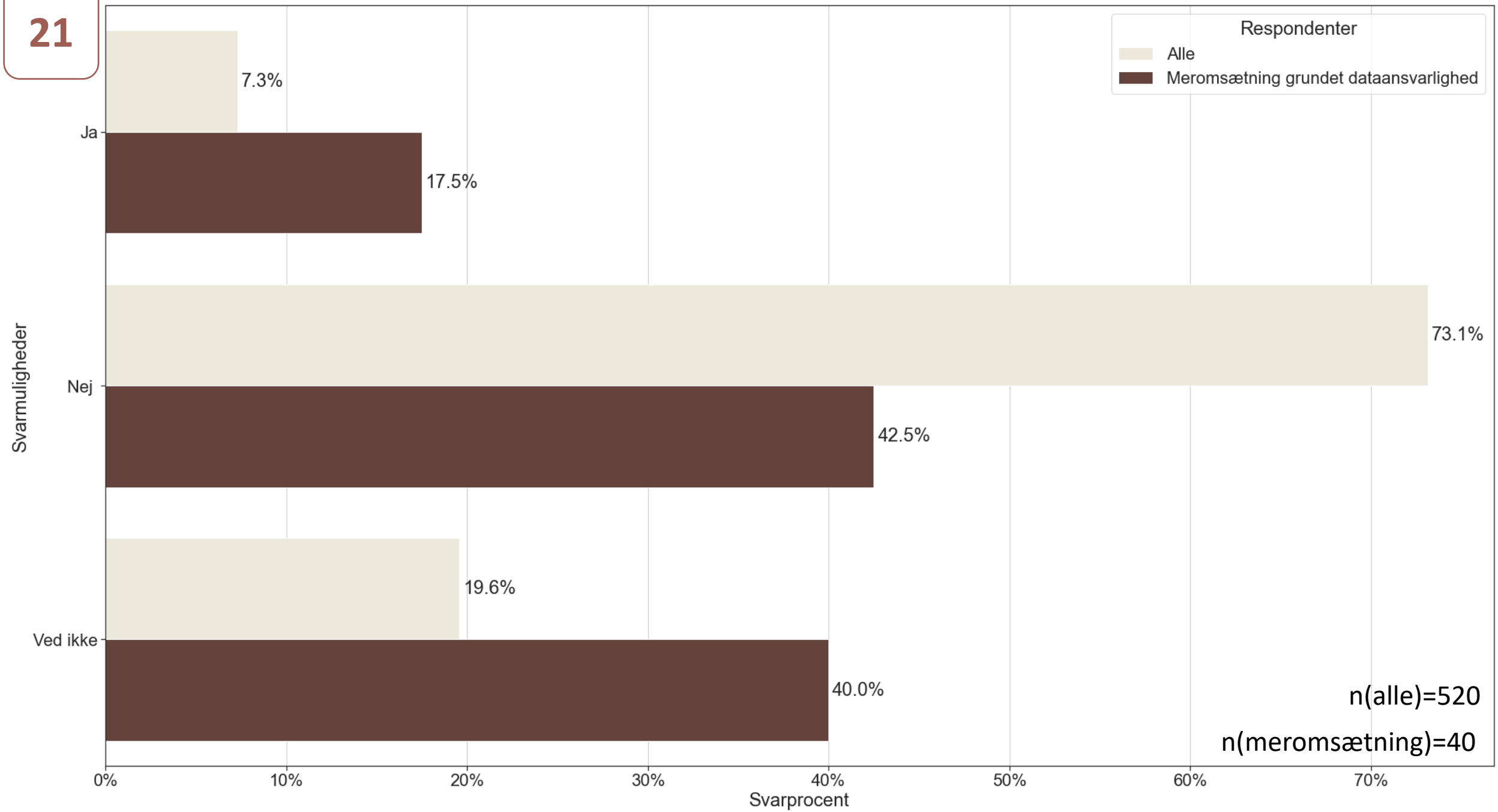
Oplever I, at lovkravene til persondatabeskyttelse har givet udfordringer i forhold til jeres: (Markér gerne flere)



Har jeres virksomhed indført nogle af nedenstående kunderettede tiltag? (Markér gerne flere)

