IDA OG FSR – DANSKE REVISORER

ANALYSE AF DATA- OG CYBERSIKKERHED

DELRAPPORT 1: DATASIKKERHED

VERSION 1.0 19/3-2018

RAMBØLL

IDA OG FSR – DANSKE REVISORER
VERSION 1.0 19/3-2018

Revision	**1.0**
Dato	**19/03/2018**

Rambøll
Hannemanns Allé 53
DK-2300 København S
T +45 5161 1000
F +45 5161 1001
www.ramboll.dk

INDHOLD

1. INDLEDNING

Formålet med denne undersøgelse er at tage temperaturen på, hvor langt danske virksomheder er med at gøre sig klar til den nye persondataforordning, der træder i kraft i maj 2018, og hvordan det står til med beredskabet i forhold til cybersikkerhed.

Hovedfokus i undersøgelsen er IDA's medlemmer i offentlige og private virksomheder. Derudover er et mindre antal kommunalt ansatte og lidt over 100 it-ansvarlige i offentlige og private virksomheder blevet spurgt.

Undersøgelsens af status på persondatasikkerhed anlægger tre perspektiver på de temaer, der berøres:

1. Medarbejdernes viden om og forståelse for emnet.
2. Medarbejdernes evne til at praktisere de relevante procedurer, enten ved selv at kunne gennemføre dem eller vide, hvem der kan.
3. Hvor meget procedurer og regeloverholdelse er understøttet af de it-systemer, medarbejderne anvender.

2. KONKLUSIONER

Persondatasikkerheden sikres ved et samspil mellem tre elementer:

- Medarbejderens kendskab til reglerne og deres forståelse for, hvorfor reglerne findes.
- Solide procedurer, som kendes af medarbejderne, og/eller viden hos medarbejderne om, hvem der kan gennemføre procedurer, man ikke selv skal kunne gennemføre.
- It-systemer, der understøtter gennemførelsen af procedurerne og overholdelse af reglerne.

Det billede, der tegner sig, er, at ingen af de tre elementer rigtig er på plads.

- **Medarbejdernes viden om reglerne og deres forståelse for, hvorfor de findes, synes at være behersket.** Under halvdelen af de medarbejdere, der har med persondata at gøre i deres arbejde, ved, fx hvad oplysningspligten går ud på.
- Medarbejderne kender også kun i begrænset omfang til de procedurer, der skal understøtte praktiseringen af reglerne, eller hvem der ville kunne gennemføre procedurerne, hvis de ikke selv kan. Det står fx kun klart for halvdelen af medarbejderne, hvad de skal gøre ved brud på datasikkerheden.
- **Ansvars- og rollefordelingen i forhold til datasikkerhed ser heller ikke ud til helt at være på plads.** Endelig er der på alle områder en utilstrækkelig systemunderstøttelse af regler og procedurer.
- **Særligt mellemstore private virksomheder ser ud til at have problemer med at sikre medarbejdernes viden.** En mulig forklaring er, at de er for store til at vidensdeling (når først viden er kommet ind i virksomheden), til at det kan ske uformelt, og for små til at have de systemer og den organisation, der kan sikre en effektiv vidensdeling på tværs af afdelinger og funktioner i en større virksomhed.
- Ser man på mønstreren i besvarelserne er det **lidt mere end halvdelen af deltagerne, der ser ud til at have en generel forståelse for databeskyttelsesforordningens elementer, men det er kun få har rigtig godt styr på det.**

I betragtning af, at den nye persondataforordning snart træder i kraft, er det bekymrende, at der stadig synes at være så meget, der ikke er på plads. Nogle af de rettigheder, forordningen giver de registrerede, vil formodentlig kun gradvis blive taget i brug, så man vil have tid til at opbygge viden, systemer og procedurer, og det vil indtil disse er på plads være overkommeligt at løse tingene på ad hoc-basis. Men der kan hurtigt opstå en ikke-ubetydelig efterspørgsel på andre rettigheder – som fx retten til dataportabilitet eller retten til at blive glemt - og her kan manglende viden, procedurer og systemunderstøttelse blive en kostbar affære. Og så er der de pligter, forordningen pålægger organisationen – som fx kravet om databehandleraftaler, der træder i kraft fra dag et, og her er der principielt ingen mulighed for gradvist at få tingene på plads.

For de mange virksomheder, der ikke helt er på plads, må det vigtigste i første omgang være at sikre, at alle medarbejdere, der arbejder med persondata, i det mindste ved, at der er noget at vide, hvem de kan spørge, og at de skal spørge, hvis de er det mindste i tvivl. Dernæst skal man have opbygget procedurer på de områder, hvor myndigheden har pligter, og der, hvor efterspørgslen på "rettigheder" kan forventes at melde sig hurtigt og i større omfang. Endelig skal man hurtigst muligt i gang med det – for mange – lange seje træk, det er at sikre den rette systemunderstøttelse af procedurer og compliance.

Alt dette kræver en effektiv governance og en klar ansvars- og rollefordeling. Men denne synes ikke at være ganske klar – i hvert fald ikke for medarbejderne.

3. DATAGRUNDLAG

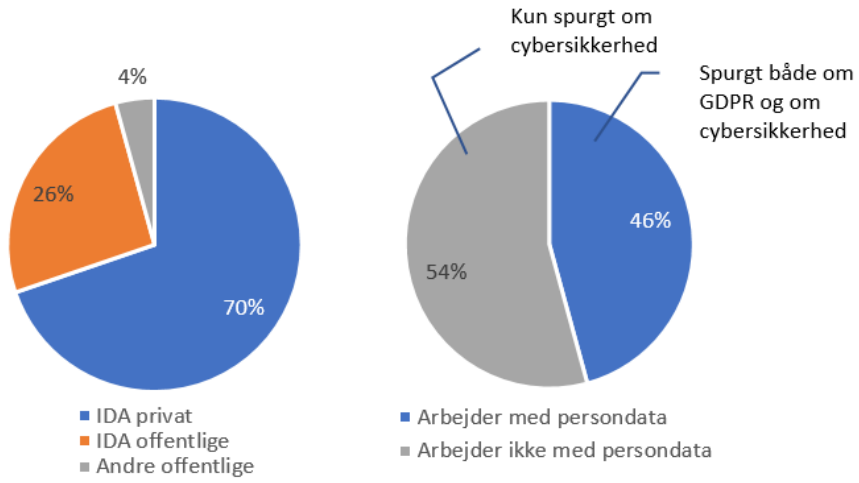
Datagrundlaget for denne rapport er en spørgeskemaundersøgelse henvendt henholdsvis til it-ansvarlige og til medarbejdere i danske offentlige og private virksomheder.

Datagrundlaget for det strategiske niveau består af 113 it-ansvarlige respondenter, hvoraf 89 er fra den private sektor, og 24 er fra den offentlige sektor.

Det lille antal respondenter betyder, at data fra det strategiske niveau kun kan bruges til at give nogle forsigtige indikationer om tingenes tilstand.

Datagrundlaget for det operationelle niveau består af 1.215 medarbejdere, hvoraf 849 respondenter er ansat i det private, og 366 respondenter er ansat i den offentlige sektor. Langt størstedelen af respondenterne på det operationelle niveau er hentet i IDA's medlemsbase og er derfor ingeniører. Der er altså tale om en speciel – og må det antages – som udgangspunkt relativt teknisk minded målgruppe. Undersøgelsens resultater kan derfor ikke uden videre tages til indtægt for alle medarbejdere.

Spørgsmålene til det operationelle niveau i Datasikkerheds- eller GDPR-delen af undersøgelsen er dog kun stillet til respondenter, der har angivet, at de arbejder med persondata i deres job. Dette gælder 555 respondenter, hvoraf 289 er fra private virksomheder, og 266 er fra det offentlige.



