Rådet for Digital Sikkerhed

22. juni 2020

Rådet for Digital Sikkerheds høringssvar vedr. National evaluering af databeskyttelsesreglerne

Justitsministeriet har indledt en national evaluering af databeskyttelsesreglerne. Selv om RfDS ikke er inviteret med i evalueringen, fremsender RfDS hermed sine bemærkninger til evalueringen. Overordnet set påpeger RfDS, at GDPR har været en succes, om end der på visse punkter kan være behov for justeringer – bl.a. mere vidensdeling, samarbejde mellem interesseorganisationer og Datatilsynet om vejledning og obligatorisk efterlevelse af ISO27701 i den offentlige sektor. Disse bemærkninger afsluttes med RfDS' samlede anbefalinger til fremtidige justeringer.

Indledning og processuelle bemærkninger

Rådet for Digital Sikkerhed (RfDS) har noteret sig, at Justitsministeriet har indledt en national evaluering af databeskyttelsesreglerne[1]. Evalueringen omfatter dels en erfaringsindsamling fra relevante interessenter og dels en række juridiske undersøgelser. Selv om RfDS ikke er inviteret med i evalueringen, fremsender RfDS hermed sine bemærkninger til evalueringen.

Rådet for Digital Sikkerhed (RfDS) bemærker, at der ikke er inddraget repræsentanter fra de registrerede i erfaringsindsamlingen. Dette er bemærkelsesværdigt henset til, at reglerne netop har til formål at "beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder" (GDPR, artikel 1). Det er således RfDS' opfattelse, at en evaluering af databeskyttelsesreglerne også burde omfatte de registrerede og vurdere dels om de registreredes rettigheder beskyttes godt nok med reglerne og dels vurdere om reglerne faktisk efterleves tilstrækkeligt til at give en de facto beskyttelse af de registrerede.

- RfDS finder det beklageligt, at Forbrugerrådet Tænk, Institut for Menneskerettigheder, Danmarks DPO-forening, patientforeninger, m.v. ikke inviteres til at give input til evalueringen og skal hermed opfordre til at udvide mængden af aktører der høres – særligt med henblik på at høre synspunkter fra repræsentanter for de registrerede og for at sikre at det input Justitsministeriet modtager er afbalanceret mellem de forskellige aktørers interesser.

Således som den juridiske evaluering er formuleret af Justitsministeriet, lægges der alene op til at begrænse databeskyttelsesforordningens anvendelse.

- Det er RfDS' opfattelse, at evalueringen i højere grad burde tage stilling til om reglerne er dækkende for området og virker efter hensigten – herunder med mulighed for at udvide reglerne til fordel for de registrerede.
- Det kan være problematisk på så tidligt et tidspunkt, hvor effekten i forhold til rettighederne efter GDPR endnu ikke opleves fuldt ud i praksis, at overveje lempelser. Ligeledes afventer vi retspraksis i EU og flere nationale afgørelser.

En stor del af de nuværende persondataretlige regler har haft virkning siden databeskyttelsesdirektivet trådte i kraft i 1995. GDPR justerede på reglerne, men en stor del af de materielle regler har således været i brug i 25 år. GDPR og de nye sanktioner i form af bøder har imidlertid startet en kulturændring i mange organisationer. Med forordningen er der langt flere der har fået kendskab til reglerne og demonstrerer villighed til at efterleve reglerne.

[1] https://www.eu.dk/samling/20191/almdel/EUU/bilag/561/2178305.pdf

Rådet for Digital Sikkerhed
Vester Farimagsgade 37B, 1.th., 1606 København V
Telefon: +45 53 36 02 23 mail: info@digitalsikkerhed.dk web: www.digitalsikkerhed.dk

Fra reglerne blev vedtaget i 2016 blev der i mange organisationer indledt en massiv transformationsproces, som mange steder endnu ikke er tilendebragt. Reglerne har også haft betydelig effekt på arbejdet med informationssikkerhed. Kravene i GDPR artikel 32 om behandlingssikkerhed for de registrerede har ført til et generelt sikkerhedsløft også i forhold til ISO27001/2. GDPR har også medført et helt nyt arbejde med beskyttelse af personoplysninger i lande udenfor EU, hvilket bidrager til at øge sikkerheden for behandling af personoplysninger globalt.

