Advokatfirman Kahn Pedersens skriftserie 2018:1

kahn pedersen

GDPR och tillsynsprocessen

– en översikt

Vi på Advokatfirman Kahn Pedersen ser det som en naturlig del av vår roll som specialistbyrå att delta i den offentliga diskussionen. Detta för att bidra till att föra fram och utveckla intressanta och inte sällan svåra rättsfrågor inom våra specialistområden. Ett led i detta arbete är denna skriftserie som kommer ut med ett till två nummer per år. Tanken med skriftserien är att lite mer djupgående utreda aktuella och mer komplicerade rättsfrågor, som vi märker är av intresse för våra klienter och samhället i stort.

Eftersom målsättningen är att vårt arbete med rapporterna ska komma inte bara våra klienter och samarbetspartners till del, utan även ska kunna bidra till utvecklingen av de rättsområden som vi är specialiserade inom, tillhandahålls alla nummer av skriftserien kostnadsfritt på vår webbplats under en Creative Commons Erkännande-Inga Bearbetningar 4.0 Internationell Licens. Detta möjliggör mångfaldigande och spridning av materialet förutsatt att inga ändringar görs och att källan anges.

Ämnet för denna rapport, som har nummer 2018:1, är tillsynsprocessen under EU:s kommande allmänna dataskyddsförordning (GDPR) som ska tillämpas från och med den 25 maj 2018.

ISBN 978-91-983215-4-8

1. Inledning

Varför en rapport om tillsynsprocessen?

Dataskyddsförordningen (GDPR)[1] (fortsättningsvis benämnd ”**dataskyddsförordningen**”) börjar tillämpas den 25 maj 2018 och innebär stora förändringar för många företag och myndigheter när det gäller hanteringen av personuppgifter.

För närvarande pågår – såväl i näringslivet som i offentlig verksamhet – ett intensivt arbete för att möta kraven i dataskyddsförordningen.

Vi har som juridiska rådgivare varit involverade i ett stort antal anpassningsprojekt gällande dataskyddsförordningen. I och med att den 25 maj nu närmar sig börjar anpassningsprojekten närma sig avslut.

Många ställer nu frågor om vad som ska hända framöver och – inte minst – hur det bäst går att förbereda sig inför en eventuell myndighetstillsyn avseende dataskydd. Som bekant är det Datainspektionen[2] som är tillsynsmyndighet för dataskyddsfrågor och som därmed ska utöva tillsyn enligt dataskyddsförordningen.[3] Det har bl.a. spekulerats i vilken mån och på vilket sätt Datainspektionens tillsynsverksamhet kan komma att förändras i och med tillämpningen av dataskyddsförordningen.

Kommer Datainspektionens tillsynsverksamhet förändras i något dramatiskt avseende? Hur ska en organisation lämpligen förbereda sig för att klara ett tillsynsärende? Vad ska organisationen tänka på under en inspektion? Vilka resurser, rättsmedel och juridiska verktyg har Datainspektionen till sitt förfogande? Erbjuder dataskyddsförordningen nya verktyg och rättsmedel? Kommer vi att få se en utveckling mot fältinspektioner i stil med konkurrensrättens s.k. gryningsräder? Hur ska en sådan fältinspektion lämpligen hanteras av ett företag eller en offentlig verksamhet som ska granskas? Finns det över huvud taget legala förutsättningar för den typen av inspektioner när det gäller dataskydd i Sverige?

Vi vill med denna skrift sammanfatta och beskriva Datainspektionens tillsynsverksamhet, hur regelverket ser ut och vilka rättsmedel som står till Datainspektionens förfogande. Vi tillåter oss även att spekulera

---

1 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 och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).

2 Vi har valt att i denna skrift använda myndighetens nuvarande namn ”Datainspektionen”, men det bör noteras att regeringen i december 2017 aviserade att Datainspektionen ska få ett nytt, vidgat uppdrag och dessutom byta namn till ”Integritetsskyddsmyndigheten”, se http://www.regeringen.se/pressmeddelanden/2017/12/datainspektionen-blir-integritetsskyddsmyndigheten/.

3 Regeringen har för avsikt att utse Datainspektionen som tillsynsmyndighet enligt dataskyddsförordningen (se prop. 2017/18:105 s. 114).

kring hur vi tror att Datainspektionens tillsyn kommer att utvecklas under dataskyddsförordningen.

Vi tillhandahåller slutligen förslag till allmänna checklistor och ”tänka-på-punkter” som vi hoppas kan utgöra ett praktiskt stöd för exempelvis en intern dataskyddsorganisation.

Vår ambition är att framställningen ska vara relevant för såväl privata som offentliga aktörer.

Den nya svenska dataskyddslagstiftningen

Personuppgiftslagen (1998:204) (”**PuL**”) utgör den huvudsakliga regleringen för dataskydd i Sverige. När dataskyddsförordningen börjar tillämpas kommer PuL att upphävas. Regeringen har därför föreslagit att riksdagen ska besluta om införandet av lag med kompletterande bestämmelser till EU:s dataskyddsförordning (”**dataskyddslagen**”)[4]. Som namnet antyder kommer dataskyddslagen innehålla kompletterande svenska bestämmelser till dataskyddsförordningen. Dataskyddsförordningen i sin tur ersätter det tidigare dataskyddsdirektivet från 1995.[5]

Dataskyddslagen föreslås träda ikraft samtidigt som dataskyddsförordningen börjar tillämpas, dvs. den 25 maj 2018. Alla hänvisningar till dataskyddslagen nedan avser det förslag till lagtext som regeringen presenterade i propositionen.

4 Regeringens förslag finns i prop. 2017/18:105 Ny dataskyddslag.

5 Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

2. Tillsynsprocessen

Datainspektionens uppdrag

Datainspektionens huvudsakliga uppdrag är enligt den nuvarande instruktionen[6] ”[...] att verka för att människor skyddas mot att deras personliga integritet kränks genom behandling av personuppgifter”. Därutöver har myndigheten i uppdrag att verka för att god sed iakttas i kreditupplysnings- och inkassoverksamhet. Enligt instruktionen ska Datainspektionen särskilt inrikta sin verksamhet på att informera om gällande regler och ge råd och hjälp åt personuppgiftsombud enligt PuL. Det är troligt att myndighetens instruktion kommer att förändras i och med dataskyddsförordningen. Detta bl.a. med anledning av att myndigheten kommer att få flera och ändrade arbetsuppgifter. Regeringen har också offentligt aviserat sådana förändringar.[7]

Det ska finnas en oberoende tillsynsmyndighet som kontrollerar att reglerna om skydd för personuppgifter efterföljs. Detta framgår av EU:s grundläggande stadga (artikel 8.3), medan närmare bestämmelser om Datainspektionens roll, uppgifter, ställning och befogenheter finns i dataskyddsförordningen (artikel 51–59). Vissa kompletterande bestämmelser finns i 6 kap. dataskyddslagen.

Genom dataskyddsförordningen införs även en skyldighet för Datainspektionen att samarbeta med andra tillsynsmyndigheter inom EU. Ett nytt EU-organ inrättas, Europeiska dataskyddsstyrelsen, som kommer bestå av cheferna från samtliga tillsynsmyndigheter i EU. Styrelsen kommer att kunna fatta beslut som är bindande för de nationella tillsynsmyndigheterna.

Datainspektionen är idag indelad i tre operativa enheter som ansvarar för bl.a. tillsynsverksamheten inom sina respektive områden. Enheterna är följande.

- Enheten för myndigheter, vård och utbildning
- Enheten för närings- och arbetsliv
- Enheten för rättsväsendet, försvar och kameraövervakning

Datainspektionens organisation kommer troligen att förändras för att bättre kunna ta hand om de arbetsuppgifter som myndigheten har fått enligt dataskyddsförordningen och regeringens beslut att vidga myndighetens uppdrag (se ovan).

6 Förordning (2007:975) med instruktion för Datainspektionen.

7 http://www.regeringen.se/pressmeddelanden/2017/12/datainspektionen-blir-integritetsskyddsmyndigheten/.

Datainspektionens tillsynsverksamhet i praktiken

Datainspektionen får in ett stort antal *tips och klagomål* från privatpersoner, företag och via media. Det är endast ett fåtal av dessa som leder till att ett särskilt tillsynsärende inleds. Datainspektionen har ansett att myndigheten i princip inte kan ta kontakt med tillsynsobjektet, dvs. den personuppgiftsansvarige, utanför ramen för ett tillsynsärende. Myndigheten kontaktar därför inte den personuppgiftsansvarige när klagomål och tips inte leder till tillsyn. Om klagomålet eller tipset gäller en komplicerad fråga som behöver utredas innan svar till anmälaren kan lämnas och innan beslut om tillsyn kan fattas, läggs ärendet upp som ett klagomålsärende.

Beslut om tillsyn innefattar vanligtvis att myndigheten även bestämmer hur tillsynen ska läggas upp. Datainspektionen väljer då mellan fyra olika former av tillsyn (se nedan).

Kontakten med den personuppgiftsansvarige sker efter det att myndigheten har fattat beslut om att inleda tillsyn. Den initiala kontakten tas normalt med personuppgiftsombudet om ett sådant finns utsett.

Datainspektionen redovisar inte hur många klagomål och tips som myndigheten får in. Dessa ingår i de drygt 12 000 (år 2017) frågor som myndigheten tar emot och besvarar via telefon och epost.[8] En grov uppskattning är att cirka 30 % av dessa gäller klagomål och tips där någon anser att en personuppgiftsansvarig behandlar personuppgifter i strid med lagen. I många fall handlar det dock om missförstånd. Antal klagomålsärenden som har anmälts under 2017 där Datainspektionen har behövt utreda frågan var 246 stycken.

Under 2017 inledde Datainspektionen tillsyn i 21 ärenden. Den siffran är dock relativt låg i jämförelse med tidigare år. Skälet är att Datainspektionen under 2017 fick sätta av stora resurser till att förbereda myndigheten för dataskyddsförordningen.[9] Av de redovisade tillsynsärendena avser vanligtvis en stor del planerad tillsyn som ibland sker i större tillsynsprojekt i s.k. tematillsyn.

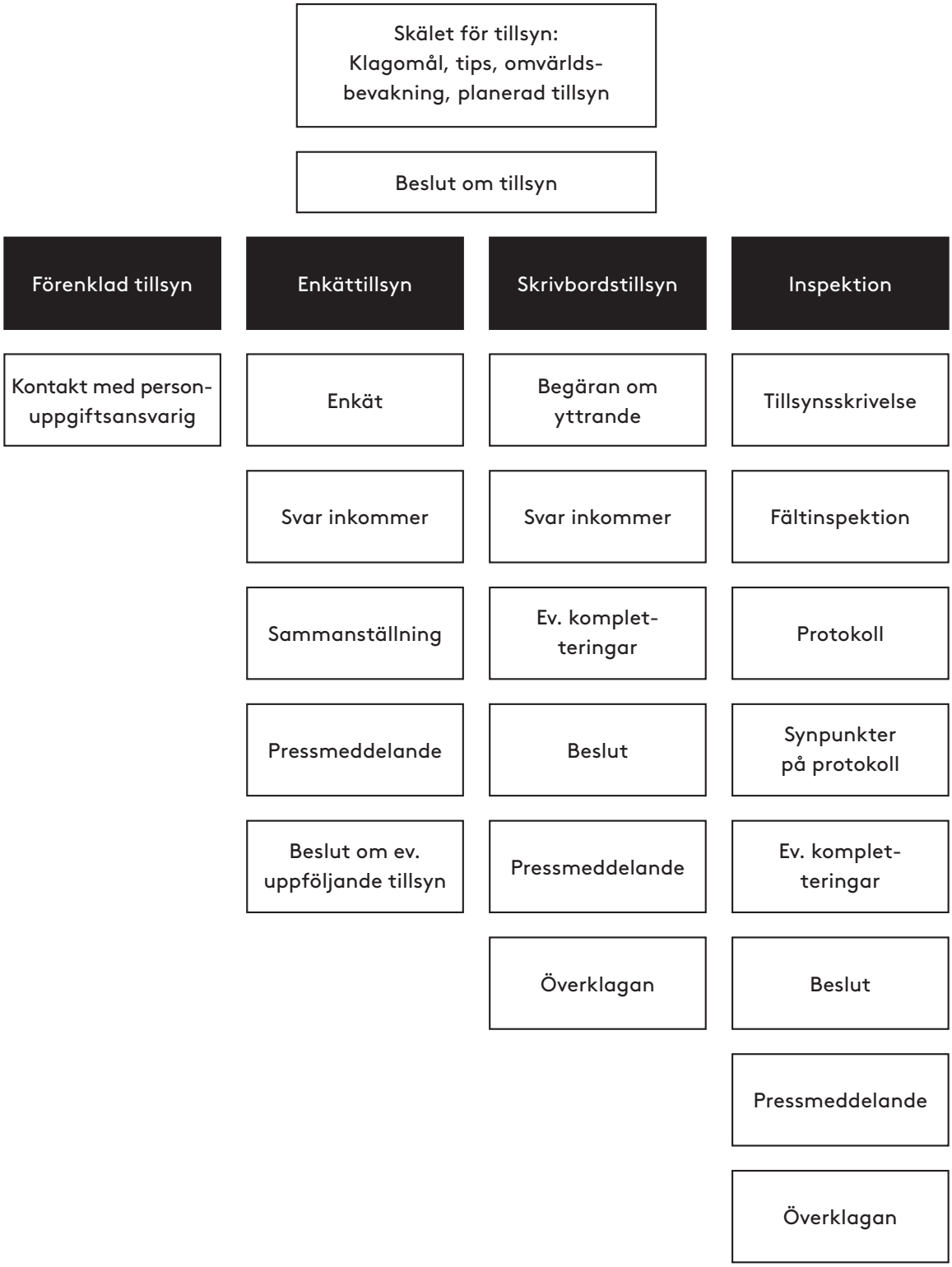
Tematillsyn omfattar en bred och djup granskning av en bransch, sektor eller företeelse och omfattar tillsynsärenden mot flera personuppgiftsansvariga. Vanligtvis väljs tematillsyn i syfte att skapa vägledning för en bransch eller för användningen av en ny företeelse, såsom sociala medier eller publika molntjänster. Ibland kan tillsynsobjekten väljas ut för att det har förekommit många klagomål och tips mot dem eller efter en inledande enkättillsyn. I andra fall kan valet falla på ett företag eller myndighet som ägnar sig åt särskild integritetskänslig personuppgiftsbehandling. Det är även vanligt att en organisation som har börjat att använda sig av ny teknik för att behandla

