Skapa inbyggt dataskydd genom bra konsekvensbedömningar

Monika Wendleby

Stämningen i rummet var spänd och det kändes som att man redan när mötet inleddes hade kommit till vägs ände. På ena sidan bordet satt den frustrerade chefen som upplevde sig hindrad att genomföra det uppdrag han fått av generaldirektören för att sköta en verksamhet som reglerades i en lagstiftning. Han hade ansvar för ett utvecklingsprojekt som arbetat hårt under ett år – och precis när projektgruppen värkt fram en lösning alla verkat kunna leva med blev det stopp på grund av dataskyddsreglerna. I ett hörn satt ett lika frustrerat dataskyddsombud, som efter att först i beslutsskedet fått se projektets förslag, lyft frågan om brister rörande konsekvensbedömning med styrelsen. Detta ledde till att chefen hade beordrats ta ett omtag i projektet, vilket chefen tyckte kändes formalistiskt i överkant. Även ett antal frustrerade medarbetare satt runt bordet, både sådana som arbetade med dataskydd och andra som ansvarade för olika sakfrågor. Ingen i rummet förmådde att helt släppa en känsla av att en oförrätt var begången, alla ansåg sig bara göra sitt jobb så gott de kunde och tyckte lite till mans att andra inte såg de perspektiv man själv såg så tydligt. Syftet med mötet var att dra i gång en konsekvensbedömning men diskussionerna tenderade mest att handla om vem som sagt vad. Gruppen hade svårt att se framåt och samarbeta. När mötet avslutades konstaterade chefen med en trött röst att gruppen nu behövde påbörja ett konkret arbete att genomföra konsekvensbedömningen enligt styrelsens uttryckliga beslut. Han tillade att han förväntade sig att arbetet skulle gå fort, vilket fick dataskyddsombudet att se stressad ut. Ingen, inte ens han själv, trodde på budskapet om en snabb och effektiv konsekvensbedömning.

Scenariot runt bordet är påhittat, men bygger på många berättelser av liknande händelser. Det finns idag inte sällan en upplevd känsla av frustration över konsekvensbedömningar, som anses ta resurser och stoppa utvecklingen av verksamheten. Inte sällan uppstår konflikter eller åtminstone tjafs, vilket varken bidrar till utveckling eller bättre inbyggt dataskydd. Detta har fått mig att fundera. Vad är egentligen problemet,

rotorsaken, som gör att arbetet ofta går trögt? Finns det inbyggda otydligheter i systemet som skapar problemen?

Med EU:s dataskyddsförordning (GDPR) kom en intressant ny reglering genom artiklarna 35 och 36 GDPR som handlar om konsekvensbedömning och samråd. Regleringen har en mycket positiv grundtanke, nämligen att personuppgiftsansvariga tidigt ska tänka igenom sina behandlingar för att landa rätt när det gäller integritetsfrågorna. Rätt tillämpat är konsekvensbedömning ett utmärkt redskap för att uppnå ett bra inbyggt dataskydd (se artikel 25 GDPR).

Ändå upplevs konsekvensbedömningar inte sällan som omständliga. Eftersom verktyget konsekvensbedömning i många fall inte nått önskat resultat är det rimligt att analysera frågan utifrån ett systemsynsperspektiv: finns det systemfaktorer som gör hanteringen mer betungande än den behöver vara eller till och med innebär att arbetet riskerar bli kontraproduktivt? I samband med att jag har gjort den analysen har jag identifierat fyra paradoxer kopplade till hanteringen. Innan jag går in på dem kommer jag dock först gå igenom vad systemsyn är och även hur väl principen om inbyggt dataskydd passar in i ett systemsynsperspektiv.

Vad är systemsyn?

> *Each system is perfectly designed to give you exactly what you are getting today.*
>
> W. Edwards Deming

Jag har länge varit intresserad av att försöka förstå mekanismer bakom vad som fungerar bra i en verksamhet och vad som inte gör det. Det var därför naturligt att i boken Lean med hjärta och kreativitet : Om autentiskt ledarskap och kommunikation[1] utgå från systemsyn, som ingår i ett intressant och modernt paradigm inom managementforskningen. I detta paradigm ingår även managementteorier som lean och agila arbetssätt, vilka mer och mer tillämpas av verksamheter för att uppnå högre kvalitet, effektivitet och delaktighet.

Systemsyn beskrivs så här i boken:

> När vi beskriver systemsynsätt utgår vi… från W. Edward Demings definition av system: *ett nätverk av oberoende delar som arbetar tillsammans för att uppnå syftet med systemet.*
>
> Systemsyn innebär att man ser verksamheten som en helhet – ett system – där alla delar är inbördes beroende av varandra. Systemet är större

[1] Ekerlids förlag, 2013. Jag skrev boken tillsammans med Isabel Runebjörk.

> än summan av delarna, och det är en produkt av hur alla delar samspelar med varandra. För att kunna samspela bra behöver alla som arbetar i delar av systemet förstå syftet med hela systemet. Detta i sin tur innebär att chefer måste kunna förklara systemets syfte för sina medarbetare…

Systemsyn kan även översättas med att se hela bilden, ha helhetssyn eller arbeta holistiskt. I ett systemsynsätt är den berörde människan i fokus. Det intressanta är hur väl delarna i systemet samverkar för att tillföra den som berörs ett över tid ökat värde. Motsatsvis är arbete som inte tillför värde för berörda människan att se som slöserier. Översatt till GDPR-språk handlar det förstås om att se den registrerade, hur hens friheter och rättigheter fortlöpande stärks.

Människan i centrum

I systemsyn är det även viktigt att förstå och värna om medarbetarna och ta till vara deras vilja att bidra. Det handlar om att ständigt förbättra, vilket organisationer gör bäst om allas insatser är inriktade på värdeskapande. Samtidigt handlar det om att fortsätta att lära sig mer om vad som skapar värde, vilket bland annat kan göras genom att utveckla förmågan att analysera.

