



# SikkerhedsBranchen

Den danske brancheforening for sikkerhed og sikring

<b>Konkret beskrivelse af problemstillingen</b>	<b>Hvilken databeskyttelsesretlig regel knytter problemstillingen sig til?</b>	<b>Hvilke databeskyttelsesretlige overvejelser har man gjort sig som led i løsningen af problemstillingen?</b>	<b>Har problemstillingen været drøftet med en DPO (data-beskyttelsesrådgiver)? Hvad blev resultatet af drøftelsen</b>
<p>Generelt: Databeskyttelsesreglerne er for komplicerede både indholdsmæssigt og teknisk (artikler på over 1½ side). Indholdsmæssigt er der en hel række grundlæggende usikkerheder hos virksomhederne.</p>	<p>Generelt</p>	<p>Vi støtter en kritisk juridisk gennemgang af GDPR. Se endvidere forslag neden for om helt konkrete vejledninger, et GDPR light system, hvor man stiller de dokumenter, der skal bruges til rådighed, så de blot skal tilrettes den enkelte virksomhed. Som Datatilsynet f.eks. har gjort med databehandleraftaleskabelonen.</p>	<p>Vi er en brancheorganisation og har samlet nedenstående udsagn og forslag blandt 250+ virksomheder. De har været drøftet med DPO'er i medlemsvirksomhederne, i vores stående udvalg og i bestyrelsen. Resultater og forslag har vi valgt at indføre i kolonnen til venstre for denne.</p>
<p>Generelt: Danmarks erhvervsliv består for størstedelen af SMV'er. Vi vurderer, at omkring halvdelen af disse virksomheder har implementeret GDPR og den danske databeskyttelseslovgivning!</p>	<p>Generelt</p>	<p>Vi foreslår en "GDPR-light" model. Selvfølgelig skal man kunne indgå samarbejde og aftaler med SMV'er uden at gå på kompromis med de væsentlige persondatabeskyttelsesregler. Det kan efter vores mening koges ned til 5 – 10 regler med henvisning til de gældende databeskyttelsesregler. Det skal være et system, der er nemt at implementere i de mange virksomheder, der endnu ikke er kommet i gang. Altså ikke bare et sæt regler, men bl.a. eksempler på hvordan de enkelte regler implementeres i praksis. Dette fritager ikke virksomhederne for at leve op til databeskyttelsesreglerne, men man kunne give frit lejde i en periode. På den måde forstået, at man ikke finder bødeblokken frem,</p>	

		hvis virksomhederne har implementeret dette system. På den måde kan vi få de sidste med og langsomt bringe dem op på niveau.	
Generelt: Der mangler praksisnære vejledninger.	Generelt	Vi ved at der findes rigtig mange vejledninger på Datatilsynets hjemmeside. Og at der findes eksempler deri. Der er bare alt for meget fortolkning overladt til virksomhederne. Og selv jurister kan have vanskeligheder. Vi foreslår, at man laver helt konkrete vejledninger til de specifikke problemer, der kommer op i denne proces. Spørgsmål for spørgsmål.	
Generelt: Vi ser en klar tendens til at vejledninger fra EDPB, f.eks. 3/2019 om tv-overvågning er stramninger af den gængse fortolkninger af GDPR og at slutkunder, som f.eks. kommuner misforstår vejledningerne og tror det er gældende ret.	Generelt	Igen er her et konkret problem som forvirrer virksomheder og borgere, og som afføde konkrete svar eller konkrete fortolkning hos Datatilsynet eller JM. Vi har til Datatilsynet fremsendt SikkerhedsBranchens FAQ'er på tv-overvågning og GDPR. De giver et godt indblik i hvilke spørgsmål vi ofte bliver stillet og dermed, hvad der burde være officielle svar og vejledninger på. Vi vedhæfter dem dette skriv.	
Generelt: Ovennævnte tydelige tendens til at EDPB ønsker at skærpe persondataskyddelsen med udvidende fortolkninger bekymrer os fordi vi kan se det har en vis gennemslagskraft i samfundet og også påvirker Datatilsynets udtalelser.	Generelt	Der er ikke behov for stramninger af praksis, der vil pålægge erhvervslivet endnu flere administrative omkostninger. Der er tværtimod brug for nogle få klare fokusområder, så vi får alle med - også de virksomheder, der reelt har givet op.	
Generelt: Overimplementering. Siden GDPR skulle være implementeret har vi set talrige eksempler på overimplementering i virksomhederne. Vi har direkte været i dialog med	Generelt	Igen: Der er brug for praksisnære fortolkninger af konkrete spørgsmål. Se vedhæftede FAQ'er, der giver indblik i de gængse usikkerheder.	

