NOVEMBER 2019

SVENSKT NÄRINGSLIV

Vad är fel med GDPR?

Beskrivning av näringslivets utmaningar samt några förslag på förbättringar

Av: Martin Brinnen och Daniel Westman

Författarbeskrivning:
Martin Brinnen, senior specialist på advokatfirman Kahn Pedersen, har mer än 25 års erfarenhet från arbete med it-rättsliga frågor särskilt med inriktning på dataskydd. Martin har tidigare arbetat på Datainspektionen och där bl.a. ansvarat för ett antal större tillsynsprojekt.

Daniel Westman, oberoende rådgivare och forskare specialiserad på it- och medierätt. Daniel har skrivit om och arbetat praktiskt med dataskydd i över 20 år. Han har varit rådgivare åt allt från startups till stora organisationer samt expert i flera statliga utredningar.

Förord

Nyheter kan vara goda, men samtidigt besvärliga att hantera. För många företag har dataskyddsförordningen inneburit både förbättringar och försämringar men också en hel del kostnader, förvirring och frustration.

I april 2016 tog Europas regeringar beslut om införandet av den generella dataskyddsförordningen, GDPR. I trialogförhandlingarna mellan Europaparlamentet, medlemsstaterna och EU-kommissionen var det inte helt lätt att enas. Vissa ville ha harmonisering, andra ville behålla nationella särregleringar. Vissa ville skydda medborgarna, andra ville stärka konsumenterna och ytterligare andra värnade företagens digitalisering och konkurrenskraft.

För åtta år sedan gjorde EU-kommissionen en konsekvensbedömning inför förslaget om en ny förordning. Bedömningen blev kritiserad och ifrågasatt redan då och nu behöver regelverket analyseras på nytt. Hur ser dataskyddskartan och behovet ut idag? Med ökad användning av artificiell intelligens, AI, kan dataskyddet både försvåras och drastiskt förenklas. Dokument och processer kan bearbetas och analyseras på detaljnivå. Sannolikt kommer därför ny teknik både förenkla insyn i och tillsyn av hur personuppgifter hanteras i Europa. Men det tjänar litet till om inte företagen mäktar med att följa detta detaljerade och byråkratiska regelverk. Många företag vittnar om stora kostnader och otillräcklig vägledning i hur reglerna ska tolkas och tillämpas i praktiken.

Svenskt Näringsliv har bett dataskyddsjuristerna Martin Brinnen och Daniel Westman att belysa de svårigheter företagen ställs inför vid tillämpningen av GDPR, samt föreslå åtgärder för att förbättra regelverket. Bedömningarna och slutsatserna är författarnas egna. Med denna rapport hoppas Svenskt Näringsliv kunna bidra med kunskap om vad som behöver åtgärdas för att nå ett förutsägbart och rättssäkert dataskydd som fungerar i den allt mer datadrivna ekonomin.

Stockholm november 2019
Carolina Brånby

Sammanfattning

Näringslivets anpassning och utmaningar

Dataskyddsförordningen (GDPR) har gjort att skyddet för den personliga integriteten har fått stor uppmärksamhet. Inte minst gäller detta i näringslivet. Många företag har genomfört ett omfattande och kostsamt anpassningsarbete för att uppfylla GDPR:s krav på dokumentation och rutiner. I många fall har detta lett till att dataskyddet förbättrats avsevärt. I andra fall har det lett till ökad byråkrati utan någon egentlig förbättring av skyddet för enskilda.

Genom GDPR har det blivit allt mer tydligt att det ofta finns en spänning mellan dataskyddslagstiftningen och affärsmodeller som innebär att data (som utgör personuppgifter) ses som en värdefull resurs för ett företag. En osäkerhet kring vad som är tillåtet kan ha en tillbakahållande effekt som går längre än vad som är motiverat för att skydda enskilda och kan innebära att företagen tar ut en riskpremie som i slutänden drabbar kunderna.

Näringslivets utmaningar beror bl.a. på GDPR:s ofta vaga och svårtolkade bestämmelser, bristande harmonisering mellan medlemsstaterna, avsaknad av vägledning samt oklarheter kring internationella dataflöden. Detta leder till en osäkerhet hos många företag om vad som gäller och hur de bör agera. Det breda tillämpningsområdet och den långtgående ambitionen att reglera all behandling av personuppgifter gör att det uppstår direkta motsättningar eller åtminstone spänningar i förhållande till andra regelverk, vilket ytterligare komplicerar tillämpningen av GDPR.

Vad kan göras för att förbättra för företagen?

GDPR är en viktig rättighets- och skyddslagstiftning som har kommit för att stanna, men det finns samtidigt anledning att diskutera utformningen och tillämpningen i vissa delar.

De ***verktyg som står till buds*** är flera. Ändringar, förtydliganden och kompletteringar av regelverket är en metod som i många fall kan ta lång tid. Det gäller såväl GDPR och annan unionsrätt som nationell reglering. Vägledning från tillsynsmyndigheterna får effekt snabbare. Vilken metod som är lämpligast beror förstås på vilket problem som ska lösas.

Vi konstaterar att nationell reglering i vissa fall kan vara ett lämpligt verktyg för att komma till rätta med oklarheter. För att undvika bristande harmonisering inom EU bör sådan reglering tas fram i samråd med andra medlemsstater.

Vad kan göras för att förbättra regelverket?

I vissa delar är problemen av sådan art att det inte är lämpligt att åtgärda dessa genom ändringar i regelverket. I dessa fall är vägledning från EDPB och Datainspektionen att föredra. Oklarheterna kring *GDPR:s tillämpningsområde* och *rollfördelningen mellan den personuppgiftsansvarige och personuppgiftsbiträdet* bör t.ex. hanteras på detta sätt.

Vad gäller utformningen av GDPR anser vi att *den så kallade riskbaserade ansatsen* som var avsedd att underlätta för bl.a. mindre företag bör få ett bättre genomslag i förordningstexten genom uttryckliga begränsningar av ansvar och skyldigheter vid personuppgiftsbehandling som innebär begränsade integritetsrisker.

Vi kan konstatera att utrymmet för att få *behandla känsliga personuppgifter* och *uppgifter om brott* är oklart. Det bör därför införas förtydliganden och ytterligare undantag i svensk rätt, naturligtvis inom ramen för vad GDPR tillåter.

Bestämmelsen om *automatiserat beslutsfattande* i artikel 22 GDRP är oklar och har tolkats restriktivt av Europeiska dataskyddsstyrelsen, (EDPB) och därmed i onödan begränsat möjligheterna att utveckla tjänster med stöd av artificiell intelligens, AI. Vi föreslår att EU-kommissionen analyserar detta i sin översyn av GDPR och att EDPB ser över den befintliga vägledningen. EU bör överväga att ta fram verksamhetsspecifika regler som kompletterar GDPR i syfte att underlätta integritetsvänlig användning av AI.

Förhållandet till amerikansk rätt har under längre tid medfört oklarheter och flera domar från EU-domstolen. Vi föreslår att Datainspektionen i avvaktan på att rättsläget klarläggs tar fram vägledning för hur företagen bör agera.

Hur kan man skapa mer och bättre vägledning?

Genom ökad öppenhet mot de som ska tillämpa GDPR kan Datainspektionen skapa vägledning som tar hänsyn till de utmaningar som dessa står inför. Vi föreslår därför att Datainspektionen skapar nätverk för dialog och erfarenhetsutbyte med berörda parter. Vägledningen bör dessutom innehålla mer konkreta råd bl.a. i form av exempel, checklistor och mallar. Av särskild betydelse är att Datainspektionen ger vägledning om vilka typer av verksamheter som typiskt sett inte innebär särskilda integritetsrisker och hur ansvaret enligt GDPR för dessa bör utövas. I syfte att skapa vägledning i komplicerade och oklara rättsfrågor föreslår vi att Datainspektionen tar fram välmotiverade rättsliga ställningstaganden. Vidare bör Datainspektionens webbplats kunna förbättras genom mer komplett information och bättre funktionalitet, t.ex. videoinspelade utbildningspass och en offentlig version av myndighetens diarium. Staten bör även använda kravställning i samband med offentlig upphandling och innovationsutlysningar för att stimulera framtagande av dataskyddsvänlig teknik.

Effektivare och mer förutsebar tillsyn

I de fall rättsläget förändras, t.ex. genom ny rättspraxis, är det lämpligt att företag får tid på sig att anpassa sin verksamhet. Datainspektionen bör därför tillåta övergångsperioder innan tillsyn inleds.

Sanktionsavgifter som Datainspektionen kan besluta om har medfört en stor rädsla för att göra felaktiga bedömningar av vad som är tillåtet och resulterat i att projekt stoppats eller begränsats i onödan. Det är därför viktigt att Datainspektionen klargör när företag riskerar att drabbas av sanktionsavgifter.

Att överklaga Datainspektionens beslut tar i regel lång tid och är oftast kostsamt. Det finns samtidigt ett stort behov av ny domstolspraxis. Det kan därför finnas anledning att utreda olika förslag för att underlätta överklaganden av Datainspektionens beslut.

Sammanfattningsvis konstaterar vi att GDPR är här för att stanna och att den grundläggande regleringsmodellen inte bör förändras. Det krävs dock bättre harmonisering av nationella regler och tillämpningen av dessa. Den svenska kompletterande regleringen i dataskyddslagen tillkom under tidspress och med ambitionen att ändra så lite så möjligt. Det finns därför redan nu ett behov av att se över dataskyddslagen. En stor börda för att komma till rätta med problemen med GDPR faller på Datainspektionen och vi ser därför behov av att stärka Datainspektionens förebyggande verksamhet.

Innehåll

1. Inledning

Dataskyddsförordningen (GDPR)[1] har nu tillämpats i över ett år. Även om det krävs längre tid för att fullt ut bedöma effekterna av GDPR finns det redan nu anledning till reflektion och förbättringsförslag.

Denna rapport analyserar näringslivets utmaningar på dataskyddsområdet och diskuterar vilka åtgärder som kan vidtas för att skapa en mer ändamålsenlig reglering.

När dataskyddsregler utformas, vägledning ges och tillsyn utförs måste naturligtvis en mängd olika intressen beaktas. Att fokus här riktas mot näringslivets utmaningar och hur företagens dataskyddsarbete kan förenklas innebär inte att andra intressen anses oviktiga. Tvärtom måste företagens utmaningar och förslag på nya lösningar alltid relateras till de registrerades rättigheter och intressen. Utgångspunkten är att de registrerades skydd inte ska försämras i någon beaktansvärd utsträckning när vi föreslår förändringar.

Rapporten bygger inte på någon egen empirisk undersökning. Vi har framför allt utgått från våra erfarenheter av många års praktiskt dataskyddsarbete. Vi har emellertid tagit del av utvärderingar som andra har gjort och synpunkter som har förts fram, t.ex. till EU-kommissionen, Datainspektionen och Svenskt Näringsliv. Vi har också samtalat med bolagsjurister och branschföreträdare inom näringslivet om deras erfarenheter.

Dataskyddslagstiftningen är omfattande och komplex. Den berör många verksamheter och ger upphov till skiftande tillämpningsutmaningar i olika sammanhang. Vi har trots detta försökt begränsa denna rapports omfattning. Vi inventerar näringslivets dataskyddsutmaningar och skissar olika typer av lösningar. Fördjupade analyser får göras i andra sammanhang.

En stor börda för att komma till rätta med de problem som vi diskuterar i denna rapport faller på Datainspektionen. Vi vill redan inledningsvis göra klart att vi har förståelse för Datainspektionens utmaningar. Datainspektionens uppdrag och verksamhet har i och med dataskyddsreformen förändrats i grunden. Samtidigt som förväntningarna från omvärlden på vägledning m.m. har ökat, har en mängd nya uppgifter lagts på myndigheten. Det är förståeligt att myndigheten inte har hunnit med alla nya utmaningar trots ökade resurser. Utvecklingen går dock i rätt riktning. Datainspektionen har tagit flera vällovliga initiativ till att öka det förebyggande arbetet med vägledningar. I rapporten ger vi förslag på hur detta arbete kan fortsätta på olika områden.

[1] EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679 av den om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EC (allmän dataskyddsförordning).