For yderligere information om datagrundlaget og undersøgelsens metode henvises til Bilag 1: Metode.

3.1 Profil af deltagerne

Dette afsnit indeholder en række tabeller, der beskriver fordelingen af respondenter på geografi, virksomhedsstørrelse og kommunestørrelse. Tabellerne giver en indikation af datagrundlaget og dermed de "stemmer", der er hørt i undersøgelsen.

3.1.1 Fordeling af respondenter på geografi (i pct. af det samlede antal deltagere i kategorierne)

Vi har respondenter fra hele landet. Region Nord og Region Sjælland er antageligt noget underrepræsenteret i undersøgelsen. Men da vi ikke har data om, hvor i landet de IDA-medlemmer, vi har spurgt, bor, er det vanskeligt at sige noget præcist om den geografiske repræsentativitet.

(Tabel på næste side).

Regioner			Nord	Midt	Syd	Sjælland	Hovedstaden	I alt
Strategisk	Offentlig	n	1	8	4	2	9	24
		%	4%	33%	17%	8%	38%	100%
	Privat	n	2	22	17	4	44	89
		%	2%	25%	19%	4%	49%	100%
	I alt	n	3	30	21	6	53	113
		%	3%	27%	19%	5%	47%	100%
Operationelt	Offentlig (IDA-medlemmer)	n	47	74	74	32	88	315
		%	15%	23%	23%	10%	28%	100%
	Offentlig (via fagchefer)	n	3	10	21	15	3	52
		%	6%	19%	40%	29%	6%	100%
	Privat (IDA-medlemmer)	n	48	169	114	41	474	846
		%	6%	20%	13%	5%	56%	100%
	I alt	n	98	253	209	88	565	1.213
		%	8%	21%	17%	7%	47%	100%

3.1.2 Fordeling af offentlige respondenter på kommunestørrelse

Langt de fleste deltagere i den operationelle undersøgelse har svaret på spørgsmålet om kommunestørrelse og arbejder derfor antageligt i en kommune*. Der er her en ret ligelig fordeling mellem stor og små kommuner.

Kommunestørrelse (målt på antal borgere)		Små	Mellemstor	Store	I alt
Strategisk	n	3	4	11	24
	%	17%	22%	61%	100%
Operationelt	n	133	113	106	366
	%	38%	32%	30%	100%
I alt	n	136	117	117	390
	%	37%	32%	32%	100%

Procentsatsen viser andelen af respondenter fra små, mellemstore og store kommuner for henholdsvis strategisk niveau, operationelt niveau og i alt.

*Oprindeligt blev dette spørgsmål stillet til alle på den "offentlige" liste, uanset om de arbejdede i en kommune eller ej. Antagelig er der en del, der har svaret på spørgsmålet alene for at kunne komme videre i undersøgelsen – også selvom de evt. ikke arbejdede i en kommune. Det blev dog ret hurtigt rettet, så man kun skulle svare, hvis man arbejdede i en kommune.

3.1.3 Fordeling af private respondenter på virksomhedsstørrelse

Medarbejdere fra store virksomheder er overrepræsenterede i undersøgelsen, mens medarbejdere i små virksomheder er underrepræsenterede. Dette kan dog skyldes frekvensen af ingeniører, som antageligt er større i store end i små virksomheder. Undersøgelsen kan derfor stadig godt være repræsentativ for virksomhedsstørrelse i forhold til ingeniørerne.

Virksomhedsstørrelser	Antal ansatte
Små	1-50
Mellemstore	51-250
Store	251+

(Tabel på næste side).

Virksomhedstørrelse (målt på ansatte)		Små 0-50	Mellemstor 51-250	Store 250+	I alt
Population	% af alle DK-virksomheder	97,4%	2,1%	0,5%	165.667
	% af medarbejder i all DK-virksomheder	31%	16%	53%	2.195.576
Strategisk	N	7	24	58	89
	%	8%	27%	65%	100%
Operationelt	N	151	181	515	849
	%	18%	21%	61%	100%
I alt	N	158	205	573	938
	%	17%	22%	61%	100%

Procentsatsen viser andelen af respondenter fra små, mellemstore og store virksomheder for henholdsvis strategisk niveau, operationelt niveau og i alt.

3.1.4 Fordeling af respondenter på branche (operationel del)

Branche	Fremstilling	Forsyning	Handel/ service	Offentlig	Finans	It og tele	Bygge og anlæg	Andet
n	315	87	158	27	12	121	84	45
Fordeling	37%	10%	19%	3%	1%	14%	10%	5%

Procentsatsen viser andelen respondenter fordelt på forskellige brancher.

3.1.5 Fordeling af respondenter på roller i forhold til data- og cybersikkerhed

Respondenterne er altovervejende medarbejdere, der ikke har data- eller cybersikkerhed som en selvstændig del af deres arbejde. Deres svar kan altså betragtes som værende repræsentative for "almindelige" medarbejdere (eller rettere "almindelige" ingeniører).

Hvad er din rolle i forhold til virksomhedens cyber- og datasikkerhed?		Jeg arbejder med cyber- og datasikkerhed som den vigtigste del af mit job	Jeg arbejder med cyber- og datasikkerhed som en del af mit job	Jeg arbejder i it-afdelingen, men har ikke så meget med cyber- og datasikkerhed at gøre	Jeg arbejder i andre dele af virksomheden og arbejder ikke med cyber- og datasikkerhed som en selvstændig del af mit arbejde	Andet	N
	Privat	1%	9%	6%	84%	1%	849
	Offentlig	1%	7%	1%	89%	2%	367
	Alle	**1%**	**8%**	**5%**	**85%**	**1%**	**1216**

Procentsatsen viser fordelingen af respondenterne set i forhold til, hvordan de arbejder med cybersikkerhed.

4. ANALYSE

4.1 Introduktion

Såvel private som offentlige virksomheder indsamler i stadig stigende omfang data og information fra og om kunder, borgere og medarbejdere. En betydelig del af den information, der indsamles, kan derfor henføres til specifikke personer og karakteriseres derfor som persondata.

Den 25. maj 2018 træder den nye databeskyttelsesforordning i kraft. Dette medfører blandt andet skærpede krav til virksomhedernes indsamling og behandling af persondata og stærkere sanktionsmuligheder – først og fremmest i form af muligheden for markant større bøder end hidtil set i Danmark ved overtrædelse af forordningen.

Dette afsnit om persondatasikkerhed har fokus på implementering af persondataforordningen i virksomhederne, gennem information, procedurer og politikker.

4.2 Temaer

Tabeller med data fra undersøgelsen blandt IDA's medlemmer er markeret med en grøn header. Data fra undersøgelsen blandt kommunale ledere er markeret med en blå header.

4.2.1 Databehandleraftale

Dette tema handler om offentlige og private virksomheders anvendelse af databehandleraftaler. Databehandleraftalen er et centralt element i databeskyttelsesforordningen. Den har til formål at præcisere, hvordan en virksomhed foretager databehandling på vegne af en anden virksomhed i en given situation og hermed sikre, at databehandling foretages efter databeskyttelsesforordningens retningslinjer.

Deltagerne er for de fleste af spørgsmålene i undersøgelsen, blevet bedt om at svare, i hvor høj grad de mente, at udsagnene passede på dem/deres virksomhed, på en skala fra 1 til 5, hvor 1 betød "passer slet ikke", og 5 betød "passer i meget høj grad". I undersøgelsen er svarene 1 og 2 tolket som, at ingen eller meget beskeden overensstemmelse i forhold til viden, kendskab, kompetence, eller hvad udsagnet ellers handlede om, mens svar 4 eller 5 er tolket som høj eller meget høj grad af overensstemmelse. Svaret 3 er tolket som hverken eller.

