Datainspektionen

Datainspektionens styrdokument

Dnr: 345-2018

Beslutsdatum: 2018-12-19

Datainspektionens riktlinjer för korrigerande befogenheter enligt artikel 58.2 dataskyddsförordningen

Innehåll

1. Inledning

1.1 Bakgrund och syfte

Datainspektionen är ansvarig för att övervaka att dataskyddsreglerna tillämpas på ett riktigt sätt när personuppgifter behandlas. I syfte att uppnå denna regelefterlevnad ger dataskyddsförordningen[1] Datainspektionen ett antal korrigerande befogenheter:

Artikel	Befogenhet
58.2 a	Varning
58.2 b	Reprimand
58.2 c–h och j	Förelägganden (inklusive förbud, begränsning och återkallelse)
58.2 i	Administrativa sanktionsavgifter

Dessa riktlinjer har till syfte att säkerställa att Datainspektionen har en enhetlig och likvärdig bedömning och tillämpning avseende de korrigerande befogenheterna.

1.2 Tillämpningsområde och avgränsning

Datainspektionens korrigerande befogenheter gäller vid tillsyn[2] över bestämmelserna i dataskyddsförordningen. Med stöd av 6 kap. 1 § dataskyddslagen[3] kan Datainspektionen använda sina korrigerande befogenheter även vid överträdelser av dataskyddslagen och andra bestämmelser som kompletterar dataskyddsförordningen, såsom de sektorsspecifika författningarna. Datainspektionen får dock bara påföra administrativa sanktionsavgifter vid sådana överträdelser som anges i artikel 83 dataskyddsförordningen.[4]

För att kunna besluta om en sanktionsavgift vid överträdelse av en kompletterande nationell bestämmelse krävs därför att det också är fråga om överträdelse av en artikel i dataskyddsförordningen. Både de nationella bestämmelserna och de aktuella artiklarna i dataskyddsförordningen ska anges i beslutet.

---

[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] Notera att de korrigerande befogenheterna, i tillämpliga fall, även gäller vid förhandssamråd enligt artikel 36.2 dataskyddsförordningen.

[3] Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

[4] För att Datainspektionen ska kunna besluta om administrativa sanktionsavgifter i andra fall än de som avses i artikel 83 dataskyddsförordningen krävs en särskild reglering om detta, se prop. 2017/18:105 s. 156. I 6 kap. 3 § dataskyddslagen framgår därför att sanktionsavgifter även kan tas ut vid överträdelser av artikel 10 dataskyddsförordningen.

Dessa riktlinjer ska tillämpas på överträdelser som har ägt rum från och med den 25 maj 2018. Notera att ett tillsynsbeslut kan innehålla brister avseende olika behandlingar eller sammankopplade behandlingar (som i sig kan innehålla överträdelser av olika bestämmelser). Dessa riktlinjer utgår från att sådana behandlingssituationer ska hanteras var för sig – och som utgångspunkt att överträdelser avseende en och samma behandling eller sammankopplade behandlingar ska hanteras tillsammans – när det gäller val och användning av korrigerande befogenhet, se även avsnitt 4.3.1.4 (om maxbeloppet för sanktionsavgiften) och 4.3.3 (om att sanktionsavgifter ska vara effektiva, proportionella och avskräckande).

Dessa riktlinjer omfattar inte sådana förebyggande och korrigerande befogenheter som regleras i brottsdatalagen (BDL)[5], se i stället ”Datainspektionens riktlinjer för förebyggande och korrigerande befogenheter samt administrativa sanktionsavgifter enligt brottsdatalagen”.

Det kan noteras att Datainspektionen, utöver sina korrigerande befogenheter, också har utredningsbefogenheter, till exempel att beordra den personuppgiftsansvarige eller personuppgiftsbiträdet att lämna den information som Datainspektionen behöver för att kunna fullgöra sina uppgifter samt att genomföra undersökningar i form av dataskyddstillsyn.[6] Vidare har Datainspektionen befogenheter att utfärda tillstånd och att ge råd.[7] Sådana befogenheter faller utanför dessa riktlinjers tillämpningsområde.