8 Datainspektionens årsredovisning 2017.

9 Datainspektionens årsredovisning 2017.

personuppgifter, t.ex. sociala medier och profilering, blir föremål för tillsyn. Vid tematillsyn är det alltså inte nödvändigt att de personuppgiftsansvariga misstänkts för att ha behandlat personuppgifter på ett felaktigt sätt.

Schematisk beskrivning av Datainspektionens tillsynsverksamhet



Olika former av tillsyn

Datainspektionen kan utöva tillsyn på flera olika sätt. Dessa är förenklad tillsyn, enkättillsyn, skrivbordstillsyn och s.k. fältinspektion.[10] Därutöver förekommer även ovan nämnda tematillsyn.

I ett och samma tillsynsärende kan olika tillsynsmetoder kombineras. En tillsyn kan t.ex. inledas med en enkättillsyn som sedan följs upp med skrivbordstillsyn mot vissa av de organisationer som ingick i enkättillsynen. En skrivbordstillsyn kan också kompletteras med en fältinspektion om det under handläggningen bedöms lämpligt.

Förenklad tillsyn kan användas när det står klart från början att ett klagomål eller tips grundar sig på ett fel som kan åtgärdas med en enkel och snabb kontakt med den personuppgiftsansvarige. Det är t.ex. vanligt i de fall då det har uppstått ett missförstånd i kommunikationen mellan den personuppgiftsansvarige och den registrerade vid en begäran om registerutdrag.

Vid en **enkättillsyn** skickas frågor om personuppgiftsbehandlingen till ett urval av företag, myndigheter eller organisationer t.ex. i syfte att kartlägga hur vanligt förekommande en viss företeelse är. Enkättillsyn kan ibland följas upp av andra tillsynsåtgärder.

Skrivbordstillsyn är den vanligaste tillsynsformen och innebär att den personuppgiftsansvarige får redogöra för sin personuppgiftsbehandling och svara på ett antal skriftliga frågor. Datainspektionen skickar då en ”begäran om yttrande”. Normalt är det tillräckligt med de svar som Datainspektionen får in vid första tillfället. Det förekommer även att kompletterande frågor måste ställas och ibland att tillsynen följs upp med fältinspektion.

Fältinspektion innebär att representanter från Datainspektion kommer till den personuppgiftsansvariges lokaler dels för att inspektera it-system m.m. dels för att ställa frågor om verksamheten. Fältinspektion är den mest omfattande tillsynsåtgärden och kan kombineras med skriftväxling både före och efter besöket. Fältinspektionen kan också förekomma efter en enkättillsyn. Inspektionsformen används om Datainspektionen har många frågor och det finns ett behov av att undersöka hur it-system är utformade t.ex. för att kontrollera att det finns tillräcklig it-säkerhet.

Datainspektionen har möjlighet att göra *oanmälda inspektioner,* men det har varit sällsynt under PuL. Det anses normalt inte särskilt effektivt eftersom det finns risk för att de ansvariga personerna inte finns på plats eller att tillsynsobjektet vägrar att släppa in Datainspektionens personal. Datainspektionen har ingen rätt att ta hjälp av kronofogdemyndigheten eller polis vid sina inspektioner. Detta är

10 Redogörelsen om Datainspektionens tillsynsformer och om Datainspektionens tillsynsverksamhet i övrigt i denna skrift bygger huvudsakligen på Datainspektionens tillsynspolicy daterad 2010-02-09.

en stor skillnad jämfört med de s.k. gryningsräder som förekommer inom konkurrensrätten.

En tillsyn omfattar sällan eller aldrig all personuppgiftsbehandling som förekommer hos en personuppgiftsansvarig. Tillsynen avgränsas normalt till en mindre del t.ex. hantering av personuppgifter om kunder vid kortbetalningar eller hantering av personuppgifter i publika molntjänster. Om tillsynen har inletts med anledning av ett klagomål kan den begränsas till hanteringen av personuppgifter om t.ex. den klagandes rätt att få ett s.k. registerutdrag.

Vår bedömning är att Datainspektionen i huvudsak kommer att fortsätta att arbeta med de former av tillsyn som används idag. Det är dock tänkbart att genomförandet av gemensamma tillsynsprojekt och influenser från andra tillsynsmyndigheter på sikt kan komma att medföra olika former av förändringar i Datainspektionens tillsynsverksamhet, t.ex. ett ökat inslag av oanmälda inspektioner.

En viktig förändring som införs genom dataskyddsförordningen är att även personuppgiftsbiträden kan bli föremål för tillsyn.

I andra medlemsstater inom EU förekommer en form av frivillig tillsyn vilken förutsätter att den granskade organisationen godkänner att tillsynsmyndigheten kommer på besök och ställer frågor om organisationens personuppgiftsbehandling.[11] Någon sådan tillsyn har inte förekommit i Sverige. När dataskyddsförordningen nämner dataskyddstillsyn (artikel 58.1 b) kan det vara en sådan frivillig tillsyn som avses. Det torde dock vara upp till varje tillsynsmyndighet att själva bestämma om myndigheten ska erbjuda frivillig tillsyn.

När inleder Datainspektionen tillsyn?

Datainspektionen inleder tillsyn med anledning av klagomål, tips eller för att myndigheten fått en indikation via sin omvärldsbevakning, media, visselblåsare eller på annat sätt att en pågående personuppgiftsbehandling kan vara olaglig. Tillsynen kan även inledas utan att det i det enskilda fallet finns misstanke om att regler inte följs. Syftet är då att skapa vägledning om hur reglerna ska tillämpas när det gäller tidigare inte bedömda företeelser t.ex. sociala medier, appar, drönare, självkörande bilar etc.

Genom dataskyddsförordningen tillkommer ett antal nya situationer som kan komma att leda till tillsyn. En situation är vid begäran om ömsesidigt bistånd från en annan tillsynsmyndighet. En annan situation som kan tänkas föranleda tillsyn är då anmälan av en personuppgiftsincident har gjorts.

11 Se t.ex. *Auditing data protection, a guide to ICO data protection audits*, version 3.5, juni 2015.

Några faktorer som kan tala för att tillsyn inleds är bl.a. följande:[12]

- När det finns misstanke om allvarliga brister i personuppgiftsbehandlingen.
- När personuppgiftsbehandling utförs av myndigheter, stora företag eller stora föreningar.
- När den registrerade befinner sig i beroendeställning till den personuppgiftsansvarige.
- När det är fråga om integritetskänsliga behandlingar, större uppgiftsmängder som rör en person eller behandlingar som berör många människor.
- När Datainspektionen har tagit emot många klagomål och tips om samma behandling.
- När det är fråga om nya företeelser där det kan finnas risk för integritetsintrång och betydande brister i säkerheten för personuppgifterna.
- När det finns behov av vägledning på ett visst område och tidigare praxis saknas.

Beslut om tillsyn och om planering av tillsynsverksamheten fattas huvudsakligen på enhetsnivå, i enklare fall, av en ensam handläggare. Beslut av principiell karaktär eller som är av större betydelse fattas av generaldirektören.

Beslut om att inleda tillsyn kan inte överklagas. Detsamma gäller beslut om att inte inleda tillsyn med anledning av ett klagomål eller ett tips (53 § PuL och 7 kap. 5 § dataskyddslagen).

Särskilt om fältinspektion

Beskrivningen nedan avser fältinspektioner som de typiskt sett har genomförts under PuL. Förmodligen kommer fältinspektioner i stora drag att genomföras på sådant sätt även i framtiden. Det kan dock inte uteslutas att det flyter in nya inslag eller alternativa möjligheter som ett resultat av influenser från och samarbete med andra tillsynsmyndigheter.

Tillsyn som innefattar fältinspektion hos den personuppgiftsansvarige inleds normalt med att ansvarig handläggare hos Datainspektionen tar kontakt via telefon eller e-post med någon hos den personuppgiftsansvarige, vanligtvis personuppgiftsombudet om sådant har utsetts. Syftet är att komma överens om tid, plats och de närmare detaljerna för inspektionen. Datainspektionen brukar berätta vad som är skälet till

12 Datainspektionens Tillsynspolicy avseende PuL daterad 2010-02-09.

att tillsyn har inletts och vilka personer som Datainspektionen vill prata med vid inspektionen. Ett vanligt önskemål från Datainspektionen är att följande personer är närvarande vid (delar av) inspektionen:

- Personer som fattar beslut om personuppgiftsbehandlingen
- Personuppgiftsombud
- Jurist, om sådan finns i organisationen
- Personer med kunskap om de aktuella it-system

Ibland kan det vara lämpligt att representanter från personuppgiftsbiträden närvarar vid inspektionen. Det är alltid den personuppgiftsansvarige som bestämmer vilka personer som ska närvara vid inspektionen.

Efter den inledande kontakten bekräftas tid och plats för inspektionen m.m. i en tillsynsskrivelse som skickas till den personuppgiftsansvarige. Adressaten för tillsynsskrivelsen är alltid det företag, den myndigheten eller den organisation som Datainspektionen bedömer bär personuppgiftansvaret. En kopia skickas även i förekommande fall till personuppgiftsombudet.

I skrivelsen kan Datainspektionen även skicka med underlag för inspektionen t.ex. i form av frågor som kommer att ställas och it-system som Datainspektionen vill undersöka. Det förekommer även att en agenda överenskoms gemensamt.

Inspektionen genomförs vanligtvis av den ansvariga handläggaren (inspektionsledaren) som är jurist och en protokollförare som normalt sett också är jurist. Beroende på inriktningen och omfattningen av inspektionen kan även en informationssäkerhetsexpert följa med.

Ordningen på en fältinspektion bestäms av den ansvariga handläggaren och kan anpassas efter förutsättningar i det enskilda fallet. Under inspektionen är det den ansvariga handläggaren som agerar som ordförande och bestämmer vad som är relevant. Det är vanligt att den som ska inspekteras vill lämna en redogörelse för sin verksamhet. Det kan också vara lämpligt att förbereda en presentation. Datainspektionen kan dock välja att korta ner sådana presentationer.

Ett vanligt sätt att lägga upp en fältinspektion är erfarenhetsmässigt följande:

- Presentation av de närvarande.

- Datainspektionen berättar om hur inspektionen går till, att det handlar om formell tillsyn om regelefterlevnad och lämnar anvisningar om hur Datainspektionen anser att den personuppgiftsansvarige bör svara på frågor.