Översatt till arbetet med dataskydd och konsekvensbedömningar behöver de som arbetar med sådana förstå vad konsekvensbedömningar är och vad de förväntas åstadkomma. Alla behöver förstå värdet av att på ett tidigt stadium bedöma det man vill utveckla utifrån den berördes (den registrerades) synvinkel. Detta är viktigt för att sedan kunna väga positiva och negativa konsekvenser för hen med det som tillför nytta för organisationen och andra (kallas proportionalitetsbedömning i konsekvensbedömningssammanhang). En viktig aspekt att förstå är att en människa inte bara existerar i rollen ”registrerad”, det i sig är ett konstruerat begrepp för att definiera den berörde på ett juridiskt sätt.[2] För människor är förstås många saker viktiga (olika för olika personer), där integritet bara är en aspekt bland många. Om man inte tydligt väger in andra mänskliga rättigheter och friheter[3] i de juridiska bedömningarna blir det alltså fel. Detta är också ett krav enligt förordningstexten (se artikel 35.1 GDPR).

[2] I andra språkversioner av GDPR har man använt ord som bättre speglar detta, att det finns en människa som berörs.

[3] Se Europeiska unionens stadga om de grundläggande rättigheterna som reglerar vilka grundläggande friheter och rättigheter som EU upprätthåller. Artikel 7 beskriver respekt för privatliv och familjeliv och artikel 8 skyddet för personuppgifter.

Arbeta framtungt!

I ett systemsynsperspektiv är det även viktigt att tidigt undanröja felaktigheter eller oklarheter eftersom sådana senare skapar onödigt arbete (slöserier med tid och andra resurser). Det är alltså viktigt att arbeta framtungt – ju tidigare, desto bättre.

Konsekvensbedömningar är tänkta att genomföras innan behandlingen påbörjas. Syftet är att skapa förutsättningar för ett bra inbyggt dataskydd. Om alla organisationer arbetar med konsekvensbedömningar framtungt och tidigt bör samhället över tid få en högre och högre nivå av respekt för den personliga integriteten.

Av samma skäl är det förstås även bra att så tidigt som möjligt involvera dataskyddsombudet, eftersom hen ska delta i bedömningen (se artikel 35.2 GDPR). Jag möter ganska ofta dataskyddsombud som är frustrerade över att de får komma in först när allt utvecklingsarbete är i princip klart. Risken för organisationen är att dataskyddsombudet ser avvikelser som måste hanteras. Detta skapar ofta onödiga konflikter som inte tillför något värde.

Ständigt lärande

För att vara framgångsrik och effektiv är det viktigt att analysera och lära sig. En lärande organisation är en viktig komponent i systemsyn. Ett verktyg som konsekvensbedömning ger rätt tillämpat god möjlighet till analyser och reflektion, vilket är positivt.

Förstå helheten

Systemet börjar och slutar inte i den personuppgiftsansvariges organisation utan arbetet beror i högsta grad på faktorer som ligger utanför dennes kontroll. Om arbetet inte fungerar effektivt kanske problemet uppstått utanför den egna organisationen. Även om man inte alltid kan avhjälpa sådana avvikelser kan det underlätta att se var problemet uppstått.

För att förstå helheten i dataskyddsarbetet behöver man självklart även titta på hur lagstiftaren och tillsynsmyndigheterna agerar i systemet.

Varje oklarhet som skapas i en lagstiftning kommer ovillkorligen att leda till slöserier i tillämpningsstadiet (jag återkommer till detta när jag beskriver den första paradoxen jag sett).

Vidare kan tillsynsmyndigheter skapa otydlighet till exempel genom att inte tidigt tydliggöra sin syn på frågor. Utifrån ett systemsynsätt är det därför utmärkt att Europeiska dataskyddsstyrelsen (EDPB) ger

ut riktlinjer och att Integritetsskyddsmyndigheten (IMY) arbetar med rättsliga ställningstaganden. Det finns dock en risk i att både EDPB och nationella tillsynsmyndigheter i sin rättsliga styrning även ger förslag på metoder som inte bottnar i ett systemsynsätt.

Trots goda ansatser finns det en förbättringspotential för myndigheter att tydligt se sin roll i systemet. Det är därför intressant att Ekonomistyrningsverket (ESV) starkt förordar systemsyn[4], vilket borde leda till att fler blir intresserade av att tillämpa detta. Detta vore en spännande utveckling nu när dataskyddet firar 50 år i Sverige och GDPR firat sin 5-årsdag!

Enligt W. Edward Deming är det vi får ut av systemet en produkt av hur vi skapat det. Jag tror därför att det finns mycket att vinna på att titta på varför ett system inte fungerar optimalt och vad vi alla kan göra för att förbättra det.

Inbyggt dataskydd en agil tanke

> *It is not enough for everyone to do his best. Everyone is already doing his best. Efforts, to be effective, must go in the right direction.*
>
> W. Edwards Deming

Innan jag fördjupar mig i beskrivningen i av de paradoxer jag sett vill jag först kort beskriva hur väl principen om inbyggt dataskydd passar in i ett systemsynsperspektiv.

Sambandet mellan inbyggt dataskydd och konsekvensbedömning

I artikel 25.1 GDPR klargörs att en personuppgiftsansvarig – med ”beaktande av den senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål” – ska genomföra ”lämpliga tekniska och organisatoriska åtgärder”. Artikeltexten slår således fast att den personuppgiftsansvarige måste ha helhetssyn när organisationen arbetar med personuppgiftsbehandling. Vidare måste den fortlöpande utvecklingen beaktas, vilket innebär att ingen kan anse sig klar med arbetet. Finns det något att förbättra kan det behöva göras om de andra rekvisiten är för handen. Detta ska göras både vid fastställandet av vilka medel behandlingen utförs med och vid själva behandlingen.

