SVENSKT NÄRINGSLIV

Vad är fortfarande fel med GDPR?

FÖRSLAG SOM MINSKAR BYRÅKRATIN OCH STÄRKER KONKURRENSKRAFTEN

NOVEMBER 2022

Författare:

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 bland annat 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 startup-företag till stora organisationer samt expert i flera statliga utredningar.

Innehåll

Förord av Svenskt Näringsliv

Många företag beskriver bekymmersamt hur dataskyddsregler negativt påverkar deras affärer och möjligheter att skapa nya produkter och tjänster. Dataskyddsförordningen, GDPR, styr både om och hur företag får behandla personuppgifter. Att dataskyddsregler finns är i grunden självklart, men utformningen och omfattningen av dataskyddsreglerna kan obefogat försvåra, fördyra och förhindra datahantering. Det är inte helt ovanligt att personuppgiftsskyddet beskrivs som en absolut rättighet, vilket det inte är. I det datadrivna samhället är det av stor vikt att integritetsskyddet på ett korrekt sätt balanseras mot andra rättigheter, så att nyttan och de enorma möjligheter som öppnar sig genom dataanvändning kan realiseras.

Europas konkurrenskraft kommer i allt högre grad att vara beroende av hur företagen kan analysera data och använda data i AI-system. Inom de närmsta åren kommer flera datalagar att träda i kraft. Förutom nya lagar som Digital Services Act, Digital Markets Act, Data Act och AI Act, är det fortsatt eDataskyddsdirektivet och GDPR som främst styr hur data som innehåller personuppgifter får användas.

Med rapporten *Vad är fortfarande fel med GDPR?* vill Svenskt Näringsliv belysa näringslivets utmaningar inom dataskyddsområdet. Författarna Martin Brinnen och Daniel Westman har fått i uppdrag att beskriva vad som behöver göras för att nå ett relevant integritetsskydd, genom tillämpbara och proportionerliga regler som möjliggör innovation, internationell konkurrenskraft och konkurrens på lika villkor.

Rapporten är en uppföljning av *Vad är fel med GDPR?* från 2019, och behandlar kvarstående GDPR-relaterade problem samt nya problem som tillkommit eller befaras tillkomma genom annan lagstiftning eller praxis. Rapporten innehåller förslag på förbättringar som skulle kunna ingå i EU-kommissionens kommande utvärdering av GDPR 2024, eller genomföras i nationell lagstiftning och av dataskyddsmyndigheter på nationell och europeisk nivå.

Stockholm i november 2022

Karin Johansson
Vice vd Svenskt Näringsliv

Sammanfattning

EU:s dataskyddsförordning har nu tillämpats i över fyra år. Rapporten beskriver näringslivets utmaningar på dataskyddsområdet och presenterar ett antal lösningsidéer för att förbättra situationen.

”Lagen som styr allt” – bakgrunden till utmaningarna

Dataskyddsförordningen är krävande för de flesta företag. Personuppgifter hanteras i nästan alla delar av verksamheten, och förordningen blir därmed tillämplig på nästan allt vad ett företag gör. Möjligheterna att överhuvudtaget behandla personuppgifter för vissa ändamål eller på ett visst sätt begränsas genom de krav som förordningen ställer upp. För att efterleva dataskyddsreglerna är det nödvändigt att bedriva ett systematiskt och inte sällan resurskrävande arbete.

I en alltmer datadriven värld riskerar förordningen att bli ”lagen om allt”. En restriktiv tillämpning gör dessutom att andra intressen än skyddet för personuppgifter ofta får stryka på foten.

Ett starkt skydd för personuppgifter är motiverat, och de grundläggande elementen i dagens dataskyddsreglering är här för att stanna. Det krävs dock åtgärder för att aktivt motverka negativa effekter i form av onödig byråkrati, rättsosäkerhet och omotiverade begränsningar av legitima verksamheter.

Omotiverade begränsningar av innovations- och konkurrenskraft

En stor del av näringslivets innovationer är idag på ett eller annat sätt kopplade till analys av stora datamängder och till maskininlärning för att skapa tillämpningar av artificiell intelligens (AI). Det kan till exempel handla om att ställa medicinska diagnoser, minska energianvändningen, ta fram nya produkter och tjänster, effektivisera industriell produktion och förbättra kundservicen.

Det finns politiska ambitioner och nya regelverk på EU-nivå som syftar till att möjliggöra vidareanvändning av data. Dataskyddslagstiftningens vida tillämpningsområde och restriktiva tillämpning drar emellertid åt ett annat håll. Det krävs därför ett antal aktiva åtgärder för att avlägsna omotiverade hinder mot legitim innovationsverksamhet och för att minska rättsosäkerheten.

I rapporten föreslås hur det kan göras enklare för företag att veta om de vidtagit tillräckliga åtgärder för att anonymisera data och på det sättet säkerställt att dataskyddsförordningen inte blir tillämplig. Har den personuppgiftsansvarige använt sig av vissa författningsreglerade anonymiseringstekniker ska det anses vara tillräckligt.

Vidare föreslås en kompletterande EU-reglering som tydliggör att maskininlärning och kraftfull analys av personuppgifter får ske för samhällsnyttiga ändamål. Ett villkor är dock att behandlingen syftar till att utvinna aggregerad kunskap på gruppnivå och att slutresultatet inte innehåller några personuppgifter. Dessutom ska det krävas att kraftfulla säkerhets- och skyddsåtgärder vidtas.

För mycket byråkrati utan tydlig förbättring av integritetsskyddet

Dataskyddsförordningen förutsätter stora insatser av de som behandlar personuppgifter och en omfattande tillsynsorganisation hos dataskyddsmyndigheterna. Under de år som dataskyddsförordningen har tillämpats har integritetsskyddet för personuppgifter förstärkts till priset av stora kostnader för näringslivet och samhället i stort. Inte minst har det visat sig genom en övermäktig arbetsbörda för dataskyddsmyndigheterna. Det finns därför ett behov av att **effektivisera regelverket** så att resurser hos företagen och dataskyddsmyndigheterna används på ett sätt som ger bästa möjliga integritetsskydd och som står i proportion till negativa bieffekter på andra intressen.

Mot den bakgrunden föreslås i rapporten bland annat att mindre integritetskänsliga behandlingar bör kunna hanteras enklare, till exempel genom att EU-kommissionen får mandat att i delegerade akter fastställa under vilka förutsättningar vissa typiskt sett harmlösa behandlingar får utföras. Vidare föreslås att utrednings- och dokumentationsskyldigheten för sådana behandlingar begränsas och att dataskyddsmyndigheterna ges möjlighet att hantera klagomål på ett mer effektivt sätt och därigenom styra tillsynsverksamheten till områden med de största integritetsriskerna.

För ensidigt fokus på dataskyddsintresset

Rätten till skydd för personuppgifter är inte en absolut rättighet; den måste förstås utifrån sin uppgift i samhället och vägas mot andra grundläggande rättigheter i enlighet med proportionalitetsprincipen. Av detta följer att rätten till skydd för personuppgifter måste vägas mot motstående intressen. Det gäller inte bara andras rättigheter och friheter såsom yttrande- och informationsfrihet samt näringsfrihet, utan även mot behovet av ett fritt flöde av personuppgifter. EU-domstolen och dataskyddsmyndigheterna har hittills tolkat rätten till skydd för personuppgifter enligt EU-stadgan och dataskyddsförordningen restriktivt.

Det finns, enligt vår uppfattning, anledning att denna inställning i vissa fall bör **nyanseras**, i vart fall inom den yttre ram som följer av EU-domstolens tolkning av EU-stadgan, men det förutsätter ändringar i dataskyddsförordningen. Mot den bakgrunden föreslås bland annat att dataskyddsmyndigheterna bör ha en skyldighet att beakta motstående intressen, vilket bör komma till uttryck i myndigheternas uppgifter i artiklarna 57 och 70. Vidare föreslås åtgärder för att underlätta bedömningarna av tredjelandsöverföringar samt mer flexibla möjligheter att behandla känsliga personuppgifter och uppgifter om lagöverträdelser.

Bristande förutsebarhet och harmonisering

Dataskyddsförordningen innehåller som bekant många vaga och oklara principbestämmelser, vilket i stor utsträckning är oundvikligt med hänsyn till förordningens breda tillämpningsområde och att digitaliseringen av samhället medför behov av ett dynamiskt regelverk. Men det vaga regelverket skapar även bristande förutsebarhet och harmonisering inom EU, vilket leder till konsekvenser för såväl företagen som ska efterleva regelverket som för dataskyddsmyndigheterna – bland annat ökat behov av vägledning och ärendeinflöde.

Det finns ett behov av att regelverket **konkretiseras**. I rapporten föreslås därför bland annat att EU-kommissionen ges mandat att komplettera och konkretisera bestämmelserna i dataskyddsförordningen, till exempel genom att ange vissa typsituationer där behandling av personuppgifter kan stödjas på en intresseavvägning. Vidare föreslås att personuppgiftsansvariga ska kunna begära förhandssamråd i oklara rättsfrågor och att det även kan övervägas om bindande förhandsbesked ska kunna lämnas. EU-kommissionen bör vidare ges ett större ansvar för arbetet med uppförandekoder.