- Datainspektionen redogör för tillsynsärendet; vad som är syftet med tillsynen och hur tillsynen har avgränsats till t.ex. en viss personuppgiftsbehandling.

- Den personuppgiftsansvarige redogör för sin verksamhet och den personuppgiftsbehandling som är föremål för inspektionen.

- Datainspektionen ställer frågor för att undanröja oklarheter i tillsynsobjektets redogörelse eller för att få svar på frågor som inte har besvarats.

- Datainspektionens personal inspekterar de aktuella it-systemen, gör slagningar i register för att t.ex. kontrollera vilka personuppgifter som finns, vilka sökmöjligheter som är möjliga, hur gamla personuppgifter som finns sparade i registret etc.

- Datainspektionens personal, vanligtvis informationssäkerhetsexperter, ställer frågor om säkerheten vid personuppgiftsbehandlingen.

- Datainspektionen sammanfattar vad som har kommits överens om ev. kompletteringar och vad som händer efter inspektionen och om den granskade organisationen har något ytterligare att tillföra.

Under inspektionen för Datainspektionen ett protokoll i vilket personuppgiftsansvariges redogörelse och svar antecknas i huvuddrag. Det är vanligt att protokollet hänvisar till handlingar som lämnas in under inspektionen. Efter inspektionen renskrivs protokollet av protokollföraren vilket typiskt sett brukar ta en eller två veckor. Därefter skickas protokollet till den personuppgiftsansvarige för synpunkter. Denne får normalt två eller tre veckor på sig att svara. Eventuella synpunkter innebär inte att protokollet ändras. Datainspektionen tar i stället hänsyn till synpunkterna vid utformningen av beslutet.

Protokollet och alla handlingar som lämnas under inspektionen blir allmänna handlingar hos Datainspektionen. De ska lämnas ut till vem som helst som begär det om det inte finns anledning att belägga dem (eller delar av dem) med sekretess. Det är vanligt att Datainspektionen frågar om det finns något i materialet som kan tänkas omfattas av sekretess t.ex. om det innehåller affärshemligheter eller uppgifter om säkerhetsåtgärder. Se vidare avsnittet *Sekretess hos Datainspektionen* nedan.

En vanlig fältinspektion tar cirka tre timmar men vid mer komplicerade ärenden kan inspektionen ta en hel dag och ibland följas upp med ytterligare kontakter.

Vanliga frågor som ställs vid en fältinspektion

Vilka frågor som ställs av Datainspektionen vid en fältinspektion bestäms till stor del av inriktningen och omfattningen med tillsynen.

Nedan anges ett antal grundläggande frågor som erfarenhetsmässigt typiskt sett brukar ställas vid fältinspektioner enligt PuL[13].

1. Personuppgiftsansvaret
   a. Vem anser ni är personuppgiftsansvarig?
   b. Vem bestämmer att personuppgiftsbehandlingen ska utföras?
   c. Vem bestämmer hur personuppgiftsbehandlingen ska utföras?

2. Syftet med och den rättsliga grunden för personuppgiftsbehandlingen
   a. För vilket eller vilka ändamål behandlas personuppgifterna?
   b. Vilken är den rättsliga grunden för behandlingen?
   c. Mer detaljerade frågor om den rättsliga grunden, t.ex. samtycket, avtalet, rättsliga förpliktelsen, det berättigade intresset.
   d. Hur bedömer ni att behandlingen är nödvändig?

3. Beskrivning av personuppgiftsbehandlingen
   a. Vilka personuppgifter samlas in?
   b. Hur samlas personuppgifterna in och från vem?
   c. Vilka sök- och sammanställningsmöjligheter finns?
   d. Förekommer det fritextsfält?
   e. Vilken utbildning om dataskyddslagstiftning och interna styrdokument har personalen?

4. Grundläggande krav vid personuppgiftsbehandling
   a. När och hur gallras personuppgifterna?
   b. Vilka rutiner finns för rättelse och radering?
   c. Vilka har tillgång till personuppgifterna?

5. De registrerades rättigheter
   a. Vilken information om behandlingen har de registrerade fått?
   b. Hur lämnas registerutdrag ut?

6. Personuppgiftsbiträden
   a. Anlitas personuppgiftsbiträden och vilka är de?
   b. Hur sker överföringen till personuppgiftsbiträdena?
   c. Finns biträdesavtal (kopia begärs ofta in)?
   d. Vilka instruktioner har personuppgiftsbiträdet fått för behandling av personuppgifter?
   e. Omfattas personalen hos personuppgiftsbiträdena av sekretessåtaganden?

7. Säkerhet vid personuppgiftsbehandlingen[14]
   a. Fysisk säkerhet.
   b. Tillträdeskontroll.
   c. Behörighetsstyrning.
   d. Behandlingshistorik (logg).

---

13 De grundläggande frågorna är i allt väsentligt relevanta även vid tillsyn mot personuppgiftsansvariga enligt dataskyddsförordningen, även om antalet frågor om den registrerades rättigheter av allt att döma kommer att utökas.

14 Se Datainspektionens allmänna råd om säkerhet för personuppgifter, reviderade november 2008.

e. Inloggning och säkerhet.
f. Säker kommunikation.
g. Åtgärder mot förlust av information.
h. Utplåning.
i. Reparation och service.
j. Skydd mot skadliga program.
k. Verifiering av säkerheten.

Dataskyddsförordningens princip om ansvarsskyldighet (”accountability”) innebär att tillsynsobjektet ska kunna visa hur denne uppfyller dataskyddsförordningen bl.a. genom att visa upp en förteckning av personuppgiftsbehandlingar enligt artikel 30. Det medför troligen att inspektionerna förenklas och att frågor kan fokuseras på det som är oklart.

Datainspektionens befogenheter vid tillsyn

Tillsynsmyndighetens utredningsbefogenheter enligt dataskyddsförordningen (artikel 58.1) motsvarar i stora drag de befogenheter som myndigheten har enligt PuL (43–47 §§). En skillnad som redan har nämnts är dock att Datainspektionen enligt dataskyddsförordningen kan bedriva tillsyn direkt mot ett personuppgiftsbiträde. Enligt PuL kan tillsynsåtgärder endast riktas mot personuppgiftsansvarige.

Datainspektionen har enligt dataskyddsförordningen rätt enligt artikel 58.1 bl.a. att

- beordra den personuppgiftsansvarige eller personuppgiftbiträdet att lämna all information som myndigheten behöver för att kunna fullgöra sina uppgifter,

- genomföra undersökningar i form av s.k. dataskyddstillsyn,

- meddela den personuppgiftsansvarige eller personuppgiftsbiträdet om en påstådd överträdelse av förordningen,

- av den personuppgiftsansvarige och personuppgiftsbiträdet få tillgång till alla personuppgifter och all information som tillsynsmyndigheten behöver för att kunna fullgöra sina uppgifter,

- få tillträde till alla lokaler som tillhör den personuppgiftsansvarige och personuppgiftsbiträdet, och även tillgång till all utrustning och alla andra medel för behandling av personuppgifter i överensstämmelse med unionens processrätt eller medlemsstaternas nationella processrätt.

Enligt 6 kap. 1 § dataskyddslagen kommer Datainspektionen få samma befogenheter vid tillsyn som avser bestämmelser i dataskyddslagen och andra bestämmelser som kompletterar dataskyddsförordningen.

Datainspektionen har inte rätt att med tvång genomföra undersök-

ningar av den personuppgiftsansvariges eller personuppgiftsbiträdets lokaler eller utrustning (se prop. 2017/18:105 s. 157). Om Datainspektionen nekas tillträde till lokaler eller tillgång till utrustning kan det tänkas leda till att Datainspektionen beslutar om en tillfällig begränsning av eller tillfälligt förbud mot personuppgiftsbehandlingen hos den personuppgiftsansvarige eller personuppgiftsbiträdet enligt artikel 58.2 f.[15]

Att neka Datainspektionen tillgång till lokaler, utrustning, personuppgifter och information kan även innebära att Datainspektionen beslutar om sanktionsavgifter enligt artikel 83.5 e.[16] Detsamma gäller om den personuppgiftsansvarige eller personuppgiftsbiträdet inte rättar sig efter ett föreläggande från Datainspektionen.

Den aktuella sanktionsavgiften ligger på den högsta nivån, dvs. upp till 20 miljoner euro, eller om det beloppet är högre, upp till fyra procent av årsomsättningen.[17]

Datainspektionen har hittills sällan haft problem med att den granskade organisationen vägrar att samarbeta. Den rätt som Datainspektionen har enligt 44 § PuL att vid vite förbjuda den personuppgiftsansvarige att behandla personuppgifter på något annat sätt än genom att lagra dem, har såvitt känt, aldrig använts av Datainspektionen.

Tillsyn vid behandling i flera EU/EES-länder – one-stop-shop

Med dataskyddsförordningen införs nya regler om hur tillsynsmyndigheterna ska samarbeta dels genom att lämna varandra bistånd dels genom gemensamma insatser.

Ömsesidigt bistånd innebär bl.a. informationsutbyte och begäran om information eller tillsynsåtgärder såsom inspektioner och utredningar. Den tillsynsmyndighet som får en begäran om bistånd från en annan tillsynsmyndighet får endast under vissa speciella förutsättningar vägra att tillmötesgå begäran (artikel 61.4).

Gemensamma insatser innebär att tillsynsmyndigheterna kan genomföra gemensamma utredningar och gemensamma verkställighetsåtgärder. I sådana åtgärder kan personal från andra medlemsstaters tillsynsmyndigheter delta. Det kan t.ex. handla om att tillsynsmyndigheterna agerar samordnat och samtidigt i ett tillsynsärende mot ett företag eller en bransch.

---

15 Se prop. 2017/18:105 s. 158. Det kan dock ifrågasättas om *enbart* det förhållandet att tillsynsobjektet vägrar tillgång till lokaler eller utrustning kan föranleda sådant beslut.

16 Av den svenska språkversionen av bestämmelsen kan intrycket ges att sanktionsavgift endast kan påföras vid nekad tillgång till personuppgifter och information. Av den engelska versionen framgår dock att det även måste kunna omfatta nekad tillgång till lokaler och utrustning.

17 För myndigheter är avgiften upp till 10 miljoner euro, 6 kap. 2 § dataskyddslagen.

Vid personuppgiftsbehandling som sker vid den personuppgiftsansvariges eller personuppgiftsbiträdets verksamhetsställen som finns i flera medlemsstater eller om personuppgiftsbehandlingen i väsentlig grad påverkar, eller sannolikt kan komma att påverka, registrerade i flera medlemsstater, s.k. *gränsöverskridande behandling* (artikel 4.23), kan flera tillsynsmyndigheter vara inblandade i tillsynen.[18] Den personuppgiftsansvarige eller personuppgiftsbiträdet ska dock bara behöva ha kontakt med en tillsynsmyndighet, den s.k. ansvariga tillsynsmyndigheten (”lead authority”). Den ansvariga tillsynsmyndigheten samordnar arbetet med alla berörda tillsynsmyndigheter och sköter kontakten med tillsynsobjektet. Det kallas för *one-stop-shop*.

Den ansvariga tillsynsmyndigheten är myndigheten i det land där den personuppgiftsansvarige eller personuppgiftsbiträdet har sitt huvudsakliga verksamhetsställe (artikel 56.1). Med huvudsakligt verksamhetsställe avses i första hand platsen där den centrala förvaltningen finns när den personuppgiftsansvarige eller personuppgiftsbiträdet är etablerat i flera medlemsstater. Om besluten om den aktuella personuppgiftsbehandlingen fattas av ett annat verksamhetsställe inom unionen är det tillsynsmyndigheten i det landet som är ansvarig för tillsynen. För det fallet ett personuppgiftsbiträde saknar central förvaltning inom unionen är tillsynsmyndigheten i det land där den huvudsakliga behandlingen sker inom ett av biträdets verksamhetsställen den ansvariga tillsynsmyndigheten (artikel 4.16).

Det görs undantag från samarbetsskyldigheten mellan tillsynsmyndigheterna och principen om one-stop-shop i två fall:

- Myndigheter eller privata organ som utför personuppgiftsbehandling som är nödvändig för att fullgöra en rättslig förpliktelse (artikel 6.1 c) eller nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i dennes myndighetsutövning (artikel 6.1 e). I sådana fall är alltid tillsynsmyndigheten i den berörda medlemsstaten ensam behörig (artikel 55.2). Behandling som utförs på dessa grunder måste ha stöd i nationell rätt – t.ex. genom lagstiftning – och det bör därför vara tillsynsmyndigheten i det land vars nationella rätt som ger stöd för behandlingen som är behörig.