2. Dataskyddslagstiftningen

2.1 Grunder och utveckling

Dataskyddslagstiftningen reglerar hur personuppgifter får behandlas och ger den vars personuppgifter behandlas (den registrerade) vissa rättigheter. Som personuppgifter räknas alla uppgifter som avser en identifierad eller identifierbar fysisk person.

Ett företag som behandlar personuppgifter, t.ex. om sina anställda och kunder, räknas som personuppgiftsansvarig. Den personuppgiftsansvarige måste följa dataskyddslagstiftningens grundläggande behandlingsprinciper, säkerställa att det finns rättsligt stöd för alla behandlingar, vidta teknisk och organisatoriska åtgärder för att skydda personuppgifterna samt följa vissa rutiner, t.ex. rörande dokumentation och rapportering av personuppgiftsincidenter.

Av mediebevakningen kan man lätt få intrycket att dataskyddsreglering är något helt nytt som har införts genom GDPR, men Sverige har haft regler om personregister (datalagen) och behandling av personuppgifter (personuppgiftslagen) sedan 1970-talet. Syftet har varit att skydda den personliga integriteten och särskilt att motverka de risker som digital behandling av personuppgifter har ansetts medföra.

Dataskyddslagstiftningen har med tiden fått allt större betydelse. Det beror dels på den tekniska utvecklingen, som innebär att en alltmer omfattande behandling av personuppgifter blivit möjlig, dels på att dataskyddslagstiftningen i flera omgångar har byggts ut, bl.a. för att möta de risker som en mer omfattande behandling har ansetts innebära. De grundläggande principerna från 1970-talet är dock i stora delar oförändrade.

Dataskyddslagstiftningen har under lång tid varit starkt internationellt präglad, tidigare främst genom Europarådet och OECD. Sedan 1995, när det så kallade dataskyddsdirektivet[2] antogs, har emellertid EU varit den viktigaste aktören på dataskyddsområdet. Syfte med EU:s dataskyddsregler är dubbelt dels att skydda enskildas personuppgifter och privatliv, dels att förhindra att divergerande nationella dataskyddsregler hindrar den fria rörligheten inom EU.

Dataskyddet är emellertid inte längre en rent europisk företeelse. Över 130 stater har idag dataskyddslagstiftningar av europeiskt snitt, även om alla inte är lika strikta som de nu gällande EU-reglerna. USA sticker i detta sammanhang ut eftersom landet saknar en heltäckande dataskyddslagstiftning på federal nivå. På senare tid har emellertid flera delstater infört lagstiftningar av detta slag, samtidigt som det har förts en intensiv diskussion om en federal lagstiftning.

[2] Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter..

2.2 Dataskydd som en grundläggande rättighet

Genom EU:s rättighetsstadga – som blev bindande när Lissabonfördraget trädde i kraft 2009 – har skyddet av personuppgifter i sig uppgraderats till en grundläggande rättighet enligt EU-rätten. I praktiken innebär detta att det sätts en större juridisk tyngd bakom dataskyddslagstiftningen. Med hänvisning till rättighetsstadgan har EU-domstolen i flera uppmärksammade mål givit reglerna om behandling av personuppgifter en strikt tolkning.

Denna utveckling påverkar inte bara myndigheters behandling av personuppgifter, utan även dataskyddslagstiftningens ställning i den privata sektorn.

Rätten till skydd av personuppgifter är inte någon absolut rättighet. En avvägning måste göras med andra grundläggande rättigheter, t.ex. skyddet för yttrandefriheten och rätten till näringsfrihet. I EU-domstolens rättspraxis har dock näringsfriheten ansetts väga relativt lätt i förhållande till skyddet för personuppgifter.

Man kan – enkelt uttryckt – säga att den EU-rättsliga utgångspunkten är att den registrerade har en principiell rätt att kontrollera behandlingen av sina personuppgifter och att denna rätt bara får begränsas på ett sätt som är proportionerligt.

2.3 Viktiga nyheter i dataskyddsreformen

Dataskyddsreformen innebar bl.a. att dataskyddsdirektivet och den svenska personuppgiftslagen den 25 maj 2018 ersattes av GDPR och vissa kompletterade bestämmelser i den så kallade dataskyddslagen och i andra specialförfattningar.

De uttryckliga syftena bakom dataskyddsreformen var att modernisera dataskyddet, att öka harmoniseringen mellan medlemsstaterna och att stärka de registrerades skydd i vissa delar.

Den grundläggande dataskyddsrättsliga regleringsmodellen, som bygger på att i princip all behandling av personuppgifter regleras, är densamma. Behandlingen av personuppgifter är bara tillåten om ett antal grundläggande behandlingsprinciper iakttas och det finns ett tydligt rättsligt stöd för behandlingen. Särskilt restriktiva regler gäller liksom tidigare för vissa behandlingar. Behandlingsreglerna kompletteras med krav på informationssäkerhet samt vissa rättigheter för de registrerade, t.ex. rätt till information och insyn i behandlingen.

Några viktiga materiella nyheter i förordningen beskrivs i det följande.

En viktig nyhet är att förordningen saknar motsvarighet till den så kallade missbruksregeln (5 a § personuppgiftslagen), som i praktiken innebar betydligt friare tyglar för behandling av personuppgifter i ostrukturerad form, t.ex. i löpande text.

Samtidigt har kraven för att behandling ska få ske med stöd av samtycke skärpts, bl.a. genom att kraven på vad som är ett giltigt samtycke har stramats upp.

Det principiella förbudet mot behandling av känsliga personuppgifter har fått ett vidare tillämpningsområde och omfattar nu även genetiska och biometriska uppgifter. Regleringen träffar därmed t.ex. ansiktsigenkänning.

Den personuppgiftsansvarige är numera skyldig att lämna mer omfattande information om behandlingen till den registrerade och den registrerades ges en principiell rätt att få så kallade registerutdrag även i elektronisk form.

Två nya – mycket omtalade och politiskt omhuldade – rättigheter har införts: rätten till radering (”rätten att bli bortglömd”) och rätten till dataportabilitet. Även om dessa rättigheter innebär en viss förstärkning av den registrerades rättsskydd är det i huvudsak fråga om en kodifiering och en begränsad utvidgning av redan existerande rättigheter.

Det krävs uttryckligen att IT-system eller arbetsprocesser utformas så att dataskyddet praktiskt implementeras (”inbyggt dataskydd” och ”dataskydd som standard”).

Skyldigheter att dokumentera och i många fall rapportera så kallade personuppgiftsincidenter till Datainspektionen och till berörda registrerade införs.

Krav på konsekvensbedömning och, i vissa fall, samråd med Datainspektionen har införts för behandlingar som innebär hög risk för integritetskränkningar.

I många verksamheter har det blivit obligatoriskt att ha ett så kallade dataskyddsombud som granskar personuppgiftsbehandlingen och ger råd till verksamheten. Förordningen ställer särskilda krav på ombudets kompetens, mandat och ställning.

Förordningen ställer mer utförliga krav på personuppgiftsansvariga som vill använda sig av så kallade personuppgiftsbiträden (t.ex. leverantörer av drifts- eller molntjänster som hanterar kundens personuppgifter). Därutöver innebär förordningen att biträdena får vissa direkta skyldigheter, t.ex. att ha en godtagbar säkerhet i sin tjänst, och ett därtill kopplat ansvar om de bryter mot dessa skyldigheter.

Det har även blivit möjligt att utdöma mycket höga administrativa sanktionsavgifter om förordningens regler inte efterlevs (upp till 20 miljoner euro eller, om det är högre, 4 % av den personuppgiftsansvariges globala årsomsättning).

3. Näringslivets anpassningar till GDPR

3.1 Utgångsläge och ambitionsnivå

Svenska företags *utgångsläge* inför anpassningen till GDPR varierade stort. Många företag hade redan ett fungerande dataskyddsarbete och kunde sägas leva upp till stora delar av personuppgiftslagens krav. Men det är ingen hemlighet att det också fanns många företag där situationen var otillfredsställande. Utgångläget har naturligtvis påverkat förutsättningarna för anpassningen till GDPR:s mycket höga krav.

Även *ambitionsnivån* i anpassningsarbetet har varierat från företag till företag. Många har tagit dataskyddsarbetet på stort allvar och t.ex. utnyttjat GDPR till att få bättre kontroll på sin informationshantering och sitt säkerhetsarbete, något som har lett till positiva effekter även i andra sammanhang.

Andra företag har – av olika skäl – begränsat sin insats till de utåt mest synliga delarna av dataskyddet, t.ex. dataskyddspolicyn, och till att uppfylla formkrav, t.ex. skyldigheten att föra ett register över behandlingar och skyldigheten att utse ett dataskyddsombud. För dessa företag – ofta mindre och medelstora företag – återstår stora delar av anpassningsarbetet.

3.2 Ett omfattande och kostsamt genomförandearbete

Många företag har vittnat om ett omfattande och kostsamt genomförandearbete. Arbetskrävande moment har t.ex. varit att inventera befintliga system och gå igenom rutiner, att göra rättsliga bedömningar och att anpassa IT-system och organisatoriska rutiner. Även uppdatering av informationstexter och utbildning för olika yrkesgrupper har varit krävande.

I vissa fall kan de höga kostnaderna förklaras av att företaget har haft en ”dataskyddsskuld”, men även företag med ett relativt gott utgångsläge har haft stora genomförandekostnader. Dessa kostnader har inte i alla fall lett till en motsvarande förbättring av det reella skyddet för enskildas personuppgifter. En förklaring till detta är att delar av dataskyddsreformen kan sägas innebära en ökad byråkrati som inte automatiskt ger resultat i form av ett förbättrat skydd.

I vissa fall tycks genomförandearbetet dessutom ha bedrivits mindre effektivt. Flera stora företag har t.ex. initierat kostsamma konsultdrivna genomförandeprojekt. Det har förekommit att sanktionsrisken använts för att sälja in större insatser än vad som framstår som motiverat och ibland har kompetensen hos konsulterna varit bristande. Ett annat problem som har observerats är att det ibland har varit svårt att föra över kompetens från ett genomförandeprojekt till den operativa organisationen, vilket medfört att gjorda investeringar inte fullt ut har kunnat tas till vara.

Ett område som medfört höga konsultkostnader är t.ex. upprättande, granskning och förhandling av personuppgiftsbiträdesavtal. Genom större samordning och framtagande av malldokument borde dessa resurser i många fall ha kunnat använts mer effektivt. I vissa andra länder har t.ex. tillsynsmyndigheten tagit fram standardvillkor för biträdesrelationen. Samtidigt har det visats sig att det i mer komplicerade fall finns risker med använda mallar.

3.3 Nya rutiner och arbetssätt

I många företag har dataskyddet förbättrats avsevärt genom nya rutiner och genom nya tekniska och organisatoriska åtgärder. I andra fall har anpassningsarbetet resulterat i en ökad byråkrati som inte förbättrar det reella skyddet för de registrerade.

En viktig framgångsfaktor för ett effektivt, men samtidigt smidigt, dataskydd är att det byggs in i tekniska lösningar och organisatoriska rutiner på det sätt som förutsätts i artikel 25 GDPR. Det är emellertid många gånger lättare sagt än gjort. Ofta krävs grundläggande förändringar av företagets sätt att arbeta i kombination med en ny utformning av tekniska system, vilket dels kräver att dataskyddet har den ställning i organisationen att det tillåts påverka på detta sätt, dels att det finns tid och resurser för sådana förändringar.

3.4 Direkt påverkan på affärsverksamheten

Vi har inte stött på några fall där dataskyddsreformen resulterat i att ett företag helt har tvingats upphöra med en sund affärsverksamhet. Däremot finns naturligtvis många exempel där krav på en mer begränsad behandling av personuppgifter har lett till förändringar i hur verksamheter bedrivs.

Ett sådant exempel är användningen av personuppgifter för direkt marknadsföring. I samband med genomförandearbetet har t.ex. många företag gallrat personuppgifter om icke-aktiva kunder och de kan därmed inte längre nå dessa med direktmarknadsföring. GDPR har också lett till en mer kritisk diskussion kring automatisk insamling av personuppgifter om webbplatsbesökare, som sedan ofta används för marknadsföring. I förlängningen kan GDPR komma att leda till mer begränsade möjligheter att använda tredjepartsaktörers befintliga annonseringslösningar, eftersom dessa många gånger innebär en omfattande delning av personuppgifter mellan företag och inte sällan en överföring till länder utanför EU.