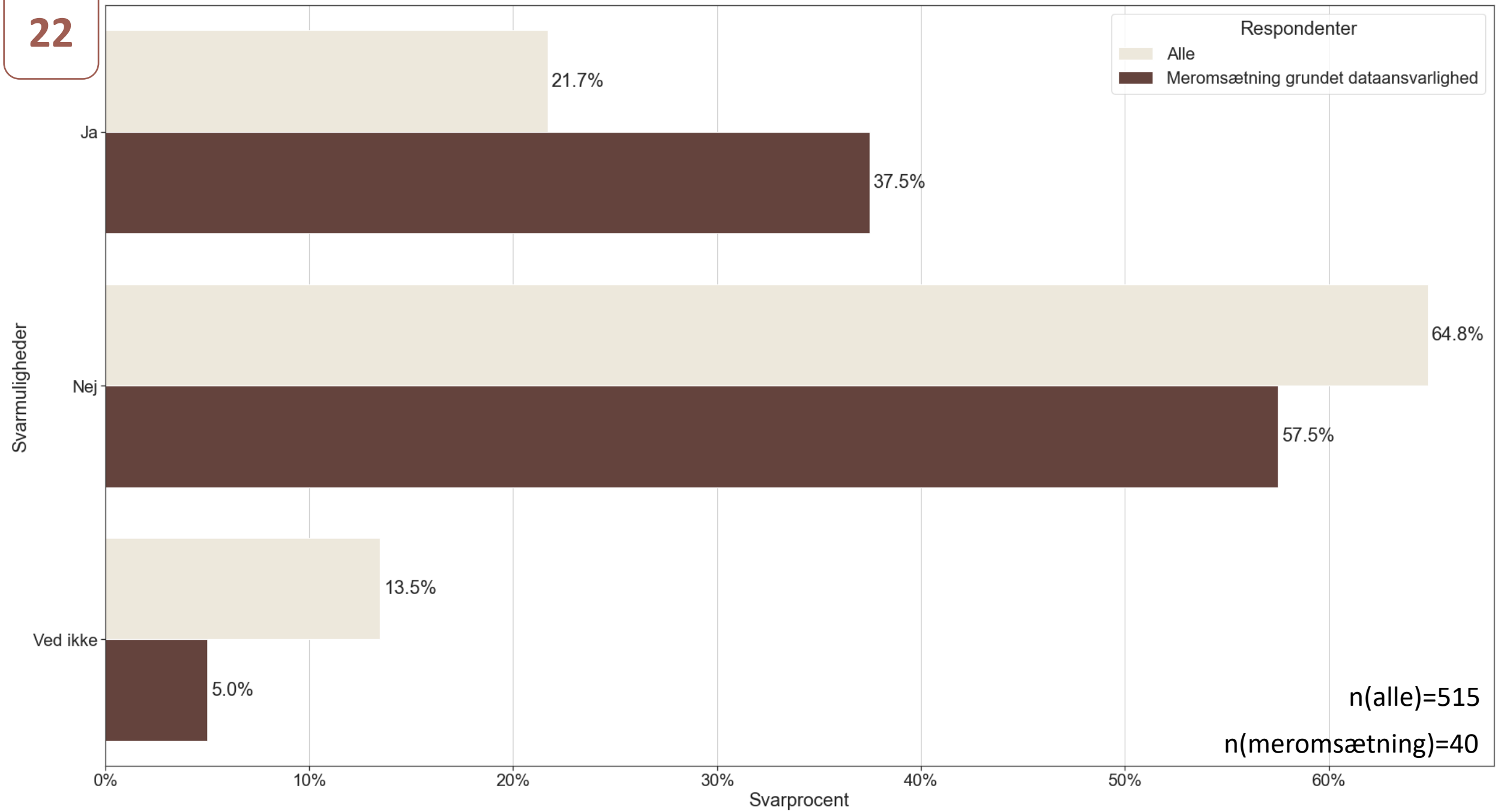


Oplever I, at jeres arbejde med persondatabeskyttelse forbedrer jeres konkurrenceevne?