1 Inledning

EU:s dataskyddsförordning (GDPR)[1] har nu tillämpats i över fyra år. Senast i maj 2024 ska EU-kommissionen lämna en rapport som utvärderar och ser över förordningen.[2] Inför detta arbete är det lämpligt att kort beskriva näringslivets utmaningar på dataskyddsområdet och skissa vissa lösningsidéer.

Redan 2019 skrev vi rapporten *Vad är fel med GDPR?*[3] Problembeskrivningen och förslagen som vi lämnade där är i huvudsak fortfarande relevanta, även om vi noterar att vissa förslag har resulterat i åtgärder, bland annat från Integritetsskyddsmyndighetens sida. Samtidigt motiverar teknikutvecklingen, ytterligare praktiska erfarenheter samt nya lagstiftningsinitiativ på närliggande områden en ny analys. Vi inriktar oss i denna uppföljande rapport i större utsträckning på själva dataskyddsförordningen än vad som var motiverat när förordningen var alldeles färsk och det stod klart att någon revidering inte skulle ske i närtid. Även denna rapport innehåller emellertid förslag på hur den svenska lagstiftaren och svenska myndigheter kan agera för att underlätta för näringslivet inom ramen för den gällande förordningen. Vissa av förslagen från *Vad är fel med GDPR?* återkommer och utvecklas i denna rapport.

Sedan vår rapport 2019 har företagens utmaningar på dataskyddsområdet även uppmärksammats i andra sammanhang. EU-parlamentarikern Axel Voss har exempelvis tagit fram en översiktlig rapport.[4] Förslaget till reformerade dataskyddsregler i Storbritannien efter brexit är på samma sätt som vår rapport inriktat mot att undanröja onödiga hinder för näringslivet, utan att i grunden avvika från den europeiska skyddsnivån för personuppgifter.[5]

Vårt uppdrag har varit att skriva en koncis rapport som sammanfattar näringslivets utmaningar på dataskyddsområdet samt att skissa på föreslagna åtgärder. Vi har inom ramen för detta arbete inte haft möjlighet att genomföra några djupgående utredningsinsatser. De förslag vi presenterar ska ses som lösningsidéer som kan behöva analyseras närmare och utvecklas.

1 Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 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/EG (allmän dataskyddsförordning).

2 Se artikel 97.1. Se Meddelande från kommissionen till Europaparlamentet och rådet Dataskydd som en pelare för medborgarnas egenmakt och EU:s strategi för den digitala övergången – tillämpning av den allmänna dataskyddsförordningen under två års tid COM(2020) 264 final.

3 Brinnen, Martin & Westman, Daniel, *Vad är fel med GDPR? Beskrivning av näringslivets utmaningar samt några förslag på förbättringar,* Svenskt Näringsliv, 2019 [nedan *Vad är fel med GDPR?*].

4 Position paper on Fixing the GDPR: Towards Version 2.0, 25 May 2021.

5 Data: a new direction - government response to consultation, Updated 23 June 2022.

Att fokus här riktas mot näringslivets utmaningar på dataskyddsområdet innebär inte att andra intressenters perspektiv är oviktiga för oss. Vår ambition har varit att de förslag vi lägger fram inte ska försämra de registrerades situation i någon beaktansvärd utsträckning. Vi bedömer att våra förslag är förenliga med Europarådets moderniserade dataskyddskonvention (”Konvention 108+”).[6]

Rapporten är upplagd på följande sätt: I avsnitt 2 visar vi hur dataskyddslagstiftningen i ett datadrivet samhälle riskerar att bli en restriktiv ”lag om allt” och att det krävs välriktade åtgärder för att motverka vissa negativa konsekvenser för näringslivet. I de följande fyra avsnitten ger vi mer konkreta exempel på problem och utmaningar samt skisserar lösningsförslag. Avsnitt 3 behandlar omotiverade begränsningar av innovations- och konkurrenskraft, till exempel möjligheten att utveckla och använda artificiell intelligens (AI). I avsnitt 4 ger vi exempel på hur vissa delar av dataskydds-förordningen riskerar att skapa en långtgående byråkrati som går längre än vad som är motiverat. I avsnitt 5 diskuteras utmaningar med en alltför restriktiv tillämpning av grundläggande dataskyddsprinciper, till exempel reglerna om överföring till tredjeland. Avsnitt 6 behandlar problem med bristande förutsebarhet och harmonisering inom EU och lämnar förslag på åtgärder.

I rapporten beaktas material som presenterats innan den 1 september 2022.

6 Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, Adopted by the Committee of Ministers at its 128th Session of the Committee of Ministers (Elsinore, 18 May 2018).

2 ”Lagen som styr allt” – bakgrunden till utmaningarna

Dataskyddsförordningen är krävande för de flesta företag.[7] Personuppgifter hanteras i nästan alla delar av verksamheten och förordningen blir därmed tillämplig på nästan allt vad ett företag gör. Möjligheterna att överhuvudtaget behandla personuppgifter för vissa ändamål eller på ett visst sätt begränsas genom de krav som förordningen ställer upp. För att efterleva dataskyddsreglerna är det nödvändigt att bedriva ett systematiskt och inte sällan resurskrävande arbete.

Att det ska finnas rättsliga gränser för hur företag får hantera personuppgifter är självklart, och att företag måste lägga ner vissa resurser för att skydda personuppgifter som rör till exempel anställda eller kunder är fullt rimligt. Skyddet för personuppgifter utgör en grundläggande rättighet i den europeiska rättsordningen och samtidigt ligger det i varje seriöst företags eget intresse att skapa tillit för sin verksamhet.

Den regleringsmodell som dataskyddsförordningen och flera andra dataskydds-regelverk bygger på riskerar emellertid att skapa onödig byråkrati, omotiverade begränsningar av legitima verksamheter och motstående samhälleliga intressen samt leda till rättsosäkerhet.

I en värld som i allt högre grad bygger på användning av data för att lösa olika uppgifter, riskerar den vida synen på vad som utgör en personuppgift leda till att dataskyddslagstiftningen blir ”lagen om allt”.[8] I praktiken innebär det att dataskyddsintresset får ett tydligt försteg framför de flesta andra intressen som är förknippade med hanteringen av data. Det kan inverka negativt på möjligheterna att använda stora datamängder för maskininlärning och analys, vilket i sin tur till exempel kan försvåra utvecklandet av nya samhällsnyttiga tjänster och begränsa möjligheterna att effektivisera olika verksamheter.[9]

En viktig förklaring till restriktiviteten är de grundläggande principerna, till exempel uppgifts- och lagringsminimering (artikel 5). En annan är att dataskyddsförordningen

7 Se *Vad är fel med GDPR?*, s. 13-16.

8 Se t.ex. Nadezhda Purtova (2018) *The law of everything. Broad concept of personal data and future of EU data protection law*, Law, Innovation and Technology, 10:1, 40-81 samt Förslag till avgörande av generaladvokat Michal Bobek i mål C-245/20, Autoriteit Persoonsgegevens, p. 55-65.

9 Se avsnitt 3 nedan.

kräver att behandling av personuppgifter som sker utan den registrerades samtycke ska vara ”nödvändig” (artikel 6). EU-domstolen, Europeiska dataskyddsstyrelsen (EDPB) och nationella dataskyddsmyndigheter har tolkat det senare kravet strikt. Regleringen av så kallade känsliga personuppgifter och uppgifter om lagöverträdelser är ännu mer begränsande. Sammantaget gör detta att behandlingar som kräver tillgång till stora datamängder, men där behovet av att hantera varje enskild uppgift på det aktuella sättet inte alltid kan visas på förhand, riskerar att anses vara otillåtna. Detta trots att de reella riskerna för de registrerade många gånger är begränsade.[10]

Även i situationer där det på goda grunder kan argumenteras för att behandlingen av personuppgifter faktiskt är tillåten, innebär den vaga och principbaserade regleringen i dataskyddsförordningen – i kombination med riskerna för mycket kraftfulla sanktioner – att företag kan komma att begränsa sin riskexponering och avstå från nyttig och lovande verksamhet.[11]

Genom dataskyddsförordningen tog dataskyddslagstiftningen dessutom ett kliv mot att bli mer compliance-orienterad.[12] Ett antal nya krav på struktur, organisation och arbetssätt på dataskyddsområdet framstår i grunden som vällovliga men innebär inte sällan en överdriven byråkratisering, särskilt i mindre verksamheter eller i verksamheter där riskerna förknippade med hanteringen av personuppgifter i praktiken är begränsade. Samtidigt har det visat sig svårt i praktiken att få till de delar av förordningen som syftar till att underlätta för de som behandlar personuppgifter, såsom uppförandekoder, certifiering etc.[13]

Vi kan konstatera att mycket talar för att grundelementen i den befintliga dataskyddsregleringen är här för att stanna och att strikta krav på själva hanteringen av personuppgifter faktiskt är motiverade, inte minst i en alltmer datadriven värld. De centrala elementen i dataskyddsförordningen har 50-åriga anor, och dataskyddsregler av europeiskt snitt har under de senaste trettio åren exporterats till många andra länder i världen. Det är vidare svårt att se hur det i ett samhälle med så hög utvecklingstakt som dagens skulle vara möjligt att skapa ett starkt skydd för personuppgifter med hjälp av en annan regleringsmodell, till exempel en reglering som istället förbjuder vissa uppräknade beteenden eller som kopplas till påvisade kränkningar i ett enskilt fall.

