ARTIKEL 29-ARBETSGRUPPEN FÖR SKYDD AV PERSONUPPGIFTER

17/SV

WP 253

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

Antagna den 3 oktober 2017

ARBETSGRUPPEN FÖR SKYDD AV ENSKILDA MED AVSEENDE PÅ BEHANDLING AV PERSONUPPGIFTER HAR ANTAGIT DESSA RIKTLINJER

med beaktande av Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995,

med beaktande av artiklarna 29 och 30 i det direktivet, och

med beaktande av dess arbetsordning.

Innehållsförteckning

I. Inledning

EU har slutfört en omfattande reform av den europeiska dataskyddsförordningen. Reformen bygger på flera pelare (viktiga komponenter): sammanhängande regler, förenklade förfaranden, samordnade insatser, användarengagemang, effektivare information och starkare verkställighetsbefogenheter.

Personuppgiftsansvariga och personuppgiftsbiträden har större ansvar för att se till att enskildas personuppgifter skyddas effektivt. Tillsynsmyndigheter har befogenhet att se till att både principerna enligt den allmänna dataskyddsförordningen (nedan kallad *förordningen*) och enskildas rättigheter upprätthålls i enlighet med förordningens lydelse och anda.

Ett enhetligt system för dataskydd bygger på att reglerna för dataskydd tillämpas på ett harmoniserat sätt. Förordningen inför ett nytt system för verkställighet, där administrativa sanktionsavgifter är en central del. Tillsammans med övriga åtgärder enligt artikel 58 är avgifterna ett kraftfullt verktyg för tillsynsmyndigheternas arbete.

Detta dokument är avsett för tillsynsmyndigheterna. Syftet är att myndigheterna ska kunna tillämpa och verkställa förordningen bättre. Dokumentet innehåller tillsynsmyndigheternas gemensamma tolkning av artikel 83 i förordningen och beskriver hur den artikeln samverkar med artiklarna 58 och 70 med tillhörande skäl.

Enligt artikel 70.1 e har Europeiska dataskyddsstyrelsen (nedan kallad *EDPB*) behörighet att utfärda riktlinjer, rekommendationer och bästa praxis i syfte att främja en enhetlig tillämpning av förordningen, och artikel 70.1 k ger EDPB behörighet att utforma riktlinjer för att fastställa administrativa sanktionsavgifter.

Dessa riktlinjer är inte uttömmande och förklarar inte heller skillnaderna mellan administrativa, civilrättsliga och straffrättsliga system när det gäller att utfärda administrativa sanktionsavgifter i allmänhet.

EDPB har haft som mål att skapa en strategi för att påföra administrativa sanktionsavgifter som dels är enhetlig, dels på ett lämpligt sätt återspeglar alla riktlinjernas principer, och har kommit fram till en gemensam tolkning av bedömningskriterierna i artikel 83.2 i förordningen. Därför är EDPB och enskilda tillsynsmyndigheter eniga om att använda denna riktlinje som en gemensam strategi.

II. Principer

När en tillsynsmyndighet har konstaterat en överträdelse av förordningen efter bedömning av fakta i fallet måste myndigheten välja den eller de korrigerande åtgärder som är mest lämpliga att vidta mot överträdelsen. Artikel 58.2 b-j[1] anger vilka verktyg tillsynsmyndigheterna får använda när en personuppgiftsansvarig eller ett personuppgiftsbiträde inte har uppfyllt sina skyldigheter. Tillsynsmyndigheterna måste tillämpa följande principer när de använder dessa befogenheter:

---

1. Överträdelse av förordningen bör leda till ”likvärdiga sanktioner”.

Begreppet ”likvärdig” är centralt när det gäller att avgöra hur omfattande tillsynsmyndigheternas skyldighet är, både för att den allmänna korrigerande behörigheten enligt artikel 58.2 ska användas på ett enhetligt sätt och i synnerhet för att tillämpningen av administrativa sanktionsavgifter ska vara enhetlig[2].

För att säkra en enhetlig och hög skyddsnivå för fysiska personer och för att undanröja hindren för flödena av personuppgifter inom unionen bör ***nivån på skyddet*** *av fysiska personers rättigheter och friheter vid behandling av personuppgifter* ***vara likvärdig*** *i alla medlemsstater* (skäl 10). Skäl 11 går närmare in på att en likvärdig skyddsnivå för personuppgifter i hela unionen bland annat kräver *”likvärdiga befogenheter för övervakning och att det säkerställs att reglerna för skyddet av personuppgifter efterlevs och att sanktionerna för överträdelser är likvärdiga i medlemsstaterna*”. I alla medlemsstater anser man dessutom att likvärdiga sanktioner i kombination med ett effektivt samarbete mellan tillsynsmyndigheterna i olika medlemsstater är ett sätt att ”*undvika avvikelser som hindrar den fria rörligheten av personuppgifter inom den inre marknaden*”, i linje med skäl 13 i förordningen.

Eftersom förordningen är direkt tillämplig i alla medlemsstater ger den en starkare grund än direktiv 95/46/EG för en högre grad av enhetlighet. Tillsynsmyndigheterna arbetar ”fullständigt oberoende” (artikel 52) av nationella regeringar, personuppgiftsansvariga och personuppgiftsbiträden men är skyldiga att samarbeta ”*för att se till att denna förordning tillämpas och verkställs på ett enhetligt sätt*” (artikel 57.1 g).

Förordningen kräver att sanktioner påförs på ett mer enhetligt sätt än enligt direktiv 95/46. I gränsöverskridande fall är det främst samarbetsmekanismen (mekanismen för en enda kontaktpunkt) och i viss mån mekanismen för enhetlighet som införs genom den nya förordningen som ska borga för enhetlighet.