[4] Hur gör andra? – ESV forum.

Till det anges i artikel 25.1 GDPR att den personuppgiftsansvarige även behöver beakta ”riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter”, det vill säga hur den berörde personen (den registrerade) påverkas. Även här ska en helhetssyn ingå, då alla rättigheter och friheter omfattas och alltså inte enbart den berördes rätt till sina personuppgifter och integritet. Konsekvensbedömningen kan på så sätt ses som ett verktyg för att uppnå ett gott inbyggt dataskydd, då personuppgiftsansvariga enligt artikel 35.1 GPPR inför en behandling som kan leda till en ”hög risk för fysiska personers rättigheter och friheter” behöver göra en helhetsbedömning genom att bedöma proportionaliteten i behandlingen där ”den planerade behandlingens konsekvenser för skyddet av personuppgifter” ska värderas. Liksom i det inbyggda dataskyddet är den registrerades alla rättigheter och friheter i centrum för bedömningen.

Inbyggt dataskydd i ett agilt arbetssätt

Idag arbetar man ofta med dataskyddsfrågor i separata stuprör i förhållande till utvecklingsarbetet. Detta riskerar att leda till två parallella förfaranden som skapar mycket irritation. Utvecklingssidan jobbar med sina frågor utifrån de behov organisationen har formulerat medan dataskyddet fokuserar på regelefterlevnad. Var och en arbetar utifrån egna metoder. En helhetssyn på hur respektive arbete påverkar berörda människor saknas. I slutändan skapas inte värde utan slöserier.

De legala krav som uppställs i artikel 25 GDPR passar bra in i agil verksamhetsutveckling. I en sådan är det viktigt att förbättra och omvärdera fortlöpande utifrån vilka effekter det får för dem man arbetar för. Det är självklart att ett bra inbyggt dataskydd förutsätter att medarbetare vill och förstår GDPR så de kan bidra med sin kunskap och kreativitet i förbättringsarbetet.

När man arbetar agilt med utveckling är det viktigt att få med det inbyggda dataskyddet i alla sprintar. Föreligger det ett krav på konsekvensbedömning är det därför viktigt att i varje sprint värdera resultatet (och de slutsatser man drar för arbetet med nästa sprint) tillsammans med att konsekvensbedömningen fylls på. Ändrar man viktiga antaganden inför nästa sprint kan nämligen nya dataskyddsfrågor uppstå. När vi jobbar med konsekvensbedömning i en agil verksamhetsutveckling gör vi därför inte bara ”User Stories”[5], ett vanligt sätt att fortlöpande

[5] En ”user story” är en informell, generell förklaring av de effekter ett IT-stöd förväntas ge skrivet utifrån slutanvändarens perspektiv för att pröva att värde tillförs ur ett kundperspektiv.

pröva nyttan för användare, utan även ”Data Subject Stories”[6] för att få en bättre förståelse för hur den registrerade ser på både nyttor och integritetsrisker i förhållande till alla mänskliga rättigheter och friheter. Värdet med metoder som ”User Stories” och ”Data Subject Stories” är att man behåller fokus på den berörde människans situation. Samtidigt kan metoderna öka både samarbete och kreativitet.

I det dagliga arbetet i organisationer finns några paradoxer som jag återkommer till nedan. Dessa är viktiga att fundera över om de arbetssätt man tillämpar inte fungerar optimalt. Eftersom jag förordar ett helhetsperspektiv på problem rörande konsekvensbedömning börjar jag dock där regelverk skapas och den paradox som finns i lagstiftningsarbetet.

Den första konsekvensbedömningsparadoxen: Bristande nationell lagstiftning

A system must create something of value, in other words, results.
W. Edwards Deming

Konsekvensbedömning i lagstiftning

Idag ingår konsekvensbedömningar (i den form de ska ha enligt artikel 35 GDPR) inte naturligt som metod i den svenska lagstiftningsprocessen. Detta är ett problem utifrån ett systemsynsperspektiv, eftersom genomförda konsekvensbedömningar redan på lagstiftningsstadiet skulle minska behovet av att andra aktörer behöver genomföra dem senare. Av artikel 35.10 GDPR följer nämligen att om en behandling enligt artikel 6.1 c eller e GPPR har en rättslig grund i en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av och den rättsliga grunden reglerar en behandling som den personuppgiftsansvarige vill utföra behöver punkterna 1–7 i artikel 35 GPDR inte hanteras. Detta förutsätter dock enligt artikeltexten att en konsekvensbedömning redan har genomförts som en del av en allmän konsekvensbedömning i samband med antagandet av den rättsliga grunden.

Motsvarande gäller för övrigt även EU-rättsakter där man ofta ser sådana texter. För närvarande har EU-domstolen i mål C-61/22[7] att

[6] En metod som utvecklats av mig och mina kollegor Kerstin Hermanson och Sanna Dahlberg på Passacon AB. Den handlar om att ta fram enkätfrågor där de registrerade i en konsekvensbedömning får värdera nyttor och risker. Detta underlag används sedan i den riskbedömning som ingår i konsekvensbedömningen.
[7] RL mot Landeshauptstadt Wiesbaden.

pröva vilken verkan det kan få om unionslagstiftaren, när den antar en sekundärrättsakt, inte har genomfört en konsekvensbedömning. I ett förslag till avgörande av generaladvokat Laila Medina[8] anges att frågan om skyldighet för lagstiftaren måste bedömas utifrån artikel 35.1 GDPR. Enligt Laila Medina framgår det ingenstans i GDPR att unionslagstiftaren är skyldig att genomföra en konsekvensbedömning och inte heller ”fastställs det i denna bestämmelse något kriterium mot bakgrund av vilket till exempel giltigheten av en annan av unionens sekundärrättsakter ska bedömas”.