Det er naturligt at evaluere reglerne med det formål at fastslå, om efterlevelsen af reglerne er tilstrækkelig til at sikre de registreredes rettigheder i et digitalt samfund og en digital verden.

- RfDS skal påpege, at det for at kunne fokusere en sådan evaluering kunne være nyttigt med en egentlig analyse af, i hvilket omfang reglerne faktisk efterleves hos dataansvarlige og databehandlere – f.eks. gennem en anonym undersøgelse blandt repræsentativt udvalgte virksomheder og institutioner. Udgangspunktet for en evt. justering og lempelse af reglerne bør ske på baggrund af et solidt faglig korrekt kvalitativt og kvantitativt statistisk grundlag og ikke på baggrund af fx politisk pres.
- En national evaluering kan give anledning til ændring af national lovgivning og yderligere udnyttelse af råderummet for national tilpasning, som er fastlagt i GDPR, men ikke til ændringer af GDPR som sådan.

RfDS' input til evaluering af databeskyttelsesreglerne

Undtagelser for mindre aktører

Det har fra flere parters side været fremført, at der bør indføres undtagelser for mindre aktører, der behandler personoplysninger. Argumentet har været, at det er byrdefuldt for de mindre aktører at efterleve reglerne.

I det oprindelige udspil fra EU Kommissionen var der på visse områder lagt op til lempeligere regler for mindre aktører. Med undtagelse af den næsten ikke eksisterende undtagelse i artikel 30 kom ingen af disse undtagelsesforslag igennem trilogforhandlingerne. Det må tages som udtryk for, at parterne generelt ikke har ønsket at prioritere undtagelser for mindre aktører. Der må derfor være et forholdsvist begrænset anvendelsesområde for at fastsætte nationale undtagelser baseret på organisationers størrelse.

- RfDS mener, at mindre aktører (fastlagt politisk), der ikke behandler følsomme personoplysninger og hvor risikoen for de registrerede ved behandlingen generelt må antages at være lav, bør kunne efterleve lempeligere krav – f.eks. ikke skulle gennemføre konsekvensanalyser i samme omfang eller indhente og gennemgå dokumentation fra databehandlere årligt. RfDS synes derfor, at det kunne være en farbar vej at vurdere, om der indenfor rammerne af GDPR kan håndteres sådanne lempelser.
- Det vil dog i givet fald medføre, at de registreredes garantier og frihedsrettigheder vil blive beskyttet forskelligt, alt efter om det er en stor eller en mindre aktør, der behandler personoplysningerne. Videre vil det øge den persondataretlige kompleksitet, at det skal vurderes, om man er mindre aktør, og om man kan blive omfattet af en sådan undtagelse.

Mere konkret vejledning

GDPR, Databeskyttelsesloven, vejledninger fra EDPB og Datatilsynet og praksis udgør samlet set rammerne for behandlingen af personoplysninger. Det kan virke uoverskueligt for mange, og der er stadig behov for

mere letlæste konkrete og anvendelsesorienterede vejledninger ovenpå dette materiale. Det ses fx af KL's GDPR benspændskatalog[2], hvor nogle kommuner giver udtryk for tvivl om der efter GDPR må komme et navneskilt på en plejehjembeboers dør.

GDPR er fundamentalt set kun et benspænd mod at lave behandling af personoplysninger uden kontrol og sikkerhed. Det er en beskyttelse af de registreredes personoplysninger - de registreredes fundamentale rettigheder og frihedsrettigheder - mod de interessenter som kunne finde på at behandle oplysningerne lemfældigt eller for egen vinding og egne formåls skyld. De udfordringer de dataansvarlige oplever med GDPR bunder således ikke i at GDPR giver en forkert beskyttelse af de registrerede, men skyldes i langt højere grad at vidensniveauet hos de aktører, der skal virkeliggøre reglerne, ikke er tilstrækkeligt.