I huvudsak tycks det i de nämnda fallen handla om en mer effektiv och korrekt tillämpning av sådana behandlingsregler som gällt redan under personuppgiftslagens tid. En ökad medvetenhet och risk för höga sanktionsavgifter har lett fram till ett förändrat förhållningssätt.

Genom GDPR har det emellertid blivit allt mer tydligt att det ofta finns en spänning mellan dataskyddslagstiftningen och affärsmodeller som innebär att data (som utgör personuppgifter) ses som en värdefull resurs för företaget. En osäkerhet kring vad som är tillåtet och inte kan ha en tillbakahållande effekt som går längre än vad som är motiverat för att skydda enskilda och innebära att företag tar ut en riskpremie som i slutänden drabbar kunderna.

Men en striktare dataskyddslagstiftning kan också leda till nya affärsmöjligheter. Det har t.ex. under de senaste åren växt fram en mängd nya företag som erbjuder dataskyddsvänliga lösningar och system. Troligtvis är detta område ännu bara i sin linda.

Samtidigt får de små och medelstora företagen (SME) allt svårare att konkurrera med de internationella plattformsföretagen. Samtycke från presumtiva kunder är betydligt lättare för stora och etablerade tjänsteföretag att inhämta och erhålla. Det kan innebära att företagen får allt mindre tillgång till sina kunders personuppgifter. Uppgifterna stannar hos plattformarna, som kan öka sina marknadsandelar.

4. Näringslivets utmaningar

4.1 Inledning

Svenska företag har, som konstaterats i föregående avsnitt, haft utmaningar att anpassa sig till dataskyddslagstiftnigen. I detta avsnitt analyseras närmare vari dessa utmaningar består. Möjliga sätt att hantera dessa utmaningar diskuteras i avsnitt 5.

4.2 Ett omfattande och komplext regelverk

Dataskyddslagstiftningen har ett mycket brett tillämpningsområde och personuppgifter behandlas i en lång rad olika situationer. Samtidigt har lagstiftningens materiella innehåll med åren blivit allt mer omfattande och komplext. GDPR innehåller t.ex. 99 artiklar och 173 skäl. Utöver GDPR finns ett antal kompletterande regelverk på EU-nivå och på nationell nivå.

Det är uppenbart att dataskyddet har blivit ett juridiskt specialistområde. Men den som arbetar med dataskydd behöver inte bara juridiska kunskaper, utan det krävs även kunskap om teknik, t.ex. it- och informationssäkerhet, och om den faktiska hanteringen av personuppgifter i en organisation.

4.3 Vaga och svårtolkade regler

Äldre dataskyddlagstiftning var uppbyggd kring administrativa förfaranden med tillstånd för varje behandling. Genom GDPR fullbordas de senaste tjugo årens utveckling mot ett regelverk som innebär att den som behandlar personuppgifter ska kunna visa hur denne uppfyller lagstiftningen krav. Denna ansvarsprincip kommer bl.a. till uttryck i artikel 5.2 och 24 GDPR.

Samtidigt är centrala delar av dataskyddsregleringen vag och svårtolkad. Det gäller bl.a. de grundläggande principerna i artikel 5 och bestämmelsen om rättsligt stöd i artikel 6 GDPR, där det bl.a. ställs krav på att en behandling ska vara ”nödvändig”. Även bestämmelserna i artikel 25 GDPR om inbyggt dataskydd och dataskydd som standard är vaga och svårtolkade.

Detta leder till osäkerhet hos många företag om vad som gäller och hur de bör agera. De flesta företag vill göra rätt, men ofta kan det krävas kvalificerad juridisk rådgivning för att få tydlighet om vad som faktiskt gäller.

Till saken hör att dataskyddsreglerna måste tillämpas av många olika personer i en organisation, inte bara av specialister. I sådana sammanhang är naturligtvis reglernas vaghet extra besvärlig.

Ett möjligt sätt för ett företag att hantera vagheten är naturligtvis att begränsa behandlingen av personuppgifter kraftigt. Men ett sådant förhållningssätt innebär inte bara risk för att företagets affärsintressen skadas. De registrerade kan uppleva att de får sämre service utan att motsvarande nytta för den personliga integriteten uppstår. En annan möjlig utveckling är att företag börjar ta ut en riskpremie av sina kunder.

4.4 Problematiskt förhållande till andra regelverk

Det breda tillämpningsområdet och den långtgående ambitionen att reglera all behandling av personuppgifter gör att det uppstår direkta motsättningar eller åtminstone spänningar i förhållande till andra regelverk. När det gäller företags användning av sociala medier måste det t.ex. ofta göras en avvägning mellan rätten till dataskydd och rätten till yttrandefrihet.

Särskilda regelverk, t.ex. på det finansiella området, som ålägger företag att spara eller lämna ut viss information kan många gånger dra åt ett annat håll än dataskyddsregleringen, även om det inte uppkommer en direkt regelkonflikt. Om sådana regler om bevarande och utlämnade av personuppgifter inte är precisa, t.ex. när det gäller lagringstid, riskerar företagen att hamna i kläm mellan regelverken.

Dessa problem blir särskilt tydliga i relation till de mer restriktiva reglerna om behandling av känsliga personuppgifter och uppgifter om brott. Beträffande dessa typer av uppgifter finns det inte alltid stöd för en behandling av personuppgifter på ett sätt som gör att företaget kan leva upp till ändamålen med den andra lagstiftningen (se nedan avsnitt 5.3.5 och 5.3.6).

Krav på t.ex. bevarande och utlämnande av personuppgifter som finns i lagstiftning utanför EU räknas inte som en sådan rättslig förpliktelse som ger rätt att behandla personuppgifter enligt GDPR. Detta trots att ett företag riskerar ansvar i det aktuella landet om det inte efterlever kravet. Ibland kan ett företag därmed hamna i situationer där det måste bryta antingen mot GDPR eller mot ett annat lands nationella lag (se nedan avsnitt 5.3.8).

Även förhållandet mellan olika dataskyddsregler är ibland problematiskt eller svårbedömt. Ett exempel är relationen mellan GDPR och de så kallade ePrivacy-reglerna rörande användning av kakor och liknande identifieringsteknik, i Sverige genomförda genom lagen (2003:389) om elektronisk kommunikation.

4.5 Bristande harmonisering inom EU/EES

Ett viktigt mål med GDPR var att öka harmoniseringen inom EU/EES. Även om detta mål i viss utsträckning har uppnåtts återstår nationellt skilda tolkningar i många frågor, inte sällan på grund av att äldre dataskyddstraditioner lever vidare. Detta skapar problem för företag som är verksamma i flera EU-länder, men kan också leda till snedvriden konkurrens på den inre marknaden.

GDPR tillåter nationell särreglering på vissa områden, t.ex. när det gäller förutsättningarna för att behandla känsliga personuppgifter och uppgifter om brott. Det finns i praktiken betydelsefulla skillnader mellan jämförbara länder.

Inom det område som är fullständigt harmoniserat i GDPR är tillsynsmyndigheternas vägledning inte helt samordnad. Även om den Europiska dataskyddsstyrelsen (EDPB) har kommit med EU-gemensamma vägledningar på många områden finns det dels många områden som ännu inte behandlats, dels visst tolkningsutrymme inom ramen för dessa vägledningar som har utnyttjats på olika sätt i olika länder.

4.6 Osäkerhet kring internationella dataflöden

Dataskyddslagstiftningen innehåller särskilt restriktiva regler för överföring av personuppgifter till tredje land, dvs. ett land utanför EU/EES. De mekanismer (främst de så kallade standardavtalsklausulerna och Privacy Shield) som syftar till att under vissa förutsättningar möjliggöra överföringar till bestämda mottagare är inte heltäckande. I vissa fall kan en överföring därför vara villkorad av att den registrerade lämnar sitt samtycke, trots att detta inte är ett realistiskt alternativ i praktiken.

Situationen kompliceras av att standardavtalsklausulerna och Privacy Shield för närvarande är föremål för rättslig prövning i EU-domstolen. Domstolen har vid ett tidigare tillfälle ogiltigförklarat en liknande mekanism för överföring av personuppgifter till USA, nämligen Safe Harbor-systemet (se avsnitt 5.3.8).

Ett underkännande även av standardavtalsklausulerna och/eller Privacy Shield skulle skapa stora problem i världshandeln, men även för företag som använder sig av nättjänster i sin verksamhet som tillhandahålls av amerikanska företag.

4.7 Strukturella förändringar av den egna verksamheten

Ett väl fungerande dataskydd kräver ofta strukturella förändringar i hanteringen av personuppgifter. Det kan handla om att förändra hur personuppgifter samlas in, vilken information och vilka valmöjligheter som den registrerade erbjuds och om att förse personuppgifterna med metadata om hur de får behandlas i framtiden.

Sådana förändringar blir ofta kostsamma eftersom de kräver förändringar av it-system och grundläggande arbetssätt. Även om många företag ser fördelen med att genomföra denna typ av strukturella förändringar kommer förändringarna att ta tid.

4.8 Sanktionsrisker

Personuppgiftslagen innehöll ett relativt mjukt sanktionssystem, även om det fanns fängelse i straffskalan för vissa allvarligare överträdelser av lagen. GDPR:s kraftfulla sanktionsavgifter har förändrat situationen för företag radikalt. Tillsynsmyndigheter i andra länder har redan beslutat om höga sanktionsavgifter för företag som t.ex. inte har vidtagit tillräckliga säkerhetsåtgärder, behandlat personuppgifter utan rättsligt stöd eller lämnat ofullständig och vilseledande information om personuppgiftsbehandlingen till de registrerade.

Många företag upplever kombinationen vaga och svårtolkade regler och kraftfulla sanktioner som problematisk. En rättvis och proportionerlig tillämpning av sanktionsavgifterna efterlyses och extra tolerans när rättsläget kan sägas vara oklart och företagen har utfört en behandling i god tro efter en noggrann analys.

För att seriösa företag, som enligt vad som sagts ovan har lagt ner stora resurser på att efterleva dataskyddsreglerna, inte ska drabbas av illojal konkurrens krävs samtidigt att oseriösa företag som bryter mot dataskyddsreglerna verkligen drabbas av sanktioner.

I vissa branscher uppfattas riskerna för skadeståndskrav i form av grupptalan som ett oförutsebart hot.

4.9 Hinder mot utveckling och användning av AI

En stor del av näringslivets innovation är idag kopplad till AI. De datamängder som används för upplärning av algoritmer kan innehålla personuppgifter. Även om de enskilda individerna inte står i fokus i samband med *maskininlärning* är det ibland oklart om behandlingen kan uppfylla de grundläggande dataskyddsprinciperna, krav på ett tydligt rättsligt stöd för behandling samt reglerna om transparens.

Dataskyddet påverkar även själva *användningen* av AI-system. När algoritmer används för att analysera personuppgifter, t.ex. skapa kundprofiler eller fatta beslut, blir de materiella dataskyddsreglerna också tillämpliga. Av särskilt intresse i detta sammanhang är rätten för enskilda att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inbegripet profilering, som får rättsliga följder för den enskilde eller som på liknande sätt i betydande grad påverkar denne, se artikel 22 i GDPR. EDPB:s tolkning av denna reglering har så här långt varit strikt.

Det råder ingen tvekan om att det finns betydande risker förknippade med viss användning av AI, men det finns också stora potentialer att lösa olika samhällsutmaningar. Det är viktigt att dataskyddslagstiftning ges en korrekt utformning och en balanserad tillämpning på detta område. (se avsnitt 5.3.7 nedan).

5. Vad kan göras för att förbättra för företagen?

5.1 Inledning

I detta avsnitt diskuterar vi hur näringslivets utmaningar på dataskyddsområdet kan hanteras.

I avsnittet 5.2 analyserar vi på ett generellt plan för- och nackdelar med olika verktyg som kan användas för att komma till rätta med problem med GDPR. I avsnitt 5.3 går vi igenom hur dessa verktyg kan användas för att åtgärda vissa konkreta problem som finns i unionsrätten och i svensk rätt. I avsnitt 5.4 riktas fokus på vad som kan göras även utan ändringar i regelverket, främst i form av vägledning. I avsnitt 5.5 diskuterar vi Datainspektionens tillsynsverksamhet och formerna för överklagande av myndighetens beslut.

