

Diarienummer:
DI-2021-1697

Datum:
2021-03-04

Dokumentansvarig:
Katarina Tullstedt

Beslutad av:
Lena Lindgren Schelin

IMY:s policy för tillsyn

Inledning

Integritetsskyddsmyndigheten (IMY) 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.

Enligt IMY:s övergripande effektmål skapar tillsynen praxis och bidrar till lärande för många. Tillsynen genomförs på ett effektivt och rättssäkert sätt och leder till effekt i enskilda ärenden men även på integritetsskyddet i stort i samhället. Eftersom en stor del av IMY:s tillsyn bygger på klagomål är våra mål för klagomålshanteringen också viktiga i sammanhanget dvs. att medborgarnas rättigheter när det gäller klagomål tillvaratas på ett effektivt och rättssäkert sätt

I vår tillsynsverksamhet utgår vi från vår värdegrund tillgänglighet, transparens, tydlighet, tillit och tillsammans. Det är viktigt att vi är transparenta med hur och varför vi genomför tillsyn, att vi agerar på ett sätt som skapar förtroende för myndigheten, att vi behandlar alla med respekt och att vi formulerar beslut och ger information på ett vårdat, enkelt och begripligt sätt. När tillsynen sker på ett sätt som främjar tilliten till IMY 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 IMY:s tillsynsarbete. Policyn ska ligga till grund för utformningen av myndighetens tillsynsplan och för myndighetens prioriteringar av tillsyn.

IMY:s tillsynsuppdrag

I IMY:s instruktion¹ anges myndighetens tillsynsuppdrag.

IMY är enligt instruktionen tillsynsmyndighet enligt dataskyddsförordningen², kamerabevakningslagen, brottsdatalogen, förordningen om Säkerhetspolisens personuppgiftsbehandling, förordningen om polisiärt samarbete gällande sökning i amerikanska fingeravtrycksregister, kreditupplysningslagen och inkassolagen. Myndigheten är vidare nationell tillsynsmyndighet över personuppgiftsbehandling med anledning av passageraruppgiftssamlingar (PNR-uppgifter), Schengens informationssystem (SIS II), informationsteknik för tulländamål (CIS), Europol,

Postadress:
Box 8114
104 20 Stockholm

Webbplats:
www.imy.se

E-post:
imy@imy.se

Telefon:
08-657 61 00

¹ Förordning (2007:975) med instruktion för Integritetsskyddsmyndigheten

² 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

Prümrådsbeslutet, VIS-förordningen och VIS-rådsbeslut om informationssystem för viseringar, CBE-direktivet om gränsöverskridande informationsutbyte om trafiksäkerhetsrelaterade brott, Eurodac, Eurojust och tullinformationssystemet (TIS).

Tillsyn

Tillsyn baserad på klagomål

Genom dataskyddsreglerna skyddas den enskildes rätt till privatliv vid behandling av personuppgifter. Dataskyddsförordningen (GDPR)³ har stärkt den enskilde individens rättigheter. Den enskilde har rättigheter som kan utkrävas av den personuppgiftsansvarige, men den enskilde individen har också rätt att till tillsynsmyndigheten framföra klagomål om hen anser att behandlingen av dennes personuppgifter sker på ett oriktigt sätt.

IMY ska, som tillsynsmyndighet, behandla klagomålen och, där så är lämpligt, inleda tillsyn och utreda den sakfråga som klagomålet avser. Det är även i detta sammanhang viktigt att vi utgår från effektmålen och att vi i varje ärende gör en bedömning av vad som är en effektiv och rättssäker handläggning, vad som på enklaste sätt leder till effekt i det enskilda fallet men också på integritetsskyddet i stort.

Tillsyn som baseras på klagomål ska granska den eventuella kränkning eller risk för kränkning som den klagande utsätts för vid behandling av personuppgifter. Om vi genomför en vidare granskning i en tillsyn baserad på klagomål (s.k. utvidgad klagomålstillsyn) är det med anledning av att vi bedömer att tillsynen kan ha en viktig effekt på integritetsskyddet i samhället i stort. Det är då frågan om en riskbaserad tillsyn.

Klagomål som rör brottsdatalagen kan också leda till tillsyn. Även i dessa ärenden ska granskningen enbart omfatta vad som uppges ha brustit gällande den klagande.

En särskild form av tillsyn är laglighetskontroller enligt brottsdatalagen. Det är kontroll av brottsbekämpande myndigheters behandling av personuppgifter som sker efter begäran från en enskild individ och som framförallt blir aktuell när den enskilde inte själv kan få del av sina uppgifter på grund av sekretess. Laglighetskontrollerna är på samma sätt som klagomålsbaserad tillsyn begränsade till att enbart avse behandling rörande den enskilde som begärt kontrollen.

Riskbaserad tillsyn

Tillsyn kan inledas med anledning av att det finns särskilda risker med en viss personuppgiftsbehandling. Risken bedöms utifrån behandlingens art, sammanhang och omfattning. Andra faktorer som också kan beaktas är om det är frågan om ny teknik eller ny användning av befintlig teknik eller om det finns ett särskilt behov av praxis.

³ 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

I den riskbaserade tillsynen 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 verksamheter.