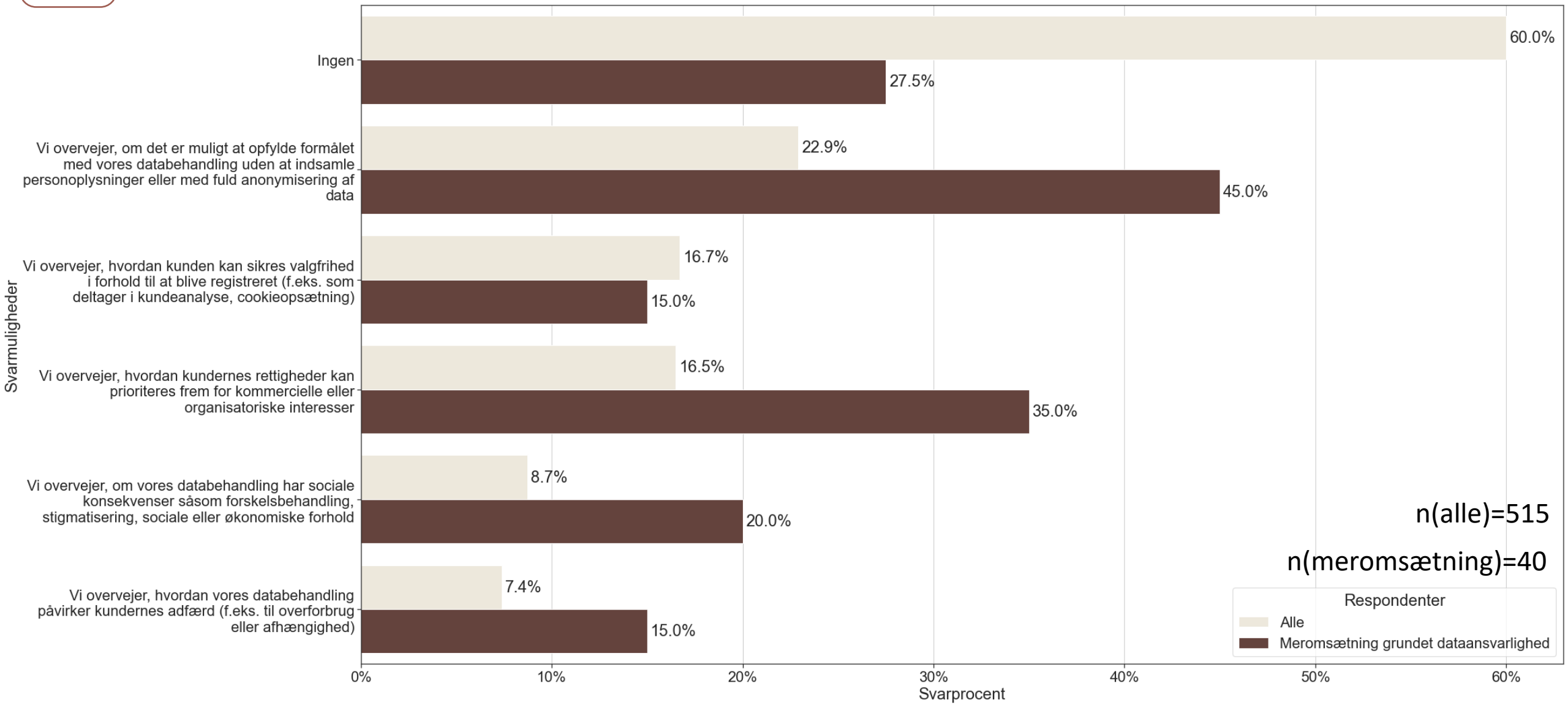


22

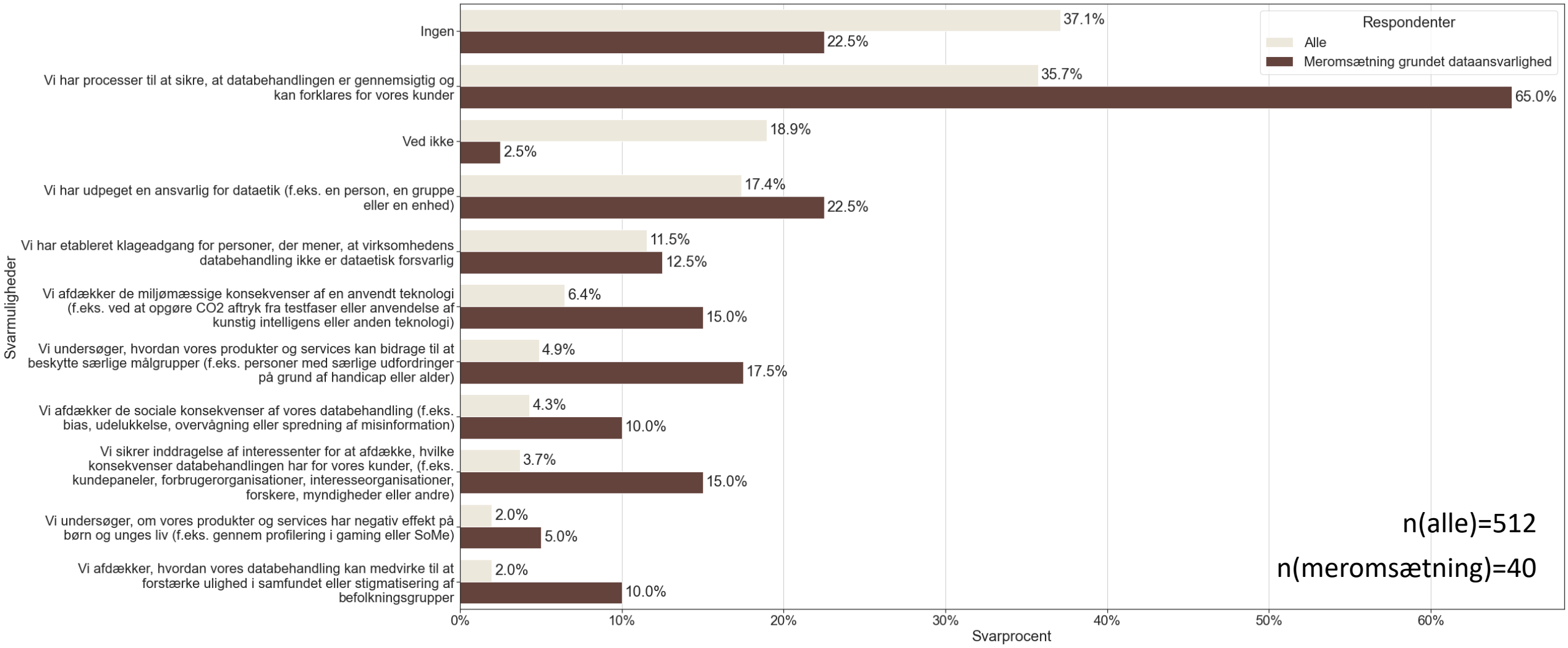
Har din virksomhed formuleret en politik eller retningslinjer for dataetik?