advokater og revisorer, der rådgav deres kunder til voldsom overimplementering. Formentlig fordi de selv var/er usikre på fortolkningen.			
Dataansvarlig, Databehandler, delt dataansvar. Hvem der er hvad hvornår giver anledning til væsentlig tvivl hos rigtig mange virksomheder	Artikel 26 - 29	Igen vi kender vejledningen fra JM og Datatilsynet. Der er brug for noget meget mere konkret. Ned til: Her er systemet. Ret det til så det passer til din virksomhed.	
Hvad er forskellen på personfølsomme og særligt følsomme personoplysninger? Hvordan skal de to kategorier af oplysninger behandles?	Artikel 6 og 9 Dbl § 11	Yderligere vejledning helt ned i detaljen med eksempler. F.eks. oplever vi usikkerhed om hvad man skal når man modtager en mail med personoplysninger i autosignaturen. Vi kender også godt f.eks. Datatilsynets udtalelse publiceret 071119 om behandling af følsomme oplysninger. Men prøv at læse den, selv erfarne jurister på dette område har svært ved at forstå meningen. Der er behov for at få en konkret vejledning eller tilkendegivelse, der undtager helt simple persondata som navn, adresse og telefonnummer. Virksomhederne er usikre på om det kræver en databehandleraftale, hvis en chauffør i en pengetransport får udleveret en liste med ti opsamlingssteder med telefonnumre og navne på kontaktpersoner, der skal adviseres inden ankomst. Det er unødvendig usikkerhed, der kan fjernes med et pennestrøg. Et lige så slående eksempel er en kursusafdeling, der nu kun udleverer deltagerlisten til den kursusansvarlige. Deltagerne kan ikke få listen!	
Generelt: Behandling af persondata.		På samme måde som ovenfor anført er der stor usikkerhed om, hvornår der er tale om behandling.	

		Generelt set er alt jo stort set behandling. Der er behov for en vejledning, der indfører en klar bagatelgrænse.	
Opbevaring af persondata i et fysisk register.	Artikel 2 og 32	Det giver anledning til usikkerhed hos mange både offentlige og private virksomheder, der stadig har papirbaserede persondata i registre, eller hvor oplysningerne ligger på fysisk tilgængelige elektroniske enheder hvordan disse skal opbevares f.eks. i forhold til tilintetgørelse (f.eks. brand), tab og uautoriseret videregivelse (f.eks. tyveri).	
Den dataansvarliges tilsyn med databehandleren.	Artikel 28 stk. 3 litra h	Det giver i praksis anledning til problemer for en række databehandlere. Den dataansvarlige, typisk en offentlig virksomhed, vil ikke selv foretage revision hos sine mange databehandlere, men forlanger at disse skal stille med en revisorerklæring efter ISAE 3000, hvilket er en udgift i 100 – 200.000 kroners klassen. Det bør præciseres at det er den dataansvarlige, der er ansvarlig for revisionen.	
Samtykke.	Artikel 7	Vi ved der findes en vejledning hos Datatilsynet, men denne sammenholdt med forskellige udtalelser fra Datatilsynet er ikke egnet til at vejlede virksomheder uden en juridisk afdeling eller med råd til en husadvokat. Det vil i praksis sige langt de fleste virksomheder i Danmark.	
Databehandleraftale.	Artikel 28	Ros til den konkrete databehandleraftale Datatilsynet stiller til rådighed. Det er præcis den slags virksomhederne har brug for og det detaljeringniveau vi taler om flere steder i nærværende skriv.	

<p>One stop shop. Ledende tilsynsmyndighed. Internationale regler håndteret af et nationalt datatilsyn.</p>	<p>Artikel 56 m.fl.</p>	<p>Ros til dette princip fra virksomheder, der opererer europæisk/internationalt.</p>	
<p>Bøder.</p>	<p>Artikel 83 m.fl.</p>	<p>Vi betragter bødestørrelserne stipuleret i GDPR som en væsentlig årsag til at der foregår overimplementering og overforbrug af ressourcer internt og ekstern bistand på processer som ingen reel værdi har for persondataskyddelsen.</p>	
<p>Gennemsigtighed.</p>	<p>Artikel 12</p>	<p>Vi betragter særligt artikel 12 som en væsentlig beskyttelse af persondatasubjektet. Den er bare blevet for vidtgående, så den åbner vide muligheder for chikane - ikke mindst af anlægsejere af tv-overvågning.</p>	
<p>Kriminalitetsbekæmpelse hindres.</p>	<p>Artikel 7</p>	<p>Når man tegner en forsikring, afgiver man typisk en samtykkeerklæring til at forsikringsselskabet kan indhente oplysninger om økonomiske forhold, mobiltelefonopkald, mastepositioner o.l. for at kunne fastlægge skadelidtes adfærd med henblik på at modvirke forsikringssvindel. Selskaberne/efterforskerne mødes trods det med krav fra teleselskaberne om endnu et samtykke fra skadelidte. Samtykkerne kan være svære at få og er ikke altid "synkroniserede" så man faktisk får de oplysninger man skal bruge. Endnu et eksempel på, at usikkerheden om reglerne og hvad man helt konkret må og skal udløser utilsigtede negative konsekvenser.</p>	