Om Laila Medinas tolkning står sig finns det således ingen skyldighet för lagstiftaren att genomföra en konsekvensbedömning. Detta kan säkert åtminstone initialt ses som en lättnad för Regeringskansliet. Att behöva göra konsekvensbedömningar enligt konstens alla regler lär upplevas som betungande av redan arbetstyngda departement.

Genom att underlåta att göra en ordentlig konsekvensbedömning vältras ansvaret dock över till de som ska tillämpa lagstiftningen i de fall kriterierna för att genomföra en konsekvensbedömning är för handen för genomförarna. Detta innebär betydande förluster både avseende effektivitet och rättssäkerhet. Regeringskansliet har mycket större möjligheter att genomföra bra utredningar än de flesta personuppgiftsansvariga har. Dessutom har man en möjlighet att ge myndigheter uppdrag att bistå. Om ordentliga konsekvensbedömningar gjordes redan under SOU-stadiet skulle det vara lättare för myndigheter, inte minst IMY, att kommentera resultatet i en remissomgång vilket skulle fördjupa analyserna. Vidare skulle man ofta få en automatisk granskning av Lagrådet, vilket skulle höja kvaliteten.

Det görs alltså inte konsekvensbedömningar framtungt redan när lagändringar utreds. Idag ser man i stället motsatta systemfaktorer. Ofta ska lagstiftningar tas fram skyndsamt vilket i sig är en både kritisk och negativ systemfaktor, eftersom den gör analyserna grundare. Analyserna av integritetsfrågor bygger ibland mer på tyckande och de krav som GDPR uppställer på lagstiftningsprocessen i sig (till exempel att uppgiftsminimera och införa skyddsåtgärder[9]) får ofta grunda genomgångar. Till det kommer att svenska förarbeten från äldre tids lagar ofta svepande beskriver mycket vidsträckta möjligheter att använda personuppgifter som illa överensstämmer med de krav som numera ställs i artiklar som 23 och 89 GDPR.

[8] **F**öredrogs den 29 juni 2023.

[9] Se artiklar som 6, 9, 10, 23 och 89 GDPR som alla ställer långtgående krav.

Hur det kan se ut

Ett talande exempel från 2023 är en komplettering av patientdatalagen (PDL) som behövt göras för att tydliggöra att personuppgiftsansvariga ska kunna vidarebehandla personuppgifter för antalsberäkningar vid klinisk forskning.

Det första slöseriet är att man försöker ”lagstifta genom förarbeten”, det vill säga rätta till otydligheter i efterhand i redan gällande lagar genom att skriva förarbetsuttalanden. I propositionen understryker regeringen många gånger att lagstiftningsändringen inte behövs, eftersom man gör den i förtydligande syfte.[10] Samtidigt införs inte några övergångsbestämmelser eftersom regeringen därmed heller inte anser sig ha ”tagit ställning för att antalsberäkning skulle vara otillåten under tiden fram till dess att lagen träder i kraft”.[11] Den här typen av hantering kommer ovillkorligen att skapa förvirring hos tillämparna. Detta särskilt eftersom PDL endast får komplettera GDPR.

Skyddsåtgärder måste till i lagstiftning som handlar om behandling av känsliga personuppgifter. En ny bestämmelse om skyddsåtgärder införs i det aktuella lagstiftningsärendet genom 5 kap. 7 § PDL. För att kunna skapa relevanta skyddsåtgärder behöver man först göra en proportionalitetsbedömning (se till exempel artikel 9.2 g och j GDPR). I detta finns det andra slöseriet.

Regeringen konstaterar nämligen att det i utredningens proportionalitetsbedömning saknas en analys av vad utredningens påpekande om risker för de registrerade (integritet, autonomi, människovärde och rättvisa) konkret innebär och därför även vilka konkreta risker för den personliga integriteten som personuppgiftsbehandling vid antalsberäkning innebär.[12] Detta är sannolikt bakgrunden till att IMY anser att förslaget ”inte innehåller de analyser som krävs för att kunna ta ställning till om lagförslaget uppfyller kraven i EU:s dataskyddsförordning” och därför inte kan tillstyrka det.

Vi kan alltså utifrån en systemsynsanalys konstatera två slöserier, vilka får effekter för tillämparna. När lagändringen i PDL tillämpas krävs konsekvensbedömning sannolikt ofta enligt artikel 35.1 GDPR eftersom behandlingen rör känsliga personuppgifter (patientdata) för en utsatt grupp registrerade (patienter). En statlig utredning, har dessutom konstaterat att det finns risker (som låter mycket allvarliga för de registrerade) utan att närmare förklara vad riskerna består av. Hos de personuppgiftsansvariga som ska tillämpa lagstiftningen för ny forskning lär det därför uppstå intrikata frågor när konsekvensbedömningar genom-

[10] Prop. 2022/23:31 s. 25 ff. och 56.
[11] Prop. 2022/23:31 s. 53.
[12] Prop. 2022/23:31 s. 52.

förs. Besvärliga diskussioner kan även uppstå beträffande redan pågående personuppgiftsbehandling, eftersom lagstiftaren inte ger entydiga signaler om vad som gällde tidigare.

I stället för att göra ett grundligare jobb i lagstiftningsarbetet läggs bördan på ett stort antal personuppgiftsansvariga. Den kliniska forskning, som anses tillföra ett så stort värde att PDL måste förtydligas riskerar därför att försenas för att ganska komplexa konsekvensbedömningar krävs. Hade det inte tillfört ett större samhällsvärde totalt sett om utredningen gjort en djupare analys?