Databehandleraftale	Sektor	1+2	3	4+5	v. ikke	**n**
Jeg ved, hvad formålet er med at indgå databehandleraftaler, og hvornår vi skal lave sådanne aftaler.	Privat	30%	14%	48%	8%	289
	Offentlig	25%	14%	47%	15%	266
	Alle	**27%**	**14%**	**48%**	**11%**	**555**
Jeg ved, hvem jeg skal gå til, hvis der er brug for at få lavet en databehandleraftale (eller jeg kan selv stå for at lave en).	Privat	23%	11%	58%	8%	289
	Offentlig	23%	8%	57%	12%	266
	Alle	**23%**	**10%**	**58%**	**10%**	**555**

Der er flere, der ved, hvordan de kan få lavet en databehandleraftale, end der er personer, der kender formålet med databehandleraftaler

Der er 58 % af de medarbejder, der arbejder med persondata, ved, hvem de skal gå til, eller hvordan de selv kan lave en databehandleraftale. 48 % kender selve formålet med databehandleraftalen og ved, hvornår en databehandleraftale skal indgås. Der er – ikke overraskende - et meget stort overlap mellem dem, der kender formålet og ved, hvordan aftaler skal indgå, og dem, der ved, hvem de skal gå til, eller selv kan stå for at udarbejde en aftale.

Når det drejer sig om data i centrale systemer, er det relativt få mennesker, der skal kende krav til og procedurer i forhold til databehandleraftaler. Men i det omfang, indsamling af persondata eller behandling af andres data sker decentralt, som fx i forbindelse med surveys og andre undersøgelser, kan der være tale om en meget bredere kreds.

Virksomhederne er længere med formaliteterne end med procedurer for praksis

Når vi spørger de it-ansvarlige, angiver 58 %, at de i har en standard databehandleraftale, som anvendes, når andre virksomheder behandler persondata på vegne af virksomheden. Men samtidig angiver 34 %, at de ikke eller kun i mindre grad har styr på underleverandørernes overholdelse af databeskyttelsesreglerne. Noget kunne altså tyde på, at man er på vej til at have styr på det formelle (databehandleraftalen), men ikke er kommet så langt med de procedurer, der skal sikre, at aftalen rent faktisk overholdes.

Databehandleraftale	Sektor	1+2	3	4+5	v. ikke	n
Vi har en standard databehandleraftale, som anvendes, når behandling af personoplysninger udføres for os af andre virksomheder.	Privat	22%	16%	56%	6%	89
	Offentlig	17%	21%	63%	0%	24
	Alle	**21%**	**17%**	**58%**	**4%**	**113**
Virksomheden har styr på underleverandørernes overholdelse af databeskyttelsesreglerne.	Privat	38%	26%	28%	8%	89
	Offentlig	17%	50%	33%	0%	24
	Alle	**34%**	**31%**	**29%**	**6%**	**113**

NB: Data fra den del af undersøgelsen, der er rettet mod de it-ansvarlige, er markeret med en blå bjælke foroven, data fra det operationelle niveau (medarbejderne) er markeret med en grøn bjælke.

4.2.2 Databeskyttelsespolitik og -proces

Dette tema berører virksomhedernes anvendelse af databeskyttelsespolitikker og -processer, eksempelvis rollefordelinger og proces for evaluering af sikkerhedsniveau.

Databeskyttelsespolitik og -proces	Sektor	1+2	3	4+5	v. ikke	**n**
Jeg er blevet informeret om, at vi har udpeget en, der er ansvarlig for persondatasikkerhed	Privat	28%	9%	54%	10%	289
	Offentlig	31%	11%	49%	9%	266
	Alle	**29%**	**10%**	**52%**	**9%**	**555**
Jeg er blevet informeret om, at vi løbende afprøver og vurderer sikkerheden i vores databehandling	Privat	28%	16%	45%	11%	289
	Offentlig	26%	12%	50%	12%	266
	Alle	**27%**	**14%**	**47%**	**12%**	**555**

Ca. halvdelen af medarbejderne ved, at der er udpeget en ansvarlig for persondatasikkerhed, og at datasikkerheden løbende afprøves

Godt halvdelen af medarbejderne har fået at vide, at der er udpeget en persondatasikkerhedsansvarlig. Knap halvdelen ved, at sikkerheden løbende afprøves og vurderes. Man kan diskutere, om glasset er halvt fuld eller halvt tomt her. Det er formodentlig ikke noget større problem, at medarbejderen ikke ved, at man afprøver sikkerheden, men det kan være et problem, at de ikke ved, hvem den persondataansvarlige er, da denne rolle dels bør tjene som et fyrtårn for datasikkerhed, dels bør være en, alle ved, de kan gå til, hvis de mener, noget kunne forbedres.

Ansvars- og rollefordelingen i forhold til datasikkerhed er ikke helt på plads

Lidt over halvdelen af de it-ansvarlige (53 %) angiver, at de har en klar ansvars- og rollefordeling for afprøvning, vurdering og evaluering af sikkerhedsniveauet på tværs af organisationen. Et stykke under halvdelen (42 %) mener, at dem af deres medarbejdere, som arbejder med persondata, ved, hvorfor afprøvning og vurdering af sikkerheden foretages. Det er problematisk, at så relativt mange ikke har ansvaret på plads for den vigtige del af den proaktive del af datasikkerhedsarbejdet. Det kan også være problematisk, at så mange medarbejdere tilsyneladende ikke ved, hvorfor sikkerheden løbende afprøves, *hvis* dette er et udtryk for en generelt lave sikkerhedsbevidsthed blandt medarbejderne.

(Tabel på næste side).

Databeskyttelsespolitik og -proces	Sektor	1+2	3	4+5	v. ikke	n
Vi har en klar ansvars- og rollefordeling for, hvordan vi afprøver, vurderer og evaluerer sikkerhedsniveauet på tværs af organisationen.	Privat	28%	17%	52%	3%	89
	Offentlig	17%	25%	58%	0%	24
	Alle	**26%**	**19%**	**53%**	**3%**	**113**
Alle medarbejdere, der arbejder med personoplysninger, ved, hvorfor det er vigtigt, at vi løbende afprøver og vurderer datasikkerheden.	Privat	28%	26%	44%	2%	89
	Offentlig	17%	46%	38%	0%	24
	Alle	**26%**	**30%**	**42%**	**2%**	**113**

4.2.3 Brud på datasikkerheden

Dette tema handler om virksomhedernes procedurer, når der er sket et brud på datasikkerheden, og medarbejdernes kendskab til disse procedurer.

Brud på datasikkerheden	Sektor	1+2	3	4+5	v. ikke	n
Jeg ved, at vi har en procedure ved brud på datasikkerheden, og hvad formålet er med den.	Privat	35%	13%	38%	14%	289
	Offentlig	31%	14%	42%	12%	266
	Alle	**33%**	**14%**	**40%**	**13%**	**555**
Det er klart for mig, hvad jeg skal gøre, hvis jeg opdager eller får mistanke om et brud på datasikkerheden i organisationen.	Privat	28%	16%	52%	5%	289
	Offentlig	23%	16%	53%	8%	266
	Alle	**26%**	**16%**	**52%**	**6%**	**555**

Det står kun klart for halvdelen af medarbejderne, hvad de skal gøre ved brud på datasikkerheden

Det står klart for 52 % af medarbejderne, hvad de skal gøre, hvis de opdager eller får mistanke om et brud på datasikkerheden i organisationen. Det er klart problematisk, da en hurtig og korrekt indsats fra medarbejderne kan være en væsentlig faktor i at begrænse skaderne. Vi har ikke spurgt til, om det er klart for medarbejderne, hvordan de spotter evt. brud, men det er naturligvis en forudsætning for, at man kan handle på dem.

