

## Sammanställning av Datainspektionens möten med verksamheter hösten 2018

Datainspektionen har under hösten 2018 genomfört en seminariereserie där inspektionens generaldirektör bjudit in högsta företrädare för verksamheter inom offentlig och privat sektor för att diskutera hur vi tillsammans kan ta steg för att skapa ett tryggt informationssamhälle.

Under seminarierna diskuterades bland annat hur vi tillsammans kan arbeta för att stärka skyddet för den personliga integriteten vid personuppgiftsbehandling, vilka de största utmaningarna är för verksamheterna och hur Datainspektionen kan bli vassare i sitt uppdrag att ge stöd och vägledning.

Under de 16 seminarier som hölls i Stockholm och Göteborg deltog drygt 220 verksamhetsföreträdare för offentlig och privat sektor.

Sammanställningen utgör en sammanfattning av vad som i huvudsak kom fram under seminarierna.

### Sammanfattning av vad som kom fram under seminarierna

Under seminarierna diskuterades en mängd viktiga frågor. Seminarierna kan sammanfattas med att det finns ett stort behov av information och vägledning från Datainspektionen. Verksamheterna synes i stora delar ha anpassat sig efter den nya regleringen. Det som behövs nu är inte primärt grundläggande kunskaper om reformen, utan möjlighet att få vägledning och stöd vid mer fördjupade avvägningar. Några av de huvudsakliga behov som lyftes under seminarierna var:

1. Mer tydlig och lättillgänglig information på webben
2. Mer stöd och vägledning från Datainspektionen
3. Ökad förståelse för de utmaningar som verksamheterna står inför

#### 4. Ökad samverkan med Datainspektionen och mellan Datainspektionen och andra myndigheter

### 1. Tydligare och mer lättillgänglig information på webben

Det finns ett stort önskemål och att få tillgång till information på Datainspektionens webbplats och att webbplatsen utvecklas.

När det gäller **information** rörde det främst frågor om:

- **vad är på gång**; vilka aktiviteter pågår nationellt och inom EU, t.ex. pågående arbeten och kommande vägledningar
- **personuppgiftsincidenter**; hur ser inkomna personuppgiftsincidenter ut och vad kan vi lära av dem
- **certifiering**; hur går arbetet och när blir det möjligt med certifiering. Även förhållandet till andra standarder, t.ex. ISO, lyftes
- **tillsyn**; information om pågående, avslutade och kommande tillsyn, samt kommande branscher för tillsyn
- **EU-samarbetet**; vilka frågor diskuteras inom EU, finns tidplan för hantering av aktuella frågor, vilken vägledande EU-praxis finns och vilka domar från EU-domstolen (som rörde tidigare lagstiftning) äger fortsatt giltighet. Det efterfrågas även en konsekvensanalys av en ev. Brexit
- **Datainspektionens uppdrag**; information om balansen mellan Datainspektionens kontrollerande respektive främjande uppdrag – vad gör Datainspektionen” på främjandesidan”.

När det gäller **webbplatsen** rörde det bland annat:

- datummärkning av dokument
- möjligheten att datumstämpla RRS-flödena på Datainspektionens webbplats så att läsaren kan se när ny information publiceras på webbplatsen
- möjlighet att via hemsidan kunna lämna förslag på områden där vägledning efterfrågas
- möjlighet att via hemsidan kunna rapportera in områden där det sker olika tolkning av regelverket inom EU, i syfte att Datainspektionen ska kunna ta initiativ till att det sker en harmonisering.

### 2. Önskemål om stöd och vägledning från Datainspektionen

Det finns önskemål om mer stöd och vägledning från Datainspektionen, gärna i form av (goda) exempel. Allmänt efterfrågas stöd och vägledning i arbetet med att anpassa verksamheterna till den nya dataskyddsförordningen. Områden som särskilt efterfrågas är:

- **PUA/PUB**; det efterfrågas vägledning för gränsdragningen mellan personuppgiftsansvarig och personuppgiftsbiträde. Området är mycket komplext. Stora globala bolag är svåra att förhandla med; man får skriva på deras avtal eller avstå från tjänsten. Vidare är det är oklart hur ansvaret ser ut i förhållande till underleverantörer. Konkreta råd och mallar efterfrågas men även exempel. I sammanhanget efterfrågades vägledning om ansvaret för att betala en ev. sanktionsavgift kan fördelas mellan PUA/PUB
- **outsourcing och molntjänster**; det behövs vägledning kring outsourcing och molntjänster. Många gånger är dessa en förutsättning för säker it-drift och det är vanligt att t.ex. driften av löne- och fakturahantering läggs ut på annan leverantör som sparar uppgifterna i molnet
- **lagring/gallring**; vägledning behövs kring hur information får hanteras i e-post och mappar. Arkiven utgör en särskild utmaning för offentlig verksamhet. Det efterfrågas stöd för gallring när det gäller e-post och indikationer på vad som är rimlig tid för hur länge uppgifter får sparas (när tidsfrister för gallring saknas). Särskilda intressekonflikter finns inom så kallade "minnesinstitutioner" (såsom muséer, bibliotek och folkminnesinstitutioner) som arbetar utifrån mycket långa perspektiv
- **vad är tillåtet**; det efterfrågas vägledning och goda exempel för vad som är tillåten personuppgiftsbehandling. Dataskyddsreformen har ibland lett till en överdriven försiktighet vilket försvårar vardagen i en del verksamheter och i samverkan med andra
- **register**; vägledning och mallar efterfrågas när det gäller upprättande av register/registerförteckningar
- **tillsyn**; vägledning i form av sammanställningar över tillsyn inom vissa sektorer eller branscher efterfrågas

