Datainspektionens styrdokument

Dnr: DI-2019-1280
Beslutsdatum: 2019-01-31
Dokumentansvarig: Stabschefen
Beslutad av: Generaldirektören
Ersätter tidigare tillsynspolicy från 2010 ”Tillsynspolicy avsende PuL”

Datainspektionens policy för tillsyn

Inledning

Datainspektionen bedriver tillsyn för att säkerställa att människors grundläggande fri- och rättigheter skyddas i samband med behandling av personuppgifter och att god sed iakttas i kreditupplysnings- och inkassoverksamhet. En effektiv tillsyn är ett viktigt verktyg i arbetet mot vår vision: *Ett tryggt informationssamhälle – tillsammans värnar vi den personliga integriteten*.

Det bästa integritetsskyddet för enskilda uppnås om Datainspektionen kan bidra till att myndigheter, företag och organisationer systematiskt arbetar med integritetsfrågorna i sina löpande verksamheter och där får stöd i att göra rätt. En central aspekt av tillsynsverksamheten handlar därför om att göra ställningstaganden och slutsatser från tillsynsverksamheten tillgängliga för många. Därmed kan tillsynen leda till ökad regelefterlevnad och lärande även för fler än den granskade.

I vår tillsynsverksamhet utgår vi från vår värdegrund *tillgänglighet, transparens, tydlighet, tillit och tillsammans*. Eftersom Datainspektionen har skarpa korrigerande befogenheter är det avgörande att informationen om hur och varför vi genomför tillsyn är transparent och att våra beslut är tydliga. Vi uppträder på ett sätt som bygger och bidrar till förtroende för myndigheten, behandlar alla med respekt och formulerar information, vägledning och beslut på ett vårdat, enkelt och begripligt sätt. När tillsynen sker på ett sätt som främjar tilliten till Datainspektionen ökar förutsättningarna att få effekter i form av ökad regelefterlevnad, lärande och verksamhetsutveckling.

Syftet med tillsynspolicyn är att på ett generellt och övergripande plan inrikta Datainspektionens tillsynsarbete. Policyn ska ligga till grund för utformningen av årliga tillsynsplaner som beskrivs närmare nedan och för de prioriteringar som löpande görs vid bedömningen av om händelsestyrd tillsyn ska inledas.

Riskbaserad tillsyn

Ett övergripande mål för tillsynsverksamheten är att nå så stora effekter som möjligt i skyddet av den personliga integriteten och att god sed iakttas i kreditupplysnings- och inkassoverksamhet. Datainspektionen kan inleda tillsyn i två olika spår – utifrån en riskbaserad, i förväg fastställd tillsynsplan eller med anledning av händelser i omvärlden. För att använda våra resurser så effektivt som möjligt prioriterar vi granskningar som bedöms få störst effekt för enskildas rättigheter i form av regelefterlevnad och lärande, både hos den verksamhet som granskas och hos andra myndigheter, företag och organisationer. Detta innebär att vi lägger huvuddelen av våra tillsynsresurser på ett antal riskområden som identifieras i en årlig tillsynsplan. Därutöver kan tillsyn inledas löpande med anledning av händelser i omvärlden.

Årlig tillsynsplan

Med riskbaserad tillsyn avses inom Datainspektionen att prioriterade områden i en årlig tillsynsplan väljs utifrån tre aspekter där särskilda risker kan identifieras:

- Prioriterade rättsområden
- Specifika branscher eller verksamheter
- Nya företeelser

De prioriterade områdena väljs ofta ut relativt långt i förväg och Datainspektionen kommunicerar till omvärlden vilka områden som kommer att stå i fokus. Att identifiera specifika tillsynsobjekt inom respektive område är dock ett löpande arbete som kan pågå över längre tid. Urvalet bygger på händelser som anmäls till Datainspektion genom klagomål eller på annat sätt kommer oss till känna.

Prioriterade rättsområden

Merparten av Datainspektionens tillsyn utgår från dataskyddslagstiftningen, där det finns ett stort behov av att utveckla praxis och harmonisera tolkningen och tillämpningen inom EU. När Datainspektionen identifierar rättsfrågor där det saknas praxis eller tolkningen är oklar kan tillsyn vara ett effektivt sätt att driva fram praxis.

Inom ramen för myndighetens uppdrag fokuserar Datainspektionen sin tillsyn på principiellt intressanta rättsområden för att utveckla rättslig praxis av intresse för

skyddet av människors grundläggande fri- och rättigheter i samband med behandling av personuppgifter eller inom områdena inkasso och kreditupplysning. Ett prioriterat rättsområde kan också röra en fråga där det finns etablerad praxis, men där Datainspektionen identifierat att regelefterlevnaden är låg.