- Klagomål från en enskild som lämnas till en tillsynsmyndighet innebär att denna tillsynsmyndighet kan behandla frågan lokalt om sakfrågan som klagomålet gäller endast rör ett verksamhetsställe i medlemsstaten eller i väsentlig grad påverkar registrerade endast i medlemsstaten (artikel 56.2). Den tillsynsmyndighet som tar emot klagomålet måste dock informera ansvarig tillsynsmyndighet och den senare har möjlighet att ta över ärendet (artikel 56.3).

I gemensamma tillsynsaktioner kan personal från andra tillsynsmyndigheter medverka vid inspektioner som utförs av Datainspektionen. Datainspektionen kan också förordna företrädare för utländska till-

18 Se vidare Artikel 29-gruppens riktlinjer om fastställande av ansvarig tillsynsmyndighet för personuppgiftsansvariga eller personuppgiftsbiträden WP 244, rev. 01.

synsmyndigheter att utföra vissa uppgifter eller att inom ramen för vissa angivna befogenheter annars agera för Datainspektionens räkning. Företrädaren för den utländska tillsynsmyndigheten omfattas i sådana fall av svenska bestämmelser om sekretess enligt offentlighets- och sekretesslagen (se prop. 2017/18:105 s. 160 f, jfr artikel 62.3).

Utländska tillsynsmyndigheter får dock inte agera på svenskt territorium utan stöd i lag eller motsvarande. Vidare har Datainspektionen inte rätt att låta utländska tillsynsmyndigheter agera på svenskt territorium med stöd av utländsk rätt.

Något om tillsyn mot statliga myndigheter och kommuner

Datainspektionen har samma befogenheter vid tillsyn mot myndigheter som vid annan tillsyn. Genom dataskyddslagen har inspektionens befogenheter enligt dataskyddsförordningen utsträckts till att gälla även vid tillsyn enligt bestämmelser i dataskyddslagen och andra föreskrifter som kompletterar dataskyddsförordningen.

Som vi tidigare har angett föreslås att Datainspektionen ska få möjlighet att ta ut sanktionsavgifter även av myndigheter. Bestämmelserna i artiklarna 83.4–6 dataskyddsförordningen ska då tillämpas men taket för de maximala beloppen är då 5 miljoner respektive 10 miljoner kronor (6 kap. 2 § dataskyddslagen).

Vid tillsyn mot svenska myndigheter och privata organ som behandlar personuppgifter med de rättsliga grunderna rättslig förpliktelse, uppgift av allmänt intresse och myndighetsutövning (artikel 6.1 c och e) är Datainspektionen alltid ensamt behörig tillsynsmyndighet. Dataskyddsförordningens bestämmelser om s.k. one-stop-shop gäller som nämnts inte vid sådan personuppgiftsbehandling (artikel 55.2).

Vid överklagan av Datainspektionens beslut i ett tillsynsärende mot myndigheter eller annan som företräder det allmänna är överklagandetiden, dvs. tiden inom vilken överklagan ska kommit in till beslutsmyndigheten, tre veckor från den dag då beslutet meddelades (23 § förvaltningslagen (1986:223), se även 44 § förslag till ny förvaltningslag).

3. Datainspektionens beslut

Beslutsprocessen hos Datainspektionen

När Datainspektionen anser att ett tillsynsärende är tillräckligt utrett skriver den ansvariga handläggaren ett utkast till beslut[19]. Vem som fattar det slutgiltiga beslutet beror på ärendets karaktär.

Datainspektionens chef, generaldirektören, fattar beslut i tillsynsärenden när beslutet gäller frågor som är av principiellt viktig karaktär; som t.ex. nya företeelser, betydelsefulla ändringar av myndighetens tidigare praxis eller massmedialt eller politiskt uppmärksammade ärenden.[20] I övrigt fattas beslut i tillsynsärenden av enhetscheferna eller av ansvarig handläggare. Beslut av mindre betydelse och som ligger inom ramen för tidigare fastställd praxis fattas normalt av den ansvarige handläggaren själv. Rutinerna för beslutsfattande varierar dock mellan de olika enheterna.

Det har hittills varit mycket ovanligt att Datainspektionen skickar ett beslutsutkast till den personuppgiftsansvarige för synpunkter, men det har förekommit i några enstaka fall. Det kan dock hända att handläggaren kontrollerar en faktauppgift per telefon eller via e-post i ett sent skede i handläggningen.

Beslutsprocessen kan komma att förändras med dataskyddsförordningen. Det gäller särskilt när tillsynsärendet gäller gränsöverskridande behandling som sker i flera EU/EES-länder (se nedan).

Beslut enligt PuL

Enligt 45 § PuL ska Datainspektionen ”genom påpekanden eller liknande förfaranden försöka åstadkomma rättelse” om myndigheten dessförinnan har konstaterat att personuppgifter behandlas, eller kan komma att behandlas, på ett olagligt sätt. Endast om det inte går att få rättelse på något annat sätt eller om saken är brådskande får Datainspektionen vid vite förbjuda den personuppgiftsansvarige att fortsätta behandla personuppgifter på något annat sätt än genom att lagra dem. Datainspektionen kan även vitesförelägga en personuppgiftsansvarig som inte frivilligt följer ett beslut om säkerhetsåtgärder.

I syfte att undvika tveksamheter i fråga om beslut är överklagbara

19 Redogörelsen i detta avsnitt bygger bl.a. på Datainspektionens arbetsordning daterad 2018-01-01.

20 Datainspektionens arbetsordning 2018-01-01.

brukar Datainspektionen erfarenhetsmässigt formulera sina beslut med förelägganden i stället för påpekanden som anges i 45 § PuL. Det förekommer att beslut också innehåller rekommendationer som enligt Datainspektionens mening inte har varit avsedda att vara överklagbara.

Om Datainspektionen konstaterar allvarligare brister i den personuppgiftsansvariges personuppgiftsbehandling förekommer det att Datainspektionen väljer att besluta om s.k. åtgärdsplan. Det innebär att den personuppgiftsansvarige får en fastställd tid på sig att åtgärda bristerna och redovisa dessa för Datainspektionen. Ärendet följs upp efter den utsatta tiden med ett nytt tillsynsbeslut. Det vanligaste är dock att tillsynsbesluten avslutas med ett föreläggande om att vidta någon form av åtgärd, t.ex. informera de registrerade om en viss behandling, utan någon fastställd tid när detta ska vara genomfört och utan någon inplanerad uppföljning. Naturligtvis ser Datainspektionen allvarligt på om det vid ett senare tillfälle upptäcks, t.ex. vid en senare tillsyn eller efter klagomål, att den personuppgiftsansvarige inte följt föreläggandet.

Beslut enligt dataskyddsförordningen

Datainspektionens beslut i tillsynsärenden kommer att förändras i och med dataskyddsförordningen, framför allt med anledning av att Datainspektionen får nya korrigerande befogenheter.

Enligt dataskyddsförordningen får Datainspektionen ett antal närmare definierade ”korrigerande befogenheter” enligt artikel 58.2.

Datainspektionen kan rikta följande sanktioner mot en personuppgiftsansvarig eller ett personuppgiftsbiträde:

- utfärda en *varning* om att en planerad behandling sannolikt kommer att bryta mot bestämmelserna i dataskyddsförordningen, dataskyddslagen och andra nationella bestämmelser som kompletterar dataskyddsförordningen,

- utfärda en *reprimand* om en behandling bryter mot bestämmelserna i dataskyddsförordningen, dataskyddslagen och andra nationella bestämmelser som kompletterar dataskyddsförordningen,

- förelägga den personuppgiftsansvarige eller personuppgiftsbiträdet att *tillmötesgå den registrerades begäran* att få utöva sina rättigheter enligt dataskyddsförordningen, dataskyddslagen och andra nationella bestämmelser som kompletterar dataskyddsförordningen,

- förelägga en personuppgiftsansvarig eller ett personuppgiftsbiträde att se till *att behandlingen sker i enlighet med bestämmelserna* i dataskyddsförordningen, dataskyddslagen och andra nationella bestämmelser som kompletterar dataskyddsförordningen,

- förelägga den personuppgiftsansvarige att meddela de registrerade att en *personuppgiftsincident* har inträffat,

- införa en tillfällig eller definitiv *begränsning* av, inklusive ett förbud mot, behandling,

- *förelägga om rättelse eller radering* av personuppgifter samt begränsning av behandling enligt artiklarna 16, 17 och 18 i dataskyddsförordningen och om att underrätta mottagare till vilka personuppgifterna har lämnats ut om dessa åtgärder enligt artiklarna 17.2 och 19 i dataskyddsförordningen,

- dra tillbaka en *certifiering* eller beordra certifieringsorganet att dra tillbaka en certifiering som utfärdats enligt artikel 42 eller 43 i dataskyddsförordningen, eller beordra certifieringsorganet att inte utfärda certifiering om kraven för certifiering inte, eller inte längre, uppfylls,

- påföra administrativa *sanktionsavgifter* i enlighet med artikel 83 utöver eller i stället för andra åtgärder, beroende på omständigheterna i varje enskilt fall (se mer om detta nedan),

- förelägga att *flödet av uppgifter till en mottagare i tredje land* eller en internationell organisation ska avbrytas.

Beslut vid behandling i flera EU/EES-länder

Vid behandling som utförs vid flera verksamhetsställen i flera olika länder inom EU/EES (gränsöverskridande behandling) leds tillsynen av den ansvariga tillsynsmyndigheten, vilket normalt är tillsynsmyndigheten där den personuppgiftsansvarige eller personuppgiftsbiträdet har sitt huvudkontor (se ovan). Denna myndighet samordnar övriga berörda tillsynsmyndigheter och tar fram ett utkast till tillsynsbeslut. De berörda tillsynsmyndigheterna har därefter fyra veckor på sig att lämna invändningar mot beslutsutkastet (artikel 60).

Om det inte lämnas några invändningar fattar den ansvariga tillsynsmyndigheten beslut och informerar de berörda tillsynsmyndigheterna om detta. Den personuppgiftsansvarige eller personuppgiftsbiträdet som berörs av beslutet ska, efter en tidsperiod som fastställs av den ansvariga tillsynsmyndigheten, meddela denna vilka åtgärder som har vidtagits för att efterleva beslutet. Den ansvariga tillsynsmyndigheten ska därefter informera de andra berörda tillsynsmyndigheterna.

Om den ansvariga tillsynsmyndigheten och övriga berörda tillsynsmyndigheter inte kan komma överens kan frågan komma att lyftas till Europeiska dataskyddstyrelsen för beslut. Sådana beslut fattas i första hand av två tredjedels majoritet av styrelsens ledamöter inom en månad med möjlighet till en ytterligare månads förlängning vid komplicerade fall (artikel 65.2). Om styrelsen inte har kunnat fatta

beslut under denna tid kan beslut därefter fattas med enkel majoritet. Styrelsens ordförande har i sådana fall utslagsröst (artikel 65.3).

Den ansvariga tillsynsmyndigheten ska därefter anta ett slutgiltigt beslut på grundval av styrelsens beslut senast en månad efter det att styrelsen fattade sitt beslut. Det slutgiltiga beslutet ska hänvisa till styrelsens beslut.

Pressmeddelande

Efter att beslutet fattats ska det skickas till tillsynsobjektet. Om Datainspektionen bedömer att det finns ett intresse av beslutet hos andra än de som direkt berörs av det är det vanligt att myndigheten tar fram ett *pressmeddelande* som publiceras på Datainspektionens webbplats och skickas via e-post till de som har anmält sig till sådana utskick.[21] Pressmeddelandet skickas normalt några dagar efter att beslutet har skickats till tillsynsobjektet. Tanken är att tillsynsobjektet ska få tid på sig att förbereda sig om det kommer frågor från massmedia om beslutet.

Syftet med pressmeddelandena är främst att ge vägledning för andra som ska tillämpa bestämmelserna. Det är inte alltid som namn på tillsynsobjektet anges i pressmeddelandet. Exempelvis undviker Datainspektionen enligt uppgift att namnge mindre företag och när det av andra skäl inte är motiverat att ange namnet på tillsynsobjektet.