I nationella fall som omfattas av förordningen tillämpar tillsynsmyndigheterna dessa riktlinjer i en samarbetsanda, i enlighet med artikel 57.1 g och artikel 63. Målet är att förordningen ska tillämpas och verkställas på ett enhetligt sätt. Tillsynsmyndigheterna kan själva välja korrigerande åtgärder bland dem som räknas upp i artikel 58.2 men bör undvika att välja olika korrigerande åtgärder i likartade fall.

Den principen gäller även när de korrigerande åtgärderna är sanktionsavgifter.

---

[1] Enligt artikel 58.2 får varningar utfärdas när ”planerade behandlingar sannolikt kommer att bryta mot bestämmelserna i denna förordning”. Med andra ord omfattar bestämmelsen tillfällen när överträdelsen av förordningen ännu inte har ägt rum.

[2] Även när rättssystemen i vissa EU-länder inte tillåter administrativa sanktionsavgifter enligt förordningen, ska tillämpningen av bestämmelserna i dessa länder ha en effekt som är likvärdig med administrativa sanktionsavgifter som utdöms av tillsynsmyndigheter (skäl 151). Domstolarna är bundna av förordningen men inte av dessa riktlinjer från EDPB.

2. Liksom alla korrigerande åtgärder som tillsynsmyndigheterna väljer bör sanktionsavgifter vara ”effektiva, proportionella och avskräckande”.

Liksom korrigerande åtgärder i allmänhet bör administrativa sanktionsavgifter vara rimliga i förhållande till typen av överträdelse, hur allvarlig överträdelsen är och vilka följder den får. Tillsynsmyndigheterna måste därför bedöma alla fakta i ett fall på ett sätt som är enhetligt och objektivt motiverat. Vad som är effektivt, proportionellt och avskräckande i ett enskilt fall beror även på syftet med den korrigerande åtgärd som väljs. Det kan antingen vara att se till att reglerna efterlevs eller att bestraffa olagligt beteende (eller båda delarna).

Tillsynsmyndigheterna bör välja en korrigerande åtgärd som är ”effektiv, proportionell och avskräckande” (artikel 83.1), både i nationella fall (artikel 55) och i fall som rör gränsöverskridande behandling av personuppgifter (enligt definitionen i artikel 4.23).

Dessa riktlinjer tar hänsyn till att nationella lagar kan innehålla ytterligare krav på verkställighetsförfarandet som tillsynsmyndigheterna ska följa. Det kan till exempel gälla adressanmälningar, format, tidsfrister för att inkomma med synpunkter, överklagande, verkställighet och betalning[3].

Sådana krav får dock inte hindra att sanktionerna blir effektiva, proportionella och avskräckande.

Både framväxande praxis hos tillsynsmyndigheterna (när det gäller såväl dataskydd som erfarenheter från andra tillsynssektorer) och rättspraxis vid tolkning av principerna kommer att leda till en tydligare bild av effektivitet, proportionalitet och avskräckande verkan.

För att kunna påföra sanktionsavgifter som är effektiva, proportionella och avskräckande ska tillsynsmyndigheten använda den definition av begreppet företag som domstolen använder vid tillämpning av artikel 101 och 102 i EUF-fördraget, det vill säga att ett företag **ska anses vara** en ekonomisk enhet som kan utgöras av ett moderbolag och alla dess dotterbolag. I enlighet med EU-lagstiftning och rättspraxis[4] måste ett företag definieras som en ekonomisk enhet som bedriver kommersiell/ekonomisk verksamhet, oberoende av berörd juridisk person (skäl 150).

3. Den behöriga tillsynsmyndigheten gör en bedömning ”i varje enskilt fall”.

Administrativa sanktionsavgifter får påföras på grund av många olika överträdelser. I artikel 83 i förordningen finns en harmoniserad strategi när det gäller överträdelser, där konkreta skyldigheter listas i punkterna 4 till 6. En medlemsstat får i sin lagstiftning låta artikel 83 omfatta offentliga myndigheter och organ i den medlemsstaten. Dessutom får medlemsstaternas lagstiftning tillåta eller till och med kräva att en sanktionsavgift påförs för överträdelser av andra bestämmelser än dem som tas upp i artikel 83.4–83.6.

[3] Ett exempel är Irlands lagstiftning, där det konstitutionella ramverket och förslaget till dataskyddslagstiftning innebär att det är möjligt att först fatta ett formellt beslut om överträdelsen i sig som förmedlas till relevanta parter, innan det fastställs hur omfattande sanktionen eller sanktionerna ska vara. Beslutet om överträdelsen i sig kan inte ses över i samband med bedömningen av sanktionens eller sanktionernas omfattning.

[4] Definitionen enligt domstolens rättspraxis är att ”begreppet företag omfattar varje enhet som utövar ekonomisk verksamhet, oavsett enhetens rättsliga form och sättet för dess finansiering” (mål Höfner och Elsner, punkt 21, ECLI:EU:C:1991:161). Ett företag ”ska förstås som en ekonomisk enhet, även om enheten i juridisk mening består av flera fysiska eller juridiska personer” (mål Confederación Española de Empresarios de Estaciones de Servicio, punkt 40, ECLI:EU:C:2006:784).

Förordningen kräver bedömning av varje enskilt fall för sig[5]. Artikel 83.2 är utgångspunkten för en sådan bedömning. Den punkten anger att *"Vid beslut om huruvida administrativa sanktionsavgifter ska påföras och om beloppet för de administrativa sanktionsavgifterna i varje enskilt fall ska vederbörlig hänsyn tas till följande …"* Detta innebär när det tolkas tillsammans med skäl 148[6] att tillsynsmyndigheten ansvarar för att välja den eller de åtgärder som lämpar sig bäst. När åtgärder väljs i de fall som tas upp i artikel 83.4–83.6 **måste** alla korrigerande åtgärder övervägas, bland annat att påföra en administrativ sanktionsavgift, antingen tillsammans med en korrigerande åtgärd enligt artikel 58.2 eller enbart.