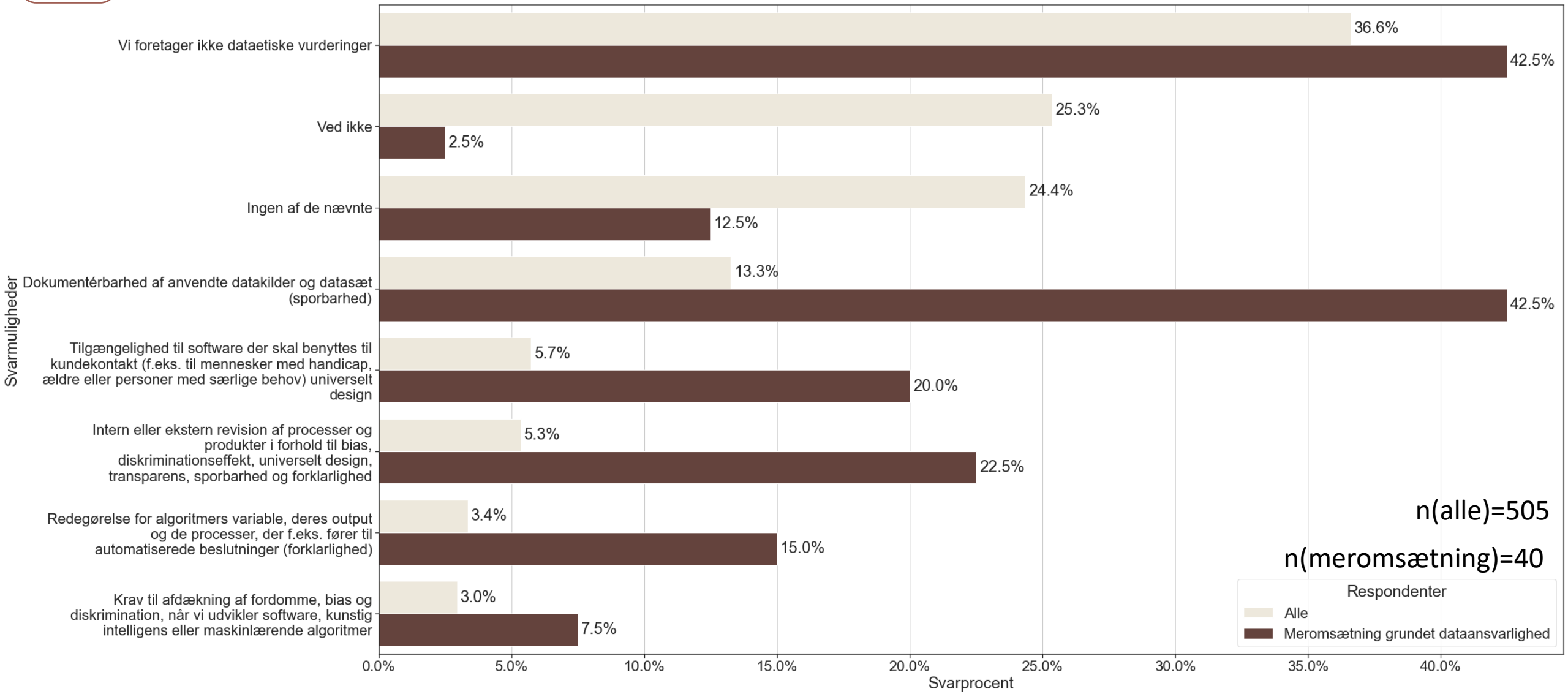
Hvilke overvejelser har I gjort, eller påtænker at gøre, ift. arbejdet med dataetik? (Markér gerne flere)