En paradox uppstår

Den bristande helhetssynen hos lagstiftaren är sannolikt ofta en systemfaktor som skapar problem på det sätt jag beskriver i PDL-exemplet. Det goda resultat som lagstiftningen vill uppnå hotas vilket är en paradox.

Att det i svensk lagstiftning saknas analys av dataskyddsfrågor, alternativt att denna är alltför rudimentär, skapar problem för den som ska tillämpa lagen. Denne har mycket lite att hålla sig i om lagstiftningen brister. Som jag beskrivit ovan med mitt exempel från PDL existerar problemet fortfarande trots att EU-domstolen i mål C-268/21[13] klargjort hur restriktivt utrymmet att tillåta vidarebehandling i nationell lagstiftning är för lagstiftare. Även det lagstiftningsarbete som genomfördes 2017–18 inför att GDPR skulle börja tillämpas är som redan nämnts ofta undermåligt, särskilt som arbetet dessutom präglades både av brådska och resursbrist. Många lagar (till exempel rättegångsbalken som var aktuell i rättsfallet) gicks inte ens igenom, så i dem saknas både analyser och säkerhetsåtgärder.

PDL är inte ett isolerat fall. När jag skrivit böcker och lagkommentarer har jag hittat flera tveksamma paragrafer med underliga förarbetsuttalanden.[14] Jag har även annars ofta stött på liknande fall när jag bistått kunder med rättsutredningar.

I den verklighet som organisationer har i det dagliga arbetet innebär otydligheter och svepande uttalanden ytterligare problem: i varje organisation kommer några anse att man måste kunna lita på förarbeten medan andra kommer att peka på alternativa uttalanden från EU-dom-

[13] Norra Stockholm Bygg mot Per Nycander AB.

[14] Böckerna Dataskyddsförordningen GDPR: Förstå och tillämpa i praktiken (Sanoma utbildning 2018; medförfattare Dag Wetterberg), Dataskyddsförordningen GDPR: För dataskyddsombud och andra ansvariga (Sanoma utbildning 2019) och Dataskyddsförordningen GDPR: Hantera registrerades rättigheter (Sanoma utbildning 2020; denna finns i en huvudbok och en arbetsbok). Lagkommentarer till lagen med kompletterande bestämmelser till EU:s dataskyddsförordning och PDL som jag skrivit för JP Infonet.

stolen, Europeiska dataskyddsstyrelsen (EDPB) eller nationella källor och mena att det som sägs i förarbetena måste vara fel.

Jag har inte sällan mött myndighetspersoner som tvekar om de verkligen kan genomföra sina uppdrag, eftersom de inte hunnit göra en konsekvensbedömning och lagstiftningen är luddig. Inte sällan har det i sådana situationer uppstått slitningar inom organisationen där dataskyddsombudet och andra inom dataskyddet ses som stoppklossar. Viktiga myndighetsuppdrag och bra digitalisering försenas som en effekt.

Det skapas alltså en paradox att inte genomföra ordentliga konsekvensbedömningar redan i lagstiftningsarbetet, eftersom detta skapar en osäkerhet längre fram om lagstiftningen kan tillämpas. Detta leder till att önskade effekter av lagstiftningen försenas, minskas eller uteblir. Till det missar lagstiftaren en möjlighet att tidigt korrigera delar som leder till oproportionella risker för integritetsskyddet i förhållande till det som ska uppnås, vilket gör att även de registrerade förlorar. Ser man det bara utifrån ett statligt perspektiv leder det dessutom till mycket större kostnader för statsbudgeten att alla myndigheter ska lägga kraft på att utreda något en utredning kunde ha gjort samtidigt som den skrev sitt betänkande. Detta samtidigt som tänkt samhällsnytta försenas eller uteblir.

Tidiga konsekvensbedömningar skulle även skapa andra vinster, nämligen att frigöra resurser för annat dataskyddsarbete i organisationer som idag lägger mycket tid på att genomföra konsekvensbedömningar för arbete som har ett lagstöd. Självklart skulle mer tid i stället kunna läggas på konsekvensbedömningar av behandlingar som inte styrs av lagstiftning. Man skulle även få mer tid att jobba med andra viktiga frågor som förbättrar det inbyggda dataskyddet.

Konsekvensbedömningar när regler skapas

Jag förordar således att större tyngd läggs på konsekvensbedömning redan när regler skapas. Det arbetet behöver inte vara så svårt. IMY har tagit fram den utmärkta publikationen Vägledning för integritetsanalys i lagstiftningsarbete[15] som guidar den som ska ta fram regelverk i hur man ska gå till väga. Denna kan även med fördel användas av myndigheter när de tar fram myndighetsföreskrifter, eftersom dessa idag riskerar skapa samma sorts paradox.

Samtidigt ska dock framhållas att man ibland även skulle vara tvungen att genomföra kompletterande konsekvensbedömningar även om sådan är genomförd i en lagstiftning, till exempel om man vill genomföra upp-

[15] IMY-2022-10835.

drag man fått i lagstiftningen på ett nytt innovativt sätt (till exempel genom användande av artificiell intelligens) om detta inte ingått i den konsekvensbedömning som redan genomförts av lagstiftaren.[16] Även i en sådan situation skulle lagstiftarens konsekvensbedömning skapa värde, eftersom den löst vissa av frågorna.

Hur kan man då göra för att påverka lagstiftaren? Var och en har inte så mycket makt i den frågan. Alla som avger remissyttranden kan dock regelmässigt efterfråga konsekvensbedömningar i sådana.