- **Rättsliga grunder, ändamål m.m.;** det är centralt att få vägledning rörande rättsliga grunder. Inom vissa branscher efterfrågas vägledning kring vad som kan göras med stöd av avtal respektive samtycke och inom arbetslivet efterfrågas vägledning då verksamheten bygger på stadgar. Man efterfrågar även vägledning kring hur exakt ett ändamål måste preciseras samt hur registrerade på bästa sätt kan få tillräcklig information, samtidigt som den är lätt att förstå.

### 3. Ökad förståelse för de utmaningar som verksamheterna står inför

Verksamheterna vittnar om att viljan att följa dataskyddsregleringen många gånger finns, men att det kan finnas hinder som försvårar detta. De efterfrågar ökad förståelse för de utmaningar som verksamheterna står inför i den dagliga driften.

Några av de utmaningar som lyftes var:

- **regelverk med målkonflikter;** många verksamheter har flera regelverk att följa (ibland med olika tillsynsmyndigheter) och de kan krocka. Bank- och försäkringsbranschen påtalade särskilt att icke harmoniserade EU-regelverk på dessa områden leder till problem för verksamheterna. Cloud Act lyftes fram som ett exempel.
- **brister i it-stöden;** många vittnade om att det är en stor utmaning att anpassa gamla system och komplexa nätverk till kraven i den nya dataskyddsförordningen
- **digitalisering OCH integritet;** verksamheterna, t.ex. vårdsektorn, har stora förväntningar på sig att uppgifter hanteras digitalt och enkelt för brukaren – det innebär utmaningar i att samtidigt värna den personliga integriteten. GDPR upplevs ofta som ett hinder för den digitala utvecklingen
- **mail;** det saknas säkra maillösningar samtidigt som mail många gånger är en förutsättning för effektiv kommunikation. Det innebär stora utmaningar för verksamheterna.

### 4. Ökad samverkan med Datainspektionen och mellan Datainspektionen och andra myndigheter

Det efterfrågas en ökad samverkan och dialog med Datainspektionen men också mellan Datainspektionen och andra aktörer med närliggande uppdrag.

Det som kom fram kan sammanfattas enligt följande:

- **ökad samverkan med andra myndigheter;** olika regelverk krockar och olika myndigheter har tillsyn över dessa – därför efterfrågas utökad samverkan mellan Datainspektionen och andra myndigheter. Post- och telestyrelsen, Finansinspektionen, Inspektionen för vård

och omsorg och Skolinspektionen var några av de myndigheter som nämndes. Det efterfrågas också ökad kunskap om dataskyddsreformen hos andra myndigheter med närliggande uppdrag. Även Kammarkollegiet, som svarar för de statliga ramavtalen, nämndes som en viktig part för att få med dataskyddsaspekterna i upphandlingsförfarandena

- **ökad samverkan med branschorganisationer**; inom privat sektor är branschorganisationerna viktiga samverkanspartners. Där kan frågeställningar av generell karaktär tas upp som därefter kan spridas inom branschen. Ökad samverkan med branschorganisationerna efterfrågas därför generellt. Flera verksamheter vittnar om att det sker olika tolkningar av dataskyddsregleringen på EU-nivå. Bland annat lyftes prospecting/direktmarknadsföring, som inte är tillåtet i någon medlemsstat med hänvisning till GDPR. Det efterfrågas därför en utökad samverkan mellan dataskyddsmyndigheter och branschorganisationer även angående den pågående implementeringen av GDPR på EU-nivå
- **ökat arbete för harmonisering inom EU**; harmoniseringen behöver drivas med kraft – det behövs därför ingångar till Datainspektionen för att få kännedom om frågor där tolkningen eller tillämpningen inte är enhetlig
- **fler forum för kontakt och dialog**; branschseminarier alternativt seminarier med blandade branscher där ny teknik eller specifika frågor diskuteras föreslogs. Även nätverk för t.ex. dataskyddsombud framfördes som förslag. Det finns också önskemål om att kunna närvara vid Datainspektionens aktiviteter (utbildningar, seminarier, föreläsningar etc.) genom webinarier. Även DSO-utbildning via webb efterfrågas liksom utbildning för medarbetare som arbetar med frågorna som en del av sin dagliga verksamhet.

2018-12-18

Seminarierna har varit mycket värdefulla för mig och för Datainspektionen. Vi har fått med oss bra input som vi kommer använda som ett viktigt inspel vid planeringen av verksamheten för 2019.

Tack till alla som deltog och lycka till i era verksamheter!

//Lena Lindgren Schelin