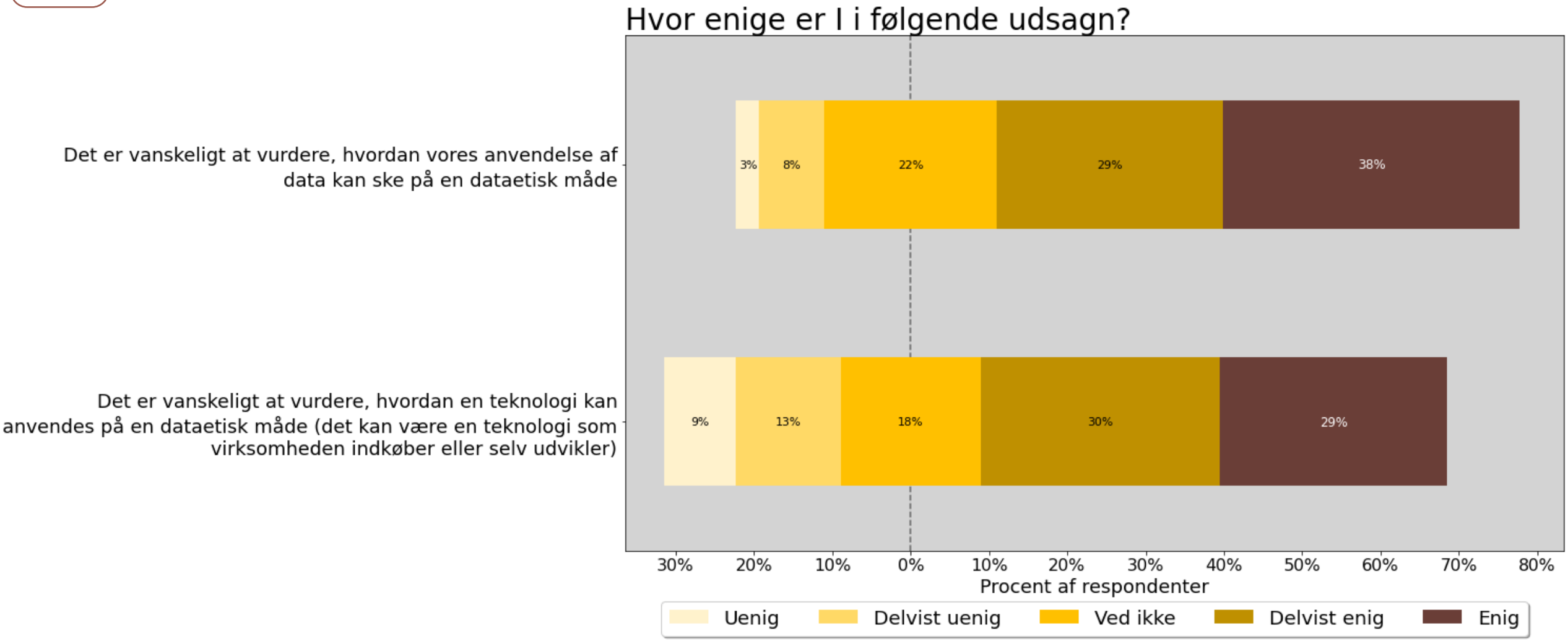


Hvilke konkrete initiativer har jeres virksomhed foretaget ift. arbejdet med dataetik? (Markér gerne flere)



Hvilke dataetiske vurderinger foretager jeres virksomhed af leverandører af teknologi eller databehandling? (Markér gerne flere)