Vi föreslår mot denna bakgrund ingen grundläggande reform av dataskyddslagstiftningen. Istället förordar vi ett antal mer begränsade åtgärder för att hantera några av de problem som näringslivet brottas med. Åtgärderna är av olika slag, till exempel begränsade ändringar av själva dataskyddsförordningen och annan EU-lagstiftning, ny nationell kompletterande reglering, tydligare och mer användbar vägledning samt förbättrad tillsyn.[14]

10 Se avsnitt 3 nedan.

11 Se avsnitt 5 nedan.

12 Se avsnitt 4 nedan.

13 Se avsnitt 6 nedan.

14 För en närmare diskussion om ”verktygslådan” för förbättringar, se *Vad är fel med GDPR?*, s. 17-20.

Det är naturligt att en stor rättslig reform som dataskyddsreformen utvärderas efter ett antal år. I samband med det bör oönskade negativa effekter åtgärdas i så stor utsträckning som möjligt, utan att det leder till att medborgarnas legitima anspråk på skydd för sina personuppgifter urholkas. Sett från ett näringslivsperspektiv bör reformarbetet främst inriktas på att säkerställa rätt balans mellan olika rättigheter och intressen som är förknippade med data, minska onödig byråkrati, förtydliga rättsläget och bidra till större harmonisering för företag som är verksamma på den inre marknaden.

Ett starkt, tydligt och balanserat dataskydd har goda förutsättningar att vinna både medborgarnas och företagens förtroende.

3 Omotiverade begränsningar av innovations- och konkurrenskraft

3.1 Problembeskrivning

En stor del av näringslivets innovationer är idag på ett eller annat sätt kopplade till analys av stora datamängder och till maskininlärning för att skapa tillämpningar av artificiell intelligens (AI). Det kan till exempel handla om att ställa medicinska diagnoser, minska energianvändningen, ta fram nya produkter och tjänster, effektivisera industriell produktion och förbättra kundservicen. För att nå framgång krävs inte bara tillgång till stora datamängder, utan också att datasamlingarna är relevanta och har hög kvalitet.

På politisk nivå finns stora förväntningar på en ökad användning av data för att lösa olika samhällsutmaningar. Både inom EU och på nationell nivå finns strategier för att nyttiggöra data.[15] Ofta framhålls i dessa sammanhang att data måste kunna delas mellan olika aktörer och att nyttan uppstår när data faktiskt används.

På EU-nivå har strategin konkretiserats genom antagandet av ny lagstiftning och genom ytterligare förslag till ny lagstiftning. *Öppna data-direktivet* syftar bland annat till att förbättra möjligheterna att vidareanvända data från den offentliga sektorn.[16] *Data Governance Act* – en ny EU-förordning – syftar till att öka mängden data från den offentliga sektorn som kan vidareutnyttjas och reglerar samtidigt förutsättningarna för vissa institutioner som främjar datadelning.[17] *Data Act* – ett förslag till en ny EU-förordning – innehåller åtgärder för att främja tillgången till och användningen av

15 Se Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén En EU-strategi för data COM(2020) 66 final samt Data — en underutnyttjad resurs för Sverige: En strategi för ökad tillgång av data för bl.a. artificiell intelligens och digital innovation, Bilaga till beslut II 5 vid regeringssammanträde den 20 oktober 2021, I2021/02739.

16 Europaparlaments och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn.

17 Europaparlaments och rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning och om ändring av förordning (EU) 2018/1724 (dataförvaltningsakten).

data bland annat genom regler om tillgång till data som finns i den privata sektorn.[18] Till detta kommer sektorsspecifik reglering på olika områden, till exempel ett förordningsförslag som bland annat syftar till att underlätta vidareutnyttjandet av hälsodata.[19]

Dataskyddslagstiftningen är elefanten i rummet. Den vida definitionen av begreppet personuppgifter gör att lagstiftningen blir tillämplig på såväl insamling och delning som användning för analys eller maskininlärning. Krav på uppgifts- och lagringsminimering och rättsligt stöd för behandling av varje uppgift verkar i många fall begränsande, och skapar i andra fall åtminstone stor osäkerhet kring vilka projekt som är möjliga.[20]

Den nya lagstiftningen som syftar till att nyttiggöra data innehåller inga undantag eller lättnadsregler för behandlingen av personuppgifter. Tvärtom tydliggörs att dataskyddslagstiftningen är fullt tillämplig. Med tanke på hur stora delar av de aktuella datamängderna som helt eller delvis består av personuppgifter, krävs kompletterande åtgärder i dataskyddet för att förverkliga målen på området.

Det råder ingen tvekan om att det i vissa fall finns risker förknippade med att samla stora mängder personuppgifter, men samtidigt finns som sagt ofta stor potential att lösa samhällsutmaningar på nya och mer effektiva sätt. För att en våt filt inte ska läggas över en stor del av de datadrivna projekten är det viktigt att vara vaksam på onödigt restriktiva inslag i dataskyddets utformning och tillämpning. Här står europeiska företags innovationsförmåga, och förmåga att konkurrera med företag från andra delar av världen, på spel.

3.2 Förenkla användningen av maskininlärning och kraftfull dataanalys

För att skapa kraftfull AI finns det, som nämnts ovan, ofta ett behov av att använda stora mängder data för maskininlärning. Det kan till exempel handla om att lära upp algoritmer i självkörande fordon eller i säkerhetssystem. Även vid sidan av maskininlärningen kan stora datamängder användas för att utvinna ny kunskap, till exempel upptäcka hittills okända korrelationer mellan företeelser.

Vid denna typ av användning av data är enskilda individer inte av direkt intresse, utan deras personuppgifter används som en resurs för att utvinna kunskap på gruppnivå. Utförs hanteringen på rätt sätt har användningen heller ingen negativ effekt på de berörda personerna. Vi har alltså här att göra med en annan typ av behandling än den som är inriktad mot att samla stora mängder uppgifter om en viss individ i syfte att erbjuda annonsörer att rikta marknadsföring. Precis som när det gäller till exempel statistik och många typer av forskning innehåller slutprodukten – om arbetet utförs på rätt sätt – inte några personuppgifter. Den vida personuppgiftsdefinitionen gör

18 Förslag till Europaparlaments och rådets förordning om harmoniserade regler för skälig åtkomst till och användning av data (dataakten), COM/2022/68 final.

19 Förslag till Europaparlaments och rådets förordning om ett europeiskt hälsodataområde, COM/2022/197 final.

20 Se t.ex. Integritetsskyddsmyndigheten, Delredovisning av uppdrag om kunskapshöjande insatser till innovationssystemet om integritets- och dataskyddsfrågor, dnr DI-2021-5817, 2022-03-31, avsnitt 3.

emellertid att dataskyddslagstiftning normalt blir tillämplig. Detta gäller även om uppgifter som används inte direkt identifierar en viss registrerad.

En rättslig analys måste naturligtvis göras utifrån omständigheterna i varje enskilt fall, men många gånger är det osäkert om denna typ av projekt är förenliga med dataskyddsförordningens materiella reglering. Det som framför allt skapar osäkerhet är finalitetsprincipen (kravet på ändamålskoppling), kravet på rättsligt stöd för behandlingen av ”vanliga” personuppgifter och kravet på särskilt rättsligt stöd för känsliga personuppgifter.[21]

I praktiken är det sällan en framkomlig väg att basera de aktuella behandlingarna på samtycke. Det beror bland annat på att många enskilda berörs, och att möjligheterna att få ett giltigt samtycke från tillräckligt många för att säkerställa ett representativt urval i praktiken är begränsade. Samtidigt är det ofta osäkert om andra mer lämpliga rättsliga grunder, till exempel legitimt intresse (intresseavvägningen), är tillämpliga. Det går givetvis inte att helt undvika behovet av att göra en rättslig bedömning projekt för projekt, men sett på en övergripande nivå framstår rättsläget idag som alltför osäkert och begränsande för att innovation på detta område ska främjas.