Vi presenterar inga färdiga förslag, utan ger endast uppslag till åtgärder som kan övervägas. Vi är medvetna om att vissa av förslagen som är avsedda att lösa ett problem kan få oönskade konsekvenser i andra avseenden. Som exempel kan nämnas att mer vägledning från Datainspektionen riskerar att leda till att harmoniseringen inom EU blir sämre.

5.2 Vilka verktyg står till buds?

5.2.1 Ändra GDPR

GDPR har av många uppfattats som en stor framgång för EU och ett viktigt verktyg för att hantera riskerna förknippade med en storskalig behandling av personuppgifter. Den europeiska dataskyddsmodellen har under de senaste decennierna spritts till ett stort antal länder i världen. Mot den bakgrunden är det inte troligt att det finns en vilja inom EU att förändra den grundläggande regleringsmodellen.

Därtill kommer att de grundläggande elementen i GDPR bygger på EU:s stadga om de grundläggande rättigheterna. EU-domstolen har vid tillämpningen av dataskyddsdirektivet tolkat stadgan på ett sätt som begränsar möjligheterna att genomföra grundläggande förändringar i regelverket.

Sammanfattningsvis är utrymmet för reformer alltså i praktiken begränsat till mindre justeringar och förtydliganden.

Ändringar av en EU-förordning – särskilt en förordning som är förknippad med många olika intressen – kräver omfattande förberedande arbete, komplicerade förhandlingar och lång övergångstid. Det kan därför ta tid innan även mindre ändringar av GDPR skulle bli tillämpliga.

Inte desto mindre är det viktigt att utvärderingsarbetet bedrivs aktivt så att behovet av ändringar kan identifieras på ett tidigt stadium. Arbetet är viktigt för att förmedla erfarenheter och förslag till det översynsarbete som EU-kommissionen är ålagd att utföra enligt artikel 97.1 GDPR.

Flera av de brister i GDPR som har påtalats under de senaste åren handlar om oklarheter i hur olika formuleringar i bestämmelserna ska tolkas. Det är en ofrånkomlig följd av förordningens generella karaktär. I många fall är det inte möjligt eller ens lämpligt att genom justeringen i förordningen försöka åstadkomma bättre tydlighet i reglerna. Förutom att sådana ändringar kan ta lång tid att genomföra finns det en risk att förtydliganden av tillämpningen i konkreta situationer leder till mindre flexibilitet och oönskade sidoeffekter.

5.2.2 Kompletterande regler i unionsrätten

Ett alternativt tillvägagångssätt för att komma till rätta med oklarheter och brister i GDPR är att särreglera vissa områden på EU-nivå. Det skulle t.ex. kunna handla om att införa särskilda regler för att skapa bättre förutsättningar för att utveckla AI-baserade tjänster inom vissa närmare angivna verksamhetsområden samtidigt som skyddet för den personliga integriteten säkerställs.

Kompletterande regler i unionsrätten främjar harmoniseringen mellan medlemsstaterna. Detta förutsätter emellertid att medlemsstaterna kan enas om att minska det nationella utrymmet för kompletterande regler som GDPR ger.

5.2.3 Kompletterande regler i medlemsstaternas nationella rätt

Varje medlemsstat har möjlighet att utfärda bestämmelser i nationell rätt som kompletterar GDPR när förordningen uttryckligen medger detta. Utrymme för nationella regler finns främst beträffande personuppgiftsbehandling som sker inom den offentliga sektorn, men även t.ex. när det gäller näringslivets möjligheter att behandla uppgifter om brott.

De kompletterande reglerna kan enligt svensk rätt ges i lag, förordning av regeringen eller myndighetsföreskrifter samt i vissa fall i kollektivavtal (jfr 2 kap. 1–2 §§ lagen 2018:218 med kompletterande bestämmelser till EU:s dataskyddsförordning, i fortsättningen dataskyddslagen).

Fördelarna med nationell reglering är att tillämpningen kan anpassas till de särskilda förutsättningar som gäller i det aktuella landet och att nationell reglering oftast kan tas fram på kortare tid än reglering i unionsrätten.

Nackdelen med nationell reglering är att det vanligtvis skapar bristande harmonisering vilket medför att företag som ägnar sig åt gränsöverskridande verksamhet måste anpassa sig till flera olika regelverk.

Vi föreslår nedan att Sverige utnyttjar möjligheten till att utfärda kompletterande regler i nationell rätt. Skälet till detta är att det kan vara det snabbaste sättet att komma till rätta med oklarheter som t.ex. drabbar näringslivet.

Vi föreslår dock att sådan reglering bör göras i samråd med andra medlemsstater för att i möjligaste mån undvika att omotiverade särlösningar för Sverige uppstår.

5.2.4 Vägledning från tillsynsmyndigheter, samarbete

Genom antagandet av GDPR har dataskyddsprinciperna, med ursprung från 1970-talet, utvecklats. Samtidigt fullbordas förflyttning från administrativa förfaranden med tillstånd för varje behandling, till ett regelverk som utgår från en riskbaserad ansats och att den som behandlar personuppgifter ska kunna visa hur denne uppfyller

principerna, se ansvarsprincipen i artikel 5.2 GDPR. Tillsammans med flera andra nyheter som har introducerats i GDPR, t.ex. anmälan av personuppgiftsincidenter och konsekvensbedömningar, har ansvarsprincipen medfört omfattande administrativa bördor för de som behandlar personuppgifter.

En nackdel med den riskbaserade metoden och ansvarsprincipen är att det huvudsakligen är upp till den som behandlar personuppgifter att uttolka reglerna och avgöra vad de innebär för den egna verksamheten. Detta sker på eget ansvar och felbedömningar kan i värsta fall resultera i höga sanktionsavgifter. Ett regelverk som bygger på tillstånd eller liknande innebär att den som ska behandla personuppgifter visserligen får genomgå krävande tillståndsansökningar, men samtidigt får ett tydligt besked om vad som är tillåtet.

Kamerabevakningslagstiftningens anpassning till GDPR illustrerar denna övergång från tillstånd till egen bedömning av personuppgiftsbehandlingens tillåtlighet, kombinerat med mer utbyggd tillsyn.

Ett tillståndsförfarande för all form av personuppgiftsbehandling är naturligtvis inte möjligt i dagens samhälle. I praktiken är inte ens ett tillståndsförfarande för vissa integritetskänsliga former av personuppgiftsbehandling särskilt effektivt. Det kan medföra en byråkrati som inte står i rimlig proportion till ökad förutsebarhet och bättre integritetsskydd. Det skulle ta stor del av tillsynsmyndighetens resurser.

Det är sådeles ofrånkomligt att dataskyddsreglerna måste utformas mer eller mindre generellt. Och även om viss förutsebarhet kan uppnås genom kompletterande regler kommer behovet av vägledning alltid att vara stort.

Den viktigaste vägledningen erhålls genom analys av EU-domstolens domar. I avsaknad av sådan praxis kan domar från nationella domstolar eller uttalanden från tillsynsmyndigheterna vara av stor betydelse. Men det är viktigt att ha i minnet att nationell praxis och tolkningsuttalanden kan behöva justeras när det kommer nya avgöranden från EU-domstolen.

Det finns också en risk att tillsynsmyndigheternas arbete med att ta fram vägledning inte samordnas och att det därför uppstår motstridigheter. EDPB har i detta arbete en mycket viktig roll för att ta fram välgrundade och välformulerade vägledningar. Men det är också en viktig uppgift för de nationella tillsynsmyndigheterna att se till att EDPB:s vägledning överförs i nationell vägledning och görs lättillgänglig för olika målgrupper. Många gånger när det klagas på bristande vägledning finns sådan faktiskt att finna i EDPB:s[3] (eller i den tidigare Artikel 29-gruppens) omfattande och ibland något svårtillgängliga dokument.

5.2.5 Vägledning från näringslivet

I avsaknaden av förtydliganden i regelverket eller vägledning från tillsynsmyndigheterna kan en lösning vara vägledning från branschorganisationer och andra aktörer inom näringslivet. Det är visserligen inte en uppgift som primärt åligger näringslivet, men icke desto mindre finns det fördelar med branschvägledning. Dels är det möjligt att spara resurser eftersom många företag idag utreder samma rättsfrågor, dels får en gemensam branschtolkning en större tyngd än en tolkning som ett enskilt företag gör. Under förutsättning att en sådan tolkning är välunderbyggd kan den skapa en

[3] https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

branschpraxis som tillsynsmyndigheterna behöver förhålla sig till t.ex. vid en tillsyn. Det är naturligtvis inte säkert att tolkningen håller vid en rättslig prövning men den bör i vart fall minska risken för det enskilda företaget att drabbas av sanktioner.

Flera vägledningar på dataskyddsområdet har redan tagits fram av näringslivet.[4] På andra rättsområden, t.ex. inom marknadsrätten, är näringslivskoder vanliga.

En jämförelse kan också göras med hur myndigheterna inom den offentliga sfären sedan flera år tillbaka har samarbetat kring bl.a. rättsfrågor i samverkansprogrammet eSam. Detta samarbete har både resulterat i dokument betecknade ”vägledningar” och dokument betecknade ”rättsliga ställningstaganden”.

5.3 Förbättra regelverket

5.3.1 Inledning

I detta avsnitt diskuteras vad som rent konkret kan göras för att förbättra det befintliga regelverket i olika hänseenden. Verktygen är, som nämnts i föregående avsnitt, främst ändringar i regelverket men även bättre vägledning när ändringar inte ses som ett realistiskt alternativ.

5.3.2 Förtydliga tillämpningsområdet

GDPR gäller, enkelt uttryckt, för helt eller delvis automatiserad behandling av personuppgifter samt i vissa fall även för manuell behandling i personregister.

De begrepp som används för att avgränsa GDPR:s materiella tillämpningsområde är vaga. Frågor om vad som är en personuppgift, automatiserad behandling och manuell behandling leder ofta till tillämpningsproblem. Av EU-domstolens praxis avseende dataskyddsdirektivet framgår att bestämmelserna ska tolkas utifrån direktivets syfte att skydda de enskildas personliga integritet.[5] Det medför svårigheter att i förväg fastställa om GDPR ska tillämpas på en viss utpekad behandling t.ex. behandling som enbart innefattar indirekta personuppgifter vilka endast med mycket stora resurser kan användas för att identifiera enskilda personer.

En tänkbar lösning skulle kunna vara att införa uttryckliga undantag från tillämpningsområdet avseende verksamheter för vilka det går att förutse att integritetsriskerna är i stort sett obefintliga. Svårigheten ligger dock i att kunna förutse vad personuppgifterna kan användas till. Även indirekta till synes harmlösa personuppgifter kan användas för att ta fram mönster som kombinerat med andra uppgifter medför integritetsrisker av mer allvarlig art. Därtill kommer att undantag oftast medför nya avgränsningsproblem. Uttryckliga undantag framstår därför inte som en lämplig lösning.

Något annat alternativ än att avvakta praxis från EU-domstolen och bättre vägledning från tillsynsmyndigheterna står troligen inte till buds. Däremot kan det vara lämpligt att, i linje med den riskbaserade ansatsen, skapa uttryckliga undantag från eller begränsningar av skyldigheterna och ansvaret i situationer där integritetsriskerna på förväg kan bedömas vara små (se nedan avsnitt 5.3.4).

Datainspektionen bör förbättra vägledningen om tillämpningsområdet för GDPR.

[4] Exempelvis Svensk Handel, GDPR – tolkningsguide och Svenskt Näringsliv, Rapport om rollfördelning för korrekt personuppgiftsansvar.

[5] Se t.ex. Jehovan todistajat, C-25/17 p. 53 och 56.

5.3.3 Förtydliga rollfördelningen

Frågan om vem som är personuppgiftsansvarig respektive personuppgiftsbiträde skapar ofta problem i samband med samarbeten mellan olika aktörer som innefattar personuppgiftsbehandling. Är det fråga om självständigt personuppgiftsansvar, delat personuppgiftsansvar, gemensamt personuppgiftsansvar, ansvar som personuppgiftsbiträde eller inget ansvar?

Av EU-domstolens senaste praxis tycks slutsatsen kunna dras att utvecklingen går mot ett utökat tillämpning av gemensamt personuppgiftsansvar.[6] Det gäller situationer när flera aktörer med gemensamma eller närliggande ändamål är inblandade i komplexa samarbeten.