Specifika branscher eller verksamheter
Datainspektionen prioriterar i sin tillsyn de branscher eller verksamheter där specifika dataskyddsrisker är vanliga, som till exempel då känsliga uppgifter behandlas i stor omfattning. Prioriterade branscher och verksamheter identifieras genom omvärldsbevakning och uppföljning av de ärenden som inkommer till Datainspektionen, till exempel i form av klagomål eller anmälda personuppgiftsincidenter.

När tillsyn genomförs i en prioriterad bransch eller verksamhet väljer Datainspektionen ofta att inrikta tillsynen på olika aspekter av det systematiska kvalitetsarbetet som utgör grunden för en säker personuppgiftsuppgiftshantering eller som säkerställer att god sed iakttas i kreditupplysnings- eller inkassoverksamhet.

Nya företeelser
Den accelererande IT-utvecklingen förändrar kontinuerligt samhället, och nya tillämpningsområden för existerande teknik uppstår ständigt. Datainspektionen prioriterar tillsyn av nya företeelser i den tekniska utvecklingen som innebär, eller kan komma att innebära, risker för den personliga integriteten.

Händelsestyrd tillsyn

För att säkerställa skyddet för enskildas rättigheter behöver Datainspektionen även ha kapacitet att inleda tillsyn utöver den årliga tillsynsplanen. Sådan händelsestyrd tillsyn kan bli aktuellt bland annat för att kunna agera på områden där konsekvenserna för den enskilde är allvarliga.

Händelsestyrt tillsynsarbete utgör ett nödvändigt och viktigt inslag i Datainspektionens arbete, men för att inte tappa fokus och bli reaktiva läggs den största resursen på de prioriterade områden som identifieras i tillsynsplanen. Händelsestyrd tillsyn kan inledas utifrån information som framkommer till exempel i klagomål, i tidigare tillsynsärenden, anmälda personuppgiftsincidenter eller på annat sätt kommer Datainspektionen till känna. Sådan tillsyn kan inledas vid särskilt allvarliga brister som till exempel

- när det är fråga om särskilt integritetskänsliga behandlingar, omfattande uppgiftsmängder eller behandlingar som berör många människor.
- om behandlingen har utförts av myndigheter, stora företag eller andra stora föreningar och organisationer
- när enskilda befinner sig i en särskild beroendeställning till den personuppgiftsansvarige
- vid indikationer på systematiska brister i kredit- eller inkassoverksamhet som kan få konsekvenser för många eller
- om en verksamhet förekommer särskilt frekvent i de klagomål som kommer in till Datainspektionen

Tillsynsmetoder och kvalitetssäkring

Dataskyddsreformen ställer nya krav på Datainspektionen. Vår ambition är att ha specialistkompetens inom tillsynsverksamhet, väl etablerade metoder av hög kvalitet och kontinuerlig kompetensutveckling inom området.

De två vanligaste metoderna för tillsyn vid Datainspektionen är inspektion och skrivbordstillsyn. Inspektion innebär att vi gör granskningen på plats hos tillsynsobjektet, det vill säga myndigheten, företaget eller organisationen som ska kontrolleras. Vid en skrivbordstillsyn skickas i stället ett antal frågor via brev eller enkäter till ett eller flera tillsynsobjekt. Ibland används en kombination av inspektion- och skrivbordstillsyn, till exempel genom att ett antal skriftliga frågor följs upp av en inspektion på plats.

För att säkerställa enhetlighet och kvalitet i tillsynsverksamheten har vi interna riktlinjer för hur våra olika korrigerande befogenheter och administrativa sanktionsavgifter tillämpas. Datainspektionen ska välja en korrigerande åtgärd som är effektiv och avskräckande, men samtidigt proportionell, dvs. rimlig i förhållande till typen av överträdelse, hur allvarlig överträdelsen är och vilka följder den får.

Som stöd i tillsynen finns också andra stöddokument som checklistor, inspektionsplaner, och beslutsmallar. För att säkerställa en hög rättslig kvalitet och en konse-

kvent bedömning av rättsliga frågor har vi också ett myndighetsövergripande rättstillämpningsforum där komplicerade frågor som kräver ett ställningstagande kan beredas.

Eftersom dataskyddsreformen är gemensam inom hela EU ska tolkning och tillämpning av regelverket ske harmoniserat. Det är av största vikt att det sker en enhetlig och konform tolkning av regelverket. Det är också viktigt att vi genom vår tillsyn bidrar till att utveckla och fördjupa tolkningen och också till att driva fram rättspraxis i olika avseenden. Vår ambition är att ha en tydlig strategi för vår löpande samverkan inom EU och annan internationell samverkan som visar vilken position vi eftersträvar, vilka områden vi ska fokusera på och hur vår EU-samverkan ska hanteras i praktiken.

Våra medarbetare får kontinuerlig kompetensutveckling inom tillsynsområdet. Vi strävar också efter ett aktivt kunskaps- och erfarenhetsutbyte med andra europeiska dataskyddsmyndigheter, såväl som med andra tillsynsmyndigheter i Sverige.

Den här tillsynspolicyn ersätter tidigare tillsynspolicy från 2010.