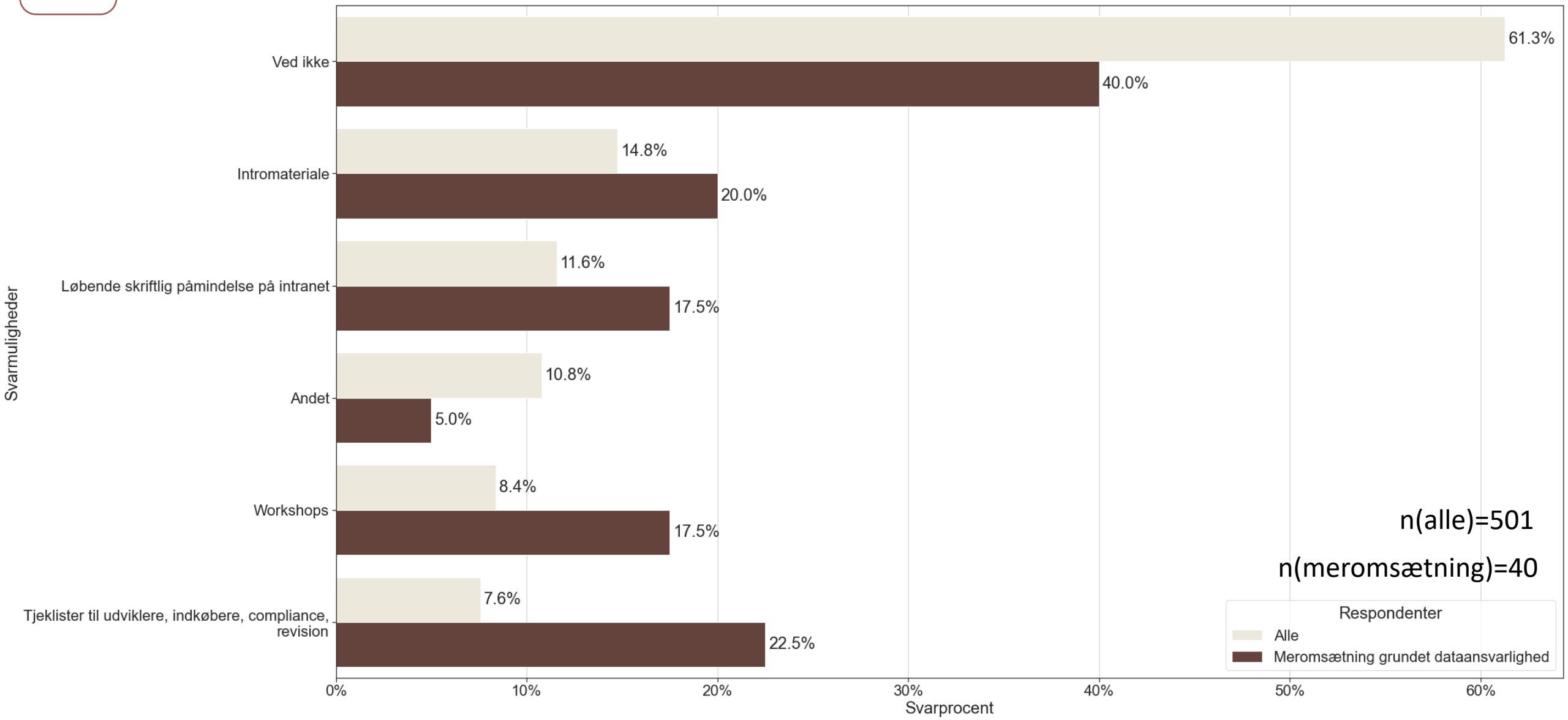




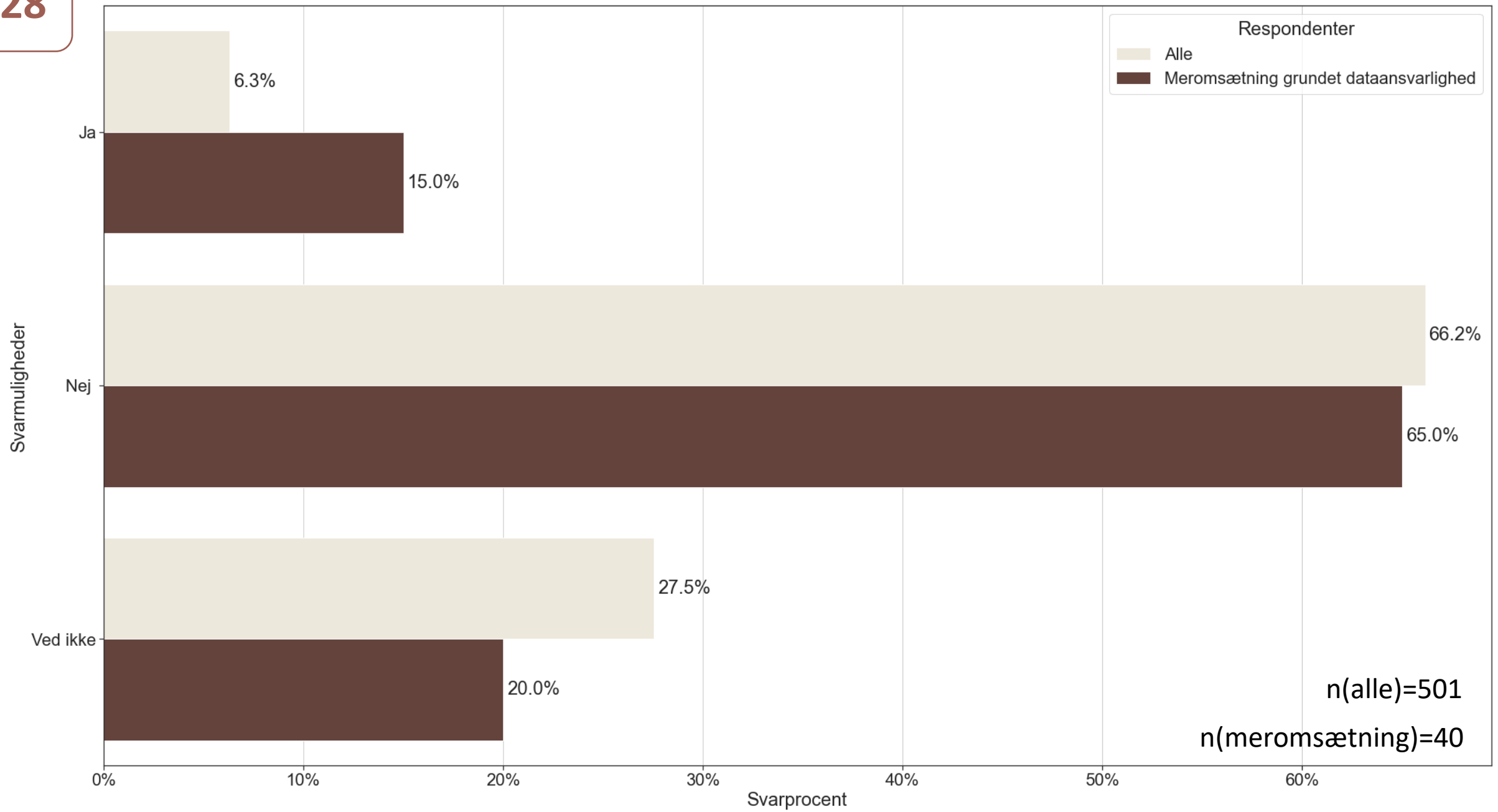
n(alle)=505

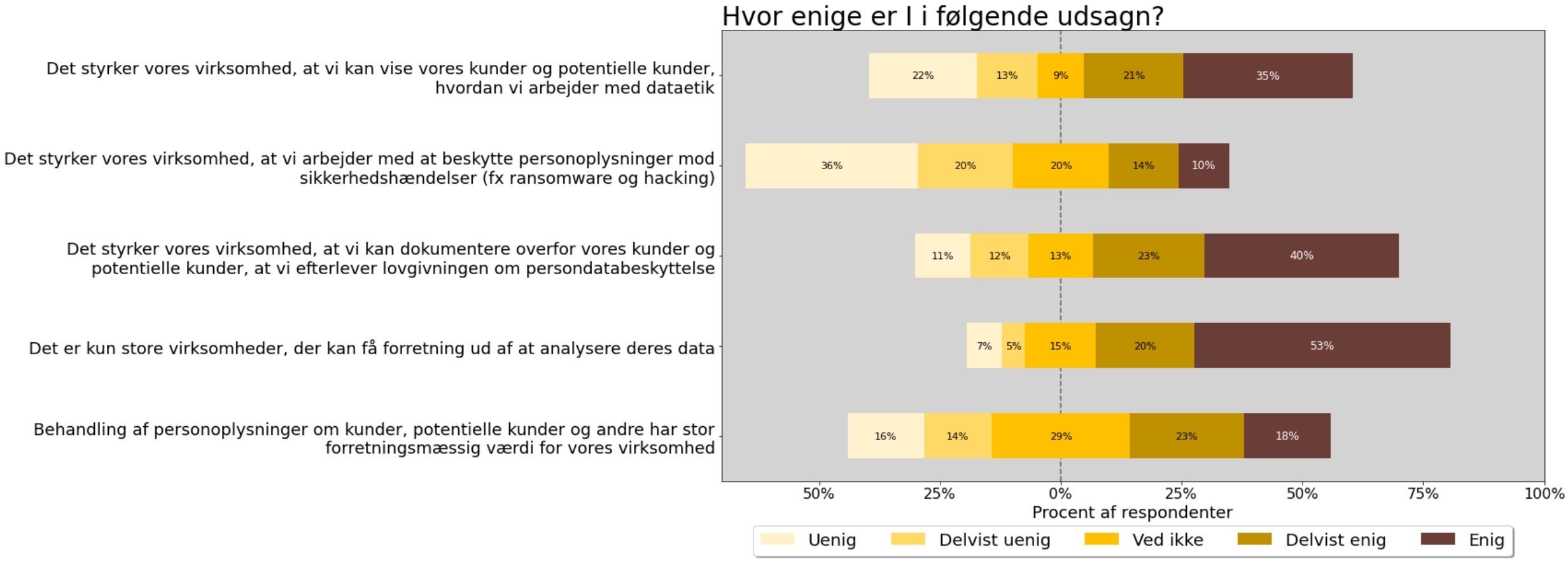
n(meromsætning)=40

Hvordan sikrer I, at medarbejderne i jeres virksomhed har kompetencer til at arbejde med dataetik? (Markér gerne flere)



Er dataetik en forretningsstrategisk satsning i jeres virksomhed? (f.eks. som krav om ingen brug af cookies, end-to-end-kryptering, design der er let tilgængeligt for alle)