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.

När EDPB är behöriga enligt artikel 65 i förordningen kommer den att utfärda ett bindande beslut i tvister mellan myndigheter, bland annat när det gäller att fastställa om en överträdelse har ägt rum. När en relevant och motiverad invändning ifrågasätter om den korrigerande åtgärden följer GDPR, diskuterar EDPB i sitt beslut även huruvida den administrativa sanktionsavgift som den behöriga tillsynsmyndigheten föreslår uppfyller principerna om effektivitet, proportionalitet och avskräckande. EDPB:s vägledning om tillämpningen av artikel 65 i förordningen följer separat. I den finns närmare information om typen av beslut EDPB fattar.

4. En harmoniserad strategi för administrativa sanktionsavgifter inom dataskyddsområdet kräver engagemang och informationsutbyte mellan tillsynsmyndigheterna.

[5] Vid tillämpningen av kriterierna i artikel 83 finns det andra bestämmelser som kan stärka grunden för strategin, till exempel

- skäl 141: *Utredningen av ett klagomål bör, med förbehåll för eventuell domstolsprövning, ske i den utsträckning som är lämplig i det enskilda fallet*.
- skäl 129: *Tillsynsmyndigheternas befogenheter bör utövas opartiskt, rättvist och inom rimlig tid i överensstämmelse med lämpliga rättssäkerhetsgarantier i unionsrätten och i medlemsstaternas nationella rätt. Framför allt bör varje åtgärd vara lämplig, nödvändig och proportionell för att säkerställa efterlevnad av denna förordning, med beaktande av omständigheterna i varje enskilt fall …".*
- artikel 57.1 f: "*Behandla klagomål från en registrerad eller från ett organ, en organisation eller en sammanslutning enligt artikel 80, och där så är lämpligt undersöka den sakfråga som klagomålet gäller.*

[6] *För att stärka verkställigheten av denna förordning bör det utdömas sanktioner, inbegripet administrativa sanktionsavgifter, för överträdelser av denna förordning utöver eller i stället för de lämpliga åtgärder som tillsynsmyndigheten vidtar i enlighet med denna förordning. Vid en mindre överträdelse eller om den sanktionsavgift som sannolikt skulle utdömas skulle innebära en oproportionell börda för en fysisk person får en reprimand utfärdas i stället för sanktionsavgifter. Vederbörlig hänsyn bör dock tas till överträdelsens karaktär, svårighetsgrad och varaktighet och huruvida den har skett uppsåtligen, vilka åtgärder som vidtagits för att lindra skadan, graden av ansvar eller eventuella tidigare överträdelser av relevans, det sätt på vilket överträdelsen kom till tillsynsmyndighetens kännedom, efterlevnad av åtgärder som förordnats mot den personuppgiftsansvarige eller personuppgiftsbiträdet, tillämpning av en uppförandekod och eventuella andra försvårande eller förmildrande faktorer. Utdömandet av sanktioner, inbegripet administrativa sanktionsavgifter, bör underkastas adekvata rättssäkerhetsgarantier i överensstämmelse med allmänna principer inom unionsrätten och stadgan, vilket inbegriper ett effektivt rättsligt skydd och korrekt rättsligt förfarande*.

Dessa riktlinjer tar höjd för att det är nytt för en del nationella tillsynsmyndigheter att ha befogenhet att påföra sanktionsavgifter inom dataskyddsområdet och att detta kan medföra problem med resurser, organisation och förfarande. De beslut som tillsynsmyndigheterna fattar när de utövar sina befogenheter att påföra sanktionsavgifter kan överklagas till nationella domstolar.

Som stöd för formella och informella informationsutbyten, såsom regelbundna workshops, ska tillsynsmyndigheterna använda samarbetsmekanismerna i förordningen för att samarbeta med varandra och i relevanta fall med Europeiska kommissionen. Samarbetet skulle vara inriktat på öka enhetligheten genom att utbyta erfarenheter och praxis när det gäller tillämpningen av befogenheten att påföra sanktionsavgifter.

Både denna proaktiva informationsdelning och den framväxande rättspraxisen för användning av de nya befogenheterna kan leda till att principerna eller detaljerna i dessa riktlinjer ses över.

III. Bedömningskriterier i artikel 83.2

Artikel 83.2 innehåller en lista med kriterier som tillsynsmyndigheterna förväntas använda, både för att avgöra om en sanktionsavgift bör påföras och bestämma hur stor den ska vara. Rekommendationen är inte en upprepad bedömning med samma kriterier utan en bedömning som tar hänsyn till alla omständigheter i varje enskilt fall, i enlighet med artikel 83[7].

Slutsatserna från den första fasen av bedömningen kan användas i den andra fasen, som gäller sanktionsavgiftens belopp. På så sätt undviker man att använda samma kriterier två gånger.

Detta avsnitt ger vägledning för tillsynsmyndigheterna om hur de ska tolka enskilda fakta i fallet med hänsyn till kriterierna i artikel 83.2.

a) Överträdelsens karaktär, svårighetsgrad och varaktighet

Nästan alla skyldigheter som personuppgiftsansvariga och personuppgiftsbiträden har enligt förordningen kategoriseras efter sin **karaktär** i bestämmelserna i artikel 83.4–83.6. Redan det faktum att förordningen anger två olika högsta belopp för sanktionsavgiften (10/20 miljoner euro) ger en fingervisning om att det kan vara allvarligare att överträda vissa av förordningens bestämmelser än andra. Genom att bedöma fakta i fallet mot de allmänna kriterierna i artikel 83.2 avgör den behöriga myndigheten om det i ett visst fall finns ett större eller mindre behov av en korrigerande åtgärd i form av en sanktionsavgift. Om en sanktionsavgift har valts som en eller flera lämpliga åtgärder tillämpas det trappstegsvisa systemet i förordningen (83.4–83.6) för att hitta rätt högsta sanktionsavgift som kan påföras med tanke på den aktuella överträdelsens karaktär.