Endnu færre medarbejdere – 40 % ved, at der er procedurer for, hvad der skal ske ved brud på datasikkerheden, og hvad formålet er med dem. Manglende kendskab til eksistensen af procedurerne er ikke nødvendigvis noget problem, med manglende kendskab til procedurer, man selv har en rolle i, ville klart være et problem. Manglende kendskab til formålet kan igen være udtryk for en generel mangel på bevidsthed i forhold til datasikkerhed i organisationen.

Det står heller ikke for godt til med procedurer og medarbejdernes viden, set fra de it-ansvarliges vinkel

Kun 28 % af de it-ansvarlige i undersøgelsen føler sig overbeviste om, at medarbejdere, der arbejder med personoplysninger, ved, hvad de skal gøre i en situation, hvor der har været brud på datasikkerheden.

Kun 28 % af de it-ansvarlige i undersøgelsen føler sig overbeviste om, at medarbejdere, der arbejder med personoplysninger, ved, hvad de skal gøre i en situation, hvor der har været brud på datasikkerheden. Det er bekymrende mange, der ikke har procedurerne på plads, selv inden for denne mindre stikprøve, som disse respondenter udgør. Det er vigtigt her at huske, at det at have "procedurerne på plads" ikke blot er et spørgsmål om at have skrevet noget ned på et stykke papir, men også om at have gearet organisationen til at gennemføre procedurerne med kort varsel, når der er behov for dem. Dem, der ikke har dette klar nu, kan også får svært ved at nå det, inden forordningen træder i kraft.

(Tabel på næste side).

Brud på datasikkerheden	Sektor	1+2	3	4+5	v. ikke	n
Vi har en klar procedure for, hvordan et brud på datasikkerheden håndteres i organisationen.	Privat	34%	18%	45%	3%	89
	Offentlig	29%	13%	58%	0%	24
	Alle	**33%**	**17%**	**48%**	**3%**	**113**
Alle medarbejdere, der arbejder med personoplysninger, ved, hvad de skal gøre i en situation, hvor der har været brud på datasikkerheden.	Privat	53%	19%	27%	1%	89
	Offentlig	33%	33%	33%	0%	24
	Alle	**49%**	**22%**	**28%**	**1%**	**113**

4.2.4 Begrænsning af opbevaring af data

Dette tema ser på, hvor parate virksomhederne er i forhold til at overholde databeskyttelsesforordningens retningslinjer om begrænsning af opbevaring af data. Her er virksomhedens evne til at slette og anonymisere data efter behandling særlig vigtigt.

Begrænsning af opbevaring af data	Sektor	1+2	3	4+5	v. ikke	n
Jeg ved, hvorfor det er vigtigt, at vi kun opbevarer personoplysninger i det tidsrum, vi har lov til det.	Privat	14%	14%	66%	6%	289
	Offentlig	12%	14%	69%	5%	266
	Alle	**13%**	**14%**	**68%**	**6%**	**555**
Jeg ved, hvor henne og hvor længe jeg må opbevare personoplysninger, og hvordan jeg begrænser opbevaring af oplysninger, jeg har på min egen pc eller drev, fx gennem sletning.	Privat	34%	21%	36%	9%	289
	Offentlig	22%	20%	50%	8%	266
	Alle	**28%**	**20%**	**43%**	**9%**	**555**

Medarbejderne kender reglerne for begrænsning af behandling, men mange ved ikke, hvordan de skal handle på det i praksis

Næsten 7 ud af 10 medarbejdere mener at have styr på reglerne for begrænsning af behandling af data, men under halvdelen ved, hvordan de skal omsætte den i praksis. Man kunne antage, at de systemer, der indeholder persondata, i mange virksomheder tog sig af den praktiske side af disse begrænsninger (eller burde gøre det), så medarbejderen ikke behøver at tænke på det, og at der kunne være en del af forklaringen på, at så mange ikke kender procedurerne. Men kun 28 % af medarbejderne angiver, at systemerne tager sig af dette.

Dertil kommer, at det ikke er alle data, der opbevares i sådanne systemer, og det er ikke al begrænsning i opbevaringen af data, der kan ske automatisk. Derfor er det vigtigt, at medarbejderne ved, hvordan de sikrer begrænsningen der, hvor den ikke sker automatisk – og hvor det er. Og derfor er det problematisk, at så mange ikke ved det eller er usikre på det. En forklaring kan dog være, at der er begyndt at blive skabt *awareness* i organisationerne i forhold til dette, men træningen af medarbejderne har endnu ikke fundet sted i mange organisationer.

Medarbejderen i det offentlige er en hel del mere sikre på den praktiske side af begrænsning af opbevaring af data end medarbejderne i det private. Det kan skyldes en generelt højere bevidsthed om og bevågenhed i forhold til persondata i det offentlige, men reglerne gælder i lige høj grad for private virksomheds persondata, og det er derfor afgørende, at man også kommer i gang her.

De it-ansvarlige ser ikke positivt på organisationens evne til at begrænse opbevaring af data i overensstemmelse med databeskyttelsesforordningen

De it-ansvarlige i undersøgelsen ser noget mindre positivt på medarbejdernes viden på dette område. Kun 28 % mener, at medarbejderne er blevet informeret om, hvordan og hvorfor personoplysninger må opbevares. Og kun 19 % mener, at alle medarbejdere ved, hvor og hvor længe de må opbevare personoplysninger, og hvordan de begrænser deres egen opbevaring.

Enten står det værre til i de virksomheder, der har deltaget i denne del af undersøgelsen, end hos de mange virksomheder, som medarbejderundersøgelsen repræsenterer. Eller også overvurderer medarbejderen deres egen viden – muligvis fordi det ikke står ganske klart for dem, hvad "reglerne for begrænsning af behandling af data" overhovedet er.

Kun 37 % af de it-ansvarlige angiver, at deres virksomhed har en klar procedure for overholdelse af reglerne om opbevaringsbegrænsning. Hvis dette er et generelt billede, kan det jo forklare,

hvorfor så mange medarbejdere ikke kender procedurerne.

Begrænsning af opbevaring af data %	Sektor	1+2	3	4+5	v. ikke	n
Vi har en klar procedure for overholdelse af reglerne om opbevarings-begrænsning.	Privat	38%	20%	39%	2%	89
	Offentlig	42%	29%	29%	0%	24
	Alle	**39%**	**22%**	**37%**	**2%**	**113**
Alle medarbejdere, der arbejder med personoplysninger, er blevet informeret om, hvordan og hvorfor personoplysninger må opbevares, så længe der er samtykke eller hjemmel til det.	Privat	46%	21%	30%	2%	89
	Offentlig	42%	38%	21%	0%	24
	Alle	**45%**	**25%**	**28%**	**2%**	**113**
Alle medarbejdere ved, hvor og hvor længe de må opbevare personoplysninger, og hvordan de begrænser egen opbevaring heraf, fx gennem sletning.	Privat	56%	22%	19%	2%	89
	Offentlig	54%	25%	21%	0%	24
	Alle	**56%**	**23%**	**19%**	**2%**	**113**

4.2.5 Konsekvensanalyse

Dette tema handler om organisationernes implementering af konsekvensanalyser. En konsekvensanalyse er en vurdering af risici i forbindelse med behandling af persondata, særligt skal konsekvensanalyser finde sted for systemer, der behandler følsomme persondata.