- RfDS mener, at der er behov for, at interesseorganisationer samler de typiske spørgsmål, som der måtte være fra baglandet og sammen med Datatilsynet laver FAQ'er, så GDPR bliver mere operationel i virkelighedens hverdag – i foreninger, i sportsklubber, på plejehjem, hos automobilforhandlere, hos elinstallatører, i vuggestuer og børnehaver osv. Udarbejdelsen af vejledningsmateriale i samarbejde mellem Datatilsynet og interesseorganisationer kan også bidrage til at styrke interesseorganisationernes faglige profil. RfDS stiller sig gerne til rådighed i forbindelse med såvel medudgivelse som distribution af sådanne vejledninger og FAQ's.
- Ud over ovenstående vejledninger/FAQ'er er det også centralt, at de dataansvarlige kan få hjælp til konkrete vurderinger (f.eks. ekstra konkretisering af tilsyn med leverandører). Datatilsynet bør i højere grad give konkret telefonisk hjælp og herunder bidrage med deres viden om praksis fremfor blot at henvise til, at den dataansvarlige må foretage konkrete vurderinger.

Gør ISO27701 obligatorisk

I efteråret 2019 udkom ISO27701-standarden. Standarden forlænger de eksisterende sikkerhedsstandarder ISO27001/2 med de persondataretlige krav fra GDPR. Standarden er forholdsvis operationel og passer direkte ind i det sikkerhedssetup som allerede er obligatorisk for staten og til en vis grad obligatorisk for regioner og kommuner. Standarden er videre letlæst for personer, som ikke har juridisk baggrundsviden, men måske i højere grad har tekniske kompetencer. Standarden har altså potentialet til at bygge bro mellem jura og teknik på det persondataretlige område og kan således operationalisere GDPR ind i et eksisterende governance framework.

- RfDS foreslår, at ISO27701 gøres obligatorisk for den offentlige sektor på linje med ISO27001/2 inden udgangen af 2021.

Udbyg og udnyt kompetencer

Det er centralt at dataansvarlige og databehandlere har de rette kompetencer eller har viljen til at købe sig til dem.

- Der er behov for at styrke den faglige dybde hos persondataretlige fagfolk lige som der er behov for at styrke bredden således at disse fagfolk kan indgå i dialog om IT-sikkerhed, governance, risiko og compliancedokumentation.

[2] https://www.kl.dk/media/22927/gdpr-benspaendskatalog.pdf

Der findes allerede glimrende uddannelser og internationale certificeringer. Der er behov for at få åbnet op så flere kan tage persondataret som enkeltfag på universiteterne. Ligeledes er der behov for at medarbejdere eksamineres i deres forståelse for de persondataretlige regler på private kurser, f.eks. ved at tage IAPP's certificeringer.

- Ledelserne skal lytte til deres fagfolk. Når en DPO/CPO er kommet med en vurdering, nytter det ikke noget, at den dataansvarlige tilsidesætter denne vurdering af hensyn til andre behov og formål. Der bør oprettes en postkasse for whistleblowere på det persondataretlige område. Formålet skal ikke være at komme efter dataansvarlige. Formålet skal i stedet være at skabe en indikation af, hvor reglerne tilsidesættes, og dermed altså gør mest ondt eller er sværest at efterleve. Der skal naturligvis sikres et minimum af dokumentation og henvisning til hvilke regler, der evt. ikke opretholdes.
- Videre skal det sikres, at DPO'er/CPO'er har mulighed for uredigeret at rapportere til topledelsen og denne ret skal beskyttes af Datatilsynet og det samme gør sig gældende for reglen om, at DPO'en skal kunne arbejde uden nogen form for instruks. En måde at sikre det på, kunne være at den redegørelse for dataetik, som under visse forudsætninger skal vedlægges årsrapporten fra 1. januar 2021, er udarbejdet af den uafhængige DPO. Det vil også være nyttigt, hvis interesseorganisationer ville etablere netværk for deres DPO'er/CPO'er, hvor de kan erfaringsudveksle om udfordringerne indenfor netop deres område.