Det finns vissa tillvägagångssätt för att minska behovet av att använda och att dela personuppgifter på ett sätt som är problematiskt enligt dataskyddslagstiftningen. Ett är att använda syntetiska data, det vill säga data som har samma karaktär som riktiga uppgifter men som inte avser verkliga människor. Ett annat är att använda så kallad federerad maskininlärning, vilken innebär att data inte behöver överföras mellan organisationer och samlas i en enda stor databas. Enkelt uttryckt flyttas istället själva maskininlärningsverksamheten runt. Men inget av dessa tillvägagångssätt utgör någon patentlösning för att hantera alla dataskyddsrättsliga utmaningar.

Ofta skulle den här diskuterade maskininlärningen eller analysen lika effektivt kunna utföras med anonyma uppgifter. Den långtgående definitionen av begreppet personuppgifter i artikel 4.1 i dataskyddsförordningen gör det emellertid svårt att med säkerhet veta om behandlingen i ett konkret fall faller utanför förordningen eller inte. En personuppgiftsansvarig har till exempel ofta svårt att överblicka vilka tillgängliga datamängder och metoder som andra aktörer kan tänkas använda för att identifiera en viss person – förhållanden som enligt EU-domstolens dom i Breyer-målet[22] kan vara relevanta vid bedömningen av om det är fråga om en behandling av personuppgifter eller inte.

21 Jfr Integritetsskyddsmyndigheten, Delredovisning av uppdrag om kunskapshöjande insatser till innovationssystemet om integritets- och dataskyddsfrågor, dnr DI-2021-5817, 2022-03-31, avsnitt 3.

22 EU-domstolens dom den 19 oktober 2016 i mål C-582/14 (”Breyer”).

Lösningsidé: EU-lagstiftningen bör ändras så att hantering av data blir tillåten om den personuppgiftsansvarige vidtagit anonymiseringsåtgärder som räknas upp i kompletterande sekundärlagstiftning (till exempel en delegerad akt från EU-kommissionen). Vilka åtgärder som listas måste bestämmas utifrån tillgänglig teknik för återidentifiering vid varje given tidpunkt.

Data som varit föremål för den aktuella typen av anonymiseringsåtgärder ska även få delas till en annan aktör som utför maskininlärningen eller analysen.

Fördelen med den föreslagna ordningen är en större förutsebarhet för den personuppgiftsansvarige samtidigt som utvecklingen och användningen av anonymiseringstekniker främjas, vilket även gagnar de registrerade.

Vi bedömer att det skulle vara mer riskfyllt för medborgarna att istället snäva in begreppet personuppgifter, och förordar därför inte denna lösning.

I vissa sammanhang är det inte praktiskt möjligt att anonymisera (eller att använda syntetiska data). I dessa fall är integritetsriskerna högre, men med tanke på den stora positiva potentialen kan det ändå vara motiverat att säkerställa att maskininlärning och kraftfull analys av stora datamängder får ske. För att motverka riskerna krävs dock – på samma sätt som när det gäller behandling för bland annat forskningsändamål och statistiska ändamål (artikel 89) – att det ställs krav på kompletterande säkerhets- och skyddsåtgärder.

Lösningsidé: Inför kompletterande EU-reglering som tydliggör att maskininlärning och kraftfull analys av stora datamängder får ske för samhällsnyttiga ändamål. Ett villkor bör vara att behandlingen syftar till att utvinna aggregerad kunskap på gruppnivå och att slutresultatet inte innehåller några personuppgifter (jämför behandling för statistiska ändamål).

Säkerhets- och skyddsåtgärder för att motverka de risker som finns kan till exempel vara pseudonymisering, korta gallringstider, förbud mot att använda insamlade personuppgifter för att vidta åtgärder rörande de registrerade och särskilda krav på åtkomstbegränsning.

Den föreslagna ordningen bör även gälla beträffande känsliga personuppgifter om sådana uppgifter är nödvändiga för att säkerställa kvaliteten i slutresultatet, till exempel att algoritmer som tas fram genom maskininlärning inte blir diskriminerande.[23]

23 I detta hänseende är artikel 10.5 i förslaget till AI Act otillräckligt. Dels är detta förslag begränsat till högrisk-AI, dels ger det bara rätt att behandla känsliga personuppgifter för att motverka snedvridning. Se Förslag till Europaparlamentets och rådets förordning om harmoniserad regler för artificiell intelligens (Rättsakt om artificiell intelligens) och om ändring av vissa unionslagstiftningsakter, COM(2021) 206 final.

I avvaktan på ett förenklat och tydligt regelverk för dataanvändning är det viktigt att företag kan få vägledning och tillgång till konstruktiva lösningar inom ramen för gällande rätt.

Lösningsidé: Integritetsskyddsmyndigheten bör ges ett permanent uppdrag att främja ansvarsfull och säker användning av personuppgifter för maskininlärning och kraftfulla analyser på gruppnivå.[24]

Detta kan bland annat ske genom så kallade regulatoriska sandlådor.

3.3 Ompröva den restriktiva hållningen till automatiserat beslutsfattande

En stor mängd arbetsuppgifter kan utföras av AI-system, bland annat olika typer av beslutsfattande. Automatiserade beslut medför inte bara effektivitetsvinster, utan innebär även att det finns möjlighet att förbättra servicen till medborgare och konsumenter och att det finns potential att höja kvaliteten på besluten.

När AI-system används för automatiserat beslutsfattande som rör enskilda är det samtidigt viktigt att vara vaksam på riskerna, till exempel felaktiga beslut och olika typer av systematisk snedvridning. Det är därför naturligt med strikta regler som säkerställer kvalitet, rätt till omprövning, rätt till insyn etc. En alltför negativ inställning till automatiserade beslut som sådana riskerar dock att kasta ut barnet med badvattnet.

Utanför dataskyddet finns allmänna regler som är tillämpliga också på automatiserade beslut, till exempel regler om diskriminering. Förslaget till en ny EU-förordning om artificiell intelligens är också till stor del inriktat på att genom olika typer av produktsäkerhetsliknande krav motverka risker som är förknippade med automatiserade beslut.[25]

Dataskyddsförordningens grundläggande bestämmelser (principerna, kravet på laglig grund för behandling med mera) tillämpas även vid automatiserat beslutsfattande som rör enskilda, eftersom sådant beslutsfattande förutsätter behandling av personuppgifter. Därmed uppställs i praktiken redan genom denna reglering vissa gränser för när automatiserat beslutsfattande överhuvudtaget kan ske och vilka uppgifter som kan användas i processen. Den registrerade ges även rätt att få information om behandlingen och vissa möjligheter att motsätta sig denna.

24 Jfr t.ex. den brittiska dataskyddsmyndighetens initiativ ICO Innovation Service (https://ico.org.uk/about-the-ico/what-we-do/ico-innovation-services/). Jfr även Integritetsskyddsmyndigheten innovationsuppdrag (Delredovisning av uppdrag om kunskapshöjande insatser till innovationssystemet om integritets- och dataskyddsfrågor, dnr DI-2021-5817, 2022-03-31, avsnitt 3).

25 Förslag till Europaparlamentets och rådets förordning om harmoniserade regler för artificiell intelligens (Rättsakt om artificiell intelligens) och om ändring av vissa unionslagstiftningsakter, COM(2021) 206 final.

Dataskyddsförordningen innehåller därutöver en specialreglering av automatiserade beslut (artikel 22), som anger att enskilda som huvudregel har rätt 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.

EDPB har genom att ställa sig bakom den så kallade Artikel 29-gruppens yttrande om bestämmelsen valt att ge artikel 22 en restriktiv tolkning.[26] Något tillspetsat kan man säga att bestämmelsens första stycke tolkas som ett principiellt förbud mot automatiserade beslut. Det skulle innebära att sådant beslutsfattande 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).

EDPB har vidare gjort bedömningen att bestämmelsen inte bara är tillämplig på automatiserat beslutsfattande som bygger på profilering. Slutligen har EDPB gjort en vid tolkning av rekvisitet ”rättsliga följder för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne”. Bland annat anses detta kunna omfatta situationer där själva beslutet inte har en ingripande effekt för den enskilde, men där beslutet grundar sig på omfattande eller känslig behandling (till exempel omfattande profilering för att visa internetannonser).

EDPB:s bedömningar har ifrågasatts, men avsändarens auktoritativa tyngd gör naturligtvis att många företag väljer att inta en restriktiv inställning till automatiserade beslut.

Som nämnts ovan är automatiserade beslut både förknippade med fördelar och risker. Det har också konstaterats att det vid sidan av artikel 22 finns andra relevanta bestämmelser i själva dataskyddsförordningen, i annan lagstiftning och i förslaget till AI Act som ger enskilda ett skydd.

Mot denna bakgrund framstår det som alltför restriktivt att i praktiken förbjuda automatiserat beslutsfattande i andra fall än i undantagssituationerna (nödvändigt för fullgörande av avtal med den registrerade, tillåtet enligt unionsrätten eller nationell rätt samt grundar sig på ett uttryckligt samtycke av den registrerade).