Her har vi kun spurgt de it-ansvarlige. Billedet, der tegner sig af de deltagende virksomheder, her er, at man er længere fremme med udarbejdelsen af procedurer for vurdering af risici, end man er med i formidling af kravene om gennemførsel af konsekvensanalyser til relevante medarbejdere. 41 % af virksomhederne har en klar procedure for risikovurderingen, men kun 19 % har informeret alle relevante medarbejdere om kravet om gennemførsel af analyserne.

Konsekvensanalyse	Sektor	1+2	3	4+5	v. ikke	n
Vi har en klar procedure for vurdering af risici i forbindelse med behandling af persondata.	Privat	38%	21%	38%	2%	89
	Offentlig	29%	17%	50%	4%	24
	Alle	**36%**	**20%**	**41%**	**3%**	**113**
Alle relevante medarbejdere er informeret om kravet om gennemførsel af konsekvensanalyser for højrisiko behandlingsaktiviteter og formålet med konsekvensanalyser.	Privat	47%	30%	18%	4%	89
	Offentlig	38%	38%	25%	0%	24
	Alle	**45%**	**32%**	**19%**	**4%**	**113**

4.2.6 Oplysningspligt

Dette tema handler databeskyttelsesforordningens oplysningspligt. Oplysningspligt omfatter indhentning af samtykke og sikring af, at der gives de nødvendige oplysninger om behandlingen af data.

Oplysningspligt	Sektor	1+2	3	4+5	v. ikke	**n**
Jeg ved, hvordan jeg inden for mit arbejdsområde kan sikre, at oplysningspligten bliver opfyldt.	Privat	33%	16%	38%	13%	289
	Offentlig	22%	16%	48%	14%	266
	Alle	**28%**	**16%**	**43%**	**14%**	**555**
Jeg ved, hvad oplysningspligten går ud på, og hvad formålet med den er.	Privat	26%	16%	46%	11%	266
	Offentlig	19%	18%	51%	12%	**555**
	Alle	**23%**	**17%**	**48%**	**12%**	289

Under halvdelen af de medarbejdere, der har med persondata at gøre i deres arbejde, ved, hvad oplysningspligten går ud på, og hvordan de sikrer, at den opfyldes

Vi har her at gøre med et helt centralt punkt såvel i den nye forordning som i den hidtidige lovgivning, og her står det altså sløjt til både i det offentlige og i de private virksomheder.

Oplysningspligten kan i praksis være opfyldt gennem de systemer, man anvende, fx i selvbetjeningsløsninger eller i teksten i standardbreve. Men det er kun 33 % af medarbejderne, der mener, at det er tilfældet på deres område, og under alle omstændigheder skal den opfyldes af medarbejderen selv, når man er i mundtlig kontakt med borgere eller kunder, eller når en korrespondance ikke er bygget op om standardtekster.

Dette billede afspejles i svarene fra de it-ansvarlige, hvor kun 23 % mener, at alle relevante medarbejdere, der arbejder med personoplysninger, er blevet instrueret i, hvordan de sikrer, at oplysningspligten bliver opfyldt.

Særligt mellemstore private virksomheder halter efter i forhold til medarbejdernes viden om, hvordan de skal praktisere oplysningspligten

Ser vi på den private sektor, mener 51 % af medarbejdere i små virksomheder og 39 % i store virksomheder, at de ved, hvordan de kan sikre, at oplysningspligten bliver opfyldt. For de mellemstore virksomheder er tallet nede på 26 %. En mulig forklaring er, at der i små virksomheder er relativt få mennesker, der arbejder med persondata, og dermed også få, der skal trænes, mens store virksomheder typisk har ressourcer og systemer til at gennemføre træningen. De mellemstore virksomheder er her i en mellemposition, hvor træningen ikke kan klares over skrivebordet mellem en lille gruppe mennesker, mens man samtidig ikke har ressourcerne og systemerne til at træne flere systematisk.

Oplysningspligt	Sektor	1+2	3	4+5	v. ikke	**n**
Jeg ved, hvordan jeg inden for mit arbejdsområde kan sikre, at oplysningspligten bliver opfyldt.	Små	33%	10%	51%	6%	**67**
	Mellemstore	37%	16%	26%	21%	**68**
	Store	31%	18%	39%	12%	**154**
	Privat i alt	33%	16%	38%	13%	**289**

4.2.7 Retten til indsigt

Retten til indsigt er et centralt element i databeskyttelsesforordningen. Retten til indsigt skal gøre det muligt for en person at få indsigt i, hvilke data der behandles om personen. Det kræver, at virksomhederne kan danne et overblik over, hvilke oplysninger der behandles om en given person.

Medarbejdere i det offentlige kender procedurerne for indsigt bedre end medarbejdere i private virksomheder

46 % af medarbejderne i den offentlige sektor angiver, at de kan gennemføre en indsigt, hvis der er brug for det, eller ved, hvem de skal henvise til. Dette gælder kun 28 % i den private sektor. Dette skel på 18 procentpoint kan skyldes, at den offentlige sektor i højere grad har været vant til at skulle give borgere indsigt end de private virksomheder i forhold til deres kunder, men det er rimeligt at antage, at ønsket om indsigt også i den private sektors kundedata vil stige fremover. Samtidig er de tankevækkende, at det kun er 46 % af de offentlige medarbejdere, der arbejder med persondata i deres arbejde, der ved, hvad de skal gøre, eller hvem de skal spørge, hvis nogen beder om indsigt.

Retten til indsigt	Sektor	1+2	3	4+5	v. ikke	**n**
Jeg kender procedurerne for at give indsigt og kan gennemføre en indsigt, hvis der er brug for det, eller ved, hvem jeg skal henvise til for at få gennemført proceduren.	Privat	44%	14%	28%	14%	289
	Offentlig	29%	11%	46%	13%	266
	Alle	**37%**	**13%**	**37%**	**14%**	**555**

4.2.8 Retten til berigtigelse

Retten til berigtigelse skal sikre, at personer kan få rettet data, som en virksomhed har registreret, hvis de er fejlbehæftede.

Ikke mange ved, hvad de skal gøre, hvis en borger eller kunde ønsker at få berigtiget data

Kun godt en fjerdedel (27 %) af medarbejderne kan hjælpe borgere eller kunder med at få rettet data eller ved, hvem der kan. Kun ganske få flere (29 %) kender reglerne for berigtigelse og formålet med at gøre det.

Dette understøttes af de it-ansvarliges besvarelser, hvor kun omtrent en fjerdedel angiver, at relevante medarbejdere er blevet informeret og instrueret i reglerne om berigtigelse.

Retten til berigtigelse	Sektor	1+2	3	4+5	v. ikke	n
Jeg kender reglerne for håndtering af ønsker om berigtigelse og formålet med dem.	Privat	37%	17%	28%	17%	289
	Offentlig	35%	17%	30%	18%	266
	Alle	**36%**	**17%**	**29%**	**18%**	**555**
Jeg kender vores procedurer for berigtigelser og er i stand til at udføre dem eller ved, hvem der skal gennemføre proceduren.	Privat	39%	16%	25%	20%	289
	Offentlig	35%	15%	30%	20%	266
	Alle	**37%**	**16%**	**27%**	**20%**	**555**

4.2.9 Retten til sletning

Offentlige organisationer er undtaget fra retten til sletning, og derfor er spørgsmålene om sletning kun stillet til medarbejdere i private virksomheder.

Reglen om sletning – dvs. retten til at blive glemt - er en nyskabelse, og det er derfor i og for sig ganske flot, at så mange allerede kender til den og ved, hvad de skal gøre, hvis nogen ønsker at få slettet data. Samtidig ser det dog ud til, at det kun er få (24 %), der positivt ved, at deres systemer understøtter sletning. Her kan ligge en ganske stor udfordring gemt for virksomhederne, da det kan være en kompliceret opgave at understøtte sletning i systemer, der ikke er bygget til det.