Samtykke

En af behandlingshjemlerne er som bekendt samtykke efter artikel 6, hvorefter den registrerede kan give samtykke til behandling af sine personoplysninger til et eller flere specifikke formål. Når der fx indhentes samtykke til indsamling af oplysninger i apps eller i forbindelse med brug af internetforbundne produkter, er der dog i praksis sjældent tale om at forbrugeren giver et udtrykkeligt, specifikt samtykke. Ofte er det uklart, hvad firmaet bag appen bruger data til, men i høj grad også i hvilket omfang de deler data med såkaldte 3. parter og hvad disse samarbejdspartnere præcis bruger data til efterfølgende.

- RfDs anbefaler, at der afsættes de fornødne ressourcer til at sikre en effektiv håndhævelse af, hvorvidt de samtykker der indhentes ved brug af digitale tjenester og IoT-produkter er gyldige efter GDPR.

Oplysning

Der skal i henhold til artikel 13 og 14 i GDPR oplyses om behandling af personoplysninger. Oplysningen skal på den ene side være kortfattet og let at forstå, men på den anden side oplyse om alle de behandlinger der foregår. Det er beklageligt, men forståeligt at de to krav vanskeligt lader sig forene. Af frygt for at informere for lidt om behandlingerne og pådrage sig en bøde bliver privacy notices ofte lange.

- RfDS anbefaler, at EU Kommissionen fremlægger forslag til fælleseuropæiske ikoner, så behandling af personoplysninger på en let tilgængelig standardiseret måde kan supplere privacy noticen.

Påbud

Antallet af bøder, som det danske Datatilsyn har indstillet, ligger på fornuftigt niveau med de øvrige EU lande. Det er ikke et formål i sig selv at udstede bøder.

- RfDS vil anbefale, at der ofte anvendes påbud i tilknytning til Datatilsynets afgørelser. Påbud pålægger den dataansvarlige at gøre noget bestemt indenfor en rimelig tid – og hvis det ikke gøres, kan der skrides til bøde. Anvendelsen af påbud vil således reducere den direkte økonomiske risiko, men samtidig være et stærkt incitament til at skabe compliance.

Det forhold at der evt. gennemføres justeringer af anvendelsen af påbud skal dog ikke resultere i at bøder udelukkes. Bøder er helt uomtvisteligt det stærkeste incitament for både offentlige og private dataansvarlige til at efterleve de persondataretlige regler og give individerne en passende beskyttelse af deres personoplysninger.

Overførsel af sager til udenlandske tilsynsmyndigheder

Databeskyttelsesreglerne indfører som bekendt en One Stop Shop mekanisme som betyder, at sagerne skal behandles i det land, hvor den virksomhed, der klages over, har sit hovedsæde. Det skal både lette virksomhedernes efterlevelse af reglerne og sikre en effektiv og ensartet beskyttelse af forbrugernes rettigheder.

Det er imidlertid vigtigt, at den samlede sagsbehandlingstid, fra man klager til Datatilsynet til sagen afgøres af et andet lands datatilsyn, ikke forlænges væsentligt. En meget lang sagsbehandlingstid er ikke til forbrugernes fordel, ligesom det betyder, at en given virksomheds ulovlige praksis ikke bringes til ophør indenfor rimelig tid.

En lang overleveringstid kan også betyde, at det efterfølgende datatilsyn (fx det irske, som er ansvarlig for at behandle klager over techgiganterne) vælger at tage en bestemt sag op af egen drift, fremfor at behandle de konkrete sager på virksomheden, som er blevet indbragt hos de respektive nationale datatilsyn af forbrugerne. Det er på nuværende tidspunkt uklart, hvilke konsekvenser det kan have.

- Der er behov for at effektivisere One Stop Shop mekanismen.

Evaluering af internationalt dataflow

RfDS sikkerhed læser med bekymring jævnligt om et internationalt flow af personoplysninger, hvor det i bedste tilfælde er uklart, om det sker i overensstemmelse med GDPR. Der har f.eks. været omtale af opkøb af anonyme lokationsdata indsamlet via apps, der kunne bruges til at kortlægge personale i det norske forsvars færden. Der har ligeledes været omtale af at Apple via Siri har adgang til uvedkommende personoplysninger.