Skäl 148 inför begreppet ”mindre överträdelser”. Sådana överträdelser kan gälla en eller flera av de bestämmelser som listas i artikel 83.4 eller artikel 83.5 i förordningen. Resultatet av bedömningen enligt kriterierna i artikel 83.2 kan dock bli att tillsynsmyndigheten tror att de konkreta omständigheterna i fallet, till exempel incidenten, varken utgör någon betydande risk för de registrerade som berörs eller påverkar skyldigheten i fråga på något väsentligt sätt. I sådana fall kan (men måste inte) sanktionsavgiften ersättas med en reprimand.

Skäl 148 tar inte upp någon skyldighet för tillsynsmyndigheten att alltid ersätta en sanktionsavgift med en reprimand vid en mindre överträdelse (... *får en reprimand utfärdas i stället för sanktionsavgifter*), utan anger snarare detta som en möjlighet som finns till hands efter en konkret bedömning av alla omständigheter i fallet.

Skäl 148 öppnar för samma möjlighet att ersätta en sanktionsavgift med en reprimand när den personuppgiftsansvarige är en fysisk person, för vilken den sanktionsavgift som sannolikt skulle utdömas skulle innebära en oproportionell börda. Utgångspunkten är att tillsynsmyndigheten måste avgöra om omständigheterna i det aktuella fallet kräver att en sanktionsavgift påförs. Om tillsynsmyndigheten fastställer att en sanktionsavgift krävs måste den även avgöra om avgiften skulle innebära en oproportionell börda för en fysisk person.

Förordningen sätter ingen prislapp på specifika överträdelser; endast maximala belopp anges. Detta kan vara en fingervisning om att en överträdelse av skyldigheterna i artikel 83.4 betraktas som relativt sett mindre allvarlig än av dem i artikel 83.5. Vad som är en effektiv, proportionell och avskräckande reaktion på en överträdelse av artikel 83.5 beror dock på omständigheterna i fallet.

[7] I vissa länder kan det på grund av konstitutionella krav finnas nationella procedurregler som innebär att det först fastställs om en överträdelse har skett och därefter separat vilken sanktion som ska tillämpas. Detta kan begränsa innehållet och mängden detaljer i förslag till beslut som utfärdas av den ledande behöriga myndigheten i sådana länder.

Det bör noteras att överträdelser av förordningen som genom sin karaktär kan falla inom kategorin ”upp till 10 000 000 EUR eller upp till 2 % av den totala globala årsomsättningen” enligt artikel 83.4, under vissa omständigheter kan placeras i en högre kategori (20 000 000 EUR). Detta skulle vara sannolikt till exempel för överträdelser som tillsynsmyndigheten har tagit upp tidigare i ett föreläggande[8] som den personuppgiftsansvarige eller personuppgiftsbiträdet inte har följt[9] (artikel 83.6). Bestämmelser i nationell lagstiftning kan i praktiken påverka bedömningen[10]. Överträdelsens karaktär, men också deras *omfattning eller syfte samt antalet berörda registrerade och den skada som de har lidit* ger information om överträdelsens **svårighetsgrad**. Om flera olika överträdelser har ägt rum tillsammans i ett enskilt fall kan tillsynsmyndigheten tillämpa administrativa sanktionsavgifter på en nivå som är effektiv, proportionell och avskräckande inom gränsen för överträdelsen med högst svårighetsgrad. Om en överträdelse av artikel 8 och artikel 12 har upptäckts kan tillsynsmyndigheten därför tillämpa de av de korrigerande åtgärderna i artikel 83.5 som motsvarar den svåraste överträdelsen, det vill säga enligt artikel 12. De närmare detaljerna för denna fas ligger utanför tillämpningsområdet för denna riktlinje (eftersom detaljerat beräkningsarbete kan komma att tas upp i en eventuell senare version av riktlinjen).

Faktorerna nedan bör bedömas tillsammans, till exempel antalet registrerade tillsammans med möjliga konsekvenser för dem.

Antalet berörda registrerade bör fastställas för att det ska gå att avgöra om det rör sig om en enstaka händelse eller ett symtom på en mer systematisk överträdelse eller en följd av att lämpliga rutiner saknas. Detta innebär inte att sanktioner inte ska vara verkställbara för enstaka händelser. Även en enstaka händelse kan påverka många registrerade. Beroende på omständigheterna i fallet och vad som är lämpligt kan detta till exempel bedömas i förhållande till antalet registrerade i den berörda databasen, antalet användare av en tjänst, antalet kunder eller i förhållandet till landets befolkning.

---

[8] Följande förelägganden tas upp i artikel 58.2:

- Förelägga den personuppgiftsansvarige eller personuppgiftsbiträdet att tillmötesgå den registrerades begäran att få utöva sina rättigheter enligt denna förordning.
- Förelägga en personuppgiftsansvarig eller ett personuppgiftsbiträde att se till att behandlingen sker i enlighet med bestämmelserna i denna förordning och om så krävs på ett specifikt sätt och inom en specifik period.
- Förelägga den personuppgiftsansvarige att meddela den 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 och underrätta mottagare till vilka personuppgifterna har lämnats ut om dessa åtgärder enligt artiklarna 17.2 och 19.
- Återkalla en certifiering eller beordra certifieringsorganet att återkalla en certifiering som utfärdats enligt artikel 42 eller 43, eller beordra certifieringsorganet att inte utfärda certifiering om kraven för certifiering inte eller inte längre uppfylls.
- Förelägga om att flödet av uppgifter till en mottagare i tredje land eller en internationell organisation ska avbrytas.