Sett från den registrerades perspektiv ger ett gemensamt personuppgiftsansvar ofta det bästa skyddet, vilket kan antas vara skälet till att EU-domstolen har valt detta alternativ. Men samtidigt skapar ett gemensamt personuppgiftsansvar en större osäkerhet för de som behandlar personuppgifterna. Det förutsätter att de inblandade aktörerna gemensamt fastställer fördelning av ansvaret och skyldigheterna enligt artikel 26 GDPR. En sådan fördelning kan i bästa fall resultera i en överenskommelse som avspeglar varje aktörs faktiska möjlighet att påverka behandlingen och en lämplig ansvarsfördelning. I avsaknad av överenskommelse skapar dock denna ordning en stor osäkerhet och en risk för att en aktör får bära ett oproportionerligt stort ansvar. Problemet är särskilt tydligt när ett mindre företag använder sig av tjänster som tillhandahålls av en dominerande aktör och saknar möjlighet att påverka innehållet i långa och komplicerade standardvillkor.

Det är inte troligt att oklarheterna i begreppen ”personuppgiftsansvarig” och ”personuppgiftsbiträde” går att åtgärda genom förtydliganden i regelverket. Förbättrad vägledning från tillsynsmyndigheterna med tydliga exempel och mallar för biträdesavtal är troligen den enda lösningen som står till buds i avvaktan på klargörande praxis från EU-domstolen. Det är därför bra att Datainspektionen har tagit på sig ordförandeskapet i en arbetsgrupp inom EDPB som ska uppdatera vägledningen som togs fram av Artikel 29-gruppen år 2010.[7]

Datainspektionen bör förbättra vägledningen om rollfördelningen mellan personuppgiftsansvariga och personuppgiftsbiträden.

5.3.4 Förstärk den riskbaserade ansatsen

Under förhandlingarna talades det mycket om att GDPR skulle bygga på en riskbaserad ansats, dvs. att omfattningen av ansvaret och skyldigheterna för de som behandlar personuppgifter skulle vara beroende av vilken risk den aktuella personuppgiftsbehandlingen medförde. Den riskbaserade ansatsen sågs bl.a. som ett verktyg för att underlätta för företagen, särskilt mikroföretag samt små och medelstora företag (se bl.a. skäl 13 GDPR). I den antagna förordningen lyser dock de uttryckliga undantagen med sin frånvaro. Den enda bestämmelse som var avsedd att underlätta för sådana företag är undantaget från den så kallade företeckningsskyldigheten i artikel 30.5 GDPR. Bestämmelsen har emellertid fått en utformning som innebär att undantaget i princip

[6] Se EU-domstolens domar i mål C-210/16 Wirtschaftsakademie, C-25/17 Jehovas vittnen och C-40/17 Fashion ID.

[7] Yttrande 1/2010 om begreppen registeransvarig och registerförare WP 169. Se https://www.datainspektionen.se/nyheter/datainspektionen-leder-arbete-med-nya-eu-riktlinjer/

aldrig blir tillämpligt. Det kan för övrigt ifrågasättas om risken med en viss behandling ska kopplas till antalet anställda i ett företag.

Den riskbaserade ansatsen tycks hittills främst åberopats för att motivera att personuppgiftsansvariga måste vidta mer omfattande åtgärder för särskild riskfylld behandling. Däremot tycks det vara ovanligt att ansatsen används för att minska de rättsliga kraven beträffande mindre riskfylld personuppgiftsbehandling.

Bättre vägledning om vilken typ av personuppgiftsbehandling som Datainspektionen anser vara relativt harmlös kan vara till stor nytta för företag och organisationer, stora som små.

I artikel 35.3 GDPR anges vissa typer av personuppgiftsbehandlingar för vilka konsekvensbedömningar är obligatoriska. Ytterligare exempel ges i de listor som tillsynsmyndigheterna har upprättat enligt artikel 35.4 GDPR. Den lista som Datainspektionen har upprättat innehåller värdefull vägledning.[8] Även informationen på Datainspektionens webbsida om konsekvensbedömningar är förhållandevis utförlig.

Datainspektionen har möjlighet enligt artikel 35.5 GDPR att upprätta en lista över sådana personuppgiftsbehandlingar som inte kräver konsekvensbedömningar. En sådan lista skulle kunna underlätta för företag som ägnar sig åt behandling som inte är särskilt riskfylld och som idag ägnar mycket tid och resurser åt att genomföra en fullständig konsekvensbedömning.

EU bör vid översynen av GDPR låta den riskbaserade ansatsen få tydligare genomslag och införa begränsningar av ansvar och skyldigheter vid personuppgiftsbehandling som innebär små integritetsrisker.
Datainspektionen bör upprätta en förteckning över sådana behandlingar som inte kräver att en konsekvensbedömning utförs.

5.3.5 Förtydliga och utöka möjligheterna att behandla känsliga personuppgifter

Omfattningen av undantag från förbudet att behandla känsliga personuppgifter enligt artikel 9 GDPR är mer begränsade i jämförelse med de rättsliga grunder som kan användas för ”vanlig” personuppgiftsbehandling, artikel 6 GDPR. Det finns naturligtvis goda grunder för att behandling av känsliga personuppgifter bör vara mer restriktiv. Men det är inte ovanligt att det begränsade utrymmet för att kunna behandla sådana personuppgifter leder till problem utan att den aktuella behandlingen kan anses vara av mer integritetskänsligt slag.

Det är särskilt tydligt för behandling som normalt utförs av personuppgiftsansvariga inom den privata sektorn. I artikel 9 GDPR saknas nämligen undantag för att behandla känsliga personuppgifter för att fullgöra ett avtal, jämför artikel 6.1 b, eller en rättslig förpliktelse, artikel 6.1 c GDPR, eller med stöd av en intresseavvägning, artikel 6.1 f. Myndigheternas behandling av känsliga personuppgifter kan i många fall stödjas på det mer generellt utformade undantaget ”viktigt allmänt intresse”, se artikel 9.1 g och 3 kap. 3-4 §§ dataskyddslagen.

[8] Datainspektionen dnr DI-2018-13200.

Det finns inget som tyder på att lagstiftaren varken i EU eller i Sverige har haft för avsikt att förbjuda behandling av känsliga personuppgifter för berättigade ändamål inom den privata sektorn. Det kan trots detta många gånger vara svårt att hitta ett tillämpligt undantag.

Samtidigt kan det konstateras att de nationella kompletterande reglerna på detta område varierar stort inom EU. Den nederländska och den brittiska dataskyddslagstiftningen innehåller t.ex. mer detaljerade regler om undantag från förbudet att behandla känsliga personuppgifter. Det gäller personuppgiftsbehandling för berättigade intressen såsom att motverka försäkringsbedrägeri och ett företags behov av att kontrollera kunder innan avtal ingås i syfte att motverka missbruk av tjänster.

Problemet tycks således främst finnas i de svenska kompletterande reglerna i dataskyddslagen. Det finns därför anledning att överväga om undantagen för att behandla känsliga personuppgifter bör utökas eller i vart fall förtydligas. Vid en sådan översyn bör hänsyn tas till behovet av harmonisering inom EU. En samsyn med andra medlemsstater bör därför eftersträvas även om det finns tillfällen då Sverige kan behöva ta ställning i frågor där enighet saknas mellan medlemsstaterna.

Vid den föreslagna översynen måste det givetvis beaktas att känsliga personuppgifter ska hanteras med stor restriktivitet. Eventuellt nya undantag måste innehålla adekvata säkerhetsåtgärder som tillgodoser de registrerades intressen.

Regeringen bör utreda möjligheterna att förtydliga och utöka undantagen för företags behandling av känsliga personuppgifter i situationer där det finns sakliga skäl för det.

5.3.6 Förtydliga och utöka möjligheterna att behandla personuppgifter om brott

GDPR överlämnar till den nationella lagstiftaren att närmare reglera under vilka förutsättningar personuppgifter som rör fällande domar i brottmål samt lagöverträdelser som innefattar brott (härefter ”personuppgifter om brott”) får behandlas av andra än myndigheter. Utrymmet enligt svensk rätt att behandla sådana personuppgifter har under tiden med personuppgiftslagen varit begränsat. Ett generellt förbud för behandling av personuppgifter om brott har gällt för andra än myndigheter. Undantagen från förbudet har getts i Datainspektionens föreskrifter och beslut i enskilda fall.

I samband med införandet av GDPR menade regeringen att utrymmet kunde utökas och valde att placera två undantag från förbudet i den förordning som kompletterar dataskyddslagen. Undantagen som avser behandling för rättsliga anspråk samt behandling för att fullgöra en rättslig förpliktelse (se vidare 5 § förordning 2018:219 med kompletterande bestämmelser till EU:s dataskyddsförordning). Undantaget för rättsliga anspråk har också utökats i förhållande till hur det var utformat i Datainspektionens äldre föreskrifter.

Regeringen konstaterade även att GDPR ger ett större utrymme än personuppgiftslagen för att genom föreskrifter och beslut i enskilda fall tillåta andra än myndigheter att behandla personuppgifter om brott. I princip torde Datainspektionens möjlighet att avslå en begäran om tillstånd vara begränsat till de fall där behandlingen skulle vara oförenlig med GDPR i övrigt, i synnerhet principerna i artikel 5 och kravet på rättslig grund i artikel 6.[9]

[9] Prop. 2017/18:105 s. 100.

De restriktiva bestämmelserna för att behandla personuppgifter om brott har lett till problem för företag som har verksamhet i flera medlemsstater och för företag som har att utföra kontroller mot olika spärr- och sanktionslistor. Regeringen ansåg att sådana företag bör få tillstånd att behandla personuppgifter om brott i vart fall om listorna är fastställda i demokratisk ordning och allmänt tillgängliga.[10] För att underlätta den administrativa bördan för företagen och Datainspektionen ansåg regeringen även att det kan finnas anledning för Datainspektionen att meddela föreskrifter i stället för att utfärda tillstånd i varje enskilt fall.[11] Med hänsyn till detta bör Datainspektionen se över föreskrifterna om att behandla uppgifter om brott i DIFS 2018:2.

Det är svårt att se hur personuppgifter om brott är mer integritetskänsliga än personuppgifter om t.ex. hälsa och sexualliv. Av den anledningen kan det diskuteras varför utrymmet för att behandla personuppgifter om brott bör vara mer restriktivt än behandling av känsliga personuppgifter. Det är t.ex. inte tillåtet att behandla sådana personuppgifter även om man har den registrerades samtycke.

I flera medlemsstater och Norge likställs behandling av känsliga personuppgifter med behandling av personuppgifter om brott på så sätt att samma eller i stort sett samma undantag gäller för förbuden att behandla sådana personuppgifter.[12] Det förekommer även nationell lagstiftning som tillåter behandling av personuppgifter om brott med stöd av en intresseavvägning.[13]

I jämförelse med andra länders bestämmelser om behandling av personuppgifter om brott framstår de svenska bestämmelserna som gäller andra än myndigheter som allt för restriktiva.

Mot den bakgrunden kan det finnas anledning att se över bestämmelserna om behandling av personuppgifter om brott både i dataskyddslagen och i förordningen som kompletterar dataskyddslagen. Om mer tillåtande bestämmelser införs kan de registrerades intressen lämpligen tillgodoses genom att den personuppgiftsansvarige åläggs att vidta olika former av säkerhetsåtgärder.

Regeringen bör ta initiativ till en översyn av det rättsliga stödet för att behandla personuppgifter om brott i dataskyddslagen och överväga om det finns anledning att likställa undantagen för att behandla personuppgifter om brott med undantagen för att behandla känsliga personuppgifter.

Regeringen bör – i avvaktan på översyn av dataskyddslagen – överväga att införa flera generella rättsliga grunder för att behandla personuppgifter om brott i förordningen som kompletterar dataskyddslagen.

Datainspektionen bör utnyttja sin föreskriftsrätt och meddela föreskrifter för att tydliggöra möjligheterna att behandla uppgifter om brott, särskilt vad gäller kontroller mot vissa spärr- och sanktionslistor.

[10] Datainspektionen har nyligen fattat ett beslut om undantag enligt den inställning som regeringen gav uttryck för i propositionen (dnr DI-2018-12122 m.fl.).

[11] Prop. 2017/18:105 s. 101.

[12] Se bl.a. 3 kap. 11 § norska personopplysningsloven. Se Data Protection Act 2018, Schedules 1, Section 10.