Sanktionsavgifter

Med dataskyddsförordningen får Datainspektionen möjlighet att besluta om s.k. administrativa sanktionsavgifter. Sanktionsavgift kan påföras antingen istället för, eller i kombination med, annan åtgärd såsom en reprimand eller ett föreläggande efter det att myndigheten har konstaterat att en personuppgiftsansvarig eller ett personuppgiftsbiträde har överträtt en bestämmelse i förordningen (artikel 58.3 i och 83). Av 6 kap. 2 § dataskyddslagen framgår att Datainspektionen kan besluta om sanktionsavgift även mot myndigheter, om än med lägre belopp.

Av dataskyddslagen framgår också att sanktionsavgift kan beslutas vid överträdelser av bestämmelsen om att behandla personuppgifter om lagöverträdelser (6 kap. 3 §), som av någon anledning (förmodligen av misstag) inte nämns i artikel 83.

Hur sanktionsavgifterna kommer att användas och hur stora avgifterna blir kommer att framgå först med praxis från Datainspektionen och de övriga tillsynsmyndigheterna. Avsikten är, och det finns anledning att utgå från, att praxis på detta område kommer att harmoniseras

21 https://www.datainspektionen.se/press/nyhetsbrev/

inom EU. Det är inte troligt att en medlemsstat kommer tillåtas ha en praxis med färre avgiftsbeslut och lägre avgiftsnivåer som märkbart skiljer sig från övriga medlemsstater. För Sverige och svenska företag kan det innebära en större omställning eftersom det i flera medlemsstater redan förekommer sanktionsavgifter och att dessa är relativt höga.

Artikel 29-gruppen, som är en oberoende rådgivande arbetsgrupp i frågor rörande dataskydd och integritet, har publicerat en vägledning i syfte att skapa en gemensam grund för tillsynsmyndigheternas bedömningar avseende sanktionsavgifter.[22] I den nämnda vägledningen förespråkar Artikel 29-gruppen en balanserad inställning till sanktionsavgifter:

"Sanktionsavgifter är viktiga verktyg som tillsynsmyndigheterna bör använda under lämpliga förhållanden. För att överträdelser ska få påföljder som är både effektiva och avskräckande men samtidigt proportionella uppmanas tillsynsmyndigheterna att använda en genomtänkt och balanserad strategi för sina korrigerande åtgärder. Det viktiga är att inte behandla sanktionsavgifter som en sista utväg eller tveka att påföra dem men att inte heller använda dem på ett sätt som gör att deras effektivitet urholkas."[23]

Vägledningen kommer troligen följas upp av Europeiska dataskyddstyrelsen när den börjar sin verksamhet den 25 maj 2018 (artikel 70.1 k).[24] De nationella tillsynsmyndigheternas beslut om sanktionsavgifter kan som nämnts komma under styrelsens bedömning när det handlar om gränsöverskridande behandling och det råder oenighet mellan tillsynsmyndigheterna (artikel 65).

HUR STORA BLIR AVGIFTERNA?

Avgifternas storlek beror på flera olika faktorer och ska beslutas utifrån förutsättningarna i det enskilda fallet. Avgiften ska bestämmas på ett sätt som är "effektivt, proportionellt och avskräckande" med hänsyn till ett antal angivna faktorer som anges i förordningen (artikel 83.1). Det finns två nivåer på avgifternas storlek som beror på överträdelsens allvarlighet.

Den lägre avgiftsnivån innebär en avgift på upp till 10 miljoner euro, eller om det gäller ett företag, upp till 2 procent av den totala globala årsomsättningen under föregående budgetår om det innebär en högre avgift än 10 miljoner euro. Sådana avgifter tas ut för personuppgiftsansvariga eller personuppgiftsbiträden för överträdelser av följande bestämmelser:

22 Riktlinjer för tillämpning och fastställande av administrativa sanktionsavgifter i enlighet med förordning 2016/679.

23 Riktlinjer för tillämpning och fastställande av administrativa sanktionsavgifter i enlighet med förordning 2016/679, s. 7.

24 Europeiska dataskyddsstyrelsen kommer att ersätta Artikel 29-gruppen.

- Villkor som gäller för barns samtycke avseende informationssamhällets tjänster (artikel 8)
- Behandling som inte kräver identifiering (artikel 11)
- Inbyggt dataskydd och dataskydd som standard (artikel 25)
- Gemensamt personuppgiftsansvariga (artikel 26)
- Företrädare för personuppgiftsansvariga eller personuppgiftsbiträden som inte är etablerade i unionen (artikel 27)
- Personuppgiftsbiträden (artikel 28)
- Behandling under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende (artikel 29)
- Register över behandlingar (artikel 30)
- Samarbete med tillsynsmyndigheten (artikel 31)
- Säkerhet i samband med behandlingen (artikel 32)
- Anmälan av en personuppgiftsincident till tillsynsmyndigheten (artikel 33)
- Information till den registrerade om en personuppgiftsincident (artikel 34)
- Konsekvensbedömning avseende dataskydd (artikel 35)
- Förhandssamråd (artikel 36)
- Utnämning av dataskyddsombudet (artikel 37)
- Dataskyddsombudets ställning (artikel 38)
- Dataskyddsombudets uppgifter (artikel 39)
- Certifiering (artikel 42)
- Certifieringsorgan (artikel 43)

Den högre avgiftsnivån innebär en avgift på upp till 20 miljoner euro eller, om det är ett företag, upp till 4 procent av totala globala årsomsättningen för föregående budgetår om det innebär en högre avgift än 20 miljoner euro. Sådana avgifter tas ut för personuppgiftsansvariga eller personuppgiftsbiträden för överträdelser av följande bestämmelser (artikel 83.5):

- De grundläggande principerna för behandling, inklusive villkoren för samtycke, enligt artiklarna 5, 6, 7 och 9
- Registrerades rättigheter enligt artiklarna 12–22
- Överföring av personuppgifter till en mottagare i ett tredjeland eller en internationell organisation enligt artiklarna 44–49
- Alla skyldigheter som följer av medlemsstaternas lagstiftning som antagits på grundval av kapitel IX (Bestämmelser om särskilda behandlingssituationer, t.ex. användning av personnummer)
- Underlåtenhet att rätta sig efter ett föreläggande eller en tillfällig eller permanent begränsning av behandling av uppgifter eller ett beslut om att avbryta uppgiftsflödena som meddelats av tillsynsmyndigheten i enlighet med artikel 58.2 eller underlåtelse att ge tillgång till uppgifter i strid med artikel 58.1

Den högre avgiftsnivån gäller även om en personuppgiftsansvarig eller ett personuppgiftsbiträde underlåter att rätta sig efter ett föreläggande som tillsynsmyndigheten beslutat, t.ex. ett föreläggande att radera personuppgifter (artikel 83.6).

Både i frågan om sanktionsavgifter ska beslutas och frågan om hur

stora avgifterna ska vara, är utgångspunkten för Datainspektionens beslut som nämnts att avgiften i varje enskilt fall är effektiv, proportionell och avskräckande (artikel 83.1). Hänsyn ska tas till följande bedömningskriterier (art 83.2):

a) Överträdelsens karaktär, svårighetsgrad och varaktighet med beaktande av den aktuella uppgiftsbehandlingens karaktär, omfattning eller syfte samt antalet berörda registrerade och den skada som de har lidit.

b) Om överträdelsen skett med uppsåt eller genom oaktsamhet.

c) De åtgärder som den personuppgiftsansvarige eller personuppgiftsbiträdet har vidtagit för att lindra den skada som de registrerade har lidit.

d) Graden av ansvar hos den personuppgiftsansvarige eller personuppgiftsbiträdet med beaktande av de tekniska och organisatoriska åtgärder som genomförts av dem i enlighet med artiklarna 25 (inbyggt dataskydd och dataskydd som standard) och 32 (säkerhet i samband med behandlingen).

e) Eventuella relevanta tidigare överträdelser som den personuppgiftsansvarige eller personuppgiftsbiträdet gjort sig skyldig till.

f) Graden av samarbete med tillsynsmyndigheten för att komma till rätta med överträdelsen och minska dess potentiella negativa effekter.

g) De kategorier av personuppgifter som påverkas av överträdelsen.

h) Det sätt på vilket överträdelsen kom till tillsynsmyndighetens kännedom, särskilt huruvida och i vilken omfattning den personuppgiftsansvarige eller personuppgiftsbiträdet anmälde överträdelsen.

i) I fall åtgärder enligt artikel 58.2 (korrigerande åtgärder beslutade av tillsynsmyndigheten) tidigare har förordnats mot den berörda personuppgiftsansvarige eller personuppgiftsbiträdet vad gäller samma sakfråga, efterlevnad av dessa åtgärder.

j) Tillämpandet av godkända uppförandekoder i enlighet med artikel 40 eller godkända certifieringsmekanismer i enlighet med artikel 42.

k) Eventuell annan försvårande eller förmildrande faktor som är tillämplig på omständigheterna i fallet, såsom ekonomisk vinst som görs eller förlust som undviks, direkt eller indirekt, genom överträdelsen.

BERÄKNING AV SANKTIONSAVGIFT FÖR FÖRETAG I KONCERNER

När tillsynsmyndigheten beslutar om sanktionsavgifter för ett företag

kan avgiften som nämnts komma att beräknas utifrån viss andel av företagets globala årsomsättning.

I skäl 150 till dataskyddsförordningen sägs att ett företag i detta sammanhang ska anses vara ett företag i den mening som avses i artiklarna 101 och 102 i EUF-fördraget. De nämnda bestämmelserna avser EU:s konkurrensregler. Enligt praxis från EU-domstolen omfattar begreppet företag (”an undertaking”) i dessa sammanhang ”varje enhet som bedriver ekonomisk verksamhet, oavsett enhetens rättsliga form och oavsett hur den finansieras”[25]. EU-domstolen har även preciserat att begreppet företag ska förstås som en ekonomisk enhet med beaktande av avsikten med ett avtal mellan parterna, även om enheten i juridisk mening består av flera fysiska eller juridiska personer.[26] Om det företag som har överträtt förordningen ingår i en koncern (i juridisk mening) eller i en annan form av sammanslutning av företag som kan betraktas som en ekonomisk enhet så kan – i analogi med hur begreppet ”undertaking” tolkats i konkurrensrätt – omsättningen som ligger till grund för beräkningen av sanktionsavgiften avse den totala omsättningen i koncernen/den ekonomiska enheten.

Överklagan

HUR ÖVERKLAGAS DATAINSPEKTIONENS BESLUT?

Den personuppgiftsansvarige eller personuppgiftsbiträdet som blir föremål för Datainspektionens tillsyn har rätt att överklaga inspektionens tillsynsbeslut om beslutet gått denne emot (22 § förvaltningslagen (1986:223))[27] och under förutsättning att det är ett överklagbart beslut (7 kap. 3–5 §§ dataskyddslagen, jfr artikel 78.1 dataskyddsförordningen).

Överklagandeskriften ska komma in till Datainspektionen inom tre veckor från den dag då den som överklagar beslutet *fick del av beslutet*. Om överklagan görs av myndigheter eller andra som företräder det allmänna ska överklagan komma in till Datainspektionen senast tre veckor efter *beslutsdatumet*. När Datainspektionen skickar beslut till enskilda, dvs. företag, organisationer och privatpersoner, bifogas ett delgivningskvitto.

Överklagandet ska lämnas in till Datainspektionen som efter en prövning om beslutet har kommit in i rätt tid skickar överklagandet vidare till Förvaltningsrätten i Stockholm.

---

25 Se även definitionen i artikel 4.18.

26 Se närmare artikel 29-gruppens *Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679*, Adopted on 3 October 2019 WP 253 s. 6 och där anförda rättsfall.

27 Enligt den nya förvaltningslagen som träder i kraft 1 juli 2018 kan beslut överklagas om det kan antas påverka någons situation på ett inte obetydligt sätt. Bestämmelsen ger uttryck för de principer som Högsta förvaltningsdomstolen har tillämpat (se 41 § lagförslaget, prop. 2016/17:180, s. 332).

Om beslutet grundar sig på ett yttrande eller beslut från Europeiska dataskyddsstyrelsen ska Datainspektionen vidarebefordra detta yttrande eller beslut till domstolen (artikel 78.4).