[9] Vid tillämpning av artikel 83.6 måste hänsyn absolut tas till nationella lagar om förfarande. Nationell lag fastställer hur ett föreläggande utfärdas, hur det meddelas, vid vilken tidpunkt det träder i kraft och huruvida det finns en frist för att arbeta på att följa reglerna. Hänsyn ska tas särskilt till verkan av ett överklagande av ett föreläggandes verkställbarhet.

[10] Lagbestämmelser om begränsning kan innebära att det inte längre går att ta hänsyn till ett tidigare föreläggande från tillsynsmyndigheten på grund av det har gått för lång tid sedan detta utfärdades. När preskriptionstiden för ett föreläggande har passerat gäller i vissa rättssystem att ingen avgift får påföras för underlåtenhet att uppfylla skyldigheterna i föreläggandet enligt artikel 83.6. I ett sådant rättssystem måste tillsynsmyndigheten själv avgöra vilka konsekvenser detta har.

Syftet med behandlingen måste också bedömas. I det tidigare WP 29-yttrandet om ”ändamålsbegränsning”[11] analyserades de två viktigaste byggstenarna för denna princip i dataskyddslagen: beskrivning av syfte och förenlig användning. När tillsynsmyndigheten bedömer syftet med behandlingen i förhållande till artikel 83.2 ska den kontrollera i hur hög grad behandlingen uppfyller principens två huvudkomponenter[12]. I vissa situationer kan tillsynsmyndigheten behöva räkna med en grundligare analys av ändamålet med behandlingen i sig inom ramen för analysen i förhållande till artikel 83.2.

Om de registrerade har lidit **skada** måste hänsyn tas till skadans nivå. Behandling av personuppgifter kan leda till risker för den enskildes friheter, vilket tas upp i skäl 75:

> *Risken för fysiska personers rättigheter och friheter, av varierande sannolikhetsgrad och allvar, kan uppkomma till följd av personuppgiftsbehandling som skulle kunna medföra fysiska, materiella eller immateriella skador, i synnerhet om behandlingen kan leda till diskriminering, identitetsstöld eller bedrägeri, ekonomisk förlust, skadat anseende, förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt, obehörigt hävande av pseudonymisering eller annan betydande ekonomisk eller social nackdel, om registrerade kan berövas sina rättigheter och friheter eller hindras att utöva kontroll över sina personuppgifter, om personuppgifter behandlas som avslöjar ras eller etniskt ursprung, politiska åsikter, religion eller övertygelse eller medlemskap i fackförening, om genetiska uppgifter, uppgifter om hälsa eller sexualliv eller fällande domar i brottmål samt överträdelser eller därmed sammanhängande säkerhetsåtgärder behandlas, om personliga aspekter bedöms, framför allt analyser eller förutsägelser beträffande sådant som rör arbetsprestationer, ekonomisk ställning, hälsa, personliga preferenser eller intressen, tillförlitlighet eller beteende, vistelseort eller förflyttningar, i syfte att skapa eller använda personliga profiler, om det sker behandling av personuppgifter rörande sårbara fysiska personer, framför allt barn, eller om behandlingen inbegriper ett stort antal personuppgifter och gäller ett stort antal registrerade.*

Om skadorna har uppstått eller sannolikt kommer att uppstå på grund av överträdelse av förordningen bör tillsynsmyndigheten ta hänsyn till detta vid sitt val av korrigerande åtgärd, även om tillsynsmyndigheten själv inte har behörighet att tilldela någon specifik ersättning för skadan.

Tillsynsmyndigheten behöver inte fastställa något orsakssamband mellan överträdelsen och den materiella förlusten för att kunna påföra en sanktionsavgift (se till exempel artikel 83.6).

Överträdelsens varaktighet kan ge en uppfattning om bland annat

a) uppsåt från personuppgiftsansvarigas sida,

b) underlåtenhet att vidta lämpliga försiktighetsåtgärder, eller

c) oförmåga att införa tekniska och organisatoriska åtgärder som krävs.

b) Om överträdelsen skett med uppsåt eller genom oaktsamhet

Generellt innefattar ”med uppsåt” både kunskap och uppsåt i förhållande till en överträdelse, medan ”oaktsamhet” innebär att det inte fanns någon avsikt bakom överträdelsen, även om den personuppgiftsansvarige/personuppgiftsbiträdet brast i sin lagstadgade aktsamhetsplikt.

[11] WP 203, yttrande 03/2013 om ändamålsbegränsning, finns på: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[12] Se även Wp 217, yttrande 6/2014 om begreppet legitimt intresse för den personuppgiftsansvarige enligt artikel 7, sidan 24, om frågan: ”Vad gör ett intresse legitimt eller icke-legitimt?”

Det är allmänt vedertaget att uppsåtliga överträdelser som visar lagtrots är allvarligare än oavsiktliga och därför med större sannolikhet motiverar att en administrativ sanktionsavgift påförs. Relevanta slutsatser om uppsåt och oaktsamhet bör dras utifrån en objektiv beskrivning av beteendet som bygger på insamlade fakta om fallet. Genom den rättspraxis som växer fram inom dataskyddsområdet vid tillämpningen av förordningen kan dessutom omständigheter utkristalliseras som ger en klarare grund för att avgöra om det funnits uppsåt bakom en överträdelse.