Den riskbaserade tillsynen kan vara händelsestyrd och initieras genom exempelvis anmälningar om personuppgiftsincidenter, tips och uppgifter i media. Det kan också vara uppgifter i klagomål som leder till en vidare tillsyn än att enbart omfatta en granskning av de brister som rör den klagande.

De särskilda riskerna och vad som kan föranleda att riskbaserad tillsyn bör prioriteras kan påverkas av händelser i omvärlden och ska därför preciseras i den årliga tillsynsplanen. Utgångspunkten för bedömningen av risken är hur allvarig risk som förelegat eller som föreligger, men det kan också vara allvaret av en händelse som inträffat. Den riskbaserade tillsynen ska utifrån allvaret av kränkningen eller risken för kränkning bedömas ha särskild betydelse för att värna enskilda individers grundläggande fri- och rättigheter i samband med behandling av personuppgifter, men också för att värna att god sed i kreditupplysnings- och inkassoverksamhet följs.

En risk kan också föreligga vid osäkerhet om rättsläget. Inom ramen för den riskbaserade tillsynen kan därför tillsyn ske avseende principiellt intressanta rättsområden för att utveckla rättslig praxis.

Behandling av personuppgifter som sker med ny teknik eller ny användning av teknik kan innebära en risk för att det etableras en oriktig tillämpning. Riskens allvar påverkas av att den digitala tekniken utvecklas och dess användning breddas i ett mycket högt tempo. Nya företeelser i den tekniska utvecklingen som innebär, eller kan komma att innebära, allvarliga risker för den personliga integriteten kan därför ligga till grund för riskbaserad tillsyn.

Årligen planerad tillsyn

IMY genomför även tillsyn som rör vissa företeelser eller vissa typer av verksamheter utan att det i det enskilda fallet finns något klagomål eller konkret brist i det specifika fallet. Denna typ av granskning sker enligt en årlig plan och består av två varianter.

Den ena varianten avser när IMY är ålagd att granska vissa verksamheter eller system, ibland med viss regelbundenhet.

Den andra varianten rör tillsyn som vi genomför för att vi utifrån en riskbedömning anser att en viss form av verksamhet eller typ av företeelse bör granskas. Risken avser kränkning av enskilda individers grundläggande fri- och rättigheter eller att god sed inte iaktas i kreditupplysnings- och inkassoverksamhet. Bedömningen av risken ska ske utifrån art, sammanhang och omfattning eller att det är frågan om ny användning av teknik eller att det finns ett särskilt behov av praxis. Det är således frågan om en riskbaserad tillsyn som är planlagd. De kriterier som gäller för den riskbaserade tillsynen gäller därför också för denna typ av planerad tillsyn.

IMY:s årligen planerade tillsyn anges i den tvååriga tillsynsplanen och planen revideras årligen.

Tillsynsmetoder och kvalitetssäkring

De två vanligaste metoderna för tillsyn vid IMY 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, effektivitet och rättssäkerhet i tillsynsverksamheten har IMY en processägare för tillsyn. Processägaren har i uppdrag att driva verksamhetsutveckling inom tillsynsprocessen, ta fram former för kvalitetssäkring och lärande och ansvara för intern kompetensutveckling inom tillsyn.

IMY arbetar även med kunskapsstärkande grupper inom såväl sakområden, som processuella frågor. IMY har också ett myndighetsövergripande rättstillämpningsforum för principiella ställningstagande. Som stöd i tillsynen finns också riktlinjer, checklistor, mallar och annan vägledning.

Eftersom dataskyddsförordningen ska tolkas och tillämpas harmoniserat inom EU är det gemensamma EU-arbetet centralt även i vår tillsynsverksamhet. IMY deltar aktivt i det EU-gemensamma samarbetet bland annat gällande frågor rörande tillsynsprocessen och de korrigerande åtgärderna. Tillsammans skapar också tillsynsmyndigheterna i medlemsstaterna rättspraxis.

Många granskningar berör behandling av personuppgifter i flera medlemsstater, andra behandlingar sker av en personuppgiftsansvarig i ett land medan den enskilde individen vars personuppgifter behandlingen rör är bosatt i en annan medlemsstat. För en enhetlig och konform tolkning är det av särskild vikt att dessa s.k. gränsöverskridande ärenden behandlas enligt de regler för samarbete som anges i förordningen. Det har stor betydelse både för den enskilde individen och för de företag och organisationer som är verksamma i flera medlemsstater. Samtidigt är även för dessa ärenden målet både effektivitet och rättssäkerhet. Det innebär att vi gör en noggrann bedömning innan vi har synpunkter på förslag i tillsynsärenden som behandlas av andra tillsynsmyndigheter.

Koppling till tillsynsplanen

I myndighetens tillsynsplan preciseras kriterierna för val av tillsyn. Kriterierna utformas efter principerna i tillsynspolicyn men anpassas också till vad som sker i vår omvärld, den tekniska utvecklingen och de erfarenheter vi fått från olika delar i vår verksamhet.

I tillsynsplanen anges också den årligen planerade tillsynen.

Tillsynsplanen fastställs senast den 31 januari varje ojämnt år och planen revideras årligen.

Den här tillsynspolicyn ersätter tidigare tillsynspolicy från 2019.