Sekretess hos Datainspektionen

Alla handlingar som lämnas in till Datainspektionen blir allmänna handlingar som kan begäras ut från myndigheten av vem som helst. Det gäller även allt som lämnas till Datainspektionens företrädare vid en fältinspektion eller skickas till dessa via epost, sms eller på annat sätt. Datainspektionens företrädare har dessutom en skyldighet att göra tjänsteanteckningar av det som sägs t.ex. vid ett telefonsamtal om det kan ha betydelse för ärendet och om det avser myndighetsutövning mot enskild (15 § förvaltningslagen).

VAD OMFATTAS AV SEKRETESS?

Datainspektionen får inte lämna ut sådant som omfattas av sekretess enligt offentlighets- och sekretesslagen. För uppgifter som omfattas av sekretess gäller även en tystnadsplikt för befattningshavare hos Datainspektionen. Det finns ett antal olika sekretessgrunder som Datainspektionen kan använda. De vanligaste är följande:

- Sekretess gäller för uppgift om en *enskilds personliga eller ekonomiska förhållanden* om det kan antas att den enskilde eller någon närstående till denne lider skada eller men om uppgiften röjs (32 kap. 1 § offentlighets- och sekretesslagen). Med ”enskilda” avses såväl fysiska som juridiska personer. Sekretessbestämmelsen gäller således även uppgifter som avslöjar den personuppgiftsansvariges eller personuppgiftsbiträdets företagshemligheter och andra affärs- eller driftförhållanden.

- Sekretess gäller för uppgift som lämnar eller kan bidra till upplysning om säkerhets- eller bevakningsåtgärd, om det kan antas att syftet med åtgärden motverkas om uppgiften röjs och åtgärden avser bl.a. byggnader eller andra anläggningar, lokaler eller inventarier, telekommunikation eller system för automatiserad behandling av information, behörighet att få tillgång till upptagning för automatiserad behandling (18 kap. 8 § offentlighets- och sekretesslagen). Bestämmelsen omfattar både redan genomförda åtgärder och planerade säkerhetsåtgärder. Den kan även omfatta information som lämnas i samband med en incidentrapportering enligt artikel 33 i dataskyddsförordningen.

De ovan nämnda sekretessbestämmelserna har s.k. rakt skaderekvisit vilket innebär att det finns en presumtion för offentlighet, dvs. att uppgiften ska lämnas ut. Presumtionen bryts om det finns anledning att anta att skada uppstår om uppgiften röjs. I sådana fall omfattas uppgiften av sekretess och får inte lämnas ut eller röjas av myndighetens personal. Ett rakt skaderekvisit innebär vanligtvis att det är

uppgifternas karaktär som får avgöra om sekretess gäller eller inte. Om uppgiften är sådan att den genomsnittligt sett måste betraktas som harmlös ska den alltså normalt anses vara offentlig. Om uppgiften i stället typiskt sett måste betraktas som känslig omfattas den normalt av sekretess. Skaderekvisitet kan alltså uppfattas som en metod att precisera föremålet för sekretessen eller dess räckvidd (se prop. 2017/18:105 s. 128).

Datainspektionen har föreslagit att ett förstärkt sekretesskydd, dvs. absolut sekretess eller omvänt skaderekvisit, i viss utsträckning ska gälla för dess verksamhet[28]. Regeringen har dock gjort bedömningen att de befintliga sekretessbestämmelserna ger ett tillräckligt skydd för skyddsvärda uppgifter i Datainspektionens verksamhet (se prop. 2017/18:105 s. 126 ff).

SEKRETESSPRÖVNING I PRAKTIKEN

En sekretessprövning görs när någon begär ut handlingar. I första hand görs en preliminär sekretessbedömning av ansvarig handläggare. Den som begär handlingarna kan då få ut handlingarna i sin helhet eller med s.k. maskning av de delar som omfattas av sekretess, dvs. att de sekretessbelagda delarna stryks över eller på annat sätt döljs. Det är vanligt att handläggaren tar kontakt med tillsynsobjektet och frågor vilka delar som kan omfattas av sekretess och vad som är skälen för detta. Det är dock alltid handläggaren som självständigt avgör vad som ska lämnas ut och vad som inte ska lämnas ut. Erfarenhetsmässigt är det långt ifrån säkert att handläggaren delar tillsynsobjektets inställning.

Om den som begär ut handlingarna inte är nöjd med det som denne har fått ut har han eller hon en rätt att få ett skriftligt beslut från myndigheten som kan överklagas (6 kap. 3 § offentlighets- och sekretesslagen 2009:400). Sådana beslut fattas av särskilt förordnade tjänstemän på myndigheten.

Det är värt att uppmärksamma att Datainspektionens verksamhet, liksom många andra myndigheters verksamheter, kontinuerligt bevakas av nyhetsbyrån Siren. Nyhetsbyrån samlar systematiskt och regelbundet in allmänna handlingar som kommer från myndigheten. Alla handlingar blir sökbara i deras databaser som normalt endast tillhandahålls journalister. Insamlingen sker med stöd av offentlighetsprincipen och innebär att en begäran om utlämnande skickas till myndigheten en eller flera gånger i veckan. Från Datainspektionen inhämtas bl.a inspektionens beslut om att inleda tillsyn och underliggande anmälan, beslut i tillsynsärenden och underliggande anmälan, skrivelser till polis, åklagare och domstolar.

28 Se Datainspektionens skrivelse till Justitiedepartementet den 17 juli 2017, Dnr 1704-2017.

4. Hur kan tillsynsverksamheten komma att förändras med anledning av dataskyddsförordningen?

HARMONISERING FÅR KONSEKVENSER FÖR TILLÄMPNINGEN

Ett av skälen till att införa dataskyddsförordningen var att komma till rätta med den bristande enhetligheten i genomförandet av dataskyddsregleringen i olika medlemsstater som dataskyddsdirektivet har medfört. Det har ansetts att sådana brister kan utgöra ett hinder för att bedriva ekonomisk verksamhet på unionsnivå, snedvrida konkurrensen och hindra myndigheterna att fullgöra sina skyldigheter enligt unionsrätten (se skäl 9). Det finns därför ett starkt intresse av en ökad harmonisering inom dataskyddsregleringen. Det var också skälet till att det blev en förordning och inte ett direktiv som hade gett medlemsstaterna större frihet att behålla avvikande lagstiftning.

Harmoniseringen innebär att utrymmet för nationell särlagstiftning inom förordningens tillämpningsområde minskar betydligt. Den svenska missbruksregeln i 5 a § PuL är en sådan regel som inte är förenlig med dataskyddsförordningen och därför försvinner.

Harmoniseringen kräver också en mer enhetlig tillämpning av reglerna. Det i sin tur leder till att tillsynsmyndigheterna i de olika medlemsstaterna måste ha en enhetlig tolkning av bestämmelserna i förordningen. Principen om one-stop-shop, dvs. att personuppgiftsansvariga och personuppgiftsbiträden bara ska behöva ha kontakt med en tillsynsmyndighet, innebär också att tillsynsmyndigheterna måste samarbeta i betydligt större omfattning än tidigare. Dataskyddsförordningen innehåller av detta skäl ett antal bestämmelser om skyldigheter för tillsynsmyndigheter att samarbeta (artikel 51.2) och om hur tillsynsmyndigheterna ska samarbeta och tillsammans åstadkomma en enhetlig tillämpning av förordningen (artikel 60–67). För denna uppgift inrättas även Europeiska datasskyddsstyrelsen som ett självständigt EU-organ (artikel 68). Styrelsen har bl.a. till uppgift att lösa tvister mellan tillsynsmyndigheterna t.ex. i gemensamma tillsynsärenden (artikel 65).

Mot den bakgrunden finns det anledning att anta att Datainspektionens sätt att utöva tillsyn kommer att förändras. Det tidigare förhållandevis informella och flexibla förhållningssättet som Datainspektionen har haft under tiden med PuL kan komma att påverkas av det mer byråkratiska och striktare förhållningssätt som många tillsynsmyndigheter i Europa har haft sedan många år. En motsatt trend kan dock skönjas i den vägledning om dataskyddsförordningen som under

det senaste året har publicerats av många tillsynsmyndigheter. Stor vikt läggs numera på det förebyggande arbetet, dvs. att hjälpa personuppgiftsansvariga och personuppgiftsbiträden att göra rätt.[29]

Digitaliseringen av samhället och utvecklingen av den digitala inre marknaden kommer också innebära att tillsynsmyndigheterna måste vara mer proaktiva och bistå med vägledning för att hitta integritetsvänliga lösningar vid användning av nya tekniska företeelser. EU-kommissionen som deltar i dataskyddsstyrelsens verksamhet (dock utan rösträtt), har en viktig funktion för att upprätthålla den inre marknaden. Det är troligt att kommissionen kommer att bevaka tillämpningen av dataskyddsförordningen och vidta åtgärder om tillämpningen i onödan innebär handelshinder för den inre marknaden.

MER SYSTEMATISKT INRIKTAD TILLSYN

Med dataskyddsförordningen kommer Datainspektionen att få ett mer omfattande och bättre underlag för att bedöma inriktningen på tillsynsverksamheten. Klaganden, dvs. den registrerade som gör gällande att dennes personuppgifter har behandlats i strid med dataskyddsförordningen, får en starkare ställning. Som en konsekvens av detta kommer troligen inflödet av klagomål till Datainspektionen att öka.

Även om Datainspektionen saknar möjligheter att inleda tillsyn i varje klagomålsärende så kan klagomålen ligga till grund för analyser för hur tillsynsverksamheten ska inriktas. Om det t.ex. kommer in många klagomål mot ett företag eller en viss bransch under en kortare tidsperiod finns starka skäl för att inleda tillsyn. På samma sätt kan de anmälningar av personuppgiftsincidenter som Datainspektionen ska ta emot (artikel 33) också ligga till grund för tillsynsplaneringen när det gäller säkerhetsbrister vid personuppgiftshantering. Den ökade uppmärksamheten i samhället kring integritetskyddsfrågor kommer troligen att leda till att antalet tips till Datainspektionen ökar. En ytterligare källa för tillsynsplanering kommer att vara en den omvärldsbevakning som Datainspektionen planerar att införa. Slutligen ska nämnas att information från andra tillsynsmyndigheter också kan ligga till grund för tillsynsplaneringen.

Analyser av det ökade inflödet klagomål, tips och incidentanmälningar m.m. förutsätter att Datainspektionen får resurser för att skapa en organisation och att myndigheten skaffar it-system som kan hantera den omfattande informationsmängden. Regeringen har redan beslutat om ökade resurser till Datainspektionen. Det verkar dock för närvarande som om Datainspektionen har svårt att hinna med förberedelserna inför de nya arbetsuppgifterna som kommer med dataskyddsförordningen. Myndigheten kommer sannolikt att behöva växa

29 I ett pressmeddelande från regeringen 15 december 2017 annonserades bl.a. att Datainspektionens uppdrag kommer att ändras så att dess stödjande och rådgivande roll blir tydligare. http://www.regeringen.se/pressmeddelanden/2017/12/datainspektionen-blir-integritetsskyddsmyndigheten/

och förmodligen dubblera personalstyrkan från en väsentlig ökning av antalet anställda.

Bristen på kompetent personal kan naturligtvis komma att påverka myndighetens tillsynsverksamhet. Ökade krav på effektiv handläggning, mer avgränsade tillsynsärenden och mer kortfattade tillsynsbeslut kan bli konsekvenserna. Nya arbetsmetoder kan också komma behöva utvecklas. Datainspektionen skulle t.ex. kunna skicka klagomål för kännedom till den utpekade personuppgiftsansvarige eller personuppgiftsbiträdet. Det är något som Datainspektionen tidigare har ansett bara ske inom ramen för ett tillsynsärende, men som nu är en befogenhet som framgår av dataskyddsförordningen (artikel 58.1 d).

FLERA RÄTTSPROCESSER

Datainspektionens beslut i tillsynsärenden kommer att få större betydelse för personuppgiftsansvariga och personuppgiftsbiträden än tidigare. Det beror inte enbart på att Datainspektionen får möjlighet att besluta om sanktionsavgifter. Ett beslut från Datainspektionen i vilket inspektionen konstaterar att en personuppgiftsansvarig eller ett personuppgiftsbiträde har behandlat personuppgifter i strid med dataskyddsförordningen kan också ge upphov till skadeståndsanspråk från de registrerade. Även vid låga skadeståndsbelopp[30] kan kostnaderna snabbt bli omfattande eftersom det många gånger handlar om ett stort antal registrerade. Därtill kommer att ett beslut från Datainspektionen kan få konsekvenser för företagens affärsverksamhet eller innebära krav på att bygga om it-system.