Det kan noteras att Europarådets moderniserade dataskyddskonvention (”Konvention 108+”) har en mer tillåtande inställning till automatiserat beslutsfattande, samtidigt som den slår fast att den enskilde har rätt att få sin inställning beaktad när ingripande beslut fattas.[27]

26 Riktlinjer om automatiserat individuellt beslutsfattande och profilering enligt förordning (EU) 2016/679. Antagna den 3 oktober 2017. Senast granskade och antagna den 6 februari 2018

27 “Every individual shall have a right [...] not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration”. “[This paragraph] shall not apply if the decision is authorised by a law to which the controller is subject and which also lays down suitable measures to safeguard the data subject’s rights, freedoms and legitimate interests“ (Article 9).

Lösningsidé: EDPB bör ompröva sin restriktiva tolkning av artikel 22.

Vid en rättslig reform av dataskyddsförordningen bör artikel 22 avskaffas eller åtminstone omformuleras i linje med Europarådets dataskyddskonvention.

De särskilda riskerna förknippade med automatiserat beslutsfattande regleras lämpligare i andra regelverk, till exempel i AI Act och i diskrimineringslagstiftningen.

4 För mycket byråkrati utan tydlig förbättring av integritetsskyddet

4.1 Problembeskrivning

Det är inte tillräckligt för ett företag att respektera de registrerades rätt till skydd för sina personuppgifter och deras individuella rättigheter. Dataskyddsförordningen ställer också omfattande krav på dokumentation, organisation och arbetssätt på dataskyddsområdet. Sådana krav följer inte minst av bestämmelserna om krav på konsekvensbedömning och förhandssamråd, och av tolkningen av den så kallade ansvarsskyldighetsprincipen.

På många sätt är ett proaktivt förhållningssätt nödvändigt för att skapa ett effektivt skydd, men det finns också tydliga risker för en överdriven byråkratisering. Det gäller inte minst i mindre verksamheter eller i verksamheter där riskerna förknippade med hanteringen av personuppgifter i praktiken är begränsade.

Förordningen ger dataskyddsmyndigheterna även kraftiga tillsyns- och sanktionsbefogenheter. Krav på rättssäkerhet gör emellertid att användningen av dessa befogenheter förutsätter omfattande utredning och analys från dataskyddsmyndigheternas sida, något som riskerar att dränera myndigheternas resurser. Ett ökat fokus på klagomålsbaserad tillsyn riskerar att förvärra situationen ytterligare.[28] Som vi framhåller i avsnitt 6 har företagen stora behov av konstruktiv och lösningsinriktad vägledning, något som också kräver stora resurser från tillsynsmyndigheterna.

28 Enligt EU-parlamentets rapport avseende utvärdering av GDPR har 21 av dataskyddsmyndigheterna inom EU/EES meddelat att det saknar tillräckliga personella, tekniska och finansiella resurser, se *European Parliament resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application (2020/2717(RSP)*, p. 15. Det ska noteras att många av myndigheterna fick kraftigt förstärkta resurser i samband med dataskyddsförordningen ikraftträdande.

4.2 Mindre integritetskänsliga behandlingar bör kunna hanteras enklare

Den riskbaserade ansatsen i dataskyddsförordningen (se bland annat artiklarna 24.1 och 32.1) nämns av dataskyddsmyndigheterna så gott som uteslutande för att kräva mer omfattande skyddsåtgärder och mycket sällan för att begränsa den personuppgiftsansvariges skyldigheter i fall där integritetsriskerna är begränsade. Detta förhållande – som vi påtalade i vår tidigare rapport 2019[29] – tycks fortfarande gälla. Integritetsskyddsmyndigheten har exempelvis fortfarande inte upprättat någon förteckning med behandlingar för vilka konsekvensbedömningar inte behöver utföras (se artikel 35.5). Enligt uppgift från myndigheten finns det inte heller några planer på att göra det.[30] En sådan förteckning skulle kunna ge personuppgiftsansvariga vägledning om hur risker ska bedömas och därmed undvika onödigt arbete med konsekvensbedömningar.

Även i andra sammanhang bör det vara möjligt att begränsa skyldigheterna för de personuppgiftsansvariga vid behandling som typiskt sett kan betraktas som mindre integritetskänslig, till exempel kontaktuppgifter till anställda. Det skulle underlätta om det klargjordes under vilka förutsättningar sådana personuppgifter får behandlas, till exempel med stöd av en intresseavvägning. För att undvika bristande harmonisering inom EU bör sådana gruppundantag fastställas av EU-kommissionen i delegerade akter. En jämförelse kan göras med de så kallade adekvansbeslut som kommissionen fattar avseende skyddsnivån i vissa tredjeländer (se även avsnitt 6.2 nedan).

Lösningsidé: Integritetsskyddsmyndigheten bör fatta beslut om en förteckning på behandlingar som inte kräver konsekvensbedömningar (jämför artikel 35.5 i dataskyddsförordningen).

Det kan övervägas om EU-kommissionen bör få mandat att i delegerade akter fastställa under vilka förutsättningar vissa typiskt sett harmlösa behandlingar får utföras.

4.3 Ansvarsskyldighetsprincipen bör anpassas till behandlingens känslighet

Den så kallade ansvarsskyldighetsprincipen i dataskyddsförordningen innebär att den personuppgiftsansvarige måste kunna visa att de övriga dataskyddsrättsliga principerna efterlevs. Principen framgår av artikel 5.2 men utvecklas ytterligare i artikel 24.1. Ansvarighetsprincipen är en viktig del av integritetsskyddet men kan även medföra onödig administrativ börda för de personuppgiftsansvariga, bland annat då den medför en omfattande dokumentationsskyldighet och resurskrävande rutiner – en börda som inte alltid motsvaras av en tydlig förbättring av integritetsskyddet.

29 Se även *Vad är fel med GDPR?* s. 21.

30 Enligt besked från Integritetsskyddsmyndigheten 2022-05-09. Av EDPB:s webbplats framgår att endast tre dataskyddsmyndigheter har antagit sådana förteckningar (Frankrike, Spanien och Tjeckien).

De dataskyddsrättsliga principerna är vagt utformade och det läggs därför en stor börda på de personuppgiftsansvariga att göra en korrekt och välgrundad tolkning. Tolkningar som inte stämmer med dataskyddsmyndigheternas uppfattning om principernas innebörd kan medföra höga sanktionsavgifter. Även om den personuppgiftsansvariges tolkning inte ifrågasätts, kan dataskyddsmyndigheterna utkräva ansvar om de bedömer att den personuppgiftsansvarige inte kan visa att principen faktiskt har beaktats. Detta medför en omfattande utrednings- och dokumentationsskyldighet för de personuppgiftsansvariga. Ansvarsskyldighetsprincipen används också vanligen som stöd för att lägga en tung bevisbörda med höga beviskrav på den som behandlar personuppgifter att visa sin oskuld.

Principen om ansvarsskyldigheten är en viktig utgångspunkt för dataskyddet. Kraven på de personuppgiftsansvariga, som följer av principen, måste dock vara proportionerliga i förhållande till de integritetsrisker som är förknippade med den aktuella personuppgiftsbehandlingen. Den så kallade riskbaserade ansatsen, som för övrigt framgår av artikel 24.1, bör rimligen begränsa vilka krav som ställs på personuppgiftsansvariga i detta hänseende.

Lösningsidé: Det bör tydliggöras i dataskyddsförordningen att utrednings- och dokumentationsskyldigheten bör kunna begränsas vid mindre integritetskänsliga personuppgiftsbehandlingar, bland annat genom ett förtydligande av undantaget för små företag avseende förteckningsskyldigheten i artikel 30.5.

4.4 Begränsa skyldigheten att begära förhandssamråd

En konsekvensbedömning enligt artikel 35 i dataskyddsförordningen är många gånger ett bra verktyg för att bedöma risker förknippade med behandlingar som kan medföra hög risk. Bestämmelsen i artikel 35 ger utrymme för en relativt flexibel tillämpning, även om det kan diskuteras om tröskeln för skyldigheten att göra en sådan konsekvensbedömning är för vag. Idag föreligger en skyldighet att utföra konsekvensbedömningar när en viss behandling ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter”.

Om en genomförd konsekvensbedömning visar att behandlingen skulle leda till sådan hög risk, föreligger en skyldighet för den personuppgiftsansvarige att begära förhandssamråd med dataskyddsmyndigheten om inte de identifierade riskerna har åtgärdats (artikel 36). Begäran om förhandssamråd ska behandlas av dataskyddsmyndigheterna inom vissa tidsramar, men då myndigheterna i regel kräver omfattande dokumentation kan handläggningstiden vara betydligt längre än de 14 veckor som är den längsta tiden enligt bestämmelsen (se artikel 36.2). Det är problematiskt i branscher där digitaliseringen går snabbt. Därtill kräver handläggningen av förhandssamråd omfattande resurser hos dataskyddsmyndigheterna.