[13] Se dataskyddslag i Österrike (art. 2 § 4 Datenschutzgesetz).

5.3.7 Förtydliga möjligheterna att använda AI

I avsnitt 4.9 har det beskrivits hur dataskyddslagstiftningen många gånger begränsar både hanteringen av stora datamängder som behövs för maskininlärning och det automatiserade beslutsfattande som kan ske när AI-system används. I maskininlärningsfasen handlar det bl.a. om svårigheter att klart och tydligt uppfylla de grundläggande dataskyddsprinciperna och kraven på rättsligt stöd när stora datamängder hanteras. Vid användningen av AI för beslutsfattande handlar det främst om den restriktiva tolkning som artikel 22 GDPR har givits av Artikel 29-gruppen.

Det finns helt klart AI-tillämpningar som innebär betydande risker i samband med hanteringen av stora mängder personuppgifter, men det finns också en betydande positiv potential, inte bara för näringslivet utan för samhället som helhet. Det bör därför övervägas om det för vissa samhällsnyttiga tillämpningar finns anledning att lätta på GDPR:s krav. Det handlar om situationer där personuppgifter måste hanteras för att skapa själva AI-tillämpningen, men där den enskilda individen inte är i fokus t.ex. för beslutsfattande. För att balansera en mer tillåtande attityd när det gäller behandlingen av personuppgifter krävs kompensatoriska säkerhetsåtgärder. En tydlig parallell kan dras med den särskilda dataskyddreglering som idag finns för statistik- och forskningsverksamhet.

AI-utmaningarna förknippade med bestämmelsen om automatiserat beslutsfattande i artikel 22 GDPR är av en annan karaktär. I denna situation är den enskilde registrerade i fokus och det finns därför anledning att vara vaksam för t.ex. felaktiga beslut som påverkar denne. Av den anledningen är det naturligt med strikta regler om kvalitet, omprövning, rätt till insyn etc. En allt för negativ inställning till automatiserade beslut riskerar dock att kasta ut barnet med badvattnet.

Något tillspetsat kan man säga att Artikel 29-gruppen har tolkat artikel 22 första stycket GDPR som ett förbud mot automatiserade beslut. Det innebär att sådant beslutfattande endast är tillåtet enligt de i andra stycket angivna undantagen (nödvändigt för fullgörande av avtal med den registrerade, tillåtet enligt unionsrätten eller nationell rätt samt grundar sig på ett uttryckligt samtycke av den registrerade).[14]

Artikel 29-gruppens tolkning har ifrågasatts. Det har hävdats att den inte framstår som självklar med hänsyn till att övriga bestämmelser i kapitlet avser rättigheter som måste göras gällande av den registrerade genom särskild begäran.[15] Med en sådan tolkning skulle automatiserat beslutsfattande vara tillåtet så länge som den registrerade inte motsätter sig det. Den sistnämnda tolkningen framstår dock i sin tur som svår att förena med undantagen som anges i artikel 22.2 GDPR. Ska rätten att motsätta sig automatiserat beslutfattande inte gälla om den enskilde har lämnat sitt samtycke eller om det är nödvändigt för ingående eller fullgörande av ett avtal med den registrerade? Det talar för den tolkning som framförts av Artikel 29-gruppen.

En annan oklarhet som har diskuterats är frågan om bestämmelsen endast omfattar automatiserat beslutsfattande som inbegriper profilering eller om sådant beslutsfattande omfattas även om det inte bygger på profilering. En tredje oklarhet i bestämmelsen som har uppmärksammats är vad som avses med formuleringen ”rättsliga följder för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne”. Artikel 29-gruppen har med hänvisningen till denna formulering hävdat att bestämmelsen i vissa fall kan omfatta påträngande internetreklam.

---

[14] Artikel 29-gruppens riktlinjer om automatiserat individuellt beslutsfattande och profilering enligt förordningen (EU) 2016/679, s. 20.

[15] Se bl.a. Öman, Kommentar till Dataskyddsförordningen (GDPR) m.m. En kommentar, 2019, s. 369.

Det är uppenbart att bestämmelsen om automatiserat beslutsfattande innehåller flera oklarheter som i första hand bör åtgärdas genom ändringar i GDPR. Det bör dock noteras att bestämmelsen om automatiserat beslutsfattande också tillåter viss reglering i annan unionsrätt eller i medlemsstaternas nationella rätt. Sådana undantag måste vara förenade med lämpliga åtgärder till skydd för de registrerades rättigheter, friheter och berättigade intressen, se artikel 22.2 b GDPR.

Den tolkning som Artikel 29-gruppen har gjort av artikel 22 GDPR riskerar att fungera som en våt filt över AI-utvecklingen. Det är som sagt motiverat med strikta regler som skyddar mot potentiellt negativa effekter av automatiserat beslutsfattande, men en sådan reglering bör inrikta sig på att motverka de negativa effekterna t.ex. bristande transparens och risk för diskriminering, inte automatiseringen som sådan.

Det finns sammanfattningsvis ett behov av att närmare undersöka vad som kan göras för att skapa ett starkt dataskydd som samtidigt tar tillvara de stora potentialer som finns med AI. Att dataskyddslagstiftningen kan tillåta även känsliga behandlingar av personuppgifter, under förutsättning att det finns viktiga ändamål med behandlingarna och adekvata säkerhetsåtgärder som minskar riskerna, är ingen nyhet.

EDPB bör se över befintlig vägledning om automatiserat beslutsfattande enligt artikel 22 GDPR i syfte att skapa bättre förutsättningar för att använda AI.

EU bör överväga att ta fram verksamhetsspecifika regler som kompletterar GDPR i syfte att underlätta användningen av AI.

5.3.8 Förtydliga förhållandet till amerikansk rätt

Den europeiska dataskyddsregleringen har fått genomslag utanför EU:s gränser. I många länder har initiativ tagits till reformer med syftet att skapa en mer modern integritetsskyddslagstiftning med GDPR som förebild. En sådan utveckling kan på längre sikt underlätta internationella dataflöden eftersom GDPR uppställer ett principiellt förbud mot överföring av personuppgifter till tredjeland som inte har en adekvat skyddsnivå för personuppgifter.

För svenska företag utgör överföringar av personuppgifter till USA den största utmaningen. Det sammanhänger bl.a. med att de största molntjänstleverantörerna omfattas av amerikansk jurisdiktion. Bakgrunden till problemet är skillnaderna mellan amerikansk och europeisk dataskyddslagstiftning och framför allt amerikanska myndigheters omfattande tillgång till elektronisk information. Problemet uppmärksammades bl.a. i målet i EU-domstolen angående lagligheten att överföra personuppgifter till USA med stöd av kommissionens beslut om adekvat skyddsnivå (Safe Harbour).[16] Med hänvisning till bristerna i amerikansk rätt ogiltighetsförklarade EU-domstolen EU-kommissionens beslut i vilket kommissionen bedömde att företag i USA uppfyllde krav på adekvat skyddsnivå om de anslöt sig till de så kallade Safe harbour-reglerna. EU-kommissionens nya beslut om adekvat skyddsnivå avseende USA (Privacy Shield) och EU-kommissionens beslut om standardavtalsklausuler är för närvarande föremål för prövning i ett nytt mål i EU-domstolen. Även om framsteg har gjorts i förhållande till Safe harbour-beslut finns det fortfarande flera tveksamheter som kan medföra att EU-domstolen underkänner hela eller delar av beslutet om Privacy Shield. Domen skulle i sådana fall medföra stora problem för handeln mellan USA och EU, särskilt för användning av amerikanska molntjänster.

[16] EU-domstolen C-362/14.

Skillnaderna mellan europeisk och amerikansk integritetsskyddslagstiftning uppmärksammades även i och med antagandet av the Cloud Act. Cloud Act innebär bl.a. ett klargörande av att den amerikanska lagstiftningen Stored Communication Act (SCA) är tillämplig även på data som är lagrad utanför USA och som är tillgängliga för amerikanska företag. Europeiska dataskyddstyrelsen (EDPB) har i en preliminär bedömning ansett att utlämnande till amerikanska myndigheter med stöd av Cloud Act inte är förenligt med GDPR.[17]

Skillnaderna i synsättet på integritet mellan EU och USA skapar uppenbara problem för den fortsatta digitaliseringen inom såväl näringslivet som den offentliga sektorn. Användningen av publika molntjänster som tillhandahålls av leverantörer som omfattas av utländsk jurisdiktion medför särskilda juridiska risker. Riskerna är dock inte av sådant slag att de motiverar ett absolut förbud för företag och myndigheter att använda sådana tjänster, åtminstone om det inte handlar om uppgifter som är av betydelse för Sveriges säkerhet. Användningen av publika molntjänster bör vara tillåten om riskerna vid en noggrann bedömning anses vara rimliga.

Den oklarhet som i detta avseende har uppstått avseende sekretessreglerade personuppgifter bör kunna åtgärdas genom ett förtydliganden av begreppet röjande i offentlighets- och sekretesslagen (2009:400). Därutöver kan det vara lämpligt med någon form av föreskrift som anger under vilka förutsättningar molntjänster får användas för sekretessreglerade uppgifter.[18]

Vad gäller GDPR är det svårare att se någon snabb lösning. EU-domstolens avgörande i målet C-311/18 (Schrems 2) som väntas under första halvan av 2020 kan komma att få stor betydelse för hur olikheterna i amerikanskt och europeiskt integritetsskydd ska hanteras. Avgörandet kan komma att innebära betydande inskränkningar i möjligheterna att överföra personuppgifter till USA. EU-domstolen har tidigare haft en relativt integritetsvänlig inställning och noga värnat den rätt som tillkommer enskilda enligt EU:s stadga om de grundläggande rättigheterna. EU-domstolen har inte heller tvekat att göra en strikt juridisk bedömning utan att ta hänsyn till eventuella konsekvenser för handeln.

De pågående förhandlingarna mellan EU och USA om brottsbekämpande myndigheters tillgång till elektroniska bevis kan till viss del klargöra rättsläget.[19]

Datainspektionen bör – i avvaktan på att rättsläget klarnar och i samråd med övriga tillsynsmyndigheter – ta fram rekommendationer för hur företagen och myndigheter bör agera vad gäller publika molntjänster som omfattas av utländsk jurisdiktion. Det bör företrädesvis ske i samråd med övriga tillsynsmyndigheter.

[17] EPDB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection Brussels, 10 July 2019.

[18] Regeringen har tillsatt en statlig utredning som bl.a. ska tydliggöra de rättsliga förutsättningarna för att på ett säkert sätt kunna anlita privata leverantörer av it-drift. Pressmeddelanden från Infrastrukturdepartementet 2019-09-30.

[19] Se EU-kommissionens pressmeddelande, https://europa.eu/rapid/press-release_STATEMENT-19-5890_en.htm

5.4 Skapa mer och bättre vägledning

5.4.1 Utveckla dialogen med näringslivet

Det finns stor vilja inom näringslivet att göra rätt. För närvarande är det dock svårt att veta vad som är rätt. Många företag lyssnar på Datainspektionens uttalanden men känner sig ändå osäkra på hur de ska agera. Datainspektionen har också stort genomslag i media. Myndigheten har därmed en unik möjlighet att medverka till att skapa en god dataskyddskultur i samhället. En förutsättning är dock att myndigheten har en inställning till integritetsskydd som är balanserad i förhållande till andra samhällsviktiga mål såsom effektivitet och innovation.

Det är därför viktigt att Datainspektionen bedriver sin verksamhet med ett öppet förhållningssätt så att de som ska tillämpa reglerna och förena dem med andra krav upplever att de får stöd och gehör för sina synpunkter. Förutom att ge vägledning till dessa och därmed skapa en god dataskyddskultur i förebyggande syfte, kan öppenhet ge myndigheten viktig information om vilka utmaningar som dessa aktörer står inför.

Den under hösten 2018 genomförda seminarieserie med företrädare för offentliga och privata sektorn var ett vällovligt initiativ som resulterade i ett stort antal bra förslag till förbättringar.[20] Det återstår att se om och hur förslagen genomförs i Datainspektionens verksamhet.

För att skapa bättre dialog, kontinuitet och uppföljning kan det vara lämpligt att inrätta någon form av bestående nätverk eller forum, såsom återkommande rundabordssamtal med branschorganisationer och särskilda kontaktkanaler för informationsspridning och erfarenhetsutbyte.