Sammantaget medför detta enligt vår bedömning att Datainspektionens beslut i tillsynsärenden troligen kommer att överklagas i betydligt större omfattning än tidigare.

30 Enligt Högsta domstolen bör ersättningsnivån för kränkning avseende agerande i strid mot personuppgiftslagen i fall som inte kan anses allvarliga ligga under 5 000 kr. Ersättningen för en kränkning som är att bedöma som mindre allvarlig, om än inte helt obetydlig, bör normalt bestämmas till ett schablonbelopp på 3 000 kr (NJA 2013 s. 1046).

5. Förberedelser och beredskap

Allmänt

I allmän mening kan ett väl genomfört GDPR-anpassningsprojekt betraktas som en första förberedelseåtgärd som rustar den personuppgiftsansvarige eller personuppgiftebiträdet för en tillsyn. Genom den genomlysning och den dokumentation, de processer och de rutiner och den medvetenhet inom organisationen som har skapats genom projektet, så har organisationen skapat goda förutsättningar för att hantera en tillsyn på ett bra sätt.

När en organisation väl står inför en tillsyn ställs de genomförda anpassningsprojekten och den interna dataskyddsorganisationen på prov. Vid all form av tillsyn gäller som utgångspunkt att en organisation som granskas har mycket att vinna på att så långt som möjligt samarbeta i god anda med den myndighet som utövar tillsynen. Mot detta ska ställas det oundvikliga behovet hos den granskade organisationen att ges rådrum för att samla sig och på så sett kunna hantera tillsynen på bästa sätt.

Enligt vår bedömning är den avgörande faktorn för god beredskap inför tillsynsärenden att ha en etablerad och välorganiserad intern dataskyddsorganisation som med kort varsel kan mobilisera såväl interna som externa resurser och som dessutom har all nödvändig dokumentation samlad och lätt tillgänglig.

Nedan presenterar vi en checklista och pekar på några mer konkreta förberedelseåtgärder.

Checklista

☐ **UTSE HUVUDANSVARIG FÖR REVISIONEN**
En betydelsefull åtgärd är att utse en person som huvudansvarig för organisationens hantering av tillsynen. En viktig uppgift är att se till att organisationen tidigt kommer igång med förberedelserna inför inspektionen, såsom att identifiera syftet med tillsynen, ta fram efterfrågad information och annan relevant information, läsa in sig på materialet, förbereda en allmän redogörelse för den personuppgiftsbehandling som är föremål för granskning, förbereda svar på Datainspektionens frågor och att förbereda relevant personal på att närvara och biträda vid inspektionen.

Kontaktpersonen behöver också se till att praktiska detaljer genomförs, t.ex. att boka lämpliga lokaler och att se till att relevanta personer är tillgängliga liksom att extern juridisk och teknisk expertis anlitas vid behov så snart som möjligt.

I vart fall vid mer omfattande inspektioner kan det vara lämpligt att utse ett team som ansvarar för inspektionen, där olika personer från t.ex. olika avdelningar eller funktioner inom organisationen ansvarar för olika delområden.

Syftet med att utse huvudansvarig/tillsynsteam är att få till en samordnad och koordinerad insats från organisationen och, givetvis, att samla in den information som behövs. Olika delar av en organisation kan tala med olika ”språk” och ha olika infallsvinklar. Genom en samordnad insats pratar myndigheten eller företaget med en röst.

Alla kontakter som organisationen tar med Datainspektionen, t.ex. framställande av klarläggande frågor bör kanaliseras genom den huvudansvarige.

Av erfarenhet är det betydelsefullt att arbeta på motsvarande sätt även inför en skrivbordsinspektion eller en enkätinspektion Detta särskilt som sådana tillsynsåtgärder kan komma att följas upp av en fältinspektion.

☐ **IDENTIFIERA SYFTET MED TILLSYNEN**

Det är viktigt att identifiera syftet med Datainspektionens tillsyn. Det är syftet som anger ramarna för undersökningen och för vilka förberedelser som organisationen behöver vidta.

Syftet med tillsynen framförs av Datainspektionen vid de inledande kontakterna med organisationen och bör formaliseras i Datainspektionens tillsynsskrivelse. Organisationen bör även väga in de skriftliga frågor som kan ha ställts i det tidigare skedet av förfarandet och i förekommande fall i den föregående skrivbordstillsynen eller enkättillsynen. Vid eventuella oklarheter rörande syftet med tillsynen är det viktigt att söka klarlägganden från Datainspektionen.

Som framgått tidigare avgränsas tillsynen normalt till specifika behandlingar, behandlingsfenomen eller företeelser. Det kan inte uteslutas att Datainspektionen, åtminstone under en tid framöver, kan komma att formulera bredare tillsynssyften för att mer allmänt kontrollera hur väl företag och myndigheter har lyckats förbereda sig för dataskyddsförordningen. Förmodligen är skrivbordstillsyn och enkättillsyn mer lämpliga tillsynsformer för detta, men det kan inte uteslutas att uppföljningar i viss utsträckning kan komma att ske genom fältinspektioner.

☐ **SE TILL ATT FÖR TILLSYNEN RELEVANT DOKUMENTATION FINNS OCH HÅLLS UPPDATERAD**

Inom ramen för en fältinspektion efterfrågar Datainspektionen normalt olika former av dokumentation kring organisationens personuppgiftsbehandling. Inför en fältinspektion bör man samla in sådan dokumentation som, baserat på syftet med tillsynen, bedöms vara relevant. Lämpligen samlas dokumenten på ett organiserat

sätt i en pärm eller motsvande. Dokumenten bör vara i kopierad form så att de direkt kan lämnas över till Datainspektionen, om det begärs.

Som en första åtgärd bör förstås organisationen ta fram den dokumentation som uttryckligen har begärts av Datainspektionen.

Ett dokument som förmodligen kommer att få stor betydelse vid framtida tillsynsärenden är det register över personuppgiftsbehandlingar som ska föras av personuppgiftsansvariga och personuppgiftsbiträden (artikel 30). Om det inte redan har överlämnats eller efterfrågats bör dokumentet tas fram inför besöket.

Annan typ av dokumentation som typiskt sett kan komma att begäras av Datainspektionen är organisationens policyer för behandling av personuppgifter, information till registrerade, riskanalyser, konsekvensbedömningar och dokumentation över personuppgiftsincidenter etc. I förekommande fall bör samtyckestexter och dokumenterade rutiner för inhämtande och återkallande av samtycke tas fram. När det gäller konsekvensbedömningar och personuppgiftsincidenter bör man i förekommande fall ta fram eventuella motiveringar till varför en konsekvensbedömning inte har bedömts nödvändig eller varför en personuppgiftsincident inte har anmälts till Datainspektionen. Det är i sammanhanget viktigt att notera att alla personuppgiftsincidenter måste dokumenteras (artikel 33.5), alltså inte bara sådana incidenter som har anmälts till Datainspektionen.

Beroende på tillsynens ändamål kan även annan dokumentation komma att begäras av Datainspektionen i det enskilda fallet. Frågan om vilken information som i det enskilda fallet kan och bör lämnas till Datainspektionen beror på tillsynens syfte.

☐ **SEKRETESS**

I samband med att dokumentationen tas fram bör man överväga i vilken utsträckning det finns anledning att begära att handlingarna ska behandlas med sekretess hos Datainspektionen. Exempelvis kan man förbereda extra kopior där de delar som organisationen anser bör behandlas med sekretess är maskerade. Se närmare om detta i det tidigare avsnittet *Sekretess hos Datainspektionen*.

☐ **VILKA FRÅGOR KAN KOMMA ATT STÄLLAS VID FÄLTINSPEKTIONEN?**

I tillsynsskrivelsen kan Datainspektionen ha ställt ett antal frågor som myndigheten vill ha svar på. Svar på dessa frågor behöver förberedas.

Tillsynsobjektet kan även förvänta sig att olika uppföljande frågor ställs, t.ex. för att skapa klarlägganden och förtydliganden eller för att utveckla organisationen inställning på olika punkter.

Som ett led i förberedelserna inför en fältinspektion kan de frågor som anges i avsnittet *Vanliga frågor som ställs vid en fältinspektion*

tjäna som en checklista för frågor som erfarenhetsmässigt ofta dyker upp. Vilka frågor som är relevanta för ett visst projekt beror på syftet med tillsynen. Att ta sig igenom frågorna och formulera en inställning kan vara en god förberedelse inför en fältinspektion.

Även vid besvarandet av muntliga frågor bör organisationen tänka på sekretessen. Om exempelvis organisationens it- eller informationssäkerhet diskuteras kan det vara lämpligt att begära att informationen enligt organisationens uppfattning ska behandlas med sekretess hos Datainspektionen.

Frågan om vilka svar som i det enskilda fallet kan och bör lämnas till Datainspektionen beror på tillsynens syfte.

☐ VILKA PERSONER BÖR NÄRVARA VID EN FÄLTINSPEKTION?

I första hand är det Datainspektionens önskemål som styr vilka personer som bör närvara vid en fältinspektion. Som tidigare nämnts är det ett vanligt önskemål från Datainspektionen att följande personer är närvarande vid inspektionen:

- personer som fattar beslut om personuppgiftsbehandlingen
- personuppgiftsombud, om sådant har utsetts
- jurist eller advokat med kompetens inom dataskydd
- personer med kunskap om för tillsynen aktuella it-system

Det finns inget som hindrar att den personuppgiftsansvarige eller personuppgiftsbiträdet även tar med andra personer, exempelvis extern juridisk eller teknisk expertis, om det bedöms som relevant för tillsynen. Det är alltid den granskade organisationen som bestämmer vilka personer från denne som ska närvara. Ibland kan det också tänkas vara lämpligt att personer från personuppgiftsbiträden närvarar vid inspektionen.

Det är inte nödvändigtvis så att alla personer behöver medverka under hela inspektionen. Organisationens huvudansvarige, eller annan representant för tillsynsteamet, bör dock typiskt sett medverka under hela inspektionen.

Man kan fråga sig om en representant från en systemleverantör bör medverka vid en fältinspektion.[31] Enligt vår mening bör detta inte ske, annat än om det uttryckligen har begärts (exempelvis om tillsynen är inriktad på ”inbyggt dataskydd” eller ”dataskydd som standard”). Komplicerade tekniska frågor bör i första hand tas om hand under förberedelsen inför besöket. Om Datainspektionens frågor vid en fältinspektion skulle vara av sådan ingående teknisk natur att systemleverantören behöver kontaktas, är det bättre att be att få återkomma med skriftligt svar senare. En fältinspektion är knappast rätt forum att besvara den typen av frågor, särskilt om leverantörens agenda inte överensstämmer med tillsynsobjektets inställning.

31 Jfr. Integritet i fokus nr 1/2015 s. 6f.

☐ **UPPFÖLJNING**

Datainspektionen dokumenterar fältinspektionen i ett protokoll som den granskade organisationen får tillfälle att kommentera. Det kan även förekomma uppföljande frågor från Datainspektionen efter fälttillsynen. Genomgång av och framtagande av eventuella synpunkter på protokollet liksom besvarandet av eventuella uppföljande frågor – liksom för den delen hantering av eventuellt överklagande – bör hanteras under ledning av den huvudansvarige personen och genomföras på samma sätt som övrigt inom inspektionen.

Om man har relevanta synpunkter på protokollet är det viktigt att de framförs.

☐ **OANMÄLD INSPEKTION?**

Som tidigare nämnts har det varit mycket ovanligt att Datainspektion har genomfört oanmälda inspektioner.

Det kan dock tänkas att inslaget av oanmälda inspektioner kommer att öka med dataskyddsförordningen. Dels allmänt genom influenser från europeisk tillsynspraxis, dels, och kanske särskilt, inom ramen för gränsöverskridande tillsynsprojekt. Särskilt om någon eller några av de övriga myndigheterna genomför oanmäld inspektion och kanske till och med en gryningsräd, så kan det finnas stark önskan att även Datainspektionen gör detta.

En organisation bör om möjligt i förväg överväga hur den avser att ställa sig till en eventuell oanmäld inspektion. Det finns som sagt ingen skyldighet att mot sin vilja medverka vid en oanmäld inspektion. Mot den bakgrunden är det en rimlig strategi att förklara för Datainspektionen att organisationen inte i sig motsätter sig att tillsyn genomförs, men att man först behöver ha rimliga möjligheter att förbereda sig. Ett annat tänkbart alternativ är att låta exempelvis dataskyddsombudet eller chefsjuristen ta ställning till en begäran om oanmäld inspektion. Beroende på omständigheterna kan inspektionen vara mer eller mindre betungande.