Retten til sletning	Sektor	1+2	3	4+5	v. ikke	n
Jeg kender reglerne for sletning af personoplysninger og formålet med dem.	Privat	34%	14%	39%	12%	289
Jeg kender vores procedurer for sletning og er i stand til at gennemføre dem eller ved, hvem der skal gennemføre proceduren.	Privat	42%	12%	31%	16%	289

4.2.10 Retten til begrænsning

Retten til begrænsning handler om muligheden for at begrænse anvendelsen af for eksempel at sætte databehandlinger i bero.

Kun en fjerdedel af medarbejderne kender reglerne for begrænsning, og kun en fjerdedel kan selv gennemføre en begrænsning eller ved, hvem der kan

Samtidig er det kun ca. en femtedel af de it-ansvarlige, som har angivet, at virksomheden har en klar procedure, og under en femtedel, der angiver, at alle relevante medarbejdere i organisationen er instrueret i processen. Retten til begrænsning vil formodentlig typisk finde anvendelse i samspil med andre rettigheder, fx retten til indsigelse, og det er derfor problematisk, at så få kender den, og at den – i hvert fald hos de it-ansvarlige i undersøgelsen - ikke er noget, man sikrer sig, at organisationen kender til.

(Tabel på næste side).

Retten til begrænsning	Sektor	1+2	3	4+5	v. ikke	N
Jeg kender reglerne for begrænsning af behandling og formålet med dem.	Privat	40%	17%	28%	15%	289
	Offentlig	39%	17%	24%	20%	266
	Alle	**40%**	**17%**	**26%**	**17%**	**555**
Jeg kender vores procedurer for begrænsning af behandling og er i stand til at udføre dem eller ved, hvem der skal gennemføre proceduren.	Privat	42%	18%	24%	17%	289
	Offentlig	38%	16%	26%	20%	266
	Alle	**40%**	**17%**	**25%**	**18%**	**555**

4.2.11 Retten til dataportabilitet

Retten til dataportabilitet handler om personers ret til at modtage alle data, en virksomhed har om vedkommende i et almindelig anvendt og maskinlæsbart format. Det offentlige er ikke fuldt omfattet af denne regel og indgår derfor ikke i besvarelserne.

Kun få medarbejdere kender reglerne eller ved, hvordan de skal gennemføre proceduren, eller hvem der kan

27 % kender reglerne, kun 17 % kan gennemføre proceduren eller ved, hvem der kan. Når først kunderne får øjnene op for deres ret til dataportabilitet, og hvilke muligheder der kan give dem, fx ved skift af bank eller teleselskab, kunne man forestille sig, at det ville blive en relativt almindeligt forekommende procedure. Men hvis kun få i virksomheden ved, at denne ret findes, er der en risiko for, at kunderne bliver afvist eller ikke oplyst om denne ret, hvor dette måtte være relevant.

Retten til dataportabilitet	Sektor	1+2	3	4+5	v. ikke	n
Jeg kender reglerne for dataportabilitet og formålet med disse eller ved, hvem der skal gennemføre proceduren.	Privat	42%	13%	27%	18%	289
Jeg kender vores procedurer om dataportabilitet og er i stand til at udføre dem.	Privat	51%	12%	17%	20%	289

4.2.12 Retten til indsigelse

Retten til indsigelse betyder, at en person til enhver tid har ret til at gøre indsigelse mod behandlingen af sine oplysninger, hvis han eller hun ikke mener, at behandlingen er lovlig. Den dataansvarlige må ikke efterfølgende behandle personoplysningerne, medmindre der er legitime grunde til det.

Kun en fjerdedel kender regler, og kun en fjerdedel kan udføre proceduren for indsigelse eller ved, hvem der kan

Her er der desuden en markant forskel på små, mellemstore og store virksomheders beredskab. I de små virksomheder er det 34 %, der mener, at de kender reglerne, i de mellemstore er det 15 %, og i de store virksomheder er det 24 %. Igen kunne noget tyde på, at de små virksomheder har en "fordel", i at med at når først en af medarbejderne kender reglerne, er der ikke langt til, at de andre, der har brug for det, også kender dem. Når det er sagt, er tallene på ingen måde imponerende, heller ikke for de små virksomheder.

Retten til indsigelse	Sektor	1+2	3	4+5	v. ikke	n
Jeg kender proceduren for håndtering indsigelser og formålet med dem.	Privat	44%	15%	24%	17%	289
	Offentlig	39%	14%	27%	20%	266
	Alle	**42%**	**14%**	**26%**	**18%**	**555**
Jeg er i stand til at udføre proceduren for håndtering af indsigelser eller ved, hvem der skal gennemføre proceduren.	Privat	45%	14%	22%	20%	289
	Offentlig	39%	11%	30%	20%	266
	Alle	**42%**	**12%**	**26%**	**20%**	**555**

4.2.13 Organisering

Over halvdelen af de 113 virksomheder, der har besvaret dette spørgsmål, har endnu ikke udpeget en DPO. En del af dem planlægger dog at gøre det, men det er stadig 40 %, der ikke har planlagt det. Det er dog her vigtigt at huske, at private virksomheder kun behøver en DPO, hvis de behandler personoplysninger som en del af kerneforretningen. Offentlige virksomheder skal have en DPO, men de kan godt dele en med andre offentlige virksomheder eller købe løsning af DPO-opgaven hos eksterne.

Har udpeget DPO		Respondenten selv	Placeret i organisationen	Håndteres af ekstern konsulent	Planlægger at gøre det	Planlægger ikke at gøre det	Ved ikke	Ja I alt	Nej i alt	I alt
Alle	n	5	40	5	15	47	1	50	62	113
	%	4%	35%	4%	13%	42%	1%	44%	55%	100%

Ansvaret for databeskyttelse er først og fremmest placeret i it-afdelingen. Hver femte har en egentlig datasikkerhedsansvarlig, og op i mod halvdelen har også ansvaret placeret i topledelsen.

Ansvarsplacering, Databeskyttelse		It-afdelingen	I topledelsen	Flere afdelinger	Flere geografiske enheder	Datasikkerhedsansvarlig (ikke DPO)	Eksterne konsulenter	Andet	n
Alle	n	76	52	12	5	25	10	8	113
	%	67%	46%	11%	4%	22%	9%	7%	

OBS. Det var muligt at vælge flere valgmuligheder til dette spørgsmål.

4.3 Tværgående temaer

4.3.1 Systemunderstøttelses af procedurer for overholdelse af persondataforordningen

Dette afsnit afdækker virksomhedernes systemunderstøttelse af procedurerne for overholdelse af persondataforordningen.

Alle forordningens krav kan i et eller andet omfang systemunderstøttes, og nogle kræver systemunderstøttelse, hvis de skal gennemføres i praksis. Systemunderstøttelse kan, ud over at lette eller ligefrem muliggøre overholdelse af reglerne, også bidrage til at sikre, at de bliver korrekt og ensartet udført.

Vi har spurgt medarbejderne om deres kendskab til systemunderstøttelsen. Og ud fra medarbejdernes viden at dømme, er systemunderstøttelsen ret beskeden. Nu kan virksomhedens systemer reelt godt understøtte praktiseringen af en given regel, selvom medarbejderne ikke ved det. På den anden side kan medarbejderne på grund af manglende viden om systemunderstøttelsen undlade at gennemføre en procedure eller gennemføre den på en uhensigtsmæssig måde, som enten er unødvendigt ressourcekrævende eller fører til fejl.