Den andra konsekvensbedömningsparadoxen: Felaktig avgränsning

> *Best efforts are essential. Unfortunately, best efforts… can do a lot of damage. Think of the chaos that would come if everyone did his best, not knowing what to do.*
>
> W. Edwards Deming

Regleringen

Det är viktigt att genomföra konsekvensbedömningarna på ett korrekt sätt. IMY:s förteckning[17], som tagits fram med stöd av punkterna 4 och 5 i artikel 35 GDPR ger en hel del vägledning om vad som utgör hög risk i initialstadiet av konsekvensbedömningen. Förteckningen manifesterar i stor utsträckning det som artikel 29-gruppen skrivit i sina riktlinjer.[18] IMY:s förteckning får genom kopplingen till mandatet i artikel 35 GDPR en sorts föreskriftsliknande effekt, vilket gör att den är en starkare rättskälla än annat myndigheten producerar.

En paradox uppstår

Idag lägger många organisationer ner mycket arbetstid på konsekvensbedömningar. Om konsekvensbedömning i praktiken ska fungera som

[16] Se vad Artikel 29-gruppen skriver i not 21 i Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679, antagna den 4 april 2017 och senast reviderade och antagna den 4 oktober 2017.

[17] Förteckning enligt artikel 35.4 i Dataskyddsförordningen (2019-01-16, dnr DI-2018-13200).

[18] Se Artikel 29-gruppens Riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen ”sannolikt leder till en hög risk” i den mening som avses i förordning 2016/679a antagna den 4 april 2017 och senast reviderade och antagna den 4 oktober 2017.

ett verktyg för inbyggt dataskydd är det viktigt att den metodik man använder ger önskat resultat.

Felaktiga metoder kan leda till ineffektivitet utifrån ett systemsynsperspektiv. IMY:s förteckning tydliggör de kriterier som begreppet hög risk ska prövas mot. Den ger dock ingen direkt vägledning hur man ska avgränsa vad som ska bedömas enligt de två kriterierna. Därför är den personuppgiftsansvarige tvungen att själv göra avgränsningen. Blir den fel kan det leda till felaktiga slutsatser eller att man fokuserar på frågor som inte höjer det inbyggda dataskyddet.

Jag har inte sällan stött på att personuppgiftsansvariga påbörjar konsekvensbedömningar inför anskaffningen eller utvecklingen av ett nytt IT-stöd eller ett nytt arbetssätt. När avgränsningen av konsekvensbedömningen görs anges den röra systemet X eller den nya arbetsmetodiken Y.

Den valda avgränsningen gör att den personuppgiftsansvarige nagelfar det nya som ska införas. Ofta upptäcks problem, och eftersom man inte kan lösa dessa avvaktar man med införandet av det nya. Om man skulle djupare granska de problem som noterats är de oftast sådana som även finns med det befintliga arbetssättet. Om problemen även finns i befintligt arbetssätt borde detta stoppas, men så sker sällan (det man gjort i åratal i det löpande arbetet tenderar ofta vara en blind fläck). Sammantaget uppstår en paradox, eftersom nya system ofta har bättre dataskydd som standard (något att eftersträva enligt artikel 25 GDPR). Jobbar man på innebär det att man fortsätter att arbeta på ett sätt som innebär sämre inbyggt dataskydd.

Exemplet Excelfiler

Ett vanligt exempel jag stött på är att integritetskänslig behandling hanteras i Excelfiler som saknar viktiga säkerhetsåtgärder som logguppföljning och kryptering (om detta inte görs manuellt). Vidare innebär användningen av Excelfiler att organisationen ökar sin behandling av ostrukturerat material vilket gör det svårare att uppgifts- och lagringsminimera. Även tillämpningen av registrerades rättigheter försvåras.

Jag har flera gånger stött på organisationer som efter en konsekvensbedömning tvekar att införa ett modernt IT-stöd (med hög nivå av dataskydd som standard) och i stället fortsätter arbeta med Excelfiler på ett mer riskfyllt sätt. Genom att koncentrera bedömningarna bara på det nya riskerar man att alltför länge fortsätta med integritetskänsliga arbetssätt. Dessutom reds inte problem ut i befintliga arbetssätt utan man fortsätter arbeta som tidigare.

Hur ska avgränsningar göras?

Enligt min mening bör man i avgränsningen av konsekvensbedömningar anlägga ett systemsynsätt och utgå ifrån vad organisationen vill uppnå, till exempel ett effektivt arbete med statistik eller en bra kundtjänst.

När man har tydliggjort detta kan sedan olika tekniska lösningar och arbetsmetoder prövas parallellt. I mitt exempel med Excelfilerna kan det befintliga arbetssättet prövas mot de möjliga arbetssätt som man vill uppnå (till exempel med stöd av systemet X eller metodiken Y). Ett sådan avgränsning ökar även medarbetarnas förståelse för arbetet och ger större utrymme för kreativitet. Man kommer ofta också djupare ner i analysen, vilket ökar värdet i konsekvensbedömningen.

Den tredje konsekvensbedömningsparadoxen: Fokus på den registrerade missas

> *Joy in work comes from understanding why your work is important. Not from the work, but from knowledge of who's going to use it.*
>
> W. Edwards Deming

Fokus på registrerades rättigheter och friheter

Syftet med konsekvensbedömningar är att bedöma riskerna för registrerades rättigheter och friheter. Enligt artikel 35.9 GDPR ska den personuppgiftsansvarige, när det är lämpligt, inhämta synpunkter från de registrerade. Eftersom det är konsekvenserna för den registrerade som ska bedömas är det förstås rimligt att låta dem komma till tals. I verkligheten möter jag dock ofta motsatsen, att organisationer mer regelmässigt anser att det inte är lämpligt att höra den registrerade.

Enligt min mening är det ett mycket bra hjälpmedel att få ta del av de registrerades synpunkter. Här är det dock viktigt att inte bara fokusera på integritetsrisker utan bedöma frågan utifrån alla mänskliga rättigheter och friheter. Eftersom mycket digitalisering syftar till att generera nyttor för människor är det förstås även relevant att låta berörda människor (som också är registrerade) ge sin syn på den nytta som förmodas skapas.