En ökad öppenhet hos den svenska lagstiftaren kan på motsvarande sätt skapa bättre förutsättningar för en bättre utformad lagstiftning, som inte i onödan hindrar företagens konkurrenskraft.

Regeringen och Datainspektionen bör skapa nätverk för dialog och erfarenhetsutbyte med näringslivet och andra berörda parter.

5.4.2 Ta fram tydlig vägledning

Vägledningen för tillämpningen av GDPR behöver bli bättre. I många delar innehåller befintliga vägledningar från Datainspektionen och EDPB omformuleringar av det som framgår av de generella artikeltexterna i GDPR. De slutar vanligtvis med att någon form av bedömning ska göras. För att vägledningarna ska kunna underlätta för den som ska tillämpa reglerna, som i regel saknar djupare kunskaper om dataskydd, krävs mer konkreta råd.

Konkreta råd kan innebära beskrivande exempel, beskrivande av ”best practice”, mallar och checklistor. I vissa delar har den typ av vägledningar redan tagits fram såsom exemplen i vägledningen om konsekvensbedömningar, men mer behövs. Den danska tillsynsmyndighetens initiativ till att ta fram ett standardavtal för personuppgiftsbiträdesavtal är i detta avseende lovvärt.[21]

Vägledning (riktlinjer, rekommendationer, best practice m.m.) som EDPB utfärdar är för det mesta omfattande och svårtillgänglig. Det kan finnas mycket att vinna på att

[20] Se Datainspektionens sammanställning dnr DI-2018-16971.

[21] Se https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-142019-draft-standard-contractual-clauses_en

göra innehållet i dessa mer lättillgängligt för de svenska användarna. Det borde inte heller finnas något hinder för att komplettera dem med kommentarer, hänvisningar och exempel som passar svenska förhållanden.

När Datainspektionen tar fram egen vägledning kan det vara lämpligt att skicka utkast på remiss till berörda parter såsom branschorganisationer. Det kan även vara lämpligt att engagera de berörda parterna redan i ett tidigt skede, för problemidentifiering och erfarenhetsutbyte t.ex. i ett sådant nätverk som nämnts ovan (jfr ovan 5.4.1).

För att undvika att tillsynsmyndigheterna gör olika tolkningar bör Datainspektionens arbete med vägledningar innefatta en kartläggning av vad andra tillsynsmyndigheter inom EU har uttalat i samma fråga. I det avseendet kan man tycka att EDPB bör ha en samordnande roll även vad gäller de nationella tillsynsmyndigheternas vägledning t.ex. genom att sammanställa dem på sin webbplats på samma sätt som de idag sammanställer beslut från de nationella tillsynsmyndigheterna.

Att översätta och använda hela eller delar av vägledningar från andra nationella tillsynsmyndigheter är ett relativt enkelt och effektivt sätt att ta fram ny vägledning. Självfallet måste Datainspektionen granska och eventuellt anpassa innehållet. På samma sätt borde nya vägledningar kunna tas fram i samarbete med andra tillsynsmyndigheter.[22]

Vägledning som Datainspektionen har publicerat kan i vissa fall behöva ändras t.ex. för att det har kommit ny domstolspraxis. Det är i dessa fall mycket viktigt att det anges att en ändring har gjorts och när den publicerades. I annat fall är det svårt för personuppgiftsansvariga att upptäcka ändringen och rätta sig efter den.

Datainspektionen bör i samarbete med övriga tillsynsmyndigheter och EDPB ta fram vägledning med mer konkreta råd, checklistor och mallar. I detta arbete bör även samråd ske med berörda parter. När den vägledning som tidigare givits ändras måste det uppmärksammas.

5.4.3 Ta fram vägledning om mindre riskfylld personuppgiftsbehandling

GDPR har, som nämnts ovan (avsnitt 5.3.3), baserats på en riskbaserad ansats. Det finns emellertid få bestämmelser i förordningen som uttryckligen begränsar den personuppgiftsansvariges ansvar och skyldigheter vid mindre riskfylld behandling. Till stor del är den personuppgiftsansvarige tvungen att göra komplicerade riskbedömningar. Felaktiga bedömningar riskerar att leda till att sanktionsavgifter döms ut.

Det är därför lämpligt att Datainspektionen inte bara fokuserar på vilka behandlingar som innebär särskilda integritetsrisker utan även beskriver vilka typer av behandlingar som anses innebära små integritetsrisker. Detta kan t.ex. göras genom att myndigheten publicerar en sådan förteckning som avses i artikel 35.5 GDPR. Inspektionen bör även beskriva hur ansvaret och skyldigheterna i GDPR bör utövas för sådana mindre integritetskänsliga behandlingar.

Datainspektionen bör publicera vägledning om vilka behandlingar som typiskt sett inte innebär särskilda integritetsrisker och hur ansvaret och skyldigheterna i GDPR bör utövas för sådana mindre integritetskänsliga behandlingar.

[22] Se den så kallade Köpenhamnsdeklarationen av tillsynsmyndigheterna i Norden, https://www.datainspektionen.se/nyheter/2018/nordiska-dataskyddsmyndigheter-starker-samarbetet/

5.4.4 Ta fram rättsliga ställningstaganden

Ett sätt att skapa bättre och mer förutsebar tillämpning av dataskyddsbestämmelserna är att Datainspektionen tar ställning i oklara rättsfrågor. Idag gör Datainspektionen vissa tolkningsuttalande i samband med att allmän vägledning lämnas på myndighetens webbplats. Det är ofta information utformad för mottagare som saknar kunskap om den bakomliggande rättsfrågan. Sådan information är naturligtvis mycket viktig för att vägleda personuppgiftsansvariga i enklare frågor. Den saknar dock ofta den stringens och utredning som kan behövas för att ligga till grund för mer kvalificerade rättsliga ställningstaganden.

Mer kvalificerad rättslig vägledning kan fås genom att studera Datainspektionens beslut i enskilda ärenden. Där redovisas bakgrundsfakta, tillämpliga rättsregler och hur Datainspektionen har resonerat för att komma fram till beslutet.[23]

Det finns en stor efterfrågan på praxis från Datainspektionen. Med hänsyn till att det kommer att ta många år innan inspektionen hinner ta fram ny praxis på alla områden och ännu längre tid innan domstolspraxis har utvecklats bör Datainspektionen överväga andra alternativ för att skapa kvalificerad rättslig vägledning.

Ett sätt att kan vara att ta fram och publicera rättsliga ställningstagande på ett liknande sätt som många andra myndigheter har gjort under en längre tid. De innehåller förutom en specificerad frågeställning, bakgrundsbeskrivning, beskrivning av gällande rätt samt myndighetens bedömning av rättsläget.

Syftet är vanligtvis att skapa en enhetlig tillämpning av bestämmelserna inom myndigheten men då ställningstagandena publiceras ger de också värdefull vägledning om hur myndigheten beaktar olika intressen och skäl för den fråga som ställningstagandet gäller.

Ett rättsligt ställningstagande har ingen annan rättslig status än den som myndigheten själv ger det. I regel betraktas ett rättsligt ställningstagande som myndighetens kvalificerade tolkning av rättsläget i viss fråga. De är inte bindande för myndigheten men avsikten är att myndigheten följer sina egna ställningstaganden till dess att ställningstagandet ändras eller upphävs t.ex. på grund av att myndigheten ändrar uppfattning eller för att det kommer domstolspraxis som stödjer en annan tolkning än den som myndigheten har gjort.

På liknande sätt fungerade de rapporter som Datainspektionen tidigare tog fram efter att genomfört ett antal tillsynsärenden på ett visst område.[24] En nackdel med vägledning som tas fram efter genomförda tillsynsprojekt är att det vanligtvis tar lång tid och binder en omfattande del av myndighetens resurser. Rättsliga ställningstaganden bör rimligen gå att ta fram snabbare och med en mindre insats.

En komplikation med att Datainspektionen tar ställning i en viss rättsfråga är att det kan leda till bristande harmonisering i förhållande till hur andra tillsynsmyndigheter tolkar GDPR. Datainspektionen måste i möjligaste mån undvika att komma till slutsatser som inte går att förena med tolkningar gjorda av andra tillsynsmyndigheter.

---

[23] Från tiden med personuppgiftslagen finns ett stort antal beslut som kan ge vägledning för tillämpningen av GDPR. Det förutsätter dock att läsaren känner till om, och på vilket sätt, förordningen har ändrats i förhållande till personuppgiftslagen. I samband med GDPR började tillämpas i maj 2018 tog Datainspektionen bort all äldre information från webben inklusive majoriteten av de tidigare fattade besluten. Efter kritik har under år 2019 vissa delar av den äldre informationen publicerats på nytt. Den är dock inte särskilt lättillgänglig.

[24] De flesta av dessa rapporter finns inte längre kvar på Datainspektionens webb. En rapport är dock Rättsväsendets informationsförsörjning och den personliga integriteten, Rapport 2012:1.

Rättsliga ställningstaganden bör därför föregås av en kartläggning av EDPB:s och andra tillsynsmyndigheters tolkningar. Det bör dock inte vara uteslutet att Datainspektionen i vissa fall kommer fram till avvikande tolkningar t.ex. med hänsyn till särskilda förhållande i Sverige eller i svensk rätt. Om det inte finns någon etablerad tolkning av den aktuella rättsfrågan kan Datainspektionen genom att publicera sin tolkning ta initiativet för att etablera en gemensam tolkning.

Datainspektionen bör i oklara rättsfrågor ta fram och publicera välmotiverade rättsliga ställningstaganden, företrädesvis i samarbete med övriga tillsynsmyndigheter.

5.4.5 Underlätta arbetet med uppförandekoder

Uppförandekoder för en viss sektor kan vara ett värdefullt verktyg både för att specificera tillämpningen av GDPR för en viss verksamhet och för att undanröja oklarheter. Vid införandet av GDPR framhölls också uppförandekoder tillsammans med certifieringar som ett sätt att underlätta för företag. Enligt förordningen har också medlemsstaterna, tillsynsmyndigheterna, EDPB samt EU-kommissionen en särskild uppgift att uppmuntra framtagningen av uppförandekoder, se artikel 40.1 GDPR.

Arbetet med att ta fram uppförandekoder har visat sig resurskrävande och det finns såvitt känt ännu ingen uppförandekod som har godkänts i Sverige. Förutom omfattande arbete med att ta fram själva koden krävs det att det inrättas ett organ som övervakar tillämpningen av den. Få organisationer i Sverige har kapacitet och resurser att utarbeta uppförandekoder. Det kan därför vara lämpligt att regeringen ger i uppdrag och tillskjuter pengar för att utvalda myndigheter kan stödja näringslivets arbete med att utarbeta uppförandekoder.[25]

Regeringen bör ge i uppdrag till utvalda myndigheter, och tillskjuta medel för, att stödja näringslivets arbete med att utarbeta uppförandekoder på för näringslivet centrala områden.

5.4.6 Förbättra webben

I linje med den ovan efterfrågade öppenheten är det lämpligt att Datainspektionen utökar informationen som finns tillgänglig på myndighetens webbplats såsom mer information om aktuella händelser t.ex. vad som händer inom EDPB och i samarbetet med andra tillsynsmyndigheter, sammanställningar av praxis från andra länder och kommentarer till EU-domstolens domar.

Samtliga beslut och yttranden bör som huvudregel publiceras på webben. För närvarande tycks endast ett urval av Datainspektionens beslut och yttrande publiceras vilket bl.a. kan bero på sekretesskäl. I de flesta fall torde det dock vara möjligt att formulera beslut och yttranden utan att sekretessbelagda uppgifter tas med.

För att öka öppenheten och för att minska myndighetens administrativa bördor bör en offentlig version av myndighetens diarium göras tillgängligt via webben.

[25] Jfr Integritetskommitténs förslag SOU 2017:52.

Andra tänkbara förslag som framförts tidigare är datummärkning av publicerad information så att användaren kan värdera innehållet i förhållande till annan information, förbättrade sökmöjligheter t.ex. på lagrum, utökade rss-flöden, arkivfunktion för material som inte längre är aktuellt men som ändå bör finnas kvar t.ex. beslut och annan information från tiden med personuppgiftslagen.

Datainspektionen bör utöka informationen som görs tillgänglig via myndighetens webbplats samt göra den mer lättillgänglig bl.a. genom att publicera en offentlig version av myndighetens diarium.