Som det fremgår af tabellen med data for de it-ansvarlige, er der i deres virksomheder heller ikke i noget større omfang systemunderstøttelse af procedurerne. Så selvom vi ikke kender overlappet mellem de to grupper af respondenter (it-ansvarlige og medarbejdere), og selvom gruppen af it-ansvarlige deltagere er lille, så tegner der sig et samlet billede af en beskeden systemunderstøttelse.

Databeskyttelsesforordningen stiller *store* krav til organisationerne it-systemer, før processerne kan understøttes digitalt, og det er ikke overraskende, hvis ikke alle er i hus med de nødvendige tilpasninger af systemerne. På nogle områder vil man måske også vente og se, hvor stor efterspørgslen bliver, før man igangsætter evt. omfattende tilretninger af systemerne. Men så bliver det netop vigtigt, at man har procedurerne på plads for, hvordan man så vil håndtere tingene manuelt, så disse ikke skal opfindes ad hoc.

Systemunderstøttelse	1+2	3	4+5	v. ikke	**n**
Begrænsning af opbevaring af data: Vores fællessystemer (fagsystemer, ESDH-systemer etc.) sørger for at slette eller anonymisere personoplysninger, når vi ikke længere må opbevare dem.	**23%**	**8%**	**28%**	**40%**	**555**
Oplysningspligt: Vores systemer understøtter proceduren for oplysningspligt, fx ved indhentning af samtykke, hvor dette kræves, og/eller sikrer, at der gives de nødvendige oplysninger om behandlingen.	**21%**	**14%**	**33%**	**32%**	**555**
Retten til indsigt: Vores systemer understøtter proceduren for håndtering af forespørgsler om indsigt ved fx at gøre det muligt at danne et overblik over, hvilke oplysninger der behandles omkring en given registreret.	**23%**	**14%**	**26%**	**38%**	**555**
Retten til berigtigelse: Vores systemer understøtter vores procedure for håndtering af forespørgsler om berigtigelse ved fx at gøre det let at rette de pågældende oplysninger.	**18%**	**14%**	**24%**	**45%**	**555**
Retten til sletning: Vores systemer understøtter proceduren for håndtering af forespørgsler om sletning ved fx at gøre det let at identificere og slette de pågældende oplysninger (Kun medarbejdere i private virksomheder spurgt).	24%	11%	24%	40%	289
Retten til begrænsning: Vores systemer understøtter proceduren for håndtering af forespørgsler om begrænsning af behandling ved fx at gøre det muligt at sætte alle behandlingsaktiviteter omkring en given person i bero.	**21%**	**11%**	**18%**	**50%**	**555**
Retten til dataportabilitet: Vores systemer understøtter proceduren for håndtering af forespørgsler om dataportabilitet. (Kun medarbejdere i private virksomheder spurgt).	25%	8%	19%	49%	289
Retten til indsigelse: Vores systemer understøtter proceduren for håndtering af indsigelser ved fx at gøre det muligt at sætte alle behandlingsaktiviteter omkring en given person i bero.	**21%**	**11%**	**19%**	**49%**	**555**

De it-ansvarliges syn på systemunderstøttelsen matcher medarbejdernes.

Systemunderstøttelse	1+2	3	4+5	v. ikke	n
Begrænsning af opbevaring af data: Vores fællessystemer understøtter proceduren for opbevaringsbegrænsning ved at muliggøre den tekniske udførelse af fx sletning eller anonymisering.	49%	21%	25%	5%	113
Oplysningspligt: Vores systemer understøtter proceduren for oplysningspligt fx ved indhentning af samtykke, hvor dette kræves, og/eller sikrer, at der gives de nødvendige oplysninger om behandlingen	41%	30%	22%	7%	113
Retten til indsigt: Vores systemer understøtter proceduren for håndtering af forespørgsler om indsigt ved fx at gøre det muligt at danne et overblik over, hvilke oplysninger der behandles omkring en registreret.	55%	24%	16%	5%	113
Retten til berigtigelse: Vores systemer understøtter vores procedure for håndtering af forespørgsler om berigtigelse ved fx at gøre det let at rette de pågældende oplysninger.	46%	25%	25%	4%	113
Retten til sletning: Vores systemer understøtter proceduren for håndtering af forespørgsler om sletning, ved fx at gøre det let at identificere og slette de pågældende oplysninger (Kun it-ansvarlige i private virksomheder spurgt).	58%	24%	15%	3%	89
Retten til begrænsning: Vores systemer understøtter proceduren for håndtering af forespørgsler om begrænsning af behandling ved fx at gøre det muligt at sætte alle behandlingsaktiviteter omkring en given person i bero.	55%	23%	14%	8%	113
Retten til dataportabilitet: Vores systemer understøtter proceduren for håndtering af forespørgsler om dataportabilitet ved fx at muliggøre eksport af personoplysninger i et almindeligt anvendt og maskinlæsbart format (Kun it-ansvarlige i private virksomheder spurgt).	57%	24%	11%	8%	89
Retten til indsigelse: Vores systemer understøtter proceduren for håndtering af indsigelser ved fx at gøre det muligt at sætte alle behandlingsaktiviteter omkring en given person i bero.	56%	26%	12%	6%	113

4.3.2 Små og store virksomheder

Den eneste klare tendens, der tegner sig på tværs af spørgsmålene i forhold til virksomhedsstørrelse, er, at de mellemstore virksomheder er mindre tilbøjelige til at svare 4 eller 5 på spørgsmålene og lidt mere tilbøjelig til at svare 1 eller 2 end de små og store virksomheder.

En mulig forklaring kan handle om, hvordan information udbredes i de forskellige typer virksomheder. Når informationen fx om en GDPR-regel først er nået frem til én person, der arbejder med persondata i en lille virksomhed, vil det være let og uformelt at dele den med de få andre, der arbejder med persondata. Man sidder formodentlig ofte på samme kontor. I de store virksomheder vil man oftere have systemer og rutiner til at sikre udbredelsen af denne type data. Men i de mellemstore virksomheder er man for store til, at viden kan spredes uformelt, og for små til at have effektive systemer og procedurer.

4.3.3 Offentlig/privat

På tværs af temaerne tegner der sig et billede af, at de offentlige virksomheder i højere grad har styr på tingene (svarer 4 eller 5) end de private. Deltagerne fra private virksomheder er mere tilbøjelige til at svare 1 eller 2 eller svare Ved ikke.

Det offentlige har langt flere følsomme persondata, end man typisk har i private virksomheder. Derfor har der også historisk set været mere fokus på persondatasikkerhed i det offentlige. Samtidig er man i det offentlige mere vandt til, at borgerne har en række rettigheder, fx ret til indsigt og indsigelse (klage), end man typisk har i en privat virksomhed.

Det betyder så ikke, at alt er godt i det offentlige. Også her er der (for) mange deltagere, der ikke har tilstrækkeligt styr på regler og procedurer, og også her er der utilstrækkelig systemunderstøttelse.

4.3.4 Mønstre

Dette afsnit afdækker besvarelsesmønstret på tværs af databeskyttelsesforordningens elementer, ved at se nærmere på, hvor mange gange respondenter på det operationelle niveau har svaret i høj eller lav grad til de forståelses- eller evnerelaterede spørgsmål i databeskyttelsesdelen.

Nedenstående tabel viser, hvor mange gange respondenterne på det operationelle niveau har svaret et af følgende: *"1 eller 2"*, *"3"*, *"4 eller 5"* og *"Ved ikke"* til de otte af spørgsmålene om databeskyttelsesforordningen (GDPR), der er stillet til alle deltagere, undtaget de spørgsmål der handler om systemunderstøttelse. Tabellen viser med andre ord den samlede forståelse af og evne til at udføre procedurer for overholdelse af databeskyttelsesforordningen.