Mot den bakgrunden kan det vara lämpligt att skyldigheten att begära förhandssamråd omformuleras till en frivillig möjlighet för de personuppgiftsansvariga som vill ha dataskyddsmyndighetens synpunkter i förväg på en behandling som de har bedömt utgör hög risk.[31] De personuppgiftsansvariga som anser sig ha tillräcklig kompetens att bedöma riskerna kan i sådana fall på egen risk gå vidare med behandlingen utan förhandssamråd. I vart fall bör skyldigheten att begära förhandssamråd kunna begränsas till mer uppenbara fall av höga risker, det vill säga höja tröskeln när förhandssamråd är obligatoriskt.

För att ytterligare öka förutsebarheten i dataskyddsmyndigheternas tillämpning av dataskyddsförordningen kan man överväga att tillåta förhandssamråd även i andra fall än då hög risk föreligger, nämligen då befintlig rättspraxis och vägledning inte ger svar på hur dataskyddsförordningen ska tillämpas (se avsnitt 6.4 nedan).

Lösningsidé: Det bör övervägas om skyldigheten att begära förhandssamråd enligt artikel 36, kan omformuleras till en frivillig möjlighet för att få dataskyddsmyndighetens bedömning av hur risker ska hanteras.

4.5 Begränsa den klagomålsbaserade tillsynen

Integritetsskyddsmyndigheten har fram till nyligen använt inflödet av klagomål primärt för att göra en strategisk och riskbaserad inriktning av tillsynsverksamheten. Därmed har myndigheten kunnat inrikta tillsynsverksamheten mot de områden och företeelser som har bedömts ge störst effekt på integritetsskyddet totalt sett. Dataskyddsmyndigheterna inom EU har haft olika rutiner för hantering av mottagna klagomål från registrerade. Under 2021 antog EDPB interna riktlinjer om att alla klagomål från registrerade ska bedömas – bland annat med beaktande av uttalanden av EU-domstolen i Schrems II – vilket medfört att Integritetsskyddsmyndigheten har beslutat om nya rutiner för klagomålshantering.[32] De nya rutinerna har gjort att en stor del av Integritetsskyddsmyndighetens resurser tas i anspråk för denna verksamhet.[33]

Klagomål till dataskyddsmyndigheterna är självfallet en viktig del av integritetsskyddet enligt dataskyddsförordningen. Riskerna med klagomålsbaserad tillsyn är emellertid

31 Jfr det brittiska förslaget till reformerad dataskyddslagstiftning, Department for Digital, Culture, Media & Sport, Data: A new direction, 10 September 2021, p. 172–173, Consultation outcome; Data: a new direction - government response to consultation och Data protection and Digital Information Bill

32 ”Klagomål i fokus för kommande två års granskningar”, Integritetsskyddsmyndighetens webbplats, https://www.imy.se/nyheter/klagomal-i-fokus-for-kommande-tva-ars-granskningar/. Se Integritetsskyddsmyndighetens budgetunderlag 2023–2025 s. 15 f. angående bakgrund till och konsekvenser av de ändrade rutinerna.

33 Under året 2021 tog klagomålshanteringen 20 procent av myndighetens totala arbetstid, jämfört med 4 procent 2020, dvs. innan den nya ordningen infördes. Trots att Integritetsskyddsmyndighetens nya rutiner ger visst utrymme för en flexibel handläggning räknar myndigheten ändå med att hanteringen av klagomål och klagomålsbaserad tillsyn kommer kräva ytterligare 21 miljoner extra i anslag under åren 2023–24. Integritetsskyddsmyndigheten budgetunderlag 2023–2025, dnr 2022–1847.

att dataskyddsmyndigheterna inte längre kan styra över sin tillsynsverksamhet och därmed tappar möjligheten att prioritera de frågor som innebär de största integritetsriskerna i samhället. Det finns också en risk för att myndigheternas verksamhet i stor utsträckning kommer att styras av de intresseorganisationer på dataskyddsområdet som lämnar ett stort antal klagomål, för att på det sättet driva frågor som de anser viktiga. I de fall dataskyddsmyndigheterna väljer att inte inleda tillsyn kan de registrerades intressen tillgodoses genom en process i allmän domstol, såsom är brukligt på andra rättsområden.

Det tycks visserligen råda en enighet inom dataskyddsmyndigheterna och EU-kommissionen att varje klagomål ska behandlas på ett mer omfattande sätt än vad Integritetsskyddsmyndigheten tidigare har gjort. Inte desto mindre kan det vara lämpligt att se över bestämmelserna i dataskyddsförordningen om hur dataskyddsmyndigheterna ska hantera klagomål, framför allt artikel 57.1 f. Syftet med en sådan justering skulle vara att ge dataskyddsmyndigheterna möjlighet att styra sin verksamhet på ett mer effektivt sätt.

Lösningsidé: Ge dataskyddsmyndigheterna bättre möjligheter att hantera klagomål på ett mer effektivt sätt, antingen genom överenskommelser inom EDPB eller genom justering av bestämmelsen i artikel 57.1 f i dataskyddsförordningen.

5 För ensidigt fokus på dataskydds-intresset

5.1 Problembeskrivning

Syftet med dataskyddsförordningen är att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandling av deras personuppgifter samt att underlätta det fria flödet av sådana uppgifter inom EU. Det framgår av rubriken till förordningen och artikel 1.1.[34] Vidare är rätten till skydd för personuppgifter, som också anges i skälen till dataskyddsförordningen, inte en absolut rättighet; den måste förstås utifrån sin uppgift i samhället och vägas mot andra grundläggande rättigheter i enlighet med proportionalitetsprincipen.[35] Av detta följer att rätten till skydd för personuppgifter måste vägas mot motstående intressen. Enligt EU-stadgan gäller det andras rättigheter och friheter såsom yttrande-, informations- och näringsfrihet, men även ”mål av allmänt samhällsintresse” (se artikel 52 i EU-stadgan).

EU-domstolen och dataskyddsmyndigheterna har hittills tolkat rätten till skydd för personuppgifter enligt EU-stadgan och dataskyddsförordningen mycket extensivt. Rätten till skydd för personuppgifter har fått en ställning som en form av superrättighet. Det finns enligt vår uppfattning anledning att denna ställning i vissa fall bör nyanseras, i vart fall inom den yttre ram som följer av EU-domstolens tolkning av EU-stadgan. En sådan nyansering förutsätter dock troligen ändringar i dataskyddsförordningen.

5.2 Dataskyddsmyndigheterna bör vara skyldiga att balansera sina beslut

Dataskyddsmyndigheternas huvuduppgift är att övervaka tillämpningen av dataskydds-förordningen, i syfte att skydda fysiska personers grundläggande rättigheter och friheter i samband med behandling av sådana uppgifter, samt underlätta det fria flödet av uppgifterna inom unionen (artikel 51.1). Vår erfarenhet är att dataskyddsmyndigheterna

34 I skäl 4 anges att dataskyddsförordningen respekterar alla grundläggande rättigheter och iakttar de friheter och principer som erkänns i stadgan, såsom de fastställts i fördragen, särskilt skydd för bl.a. yttrande- och informationsfrihet och näringsfrihet.

35 Skäl 4.

i de flesta fall låter integritetsintresset övertrumfa andra rättigheter och intressen. Oklarheter i förordningen tolkas därför i regel i en restriktiv riktning, ibland utan närmare motivering av på vilket sätt den aktuella tolkningen medför ett bättre integritetsskydd. Vidare anger dataskyddsmyndigheternas vägledning ofta exempel som utgår från ”best practice” och inte vad som krävs för att behandlingen ska vara laglig. I vsaknad av annan vägledning betraktas vanligen dataskyddsmyndigheternas argument och vägledning som gällande rätt.

Dataskyddsmyndigheternas restriktiva tolkning kan delvis förklaras av EU-domstolens mycket restriktiva praxis på dataskyddsområdet. Att dataskyddsmyndigheterna prioriterar dataskyddet framför andra rättigheter och intressen kan också sägas ligga inprogrammerat i deras roll som dataskyddsmyndigheter för dataskydd. Därtill kommer att samtliga uppgifter som dataskyddsmyndigheterna har att fullgöra enligt artikel 57 i förordningen avser att stärka integritetsskyddet. Det finns ingen uttrycklig skyldighet för dataskyddsmyndigheterna att beakta och motivera hur motstående intressen påverkas av deras beslut och vägledning. De redogör inte för hur skyldigheterna för de som behandlar personuppgifter är proportionerliga i förhållande till den förbättring av integritetsskyddet som besluten eller vägledningen medför samt i förhållande till de konsekvenser som besluten eller vägledningen får för andra intressen.

Vi menar därför att det bör övervägas om en sådan uttrycklig skyldighet för dataskyddsmyndigheterna och EDPB bör införas i dataskyddsförordningen (artikel 57 och 70).

Lösningsidé: Det bör vara en skyldighet för dataskyddsmyndigheterna att beakta motstående intressen till dataskyddet i tillsynsbeslut och i vägledningar så att fördelarna för integritetsskyddet är proportionerliga i förhållande till begränsningar av andra rättigheter, berättigade intressen samt kostnader för samhälle och berörda parter. En sådan skyldighet bör föras in i artiklarna 57 och 70 som avser dataskyddsmyndigheternas uppgifter.

