Datainspektionen

Datainspektionens styrdokument

Dnr: DI-2019-841
Beslutsdataum: 2019-03-19
Beslutad av: Generaldirektören

Tillsynsplan 2019-2020

Mål

Enligt Datainspektionens tillsynspolicy är ett övergripande mål för tillsynsverksamheten 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.

Tillsynsplan

Tillsynsplanen avser verksamhetsåren 2019 – 2020, men uppdateras årligen. Planen omfattar ett antal prioriterade områden där Datainspektionen identifierat att det finns särskild risk för att den enskildes rättigheter kan komma att kränkas och att det därför är särskilt viktigt att dessa behandlingar blir föremål för tillsyn.

Den riskbaserade tillsynen väljs utifrån tre aspekter där särskilda risker kan identifieras:

- Prioriterade rättsområden
- Specifika branscher eller verksamheter
- Nya företeelser

Årets prioriterade områden har identifierats genom de klagomål och personuppgiftsincidenter som inkommit till Datainspektionen, erfarenheter från tidigare genomförd tillsyn, generell omvärldsbevakning och utifrån aktuella regelförändringar. Utifrån dessa källor sker också löpande under året urvalet av vilka faktiska tillsynsobjekt som blir föremål för tillsyn

Prioriterade rättsområden

En grundläggande förutsättning för god efterlevnad av dataskyddsreglerna är förståelsen för regelverken hos de verksamheter som ska tillämpa dem. Datainspektionen kommer därför under året utöva tillsyn särskilt avseende följande rättsfrågor.

Personuppgiftsansvarig eller personuppgiftsbiträde
Denna rollfördelning är central för dataskyddsreglerna och därmed för skyddet av den personliga integriteten. Vem som är personuppgiftsansvarig respektive biträde i en specifik situation kan vara svårt att avgöra.

Samtycke som rättslig grund
Kraven på samtycket har genom dataskyddsförordningen specificerats ytterligare vilket innebär att praxis behöver utvecklas för att tydliggöra hur bestämmelserna kring samtycke numera ska förstås. Granskning avseende samtycke kommer att avse såväl krav på frivillighet, information, tydlighet som samtyckets omfattning.

Gränsdragning mellan betaltjänstlagen och kreditupplysningsverksamhet
Detta rör nya tjänster som kan komma att beröra ett stort antal personer och som innefattar personuppgifter av integritetskänslig karaktär. Det finns ett behov av att klargöra när dataskyddsförordningen (GDPR) respektive kreditupplysningslagens bestämmelser blir tillämpliga.

Specifika branscher eller verksamheter

Datainspektionen avser under 2019 att genomföra tillsyn avseende följande branscher eller verksamheter.

Hälso- och sjukvården
Hälso- och sjukvårdens personuppgiftsbehandling avser stora mängder känsliga personuppgifter omfattande hela befolkningen. Fokus kommer att läggas på grundläggande strukturer såsom ansvar, transparens mot patienter och skydd för uppgifter från obehörig åtkomst och obefogad spridning, men också det rättsliga stödet för stora uppgiftssamlingar.

Skolan
Barn är särskilt skyddsvärda och skolan behandling av personuppgifter omfattar en stor del av barnens uppväxt och innehåller såväl integritetskänsliga som känsliga personuppgifter. Fokus kommer att läggas på det rättsliga stödet för att behandla

uppgifter, att det finns strukturer för att skydda uppgifterna från obehörig åtkomst och obefogad spridning, samt teknikanvändning som kamerabevakning och ansiktsigenkänning.

Rättsväsendet
Rättsväsendes personuppgiftsbehandling avser integritetskänsliga uppgifter som berör många människor. Genom brottsdatalagen, kompletterande regelverk på olika områden och lagen om passageraruppgifter i brottsbekämpningen har rättsväsendet fått nya skyldigheter. Fokus för tillsynen kommer att ligga på hur de behöriga myndigheterna lever upp till sina nya skyldigheter, men även myndigheternas teknikanvändning.

Arbetsgivares behandling av anställdas personuppgifter
Arbetsgivares behandling av anställdas personuppgifter berör många som befinner sig i beroendeställning och behandlingen kan omfatta såväl integritetskänsliga som känsliga personuppgifter. Fokus kommer att främst vara arbetsgivares övervakning av anställda. Tillsynen kommer att omfatta frågor om såväl grundläggande principer, rättsliga grunder och information till de registrerade.

Mobila operativsystem
Mobila operativsystems insamling av användares platsdata är en personuppgiftsbehandling som berör många och avser omfattade uppgiftsmängder. Fokus kommer att läggas på grundläggande principer i dataskyddförordningen såsom laglighet, korrekthet och öppenhet genom att granska det rättsliga stödet för behandlingen och den information som har lämnats till användarna i samband med att personuppgifterna har samlats in.

Detaljhandeln
Detaljhandelns behandling av personuppgifter i kundklubbar berör många människor, uppgifterna kan vara integritetskänslig, det avser omfattande uppgiftsmängder och innefattar rättsfrågor där det finns behov av att klargörande. Bland annat ska den rättsliga grunden för behandlingen granskas, av särskilt intresse är den rättsliga grunden vid profilering.

Betalningsförmedlare
Betalningsförmedlares insamling av kunders köphistorik rör många personer och en stor mängd personuppgifter. Behov finns att klargöra särskilda rättsfrågor såsom exempelvis ändamål med behandling och gallring av personuppgifter.

VIS
Visa Information System (VIS) är ett system i vilket det sker ett omfattande utbyte av uppgifter om viseringar mellan EU:s medlemsländer. Enligt VIS-förordningen ska systemet inspekteras vart fjärde år. Senast Datainspektionen inspekterade systemet var 2015.

Inkassoverksamhet
Ett övergripande mål för Datainspektionens tillsynsverksamhet gällande inkasso är att nå så stora effekter som möjligt avseende regelefterlevnaden av inkassolagen och att god sed iakttas i inkassoverksamhet. Tillsyn kommer därför bedrivas mot inkassoföretag som har ärenden rörande ett stort antal gäldenärer.

Nya företeelser
Nya tillämpningsområden för existerande teknik, men också ny eller utvecklad teknik är generellt viktiga att följa för att bedöma risker och konsekvenser för integritetsskyddet. Under 2019 kommer ansiktsigenkänning att granskas. Även annan teknikanvändning kan bli föremål för tillsyn såsom exempelvis maskininlärning, automatiserade beslut, profilering och blockkedjor.

Händelsestyrd tillsyn
Tillsyn kan även inledas utanför de prioriterade områdena ovan om det på grund av specifika händelser finns anledning att agera på områden där konsekvenserna för den enskildes rättigheter bedöms särskilt allvarligt eller påkallat av andra skäl, däribland laglighetskontroller inom rättsväsendet och tillsyn som föranleds av EU-samarbetet.