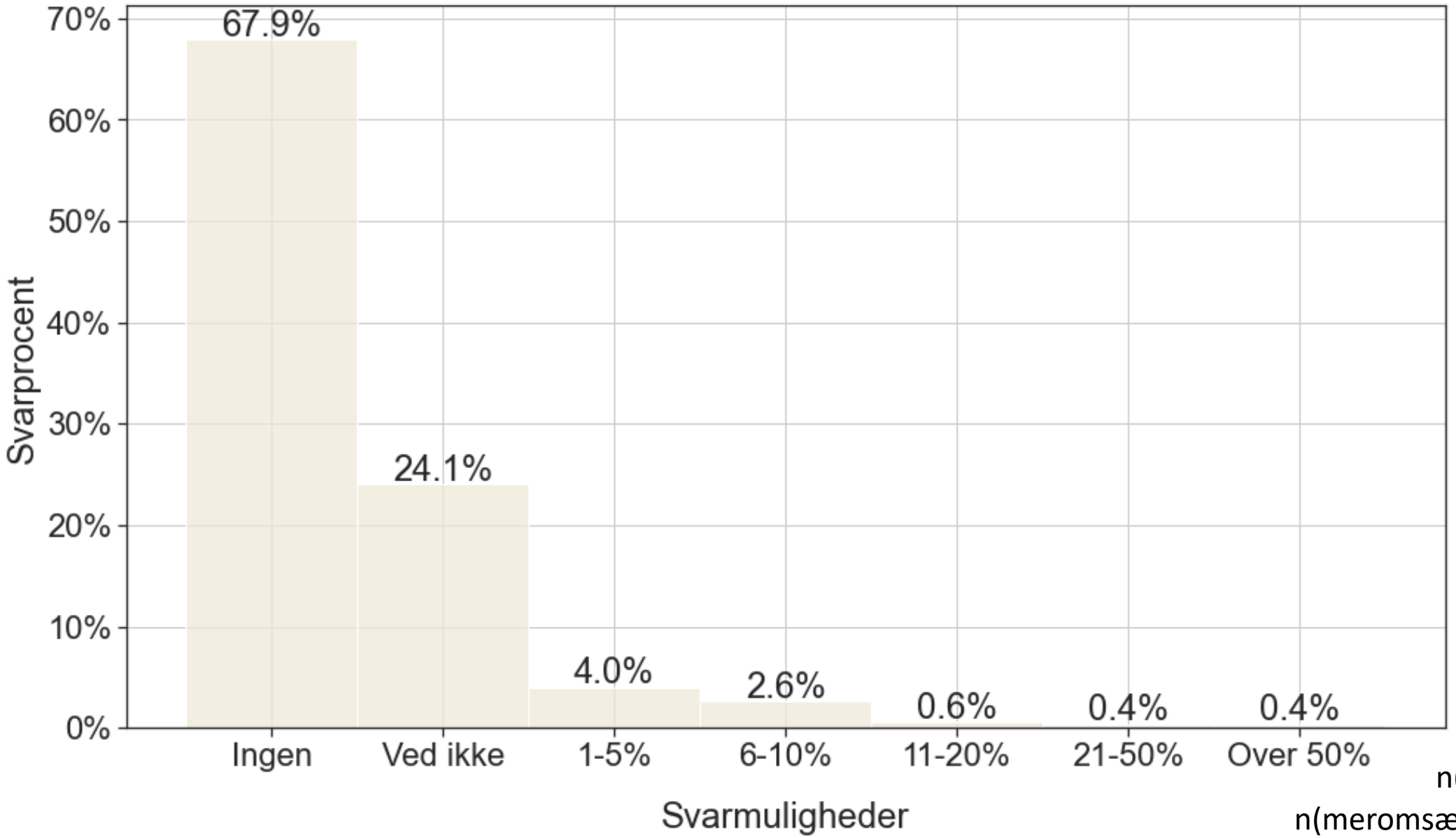




n(alle)=498

n(meromsætning)=40

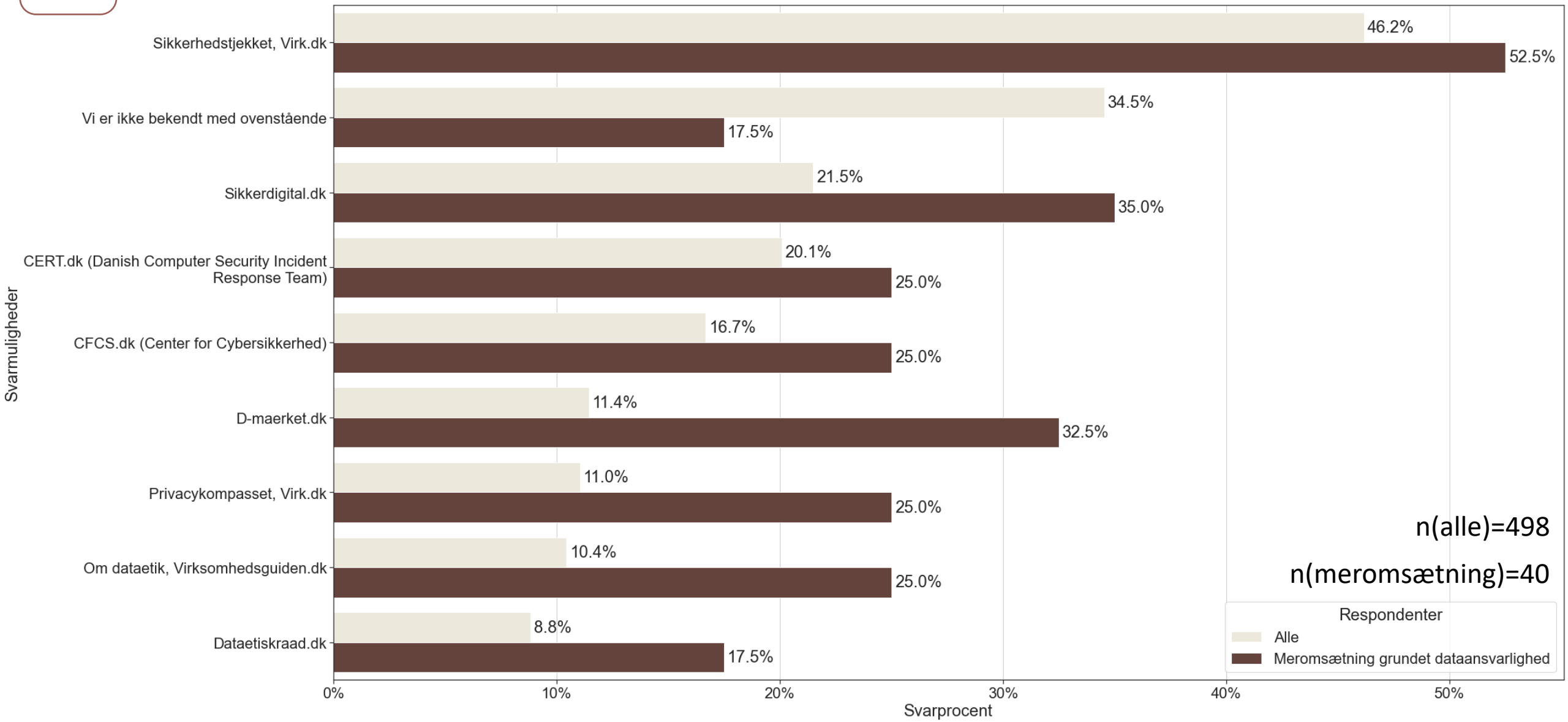
Hvor stor meromsætning vurderer I, at jeres arbejde med dataansvarlighed har skabt?



n(alle)=531

n(meromsætning)=40

Hvilke af nedenstående redskaber og hjemmesider er jeres virksomhed bekendt med? (Markér gerne flere)



CARVE