Om man inte lyssnar till den registrerades syn blir det svårt att göra bedömningar av hur hen påverkas positivt och negativt. En viktig komponent i systemsynsättet saknas, nämligen att utgå ifrån vad som skapar värde för den berörde.

Hur kan man fördjupa förståelsen?

När jag jobbar med konsekvensbedömningar använder jag oftast Data Subject Stories, som jag tidigare beskrev. I den metodiken låter jag registrerade genom enkäter både få skatta nyttan av det som ska åstadkommas och få bedöma riskerna. För att få fram relevanta frågor genomförs ofta en workshop med personer som har olika kunskaper och perspektiv. Tillsammans mejslar vi ut bra frågor.

Enligt min erfarenhet är det nästan alltid så att de personuppgiftsansvariga får ett kvitto på att de registrerade önskar att få en bättre nytta (system X eller metod Y från föregående avsnitt upplevs alltså som positiva förbättringar). Detta gör det lättare att göra en risk- och proportionalitetsbedömning.

Det blir ofta också en ögonöppnare för organisationen att se hur nyttor och risker värderas av de som berörs vilket gör att arbetet känns mer intressant. Klyftan som kan finnas mellan utveckling och dataskydd minskar. De värden man får kan hänföras till de som berörs, vilket minskar diskussionsutrymmet.

Även om sammanlagda värden från en enkät (där de som svarar får skatta konsekvensen i ett värde 1–4) inte utgör en absolut sanning upplevs värdena ha bättre legitimitet än bedömningar man gör utan att lyssna. Man får också direkta kvitton på vad som inte bedöms skapa värde och var de största integritetsriskerna är, vilket är värdefullt när man ska bedöma vilka åtgärder som ska vidtas.

Inte sällan kan man i samband med riskbedömningen enkelt komma överens om att inte genomföra saker som inte skapar någon nytta eller har höga integritetsrisker. Att lyssna till de registrerade ger fler perspektiv och fördjupar därför möjligheten att göra en bra analys. Även om det tar viss tid att skapa enkäter och ta in svar tjänar man in tiden. Det går ofta relativt fort att slutföra konsekvensbedömningen om man har bra ingående data att bedöma.

En paradox uppstår

Enligt min mening skapas en paradox när man regelmässigt undviker att ta in registrerades synpunkter. Konsekvensbedömning handlar ju om att bedöma risker för den registrerade utifrån den behandling som planeras. Glömmer man bort det perspektivet kan det bli konstiga resultat. Inte sällan har effekterna för organisationen fått nästan allt fokus i konsekvensbedömningar, medan de registrerade behandlas mer styvmoderligt.

Dessutom minskar värdet i verktyget konsekvensbedömning. När man fortlöpande ska utveckla det inbyggda dataskyddet är det viktigt att hela tiden förstå hur arbetet påverkar den registrerade (som redan nämnts är den registrerades rättigheter och friheter centrala i artikel 25 GDPR). Tar man inte tillvara den möjligheten vid konsekvensbedömningar går man miste om en bra chans att förbättra sitt inbyggda dataskydd.

Den fjärde konsekvensbedömningsparadoxen: Felaktig riskmetodik

We are being ruined by best efforts and hard work

W. Edwards Deming

En legaldefinition av hög risk

IMY:s förteckning ger en sorts legaldefinition av begreppet ”hög risk för fysiska personers rättigheter och friheter” i artikel 35.1 GDPR. I den anges nämligen att om två eller fler kriterier är uppfyllda föreligger hög risk, vilket innebär att en konsekvensbedömning ska inledas. Detta kan i och för sig motbevisas men skrivningarna om när hög risk ändå inte föreligger enligt förteckningen är luddiga.

En legaldefinition innebär att ett regelverk tydliggör ramarna för hur ett begrepp ska tolkas och tillämpas. I IMY:s förteckning är ramarna ett antal kriterier (föreligger de eller inte?). IMY har vidare gett exempel på vad varje kriterium kan innebära som ytterligare vägleder. Det blir alltså inte fråga om en sedvanlig riskbedömning där man brukar utgå ifrån begrepp som konsekvens och sannolikhet utan i stället en bedömning utifrån fastställda kriterier och exempel.

Hur hög risk ibland hanteras

Många praktiker är inte vana vid legaldefinitioner. Begreppet hög risk i artikeltexten är luddigt. Praktiker har därför funderat över begreppet ”hög risk” i förhållande till sedvanliga riskmetoder. I det arbetet har ofta personer med särskild kunskap om riskhantering konsulterats. Dessa finns ofta inom internrevision eller intern styrning och kontroll. När de som arbetar med dataskydd möter personer som arbetar med verksamhetsrisker uppstår ofta ett intresse att lägga ihop den interna riskmodel-

len med de kriterier som finns i IMY:s föreskrifter. Detta för dock tanken fel eftersom begreppet ”hög risk” ju utgör en sorts legaldefinition.

Måluppfyllelse inte relevant

Det finns även en viktig systemfaktor som skiljer. I intern riskhantering (både i interrevision och intern styrning och kontroll) finns nämligen en faktor med som inte är relevant i dataskyddsarbetet, nämligen förmågan att nå verksamhetens mål. Modeller för intern styrning och kontroll, till exempel den statliga som baseras på förordningen om intern styrning och kontroll (Fisk) innehåller modeller för att hantera målkonflikter till exempel när en myndighet upptäcker att det kan vara svårt att både genomföra myndighetens uppdrag och hantera vissa lagkrav i förhållande till de resurser man fått. ESV uttrycker sambandet så här i en handledning[19]:

> Riskhanteringen leder ofta till målkonflikter. En sådan är möjligheten till enkel, snabb och billig (effektiv och produktiv) handläggning som kan krocka med hot om att säkerheten (följa regler) eftersätts. Här ger dock förvaltningslagen vägledning ”Varje ärende där någon enskild är part ska handläggas så enkelt, snabbt och billigt som möjligt utan att säkerheten eftersätts”. När det finns en målkonflikt är det ert ansvar att välja och därmed acceptera konsekvensen av valet.