- RfDS anbefaler, at GDPR evalueres i forhold til effektiviteten til at vurdere og afgøre sådanne hændelser. Det er vigtigt for tilliden til digitaliseringen, at behandling foregår på lovlige og ensartede vilkår for alle aktører.

Økonomiske konsekvenser af GDPR implementering

Frygt for at fortolke forkert og pådrage sig en bøde sammen med besværet ved at ændre systemer og forretningsgange og de økonomiske omkostninger i tilknytning hertil synes at være baggrunden for en vis inerti i forhold til efterlevelse af de persondataretlige regler. Frygt for at fortolke forkert kan omvendt også resultere i overimplementering. Det betyder ikke, at reglerne nødvendigvis er forkerte i betydningen for vidtgående eller for skæve. Når en DPO/CPO laver en vurdering af en foranstaltning, kan det måske for nogle organisationer koste et millionbeløb på bundlinjen, og det er derfor noget, som organisationen skal

udfordre. Det er derfor, vi har brug for mere og mere konkret vejledning f.eks. i form af FAQ'er, som DPO/CPO kan tage med til sit bagland.

Samtidig er det også nødvendigt at de dataansvarlige erkender, at hvis man ønsker at behandle personoplysninger, så har det også en omkostning. Der er en økonomisk omkostning i form af betaling for foranstaltninger. Men der er også en ledelsesmæssig omkostning, hvor man må tage ansvar for sikkerheden for registrerede, som man ønsker at behandle personoplysninger om. Det vil aldrig være muligt at skrive vejledninger om alt, så alle til enhver tid vil være tilfredse.

RfDS påpeger, at det kræver faglig tillid hos de dataansvarlige til at fastholde og implementere deres eksperters vurderinger og indstillinger til ledelsen ift. implementering af GDPR. Ifølge en undersøgelse fra Danmarks DPO Forening oplever 19% af DPO'erne at ledelsen sjældent eller aldrig modtager deres input som værdifulde eller at de bliver hørt og 23% føler at det kun sker nogle dage. 16% føler at de sjældent eller aldrig har et godt samarbejde med ledelsen og 17% føler, at det kun sker nogle dage. Et sådant mod til at stå fast på GDPR er de registreredes garant for beskyttelse i et digitaliseret samfund og en digital verden.

Konklusion

RfDS finder:

- At der er behov for en kvalitativ og kvantitativ analyse af graden af implementering af og udfordringer (for dataansvarlige, databehandlere og registrerede) tilknyttet implementering af de databeskyttelsesretlige regler fremfor en politisk bestemt evaluering
- At der kan være behov for lempelser for mindre aktører, men at det er usikkert om lempelser er det bedste middel og under alle omstændigheder ikke et middel, der kan stå alene
- At der er behov for konkrete sektorspecifikke vejledninger, gerne i form af FAQ'er og gerne i samarbejde mellem Datatilsynet og en bred kreds af interessenter
- At Datatilsynet bør i højere grad tilbyde konkret hjælp til fortolkninger og anvendelse af de persondataretlige regler
- At ISO27701 bør gøres obligatorisk for den offentlige sektor inden udgangen af 2021
- At de juridiske fag om persondataret åbnes op for andre end de indskrevne studerende og at brugen af internationale persondataretlige certificeringer øges
- At der hos Datatilsynet oprettes en whistleblower-postkasse for persondataansvarlige, der kan rapportere om manglende ledelsesopbakning og efterlevelse af reglerne
- At EU Kommissionen får udarbejdet standardiserede ikoner til brug for privacy notices
- At der afsættes de fornødne ressourcer til at håndhæve samtykke-reglerne efter GDPR
- Der er behov for at effektivisere One Stop Shop mekanismen.
- At Datatilsynet bør overveje om anvendelsen af påbud kan udvides
- At det evalueres om GDPR er tilstrækkeligt effektivt til at gribe ind overfor ulovligt internationalt dataflow og hertil knyttede muligheder for aflytning og sporing

Rådet for Digital Sikkerhed
Henning Mortensen
Formand

Rådet for Digital Sikkerhed
Anette Høyrup
Næstformand