☐ **”MOCK AUDITS”**

Med *mock audit* avser vi att man låter genomföra en simulerad tillsyn, dvs. att man anlitar en tredje part som får i uppdrag att genomföra en fiktiv tillsyn som om det vore Datainspektionen som genomförde en tillsyn. Tanken är att efterlikna ett riktigt tillsynsprojekt i så stor utsträckning som möjligt med skriftliga frågor, begäran om dokumentation och genomförande av en fältinspektion. Uppdragstagaren kan även formulera ett ”beslut” och/eller på annat sätt redogöra för sina bedömningar om hur organisationen lever upp till dataskyddsförordningens regler, hur man hanterade genomförandet av inspektionen etc.

Det är viktigt att den uppdragstagare som anlitas för en *mock audit* har betydande dataskyddskompetens och har praktisk erfarenhet av att hantera ett tillsynsärende från Datainspektionen.

En *mock audit* är ett bra verktyg för att stresstesta ett företags eller en myndighets beredskap och nivå av regelefterlevnad. Det kan ses som ett av flera möjliga verktyg inom ramen för den allmänna accountability-princip som gäller enligt dataskyddsförordningen, och ett sätt att säkerställa att organisation, rutiner och processer för dataskydd är hållbart och relevant över tid.

Man kan även tänka sig att genomföra en *mock audit* som förberedelse inför en förestående fältinspektion som har initierats av Datainspektionen. Uppdragstagaren får då med utgångspunkt från tillsynsskrivelsen och eventuellt annat skriftligt material från Datainspektionen genomföra en ”fältinspektion” för att få en uppfattning hur organisationen kan tänkas klara sig i den riktiga inspektionen. Detta förutsätter att det finns tillräckligt med tid och resurser. I första hand måste organisationen givetvis förbereda sig inför Datainspektionens besök.

6. Att tänka på under en fältinspektion/tillsyn

Allmänt

I detta avsnitt ger vi några kortfattade hållpunkter som är lämpliga att tänka på vid en fältinspektion. Datainspektionen har som tidigare nämnts inte rätt att med tvång genomföra undersökningar av organisationens lokaler eller utrustning. Gryningsräder av den typ som förekommer vid konkurrensrättsliga granskningar kommer alltså inte att aktualiseras vid sådan tillsyn som utförs av Datainspektionen enligt dataskyddsförordningen.

Det saknas därmed behov av att upprätta den typen av de detaljerade gryningsräds-checklistor/handlingsplaner som förekommer inom exempelvis konkurrensrättens område. Detta innebär dock inte att det saknas skäl för organisationen att förbereda sig inför en fältinspektion av Datainspektionen. Tvärtom, goda förberedelser skapar möjlighet att komma ut ur tillsynen på bästa sätt.

Checklista

☐ **KONTROLLERA IDENTITETEN HOS INSPEKTÖRERNA**
Rutinmässigt bör den granskade organisationen som en första åtgärd kontrollera identiteten hos inspektörerna genom att begära att de visar legitimationshandling. Inspektörerna kommer att få del av hemlig och potentiellt integritetskänslig information och det är därför viktigt att säkerställa vem eller vilka som får del av information.

För god ordnings skull kan organisationen i den inledande korrespondensen inför besöket upplysa Datainspektionen om att man avser att begära legitimation, men detta är inte en förutsättning för att kunna begära legitimation.

☐ **FÖR EGNA MINNESANTECKNINGAR**
Datainspektionen för protokoll, som man får tillfälle att yttra sig över. Som tillsynsobjekt bör man, från en bevissäkringssynpunkt, föra egna minnesanteckningar över vad som sägs.

☐ **DOKUMENTERA TILLHANDAHÅLLEN DOKUMENTATION**
Den granskade organisationen bör dokumentera vilken dokumentation som har överlämnats till Datainspektionen (både vid fälttillsynen och i övrigt), exempelvis i en särskild pärm. Även korrespondensen bör samlas.

☐ **BESVARA FRÅGOR SAKLIGT OCH KORREKT**
Svara endast på de frågor som ställts och håll dina svar kortfattade,

sakliga och korrekta. Säg inte mer än vad som behövs för att svara på frågorna.

Om en fråga är oklar eller komplex, be om ett förtydligande, gärna i skriftlig form.

☐ **SVARA INTE OM DU ÄR OSÄKER PÅ SVARET**

Svara inte på frågor om du är osäker på svaret. Be istället att få återkomma vid ett senare tillfälle eller att få ta en kort paus. Om frågan behöver utredas närmare eller stämmas av med annan befattningshavare behövs rimlig tid för detta, be i första hand att få återkomma skriftligen. Spekulera aldrig om svaret.

Observera att det i skrivande stund enligt PuL är straffbart att med uppsåt eller grov oaktsamhet lämna osann uppgift till Datainspektionen vid en tillsyn. Överträdelse kan leda till böter eller fängelse i högst sex månader eller, om brottet är grovt, till fängelse i högst två år[32]. Detta upphör att gälla i och med dataskyddsförordningen.[33] Självklart gäller dock fortfarande att man ska hålla sig till sanningen vid tillsyn. Risken för att lämnandet av en osann uppgift kan betraktas som en försvårande omständighet vid bestämmande av sanktionsavgift är uppenbar. Det kan inte heller uteslutas att lämnande av osanna uppgifter i vissa situationer skulle kunna utgöra exempelvis osant intygande enligt allmänna straffrättsliga principer.

☐ **LUNCH OCH FIKA**

Var återhållsam med att bjuda på fika, luncher etc. Det är viktigt att hålla god marginal till vad som skulle kunna uppfattas som muta.

☐ **DOKUMENTERA KÖRNINGAR I SYSTEM**

Dokumentera vilka körningar i system som genomförs av, eller på instruktion av, Datainspektionen. Organisationen bör aldrig låta Datainspektionen köra systemen utan att relevant personal från organisationen är närvarande.

☐ **VEM ANSVARAR FÖR KÖRNINGARNA?**

Organisationen behöver inte bekymra sig för om den behandling av personuppgifter som aktualiseras genom körningarna strider mot dataskyddsförordningen. Datainspektionen anses som personuppgiftsansvarig för den behandling som beordras av inspektionen.[34]

☐ **SPEGLING OCH KOPIERING AV HÅRDDISKAR M.M.**

Vid konkurrensrättsliga undersökningar har Konkurrensverket under vissa förutsättningar laglig rätt att ta med speglade eller

---

32 49 § a) PuL, jämfört med 43 § PuL.

33 Prop. 2017/18:105, s. 143.

34 Eftersom det är Datainspektionen som bestämmer ändamål och medel med behandlingen, se Öman, Sören & Lindblom, Hans-Olof, *Personuppgiftslagen; en kommentar,* 4 uppl., Norstedts Juridik, Stockholm, 2011, s. 96. Samma bedömning måste gälla enligt dataskyddsförordningen.

kopierade hårddiskar etc. till Konkurrensverket för närmare undersökningar[35].

Datainspektionen har inte den möjligheten. Om Datainspektionen mot förmodan skulle framställa en sådan begäran bör den personuppgiftsansvarige eller personuppgiftsbiträdet inte gå med på åtgärden.

☐ **PERSONUPPGIFTER FÅR LÄMNAS UT**

Det kan förekomma att Datainspektionen får tillgång till personuppgifter inom ramen för ett tillsynsprojekt. Datainspektionen betraktas dock inte som *mottagare* när tillsyn genomförs.[36] Man behöver därmed inte oroa sig för om det kan anses som ett otillåtet utlämnande av personuppgifter enligt dataskyddsförordningen.

☐ **OBSTRUERA INTE UNDERSÖKNINGEN**

Var tillmötesgående, utan att vara eftergiven. Frågor som ligger inom ramen för syftet med tillsynen bör alltid besvaras efter bästa förmåga. Brett formulerade frågor utan egentlig koppling till syftet med tillsynen bör som utgångspunkt inte besvaras. Konsultera alltid jurist vid tveksamhet om information bör lämnas till Datainspektionen.

Förstör inte material eller på annat sätt försvåra eller förhindra utredningen. Att obstruera utredningen är försvårande omständigheter vid fastställande av sanktionsavgifter.

☐ **SEKRETESS**

Bevaka intresset av sekretess. Uppmärksamma Datainspektionen på när företaget eller myndigheten anser att den information som lämnas ska behandlas med sekretess av Datainspektionen.

35 5 kap 6 § 2 st. konkurrenslagen (2008:579).

36 Artikel 4.9 dataskyddsförordningen, se även 3 § PuL.

7. Sammanfattande slutsatser

Vi uppfattar att Datainspektionens tillsynsverksamhet under tiden med personuppgiftslagen huvudsakligen varit inriktad på att förmå de personuppgiftsansvariga att göra rätt och att skapa vägledning för tillämpningen av personuppgiftslagen. Tillsyn har även inletts vid allvarliga överträdelser som t.ex. när det är fråga om integritetskänsliga behandlingar, större uppgiftsmängder som rör en person eller behandlingar som berör många människor.

Vi bedömer att tillsynsverksamheten även i framtiden huvudsakligen kommer att ha samma inriktning och att vi i närtid inte kommer att se några dramatiska förändringar.

Skyldigheten att samarbeta med andra tillsynsmyndigheter kan dock innebära vissa förändringar, inte minst på sikt. Det är t.ex. inte uteslutet att det kan bli flera oanmälda fältinspektioner och tillsyn som utförs för att säkra bevis åt andra tillsynsmyndigheter. Men det återstår att se hur tillsynsverksamheten utvecklas över tiden. Vi kan också konstatera, vilket bör ha framgått av vår framställning, att det finns en hel del oklarheter kring regelverket för tillsynsfrågor.

I sammanhanget har givetvis den närliggande frågan om sanktionsavgifterna också praktisk betydelse. Det är förstås svårt att förutse i vilka fall Datainspektionen kommer utnyttja möjligheten att besluta om sanktionsavgifter och hur stora de blir för olika typer av överträdelser. Avgifterna kommer troligen vara högre för överträdelser för vilka det högre maxbeloppet gäller bl.a. överträdelse av bestämmelserna om de grundläggande kraven, de registrerades rättigheter och underlåtelse att rätta sig efter ett föreläggande från Datainspektionen.

Enligt vår bedömning finns en risk att Sverige fortsättningsvis inte kommer kunna ha en avvikande praxis på sanktionsområdet genom att exempelvis ha lägre avgifter än andra länder. Ytterst blir det en fråga för Europeiska dataskyddstyrelsen och EU-domstolen att hantera frågan om enhetlig sanktionspraxis.

Kombinationen av ett oklart och komplext regelverk och stora konsekvenser vid överträdelser ställer stora krav på förberedelser, inte minst inför en eventuell tillsyn av Datainspektionen.

Att ha genomfört erforderliga anpassningsprojekt och etablerat en intern dataskyddsorganisation med fungerande rutiner är givetvis två avgörande faktorer för att klara en tillsyn på ett framgångsrikt sätt.

Som framgår av vår redogörelse, och av våra tips, avgörs utgången av ett tillsynsärende ytterst av graden av förberedelser i det dagliga

arbetet. När väl ett tillsynsärende inletts är det dock viktigt att agera kraftfullt och snabbt samt mobilisera externa och interna resurser. Tiden till förfogande kommer alltid vara (eller upplevas som) knapp. Vårt råd är att utsätta den egna organisationen, och inte minst den interna dataskyddsorganisationen, för skarpa övningar i form av ”mock audits” eller andra stresstester av dataskyddet.

Slutligen, skulle Datainspektionen i ett tillsynsärende konstatera att personuppgiftsbehandling har skett i strid med dataskyddsförordningen finns alltid möjligheten att överklaga beslutet för att få en överprövning av Datainspektionens bedömning.

Om Advokatfirman Kahn Pedersen

Kahn Pedersen är en advokatbyrå helt inriktad på specialiserad affärsjuridik. Vi åtar oss uppdrag enbart inom våra två verksamhetsområden Digital och Public. Se www.kahnpedersen.se för mera information om vår verksamhet.

Författarna till denna rapport är:

Martin Brinnen, senior specialist.

Mikael Bock, advokat, senior specialist.

Björn Möller, advokat, senior specialist.

Johan Falk, biträdande jurist.

www.kahnpedersen.se

ISBN 978-91-983215-4-8