Den här sortens avvägning finns av naturliga skäl inte i IMY:s förteckning och är alltså inte möjlig att tillämpa som en del i arbetet med att avgöra om man ska genomföra en konsekvensbedömning. Denna avgränsning ska som tidigare nämnts enbart göras enligt de kriterier som nämns i förteckningen. Av det skälet går det inte att lägga ihop metoderna och skapa ett ”enhetligt riskbegrepp”.

En paradox uppstår

Jag tror därför inte på modeller som lägger ihop olika typer av riskbedömningar till en.[20] Genom att lägga ihop modellerna riskerar man att kortsluta både riskbedömningen enligt artikel 35 GDPR och enligt andra regelverk som Fisk. De resultat man får tenderar också att sänka ribban i IMY:s legaldefinition om när konsekvensbedömning ska göras, vilket

[19] Ekonomistyrningsverket: Handledning Att hantera verksamhetsrisker Processen enligt förordningen om intern styrning och kontroll (2012:47).
[20] Ett exempel på detta är den metodik Försäkringskassan tagit fram, se Konsekvensbedömning avseende dataskydd, Informationsmeddelande IM 2021:188.

förstås innebär att man sannolikt missar att göra konsekvensbedömningar som ska göras. Sänkningen uppstår därför att man låter andra aspekter som måluppfyllelse och generell riskaptit påverka legaldefinitionen. En riskmodell som förväntas hantera allt hanterar i praktiken inget, vilket är en paradox.

Risken med sådana modeller är dessutom att man behöver lägga ner ett ganska stort arbete med att bedöma om en konsekvensbedömning ska göras. Mycket av detta arbete hade i stället och naturligt kunnat göras inom ramen för konsekvensbedömningen och där skapat nytta utifrån gott inbyggt dataskydd. Fokus och resurser läggs på fel frågor.

Metoder som föreskrivs i Fisk eller annan reglering av intern styrning och kontroll måste enligt min mening vara helt fristående i förhållande till frågan om man måste göra en konsekvensbedömning. Däremot kan man förstås tillämpa dem parallellt. De värderingar och slutsatser man gör i en konsekvensbedömning kan förstås beaktas i annat riskarbete. I den riskhantering som görs inom intern styrning och kontroll ställs olika mål mot varandra till exempel ett högt inbyggt dataskydd mot mål att avgöra ärenden inom rimlig tid. Väljer man i en sådan riskhantering att acceptera risker rörande det inbyggda dataskyddets nivå får man, som ESV anger, också vara beredd att ta konsekvenser som sanktionsavgifter och annat som IMY kan påföra vid tillsyn eller skadeståndskrav.

Här ska även noteras att man inte kan acceptera att en hög risk[21] kvarstår när konsekvensbedömningsarbetet avslutas. I sådana fall måste enligt artikel 36 samråd med IMY inledas om man inte avstår från behandlingen. Även detta visar på att man inte kan ha en gemensam metod.

Hur gå vidare?

När många ser integritet som en självklar och viktig del blir det en mänsklig rättighet med stor tyngd, om få gör det blir rättigheten mest en papperstiger.

Det finns enligt min mening många systemfel i arbetet med konsekvensbedömningar, vilket gör det urvattnat och ibland till och med kontraproduktivt. Detta gör konsekvensbedömning till ett svagare verktyg för det inbyggda dataskyddet, vilket givetvis inte är bra.

[21] Detta begrepp har inte samma innebörd som legaldefinitionen. Det är ett problem att GDPR ofta använder begrepp som hög risk utan att de förklaras tydligt. Här utskiljer sig det hög risk-begrepp som används för att bedöma om konsekvensbedömningar ska genomföras, vilket jag förklarade i avsnittet En legaldefinition av hög risk.

I den här artikeln har jag lyft ett antal aspekter på det praktiska arbetet med konsekvensbedömningar i allt från lagstiftningsarbetet till det som sker hos de personuppgiftsansvariga. Jag hoppas förstås att med detta ha fört fram intressanta och kanske nya perspektiv att fundera över. Om vi alla tar ett steg tillbaka och försöker se hur systemet fungerar och vem det ytterst är till för tror jag på en stor förbättringspotential. Om vi kan stärka sättet vi genomför konsekvensbedömningar på kommer mycket vara vunnet.

Jag tror att verktyget konsekvensbedömning kommer att fortsätta att utvecklas. Kommer vi riktigt långt kanske konsekvensbedömningen till och med blir så bra att den skapar direkt värde för verksamheten och inte bara ses som ett verktyg i dataskyddsarbetet. Jag har sett det hända i verksamheter som bygger på starka värderingar och fokus på att skapa nytta för människor. Som en person sa till mig ”Monika, det här är inte bara något som var bra för GDPR, det inser jag nu. Jag fick massa intressanta nya insikter vad jag ska satsa på och hur jag ska göra det bra. Min affär kommer att vinna på detta”.

Sett ur ett systemperspektiv kan vi alla bidra till att skapa och ständigt förbättra det inbyggda dataskyddet genom att göra bra konsekvensbedömningar. Fungerar inte det du gör idag, avsätt tid och fundera över vad som kan förbättras! Tänk då inte för snävt utan försök se allt i ett större perspektiv! Varje steg framåt är en vinst!