5.4.7 Förändra utbildningsinsatserna

Datainspektionens utbildningar är efterfrågade. Det kan därför vara lämpligt att göra dem fritt tillgängliga på webben och att innehållet görs mer lättillgängligt genom att utnyttja webbens möjligheter att kombinera video med annan information. Korta videoavsnitt kring avgränsade frågor kan t.ex. kombineras med texter, exempel, mallar och länkar till relevant material. Innehållet vid kurstillfällena kan också bli mer levande och mer praktiskt inriktat genom att använda exempel från Datainspektionens praxis.

Datainspektionen bör göra sina utbildningar tillgängliga på myndighetens webbplats.

5.4.8 Stimulera skapandet av dataskyddsvänlig teknik

Dataskyddet är – som framhållits i avsnitt 3.3 och 4.7 – inte något som kan läggas till vid sidan om den ordinarie verksamheten. Företagens genomförande förutsätter att de ordinarie it-systemlösningarna stödjer dataskyddsarbetet. Idag använder emellertid många företag en it-infrastruktur som t.ex. saknar stöd för hanteringen av metadata om personuppgifter (grund för behandling, insamlingstillfälle etc.) och för automatisk gallring av personuppgifter.

Varje företag ska inte år 2019 behöva ställa individuella krav på funktionalitet som krävs för att i praktiken kunna följa GDPR. Det finns anledning för näringslivet att samarbeta kring en sådan kravställning.

Lång erfarenhet av dataskydd och hög teknisk kompetens gör att Sverige har potential att bli en exportör av dataskyddsvänlig teknik. Detta bör främjas t.ex. genom statliga innovationsutlysningar och offentlig upphandling.

Staten bör använda kravställning i samband med offentlig upphandling och innovationsutlysningar för att stimulera framtagande av dataskyddsvänlig teknik.

Datainspektionen bör främja utvecklingen av dataskyddsvänlig teknik genom att uppmärksamma sådan teknik i sin kommunikation.

5.4.9 Finansieringen av arbetet med vägledning

Det framstår som uppenbart att behovet av vägledning för tillämpningen av GDPR kräver stora insatser av tillsynsmyndigheterna. Datainspektionens förebyggande verksamhet behöver byggas ut väsentligt för att undvika att bristerna i regelsystemet hämmar innovation och utvecklingen i näringslivet och i samhället stort. Detta kan innebära att Datainspektionen får utökade anslag.

Regeringen bör överväga ökade anslag till Datainspektionen.

5.5 Effektivare och mer förutsebar tillsyn

5.5.1 ”Grace-period” vid ändrat rättsläge

I situationer där rättsläget förändras t.ex. genom ett nytt ställningstagande från Datainspektionen eller tillkommande rättspraxis kan det vara lämpligt att de företag som behöver anpassas sin verksamhet efter det nya rättsläget får en viss tid för anpassningsarbetet innan Datainspektionen inleder en eventuell tillsyn. I sådana situationer bör Datainspektionen inte bara offentliggöra den nya praxisen utan även meddela hur lång tid som företagen har på sig att inrätta sig efter det nya rättsläget.

Datainspektionen bör arbeta med övergångsperioder vid ett ändrat rättsläge.

5.5.2 Sanktionsavgifter

Risken för sanktionsavgifter har det positiva med sig att dataskyddsfrågorna har uppmärksammats och prioriterats. Hotet om att drabbas av höga sanktionsavgifter har dock medfört en stor rädsla för att göra felaktiga bedömningar vilket i vissa fall har resulterat i att projekt har stoppats eller begränsats i onödan. Av egen erfarenhet vet vi att risken för sanktionsavgifter har medfört att företag som är i behov av vägledning avstår från att ta kontakt med Datainspektionen.

Det är därför lämpligt att när Datainspektionen bedriver tillsyn i syfte att skapa vägledning inte i onödan använder sig av sanktionsavgifter. I vart fall när tillsynsobjektet i ett oklart rättsläge gjort vad de kunnat, och gjort en kvalificerad bedömning och dokumenterat denna. Om Datainspektionen i ett senare skede gör en annan bedömning av rättsläget bör hänsyn tas till företagets möjligheter att utreda rättsfrågan.[26]

Det är samtidigt viktigt att Datainspektionen använder sanktionsavgifter mot de som, utan godtagbar ursäkt, inte har fullgjort det förberedande arbetet och därmed kommit billigare undan än de som har lagt tid och resurser på att uppfylla kraven enligt dataskyddsregleringen.

Datainspektionen har tagit på sig ordförandeskapet i den arbetsgrupp inom EDPB som ska föreslå riktlinjer för utfärdande av sanktionsavgifter i syfte ”att skapa en enhetlig bedömning av storleken på sanktionsavgiften vid samma regelbrott, det vill säga att lika fall behandlas lika av dataskyddsmyndigheterna.”[27] Det är ett vällovligt

[26] Jfr artikel 83.2 b GDPR.

[27] https://www.datainspektionen.se/nyheter/datainspektionen-leder-eu-arbetsgrupp-om-sanktionsavgifter/

initiativ av Datainspektionen men bör följas av klargörande information till företag om riskerna att drabbas av sanktionsavgifter när de försöker göra rätt och när de har kontakt med Datainspektionen.[28]

Datainspektionen bör klargöra för företag om de riskerar att drabbas av sanktionsavgifter även i de fall där de i god tro har gjort en felaktig rättslig bedömning eller när de själva har kontaktat Datainspektionen.

5.5.3 Överklaganden och praxisbildning

Med hänsyn till att det är mycket kostsamt och att det tar mycket lång tid att få ett beslut från Datainspektionen överprövat i domstol är det viktigt att inspektionens beslut inte av misstag bygger på felaktiga förutsättningar. Det är därför lämpligt att Datainspektionen använder sig av metoden att skicka ett utkast till beslut för påseende av tillsynsobjektet, i synnerhet om beslutet innebär att sanktionsavgifter utfärdas.

Huvuddelen av vägledningen på dataskyddsområdet skapas genom praxis och uttalanden från tillsynsmyndigheterna (inklusive EDPB). Tillsynsmyndigheternas starka ställning har för- och nackdelar. De sitter ofta på omfattande expertkunskap och har – i bästa fall – bra kontakt med företag och organisationer som ska tillämpa reglerna. De har därför vanligtvis de bästa förutsättningar för att skapa en verklighetsförankrad vägledning. Å andra sidan har de oftast en ambition att betona dataskyddsintresset på bekostnad av motstående intressen.

Att överklaga Datainspektionens beslut tar lång tid och är inte sällan förenad med stora kostnader och arbetsinsatser. I regel krävs det att målet förs vidare åtminstone till kammarrätten eftersom Datainspektionen i regel har framgång i förvaltningsrätten. Det är inte många företag som kan avvakta de år som en sådan process kan ta, särskilt inte när risken för att förlora är överhängande. Den planerade verksamhetsutvecklingen eller affärsidén är oftast överspelad efter så lång tid.

Det finns således en risk för att Datainspektionens tolkning förblir oprövad och betraktas som den enda korrekta tolkningen. Det är förstås svårt att finna en lösning på detta problem eftersom domstolsprocesser alltid tar lång tid och innebär risker.

Det kan dock övervägas om det finns anledning att skapa en särskild ordning för att få snabbare prövningar av rättsfrågor av mer principiell karaktär.

Inspiration till en sådan lösning kan sökas i den norska Personvernnemnda som kan pröva Datatilsynets beslut. Det danska datarådet som är en del av Danska datatilsynet prövar frågor av principiell karaktär. I svensk rätt kan möjligheten att begära förhandsbesked i skattefrågor från Skatterättsnämnden vara en förebild.

Datainspektionen bör skicka förslag till beslut för påseende av tillsynsobjektet i syfte att undvika missförstånd m.m. Regeringen bör överväga hur praxisbildningen på dataskyddsområdet kan underlättas genom åtgärder för överklaganden av Datainspektionens beslut.

[28] Jfr artikel 83.2 h GDPR.

6. Sammanfattande slutsatser

GDPR har medfört att medvetenheten om behovet av dataskydd i dagens digitaliserade samhälle har höjts väsentligt. Arbetet har dock inneburit ett omfattande administrativt arbete för många av samhällets aktörer, särskilt företagen. Det kan visserligen diskuteras om förbättringarna för de enskildas integritetsskydd står i rimlig proportion till kostnaderna, men det råder samtidigt en stor enighet om att reformens centrala delar var nödvändiga.

Vår genomgång har emellertid visat på att det finns brister i regelverket och i det förebyggande arbetet från tillsynsmyndigheterna. Vi har också försökt presentera åtgärdsförslag. Vissa förslag är relativt enkla att genomföra, andra är mer genomgripande och kräver därför mer utredning och överväganden.

Vi vill lyfta några övergripande slutsatser som vi dragit under arbetets gång.

- **GDPR duger;** GDPR är ett omfattande och komplicerat regelverk som kan kritiseras för att inte ge tillräcklig förutsebarhet i tillämpningen. Med undantag för vissa oklarheter tycks ändå de generella bestämmelserna i GDPR vara den mest lämpade lösningen för ett harmoniserat regelverk. Den grundläggande regleringsmodellen i GDPR bör därför inte förändras.
- **Öka harmoniseringen;** Det tycks – trots ambitionen med GDPR – vara svårt att få till ett effektivt samarbete inom EU i syfte att gemensamt komma till rätta med problemen i dataskyddsregleringen, särskilt vad gäller bristande harmonisering. Det gäller såväl tillsynsmyndigheterna som de nationella lagstiftarna. Det borde finnas mycket att tjäna på att dessa utökar sitt samarbete med att ta fram mer harmoniserade nationella regler samt mer enhetlig tillämpning och vägledning från tillsynsmyndigheterna. Samtidigt måste man vara medveten om att harmoniseringen inte alltid är att föredra. Det är ju inte alltid den bästa lösningen blir den som harmoniseras!
- **Se över dataskyddslagen;** När det gäller svensk rätt kan vi konstatera att lagstiftningsarbetet som genomfördes inför att GDPR började tillämpas i maj 2018 var omfattande och utfördes med stor brådska. Ambitionen var främst att bli färdig i tid och det fanns inte mycket tid för att överväga förbättringar eller omvärdera tidigare tolkningar av dataskyddsregleringen. Det finns därför redan nu ett behov av att se över de antagna reglerna, framför allt dataskyddslagen och förordningen som kompletterar dataskyddlagen.
- **Förstärk Datainspektionens förebyggande verksamhet;** En tung börda för att avhjälpa många av problemen med GDPR faller på Datainspektionen. Vi har, som nämnts ovan, förståelse för att Datainspektionen har en besvärlig situation och hoppas med denna rapport kunna bidra med några förslag till att förbättra verksamheten. Vi menar att Datainspektionens förebyggande och rådgivande verksamhet behöver förstärkas. De ökade anslag som nyligen har tillskjutits till myndigheten räcker inte. Som det är nu drabbar de stora kostnaderna som uppstår på grund av brister i regelverket och vägledningen företagen. Det är inte rimligt att de som under sanktionshot är skyldiga att följa regelverket ska ansvara för att utreda oklarheter i regelsystemet och kompensera för statens bristande vägledning. Ur ett samhällsperspektiv bör därför höjda anslag till Datainspektionen vara mycket effektivt.

Från svenskt perspektiv kan vi konstatera att GDPR har medfört en betydligt ökad administrativ börda för företagen. Den så kallade riskbaserade ansatsen har inte i tillräcklig utsträckning använts för att underlätta för de som ägnar sig åt personuppgiftsbehandling som innebär begränsade integritetsrisker. Här kan man ibland sakna den så kallade missbruksregeln som infördes i personuppgiftslagen i syfte att förenkla tillämpning av lag vid mindre integritetskänslig behandling. Men missbruksregeln var svår att förena med dataskyddsdirektivets grundstruktur och skapade även bristande förutsebarhet.

Med GDPR tycks vi dock ha fått en detaljerad och delvis byråkratisk reglering som trots omfattande artikeltexter och kompletterande vägledning inte ger tillräcklig förutsebarhet för de som ska tillämpa reglerna.

www.svensktnaringsliv.se
Storgatan 19, 114 82 Stockholm
Telefon 08-553 430 00

Arkitektkopia AB, Bromma, 2019