5.3 Det behövs en mer nyanserad inställning till tredjelandsöverföringar och molntjänster

Sedan EU-domstolens avgörande i Schrems II år 2020 och EDPB:s rekommendationer[36] året efter är molnfrågorna och tredjelandsöverföringar ett av de största dataskyddsproblemen som företagen i EU kämpar med. De bedömningar som behöver utföras vid tredjelandsöverföringar kräver omfattande resurser och tar tid att genomföra. Under de senaste åren har tusentals sådana bedömningar genomförts av företag i EU. Det finns således samhällsvinster med att underlätta företagens bedömningar av tredjelandsöverföringar. Redan i vår rapport 2019 nämnde vi osäkerheten kring internationella

36 Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0 Adopted on 18 June 2021.

dataflöden som ett problem. Sedan dess har detta problem förvärrats,[37] till stor del på grund av EDPB:s rekommendationer och avsaknad av tydlig vägledning.

EDPB har i sina rekommendationer intagit en mycket restriktiv inställning till tredjelandsöverföringar och har i princip uteslutit en riskbaserad prövning av vilka överföringar som är tillåtna. Det är förvisso uppenbart att det kan uppstå risker för de registrerade när personuppgifter överförs till ett tredjeland som inte har en adekvat skyddsnivå. Framför allt gäller detta när det handlar om stora mängder uppgifter eller personuppgifter av mer känslig karaktär. EDPB:s rekommendationer har emellertid medfört att även överföringar av relativt sett harmlösa personuppgifter, såsom enstaka uppgifter om anställda i deras tjänsteutövning ska bedömas på samma sätt som överföring omfattande exempelvis ett mycket stort antal känsliga personuppgifter. EDPB:s rekommendationer har legat till grund för efterföljande beslut av dataskyddsmyndigheter. I ett beslut från den österrikiska dataskyddsmyndigheten avfärdas, utan närmare motivering, uttryckligen en riskbaserad prövning.[38]

EDPB:s rekommendationer grundas på EU-domstolens avgörande i Schrems II. I Schrems II ogiltigförklarade EU-domstolen EU-kommissionens så kallade adekvansbeslut om det amerikanska regelverket Privacy Shield. Därutöver konstaterade domstolen att överföringar av personuppgifter till tredjeland med stöd av 2010 års standardavtalsklausuler kan behöva kombineras med kompletterande skyddsåtgärder. Domstolen ansåg att den skyddsnivå som måste uppnås med de kompletterande skyddsåtgärderna för att överföringen ska vara tillåten ska vara väsentligen likvärdig med den skyddsnivå som gäller för personuppgifter inom EU. Domstolen uttalade sig dock inte om hur denna skyddsnivå ska uppnås, det vill säga vilka lämpliga kompletterande skyddsåtgärder som bör införas eller om en riskbaserad bedömning ska göras. Domen ger alltså inte något uttryckligt stöd för den restriktiva tolkning som EDPB har gjort.

Bedömningar av om molntjänster som innefattar tredjelandsöverföringar är tillåtna enligt dataskyddsförordningen förutsätter juridisk, teknisk och affärsmässig expertis. Vi ser att det bör finnas möjligheter att ta fram mer praktiska rekommendationer för näringslivet om dataskyddsmyndigheterna och EDPB i större utsträckning samarbetar med praktiskt verksamma dataskyddsexperter, berörda företag och myndigheter samt molntjänstleverantörer. Öppna lösningsinriktade diskussioner ger troligen bättre vägledning än den formella remissrundan som föregick EDPB:s rekommendationer. Det ger också möjligheter för dataskyddsmyndigheterna att förstå hur olika molntjänster fungerar och hur olika skyddsåtgärder verkar. De pågående tillsynsärendena ger inte möjlighet till lösningsbaserad dialog och ger troligen inte heller någon handfast vägledning förrän efter flera års processande.

37 Exempelvis har ny diabetesteknik stoppats då den bygger på användning av amerikanska molntjänster, se https://sverigesradio.se/artikel/ny-diabetesteknik-nar-inte-ut-till-patienterna-det-ar-en-frustration.

38 Preliminärt beslut av Österreichische Datenschutzbehörde, se redogörelse för och engelsk översättning av beslutet https://noyb.eu/en/update-noybs-101-complaints-austrian-dpa-rejects-risk-based-approach-data-transfers-third-countries.

Lösningsidé: EDPB bör uppdatera och ompröva sina rekommendationer efter en öppen och lösningsinriktad dialog med berörda parter, i syfte att ta fram lösningsalternativ och bättre vägledning.begränsningar av andra rättigheter, berättigade intressen samt kostnader för samhälle och berörda parter. En sådan skyldighet bör föras in i artiklarna 57 och 70 som avser dataskyddsmyndigheternas uppgifter.

5.4 EDPB bör bidra med bedömningar av skyddsnivåer i tredjeländer

Ett nytt så kallat adekvansbeslut av EU-kommissionen avseende överföringar till USA kan antagligen lösa många av de nuvarande problemen. Det kan dock dröja innan ett sådant beslut är på plats. Till dess bör EDPB och dataskyddsmyndigheter vidta andra åtgärder för att underlätta och effektivisera företagens bedömningar.

I bedömningen av tredjelandsöverföringar, såsom vid användning av amerikanska molntjänster, ingår att bedöma skyddsnivån i de aktuella tredjeländerna. Det är en uppgift som i princip är övermäktig även för större organisationer och som vanligtvis kräver utlåtanden från juridiska och tekniska experter med särskild kunskap om dessa tredjeländer. Få företag har resurser och tid att inhämta sådana utlåtanden. EDPB och dataskyddsmyndigheter som har kontakter med sina motsvarigheter i länder utanför EU bör ha betydligt bättre förutsättningar att ta fram och publicera sådana bedömningar, så att företag och myndigheter kan dra nytta av dem.

Lösningsidé: EDPB bör bistå med bedömningar av skyddsnivån i tredjeländer, om möjligt i samarbete med myndigheter i de berörda tredjeländerna.

5.5 Det behövs mer flexibilitet för att behandla känsliga personuppgifter och uppgifter om lagöverträdelser

Utrymmet för att få behandla känsliga personuppgifter enligt artikel 9 i dataskyddsförordningen är begränsat eftersom denna typ av behandling typiskt sett innebär högre integritetsrisker. De undantag från förbudet som anges i artikel 9.2 är relativt begränsade och medger ingen eller liten flexibilitet i tillämpningen. Endast i ett fall finns det utrymme för en intresseavvägning, och då med stöd i medlemsstaternas nationella rätt (viktigt allmänt intresse, artikel 9.2 g). Därutöver saknas stöd för att behandla känsliga personuppgifter för att fullgöra ett avtal med den registrerade eller för att fullgöra en rättslig förpliktelse (jämför rättsliga grunder enligt artikel 6). I kombination med en mycket

vid definition av känsliga personuppgifter – vilken har givits en vid tolkning av EU-domstolen[39] – medför det många gånger omotiverade begränsningar i behandlingen av personuppgifter, särskilt för den privata sektorn.

Till saken hör också att dataskyddsförordningen tillåter medlemsstaterna att i nationell rätt komplettera undantagen från förbudet att behandla känsliga personuppgifter, vilket medfört bristande harmonisering inom EU. Den svenska regleringen i denna del framstår som mer restriktiv än många andra medlemsstaters reglering. Det finns därför ett stort behov av en översyn av den svenska kompletterande lagstiftningen.[40]

Utrymmet för nationell reglering är större när det gäller uppgifter om lagöverträdelser enligt artikel 10 i dataskyddsförordningen, vilket på samma sätt har medfört bristande harmonisering inom EU. För företag som verkar i flera EU-länder innebär det problem. Det kan därför finnas anledning att se över bestämmelsen i artikel 10 och ange i vilka fall uppgifter om lagöverträdelser får behandlas inom den privata sektorn.

Lösningsidé: Det bör övervägas om ett nytt undantag från förbudet att behandla känsliga personuppgifter i artikel 9 i dataskyddsförordningen bör införas, vilket tillåter en kvalificerad intresseavvägning i det enskilda fallet vid tungt vägande motstående intressen eller där skyddsbehovet är begränsat.

Vidare bör det övervägas om bestämmelsen i artikel 10 – som gäller behandling av uppgifter om lagöverträdelser – bör konkretiseras i dataskyddsförordningen, i vart fall när det gäller behandling inom den privata sektorn.

Den svenska regeringen bör ta initiativ till en översyn av det rättsliga stödet för att behandla känsliga personuppgifter och uppgifter om lagöverträdelser.

Integritetsskyddsmyndigheten bör – i avvaktan på förtydligande av dataskyddsförordningen eller svenska kompletterande regler – utnyttja sin befintliga föreskriftsrätt för att tydliggöra möjligheterna att behandla uppgifter om lagöverträdelser, särskilt vad gäller kontroller mot spärr- och sanktionslistor.