Omständigheter som kan tyda på uppsåtliga överträdelser är olaglig behandling för vilken den personuppgiftsansvarige har fått tillstånd från högsta ledningen eller genomför trots att dataskyddsombudet har avrått från den eller trots befintliga policyer. Det kan till exempel vara att skaffa och behandla data om anställda hos en konkurrent i avsikt att misskreditera konkurrenten på marknaden.

Andra exempel:

- Ändra personuppgifter för att ge ett missvisande (positivt) intryck av att mål har uppnåtts – vi har sett detta i samband med mål för sjukhusväntelistor.
- Handel med personuppgifter för marknadsföringsändamål, dvs. att hävda att man säljer data med de registrerades samtycke utan att kontrollera eller ta hänsyn till hur deras data kommer att användas.

Andra omständigheter, till exempel att inte läsa och följa befintliga policyer, fel på grund av den mänskliga faktorn, underlåtenhet att kontrollera för personuppgifter innan information offentliggörs, underlåtenhet att tillämpa tekniska uppdateringar på utsatta tider och underlåtenhet att anta policyer (i stället för enbart underlåtenhet att tillämpa dem) kan vara tecken på oaktsamhet.

Företag bör ansvara för att tillhandahålla lämpliga strukturer och resurser för verksamhetens karaktär och komplexitet. Personuppgiftsansvariga och personuppgiftsbiträden kan inte legitimera överträdelser av dataskyddslagstiftningen genom att hänvisa till brist på resurser i sig. Rutiner och dokumentation av behandlingsaktiviteter följer en riskbaserad metod enligt förordningen.

Det finns gråzoner som kommer att påverka beslut om att tillämpa en korrigerande åtgärd eller inte, och myndigheten kan behöva genomföra mer omfattande utredningar för att fastställa fakta i fallet och säkerställa att tillräcklig hänsyn tas till alla specifika omständigheter i varje enskilt fall.

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

Personuppgiftsansvariga och personuppgiftsbiträden är skyldiga att genomföra tekniska och organisatoriska åtgärder för att uppnå en riskanpassad säkerhetsnivå, genomföra konsekvensbedömningar av dataskyddet och minska risker för enskildas fri- och rättigheter som uppstår på grund av behandling av personuppgifter. Om en överträdelse inträffar och den registrerade har lidit skada ska den ansvariga parten dock göra vad han eller hon kan för att minska konsekvenserna av överträdelsen för den eller de enskilda som berörs. Tillsynsmyndigheten bör ta hänsyn till ett sådant ansvarsfullt beteende (eller avsaknad av detta) både för sitt val av korrigerande åtgärd eller åtgärder och vid beräkning av den sanktionsavgift som ska påföras i det specifika fallet.

Försvårande och förmildrande faktorer lämpar sig särskilt väl för att finjustera avgiftsbeloppet efter de särskilda omständigheterna i fallet, men deras roll vid valet av korrigerande åtgärd ska inte heller underskattas. Ett exempel är när en bedömning baserad på andra kriterier gör tillsynsmyndigheten osäker på om en administrativ sanktionsavgift är lämplig som enda åtgärd eller i kombination med andra åtgärder i artikel 58. I detta fall kan sådana försvårande eller förmildrande omständigheter göra det lättare att välja lämpliga åtgärder genom att tippa vågskålen mot något som upplevs som mer effektivt, proportionellt och avskräckande i det specifika fallet.

Denna bestämmelse fungerar som en bedömning av graden av ansvar för den personuppgiftsansvarige efter överträdelsen. Den kan omfatta fall där den personuppgiftsansvarige/personuppgiftsbiträdet uppenbart inte har varit likgiltig eller oaktsam utan har gjort allt de har kunnat för att rätta till sina handlingar när de blev medvetna om överträdelsen.

Tillsynsmyndigheternas erfarenheter i samband med direktiv 95/46/EG har tidigare visat att det kan vara lämpligt att visa viss flexibilitet gentemot personuppgiftsansvarige/personuppgiftsbiträden som har erkänt överträdelsen och tagit ansvar för att korrigera eller begränsa följderna av sina handlingar. Exempel (som dock inte automatiskt ska leda till ett mer flexibelt förhållningssätt) kan vara:

- Kontakta andra personuppgiftsansvariga/personuppgiftsbiträden som kan ha varit involverade i den utökade behandlingen, t.ex. om en uppgift av misstag har delats med tredje parter.
- Den personuppgiftsansvarige/personuppgiftsbiträdet stoppar snabbt överträdelsen från att fortsätta eller utökas till en nivå eller fas som skulle ha gjort följderna mycket allvarligare än de blev.

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 och 32

Förordningen innebär att personuppgiftsansvariga får mycket mer ansvar än enligt dataskyddsdirektivet 95/46/EG.

Personuppgiftsansvarigas och personuppgiftsbiträdens ansvarsskyldighet som grund för valet av lämpliga korrigerande åtgärder kan bland annat innefatta:

- Har den personuppgiftsansvarige genomfört tekniska åtgärder enligt principerna för inbyggt dataskydd och dataskydd som standard (artikel 25)?
- Har den personuppgiftsansvarige genomfört tekniska åtgärder enligt principerna för inbyggt dataskydd och dataskydd som standard (artikel 25) på alla nivåer i organisationen?
- Har den personuppgiftsansvarige/personuppgiftsbiträdet säkerställt en lämplig säkerhetsnivå (artikel 32)?
- Är relevanta rutiner/policyer för dataskydd kända och tillämpas dessa på en lämplig ledningsnivå i organisationen? (Artikel 24).