GDPR spørgsmål		Antal gange svaret		
		0-5	6-12	13-18
Svar	1 eller 2	59%	22%	18%
	3	86%	13%	1%
	4 eller 5	46%	31%	23%
	Ved ikke	83%	12%	5%

Når en person har svaret *"1 eller 2"*, er det en angivelse af en lav grad af forståelse for eller evne til at udføre procedurerne. Har personen svaret *"4 eller 5"*, angiver det en høj grad af forståelse for eller evne til at udføre procedurerne.

Lidt mere end halvdelen har generelt forståelse for databeskyttelsesforordningens elementer, men kun få har rigtig godt styr på det

Lidt mere end hver anden har i fem eller færre tilfælde svaret, at de i lav grad har forståelse for eller evne til at udføre procedurerne. De virksomheder, hvor disse medarbejdere er ansat, kunne altså se ud til at være godt på vej med implementering og forankring af disse procedurer i organisationen. På den anden side er der hele 18 % på det operationelle niveau, der i 13 eller flere tilfælde har svaret, at de har lavt kendskab til databeskyttelsesforordningens elementer, og hvordan de kan sikre overholdelse af forordningen i deres arbejde. Det skal her tages in mente, at det kun er personer, der har angivet, at de arbejder med persondata i deres arbejde, som har svaret på disse spørgsmål. Derfor må 18 % alt andet lige ses som en stor andel, der har så lavt et kendskab inden for så mange af databeskyttelsesforordningens områder.

En mere positiv konklusion, er at næsten hver fjerde (23 %) har et højt kendskab til databeskyttelsesforordningens forskellige elementer. Der er altså mange virksomheder, der har et stort arbejde foran sig med at få udbredt forståelse for databeskyttelsesforordningens elementer, og hvordan medarbejderne kan overholde disse i deres arbejde. Og der er nogle frontløbere, der er rigtigt langt fremme.

BILAG 1: METODE

Rapporten er baseret på en spørgeskemaundersøgelse foretaget i perioden januar 2018-februar 2018. Rambøll Management Consulting (herefter Rambøll) har i samarbejde med IDA og FSR – danske revisorer udarbejdet nærværende rapport. Rambøll har været udførende i udarbejdelse af spørgeramme, dataindsamling og analyse.

4.4 Målgruppe

Undersøgelsen har til formål at undersøge udrulningen af procedurer, beredskab og awareness om cybersikkerhed og overholdelse af databeskyttelsesforordningen i den offentlige og private sektor. Med henblik på at afdække dette undersøgelsesfelt er følgende fire målgrupper defineret:

Strategisk niveau

1. It-ansvarlige i den offentlige sektor
2. It-ansvarlige i den private sektor

Operationelt niveau

3. Medarbejdere i den offentlige sektor
4. Medarbejdere i den private sektor.

4.5 Spørgeskema

Spørgeskemaet er delt i to afsnit; et, der handler om databeskyttelsesforordningen (GDPR), og et, der handler om cybersikkerhed.

4.5.1 Databeskyttelsesforordningen

På det operationelle niveau er det udelukkende personer, der i spørgeskemaet har angivet, at de arbejder med persondata, der er blevet stillet spørgsmålene omhandlende databeskyttelsesforordningen og de her tilhørende regler og procedurer.

Spørgsmålene er forsøgt stillet således, at kompleksiteten i databeskyttelsesforordningen på den ene side rummes, og at spørgsmålet på den anden side stadig er forståeligt for en almen medarbejder, der arbejder med persondata.

På det strategiske niveau spørges ind til udbredelse af viden om og træning i procedurer relaterede til databeskyttelsesforordningen, medarbejdernes kunnen samt virksomhedens it-systemers evne til at understøtte processerne.

4.5.2 Cybersikkerhed

Samtlige medarbejdere på det operationelle niveau er stillet spørgsmålene relateret til cybersikkerhed, eftersom det kan argumenteres, at alle, der arbejder med en pc eller mobil enhed, der er på nettet, er udsat for cyberangreb. Der spørges i høj grad ind til medarbejdernes egen rolle og kendskab, hvordan de kan mindske risikoen for angreb.

På det strategiske niveau spørges der i højere grad ind til virksomheden forudsætninger for at modstå angreb samt udfordringer og barrierer for at beskytte sig imod angreb.

4.5.3 Justeringer i spørgeskemaet

Der er foretaget to mindre justeringer i spørgeskemaerne, der kan have en lille effekt på besvarelserne, og dette er taget in mente undervejs i analysen. I det store hele antages disse små ændringer at have influeret undersøgelsen i meget lav grad.

Spørgsmålet ”hvor mange indbyggere er der i den kommune, hvor du er ansat?” blev ændret til ”hvis du er ansat i en kommune, hvor mange indbyggere er der så i kommunen, hvor du er ansat?”, eftersom nogle af respondenterne ikke var sikre på, hvordan det første spørgsmål skulle forstås. Yderligere blev der også tilføjet en kategori mere til dette spørgsmål ”jeg er ikke ansat i en kommune”, eftersom nogle af respondenterne ikke var ansat i en kommune.

Ændringen blev foretaget den 18. januar, hvor følgende antal respondenter havde besvaret spørgeskemaet indeholdende det konkrete spørgsmål.

Respondent	Antal
Strategisk niveau i det offentlige	12
Forsyningsvirksomheder	5
Operationelt niveau i det private	354

Yderligere blev der den 17. januar foretaget en ændring i det strategiske niveau i det private spørgeskema, hvor der ved spørgsmålet "har virksomheden indberettet angrebet?" blev tilføjet en mulighed for at afkrydse flere svarmuligheder. Ændringen blev foretaget, da der var 58 respondenter på det strategiske niveau i det private, der havde svaret på spørgeskemaet.

4.6 Dataindsamling

Undersøgelsen er sendt ud via mail til de fire målgrupper, som angivet i nedenstående tabel:

Respondenter	Antal respondenter	Antal besvarelser	Besvarelses procent
Strategisk niveau			
It-ansvarlige i kommunerne	125	24	19,2%
It-ansvarlige i den private sektor	859	89	10,3%
Operationelt niveau			
Medarbejdere i den offentlige sektor	3018	370	12,3%
Medarbejdere i den private sektor	4995	850	17,0%

Dataindsamlingen startede d. 4. januar, hvorefter der er fulgt to opfølgningsmails. Desuden er der taget direkte kontakt via telefon til respondenter i den offentlige sektor, hvor det har været muligt. Undersøgelsen blev afsluttet den 9. februar med ovenstående resultater.

Der er ikke anvendt vægtning.

For yderligere information om datagrundlaget henvises til afsnit 3. Datagrundlag, hvor selve rapportens datagrundlag beskrives.

4.6.1 Frafald af respondenter

Frafald i undersøgelsen kan kategoriseres som inaktive mails (hvor modtager ikke længere har den anvendte mailadresse), generiske svarmails (vedrørende personer, der er syge/på barsel/netop gået på pension eller skiftet job) samt personer, der ikke ønsker at deltage i undersøgelsen.

Respondentgruppe	Frafaldsårsag	Antal
Strategisk niveau		
Offentlige respondenter	Inaktiv mail	12
	Automatiske svarmails	10
	Ønsker ikke at deltage	1
Private respondenter	Inaktiv mail	69
	Automatiske svarmails	55
	Ønsker ikke at deltage	13
Operationelt niveau		
Offentlige og private respondenter	Inaktiv mail	69
	Automatiske svarmails	55
	Ønsker ikke at deltage	13