39 Se EU-domstolens dom den 1 augusti 2022 i mål C-184/20 ”Vyriausioji tarnybinės etikos komisija”

40 Detta problem påtalade vi även i vår tidigare rapport, se *Vad är fel med GDPR?* s. 22.

6 Bristande förutsebarhet och harmonisering

6.1 Problembeskrivning

Dataskyddsförordningen innehåller som bekant många vaga och oklara principbestämmelser, vilket i stor utsträckning är oundvikligt med hänsyn till förordningens breda tillämpningsområde och att digitaliseringen av samhället medför behov av ett dynamiskt regelverk. Detta leder dock till bristande förutsebarhet. En detaljerad bestämmelse som tydligt anger hur den som behandlar personuppgifter ska agera kan visserligen ge bättre förutsebarhet i de situationer som tydligt täcks av bestämmelsen, men riskerar samtidigt att leda till gränsdragningsfrågor och hinder i andra situationer.

Bristande förutsebarhet innebär inte bara en utmaning och börda för de personuppgiftsansvariga, utan även för dataskyddsmyndigheterna. Osäkerhet i tillämpningen medför ökat behov av vägledning till de personuppgiftsansvariga, ökat ärendeinflöde samt fler klagomål och överklaganden. Ökad förutsebarhet och öppenhet kan således minska bördan för både de personuppgiftsansvariga och dataskyddsmyndigheterna.

6.2 Konkretisera bestämmelserna genom delegerade akter av EU-kommissionen

Ett sätt att skapa mer förutsebarhet kan vara att öppna möjligheten att i föreskrifter konkretisera reglerna, genom att exempelvis ange att under vissa förutsättningar kan intresseavvägning användas för en specifik behandling.

Föreskrifter på nationell nivå kan samtidigt medföra bristande harmonisering på EU-nivå, vilket redan är ett välkänt problem för näringslivet inom EU. Det kan därför övervägas om EU-kommissionen ska ges ökade möjligheter att utfärda föreskrifter för att konkretisera tillämpningen av dataskyddsförordningen, till exempel under vilka förutsättningar som en viss behandling får utföras med stöd av en intresseavvägning. En jämförelse kan göras med de så kallade adekvansbeslut som kommissionen fattar avseende skyddsnivån i vissa tredjeländer (se även avsnitt 4.2 ovan).

Lösningsidé: Ge EU-kommissionen rätt att utfärda delegerade akter som kompletterar och konkretiserar bestämmelser i dataskyddsförordningen, till exempel för viss behandling som kan stödjas på en intresseavvägning.

6.3 Det krävs mer praktiskt inriktad vägledning

Dataskyddsmyndigheterna har under de gångna åren producerat omfattande vägledning. EDPB:s vägledning har täckt in många komplicerade frågor och innehåller också många användbara exempel. Det är även välkommet att Integritetsskyddsmyndigheten publicerat tre så kallade rättsliga ställningstaganden i frågor för vilka det saknas vägledande domstolspraxis eller vägledning från EDPB.[41] Därutöver har Integritetsskyddsmyndigheten förbättrat sin webbplats och publicerat flera rapporter.

Vägledning i tillämpningen av dataskyddsförordningen behövs för rättslig tolkning av tillämpliga dataskyddsrättsliga regleringar, det vill säga rena rättsutredningar såsom Integritetsskyddsmyndighetens rättsliga ställningstaganden. Men vägledning behövs även när det gäller den praktiska tillämpningen i olika typsituationer, som konkreta exempel på vilka åtgärder de personuppgiftsansvariga ska vidta såsom mallar för dokumentation och information till de registrerade.

Våra erfarenheter är att det för närvarande är behovet av mer praktiskt inriktad vägledning med exempel och mallar som är störst. Det vore även önskvärt att vägledningen från dataskyddsmyndigheterna ger en mer balanserad tolkning av dataskyddsförordningen än den relativt restriktiva tolkning som dataskyddsmyndigheterna vanligtvis ger uttryck för (jämför behovet av mer balanserade bedömningar av dataskyddsmyndigheterna i avsnitt 5.2 ovan).[42]

Från ett samhällsperspektiv är det också mer effektivt att låta dataskyddsmyndigheterna ta fram tydliga vägledningar, än att många ska uppfinna hjulet på nytt och därmed riskera att göra en felaktig tolkning eller införa ett bristande dataskydd. I detta sammanhang bör den brittiska dataskyddsmyndighetens arbete med vägledning i många avseenden fungera som förebild.

Lösningsidé: Dataskyddsmyndigheterna bör prioritera arbetet med praktiskt inriktad vägledning, exempelvis genom att göra vägledningar från EDPB mer lättillgängliga.

41 Jfr vårt förslag till sådana ställningstaganden och våra synpunkter på tydlig vägledning i *Vad är fel med GDPR?* s. 28-30.

42 Danska datatilsynets publikation ”Guidance on the use of cloud March 2022” bör dock nämnas som ett relativt bra exempel på vägledning.

6.4 Det behövs förhandssamråd i oklara rättsfrågor

För att öka förutsebarheten i dataskyddsmyndigheternas tillämpning av dataskyddsförordningen kan man överväga att ge personuppgiftsansvariga en frivillig möjlighet att begära förhandssamråd i situationer där befintlig rättspraxis och vägledning inte ger ett tydligt svar på hur dataskyddsförordningen ska tillämpas på en viss behandling (jämför även avsnitt 4.4 ovan). Det kan också övervägas om det i dataskyddsförordningen bör ställas krav på hur dataskyddsmyndigheternas svar, det vill säga samrådet, ska utformas och vad dessa ska innehålla – till exempel klara och tydliga handlingsdirigerande råd.

Ett mer långtgående alternativ är att komplettera förhandssamråd med bindande förhandsbesked, vilka kan överklagas på samma sätt som tillsynsbeslut av dataskyddsmyndigheterna. Förhandsbesked i skattefrågor är vanligt förekommande i flera EU-länder; jämför lagen (1998:189) om förhandsbesked i skattefrågor.[43] En sådan möjlighet bör naturligtvis vägas mot de resurser som kan krävas av dataskyddsmyndigheterna. Det bör därför finnas möjlighet för dataskyddsmyndigheterna att prioritera vilka begäranden som ska behandlas.

Lösningsidé: Det bör övervägas om det ska finnas en frivillig möjlighet för de personuppgiftsansvariga att begära förhandssamråd när rättsläget är oklart (jämför artikel 36). Det kan även övervägas om de personuppgiftsansvariga ska kunna begära bindande förhandsbesked.

6.5 EU-kommissionen bör få en tydligare uppgift att bidra till uppförandekoder

Medlemsstaterna, dataskyddsmyndigheterna, EDPB och EU-kommissionen har en skyldighet enligt artikel 40 i dataskyddsförordningen att ”uppmuntra utarbetandet av uppförandekoder avsedda att bidra till att denna förordning genomförs korrekt”. Det är oklart i vilken omfattning sådan uppmuntran har getts och i vilken form. Enligt vår erfarenhet är det mycket komplicerat för en branschorganisation eller liknande att ta fram en uppförandekod för godkännande av en dataskyddsmyndighet. Det är dessutom förenat med stora kostnader och åtaganden. Endast ett fåtal större branschorganisationer har fått sina uppförandekoder godkända.[44]

Uppförandekoder kan vara ett mycket lämpligt verktyg för att konkretisera de relativt vaga bestämmelserna i dataskyddsförordningen ”med hänsyn till särdragen hos de olika

43 Enligt 16 § i lagen är ett förhandsbesked som vunnit laga kraft är bindande för Skatteverket och allmän förvaltningsdomstol i förhållande till den enskilde som beskedet angår, om denne yrkar det. Förhandsbeskedet är dock inte bindande om en författningsändring påverkar den fråga som beskedet avser.

44 Se EDPB:s register https://edpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_sv

sektorer där behandling sker, och de särskilda behoven hos mikroföretag samt små och medelstora företag" (artikel 40.1). Vid införandet av dataskyddsförordningen ansågs uppförandekoder som ett viktigt verktyg för att tydliggöra och förenkla tillämpningen av förordningen.

Mot denna bakgrund kan det vara lämpligt att utreda ytterligare åtgärder för att snabbare få fram nya uppförandekoder. Ett sådant exempel kan vara att EU-kommissionen får ett mer omfattande ansvar för att – i samarbete med branschföreträdare – ta initiativ till, organisera och administrera arbetet med uppförandekoder. En sådan uppgift för EU-kommissionen utesluter inte att liknande initiativ tas på nationell nivå. I vår rapport från 2019 föreslog vi att 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.

Lösningsidé: EU-kommissionen bör få ett mer omfattande ansvar för att ta initiativ till, organisera och administrera arbetet med uppförandekoder.

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

Tryck: Arkitektkopia AB, Bromma, 2022