Enligt artikel 25 och 32 i förordningen krävs det att *personuppgiftsansvariga beaktar den senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter*. I stället för att vara skyldigheter avseende mål inför dessa bestämmelser skyldigheter avseende medel, genom att den personuppgiftsansvarige måste göra de bedömningar som krävs och dra lämpliga slutsatser. Den fråga tillsynsmyndigheten måste besvara är alltså i vilken grad den personuppgiftsansvarige har gjort ”vad som kunde förväntas” med tanke på behandlingens karaktär, ändamål eller omfattning, i förhållande till sina skyldigheter enligt förordningen.

Vid den bedömningen ska tillräcklig hänsyn tas till ”bästa praxis” när det gäller förfaranden eller metoder, där sådana finns och tillämpas. Det är viktigt att ta hänsyn till industristandarder och uppförandekoder inom respektive område eller yrke. Bästa praxis-koder kan ge en uppfattning om vad som är allmän praxis inom området och om kunskapsnivån när det gäller olika medel för att hantera typiska säkerhetsfrågor i samband med behandling.

Bästa praxis är det övergripande ideal som ska eftersträvas, men hänsyn måste tas till de särskilda omständigheterna i varje enskilt fall för ansvarsbedömningen.

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

Detta kriterium är avsett för bedömning av tidigare resultat för den enhet som begått överträdelsen. Tillsynsmyndigheterna bör tänka på att bedömningen här kan ha en relativt stor spännvidd. Skälet till det är att alla typer av överträdelser av förordningen kan vara relevanta för bedömningen, även sådana som är annorlunda till sin karaktär än den som tillsynsmyndigheten utreder för tillfället, eftersom de kan visa att den allmänna kunskapsnivån är för låg eller att dataskyddsreglerna inte beaktas.

Tillsynsmyndigheten bör bedöma följande:

- Har den personuppgiftsansvarige/personuppgiftsbiträdet gjort sig skyldig till samma överträdelse tidigare?
- Har den personuppgiftsansvarige/personuppgiftsbiträdet begått en överträdelse av förordningen på samma sätt? (till exempel inte svarat på begäranden från registrerade tillräckligt snabbt, eller dröjt omotiverat länge med att svara på begäranden och liknande, på grund av otillräcklig kunskap om befintliga rutiner inom organisationen eller olämplig riskbedömning).

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

Vid beslut om en administrativ sanktionsavgift och dess belopp ska enligt artikel 83.2 ”vederbörlig hänsyn” tas till graden av samarbete. Förordningen ger inget entydigt svar på frågan hur hänsyn ska tas till personuppgiftsansvariges och personuppgiftsbiträdens insatser för att åtgärda en överträdelse som redan har fastställts av tillsynsmyndigheten. Vidare är det uppenbart att kriterierna normalt skulle tillämpas när sanktionsavgiftens belopp beräknas.

Om den personuppgiftsansvarigas insats har lett till att de negativa följderna för enskildas rättigheter aldrig uppkom eller blev mer begränsade än de annars skulle ha blivit, skulle tillsynsmyndigheten även kunna ta hänsyn till detta när den väljer en korrigerande åtgärd som är proportionell i det enskilda fallet.

Ett exempel på en fråga som kan visa om det i ett visst fall är relevant att ta hänsyn till samarbetet med tillsynsmyndigheten är följande:

- Har enheten genom sin reaktion på tillsynsmyndighetens begäranden under utredningen av det specifika fallet begränsat inverkan på enskildas rättigheter väsentligt?

Det skulle däremot inte vara lämpligt att ta ytterligare hänsyn till samarbete som lagen redan kräver. Enheten är till exempel alltid skyldig att ge tillsynsmyndigheten tillträde till lokalerna för revisioner/inspektioner.

g) De kategorier av personuppgifter som påverkas av överträdelsen

Några exempel på viktiga frågor som tillsynsmyndigheten kan behöva besvara om de är tillämpliga på fallet:

- Gäller överträdelsen behandling av särskilda kategorier av personuppgifter enligt artikel 9 eller 10 i förordningen?
- Är data direkt eller indirekt identifierbara?
- Innefattar behandlingen uppgifter vars spridning skulle leda till direkt skada/trångmål för den enskilde (vilket faller utanför kategorin i artikel 9 eller 10).

- Är uppgifterna direkt tillgängliga utan tekniska skydd, eller är de krypterade[13]?

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

En tillsynsmyndighet kan bli medveten om överträdelsen genom utredning, klagomål, artiklar i pressen, anonyma tips eller anmälan från den personuppgiftsansvarige. Denne är enligt förordningen skyldig att anmäla överträdelser rörande personuppgifter till tillsynsmyndigheten. När den personuppgiftsansvarige endast uppfyller denna skyldighet kan det inte betraktas som en dämpande/förmildrande faktor. På motsvarande sätt gäller att tillsynsmyndigheten kan anse att personuppgiftsansvariga/personuppgiftsbiträden som har handlat vårdslöst utan att anmäla detta, eller åtminstone inte har anmält alla detaljer av överträdelsen, på grund av att de inte har uppfattat överträdelsens omfattning förtjänar en strängare sanktion. I detta fall är det alltså osannolikt att överträdelsen klassificeras som mindre.

i) När åtgärder enligt artikel 58.2 tidigare har förordnats mot den berörda personuppgiftsansvarige eller personuppgiftsbiträdet vad gäller samma sakfråga, efterlevnad av dessa åtgärder

En tidigare överträdelse kan göra att tillsynsmyndigheten redan har ögonen på en personuppgiftsansvarig eller ett personuppgiftsbiträde för kontroll av efterlevnaden. Om kontakter har förekommit med dataskyddsombudet har dessa sannolikt varit omfattande. Därför kommer tillsynsmyndigheten att ta hänsyn till tidigare kontakter.

Till skillnad från kriterierna i punkt e är detta bedömningskriterium endast en påminnelse till tillsynsmyndigheterna om att de ska hänvisa till åtgärder som de själva har utfärdat vid ett tidigare tillfälle till samma personuppgiftsansvarig eller personuppgiftsbiträde ”vad gäller samma sakfråga”.

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

Tillsynsmyndigheterna har skyldighet att *Övervaka och verkställa tillämpningen av denna förordning* (artikel 57.1 a). Enligt artiklarna 24.3, 28.5 eller 32.3 i förordningen kan personuppgiftsansvariga och personuppgiftsbiträden visa efterlevnad genom att följa godkända uppförandekoder.

Vid en överträdelse av någon av förordningens bestämmelser kan tillämpningen av en godkänd uppförandekod ge tillsynsmyndigheten en uppfattning om hur stort behovet är av att den sätter in en effektiv, proportionell och avskräckande administrativ sanktionsavgift eller någon annan korrigerande åtgärd. Enligt artikel 40.4 ska godkända uppförandekoder innehålla *mekanismer som gör det möjligt för det (övervakande) organet att utföra den obligatoriska övervakningen av att dess bestämmelser efterlevs*.

När personuppgiftsansvariga eller personuppgiftsbiträden har följt en godkänd uppförandekod kan tillsynsmyndigheten förlita sig på att den organisation som står bakom koden själv vidtar lämpliga åtgärder mot sin medlem, till exempel genom övervaknings- och verkställighetsprogram som uppförandekoden innefattar. Tillsynsmyndigheten kan därför anse att sådana åtgärder är tillräckligt effektiva, proportionella eller avskräckande i det enskilda fallet och att det inte behövs några ytterligare åtgärder från myndigheten själv. När skyldigheter inte uppfylls kan vissa former av sanktioner ske genom övervakningssystemet, i enlighet med artikel 41.2 c och 42.4. Det gäller bland annat avstängning eller uteslutande av den personuppgiftsansvarige eller personuppgiftsbiträdet från uppförandekoden. Det övervakande organets befogenheter gäller dock *utan att det påverkar den*

[13] Det bör inte alltid ses som en ”bonus” i form av en förmildrande faktor att överträdelsen endast rör indirekt identifierbara eller till och med pseudonymiserade/krypterade uppgifter. För dessa överträdelser kan en allmän bedömning av övriga kriterier ge en viss eller stark indikation på att en sanktionsavgift bör påföras.

berörda tillsynsmyndighetens uppgifter och befogenheter. Detta innebär att tillsynsmyndigheten inte är skyldig att ta hänsyn till tidigare påförda sanktioner inom ramen för systemet med egentillsyn.

Bristande efterlevnad av egentillsynsåtgärder kan även avslöja att den personuppgiftsansvarige eller personuppgiftsbiträdet visar vårdslöshet eller uppsåtlig underlåtenhet när det gäller att uppfylla sina skyldigheter.

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

Bestämmelsen i sig innehåller exempel på andra faktorer att ta hänsyn till vid beslut om lämpligheten av en administrativ sanktionsavgift för en överträdelse av bestämmelserna i artikel 83.4–83.6.

Information om förtjänst på grund av en överträdelse kan vara särskilt viktig för tillsynsmyndigheten eftersom ekonomisk vinning genom överträdelsen inte kan kompenseras genom åtgärder som inte har några ekonomiska konsekvenser. Det faktum att en personuppgiftsansvarig har haft vinning av överträdelsen av förordningen kan i sig utgöra en stark indikation på att en sanktionsavgift bör påföras.

IV. Slutsats

Reflektioner kring frågor som dem i avsnittet ovan gör det lättare för tillsynsmyndigheterna att använda relevanta fakta i fallet för att välja de kriterier som är mest användbara när myndigheten ska avgöra om en lämplig administrativ sanktionsavgift ska påföras utöver eller i stället för andra åtgärder enligt artikel 58. Genom att ta hänsyn till det sammanhang som framkommer vid bedömningen kan tillsynsmyndigheten välja den korrigeringsåtgärd som är mest effektiv, proportionell och avskräckande i förhållande till överträdelsen. korrigeringsåtgärden

Artikel 58 innehåller en del vägledning om vilka åtgärder en tillsynsmyndighet kan välja, med tanke på att de korrigerande åtgärderna är olika till sin karaktär och i första hand lämpade för olika ändamål. Det kan även gå att kombinera vissa av åtgärderna i artikel 58 för att utforma en tillsynsåtgärd som innefattar mer än en korrigerande åtgärd.

Det är inte alltid nödvändigt att komplettera åtgärden med en annan korrigerande åtgärd. Enbart sanktionsavgiften kan till exempel räcka för önskad effektivitet och avskräckande verkan om tillsynsmyndigheten tar tillräcklig hänsyn till vad som är proportionellt i ett visst fall.

I huvudsak gäller det för myndigheterna att återupprätta efterlevnaden genom att tillämpa de korrigerande åtgärder som står till buds. Tillsynsmyndigheterna kommer också att behöva välja den lämpligaste kanalen för tillsynsåtgärder. Detta kan till exempel innefatta straffrättsliga åtgärder (om sådana är tillgängliga på nationell nivå).

Praxisen att tillämpa administrativa sanktionsavgifter håller på att utvecklas i EU, och tillsynsmyndigheterna bör samarbeta vid tillämpning av åtgärderna för att kontinuerligt öka enhetligheten. Samarbetet kan bestå i regelbundna utbyten genom workshops om fallhantering eller andra evenemang som ger möjlighet att jämföra fall på regional, nationell och gränsöverskridande nivå. En rekommendation är att stödja pågående samarbete genom att skapa en permanent undergrupp med anknytning till en relevant del av EDPB.