2. Principer för val av korrigerande befogenhet

2.1 Effektivt, proportionellt och avskräckande

Datainspektionen ska välja en korrigerande åtgärd som är effektiv och avskräckande, men samtidigt proportionell, dvs. rimlig i förhållande till typen av överträdelse, hur allvarlig överträdelsen är och vilka följder den får. Dessa principer gäller för valet av korrigerande åtgärd, men även vid bestämmande av storleken på en eventuell administrativ sanktionsavgift.[8]

2.2 Bedömning i varje enskilt fall – kriterier

Vid valet av korrigerande åtgärd ska en bedömning göras av alla relevanta omständigheter i det enskilda fallet. Om det är fråga om en överträdelse som

[5] Brottsdatalagen (2018:1177).
[6] Artikel 58.1 dataskyddsförordningen.
[7] Artikel 58.3 dataskyddsförordningen.
[8] Artikel 83.1 och Artikel 29-gruppens riktlinjer för tillämpning och fastställande av administrativa sanktionsavgifter i enlighet med förordning 2016/679 (WP 253) s. 6. Se även avsnitt 4.3.3 nedan.

omfattas av artikel 83.4–6 dataskyddsförordningen (dvs. att en sanktionsavgift kan påföras) ska Datainspektionen överväga samtliga korrigerande åtgärder, inklusive administrativa sanktionsavgifter, och välja den eller de åtgärder som lämpar sig bäst. Utgångspunkten för en sådan bedömning är nedan angivna faktorer[9].

Nedan följer även förslag på hur varje faktor kan värderas. Förslagen baserar sig på Datainspektionens bedömning av den mest sannolika användningen av respektive kriterium. Det ska dock noteras att flera av dessa bedömningskriterier, oavsett vad som anges nedan, sannolikt skulle kunna beaktas i såväl försvårande som förmildrande riktning, beroende på omständigheterna i det enskilda fallet.

Artikel	**Bedömningskriterium**	**Värdering**
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).	Försvårande/ förmildrande
83.2 b	Om överträdelsen skett med uppsåt eller genom grov oaktsamhet.	Försvårande
83.2 c	De åtgärder som den personuppgiftsansvarige eller personuppgiftsbiträdet har vidtagit för att lindra den skada som de registrerade har lidit.	Förmildrande
83.2 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) dataskyddsförordningen.	Förmildrande
83.2 e	Eventuella relevanta tidigare överträdelser som den personuppgiftsansvarige eller personuppgiftsbiträdet gjort sig skyldig till.	Försvårande
83.2 f	Graden av samarbete med tillsynsmyndigheten för att komma till rätta med överträdelsen och minska dess potentiella negativa effekter.	Förmildrande
83.2 g	De kategorier av personuppgifter som omfattas av överträdelsen.	Försvårande
83.2 h	Det sätt på vilket överträdelsen kom till tillsynsmyndighetens kännedom, särskilt om den personuppgiftsansvarige eller personuppgiftsbiträdet själv	Förmildrande

[9] Kriterierna framgår av artikel 83.2 dataskyddsförordningen. Se även skäl 148 dataskyddsförordningen och WP 253 s. 9 ff.

	anmälde överträdelsen (gäller inte anmälan av personuppgiftsincident).	
83.2 i	Brist på efterlevnad av korrigerande åtgärder (enligt artikel 58.2) som tidigare har förordnats mot den personuppgiftsansvarige eller personuppgiftsbiträdet vad gäller samma sakfråga.	Försvårande
83.2 j	Tillämpandet av godkända uppförandekoder (enligt artikel 40) eller godkända certifieringsmekanismer (enligt artikel 42).	Förmildrande
83.2 k	Eventuell annan försvårande eller förmildrande faktor som är tillämplig på omständigheterna i fallet. Exempel på en försvårande faktor är ekonomisk vinst som görs eller förlust som undviks genom överträdelsen.	Försvårande/ förmildrande

I avsnitt 4.3.2 nedan beskrivs dessa bedömningskriterier mer ingående.

3. Varning, reprimand och föreläggande m.m.

3.1 Varning

En varning kan utfärdas om planerade behandlingar sannolikt kommer att bryta mot bestämmelserna i dataskyddsförordningen eller kompletterande författningar.[10] Med andra ord kan en varning endast utfärdas då någon överträdelse ännu inte har ägt rum.[11]

En varning ska vara skriftlig och tydligt ange på vilket sätt behandlingen riskerar att strida mot regelverket. En varning kan avse vilken form av förändring som helst i behandlingen. Som utgångspunkt är en varning inte bindande och leder därmed inte till något överklagbart beslut.[12]

Varningar kan kombineras med samtliga övriga korrigerande åtgärder. I praktiken kommer dock varningar sannolikt att kombineras främst med olika förelägganden (inklusive förbud), till exempel att företa en konsekvensbedömning eller vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder.

[10] Artikel 58.2 a dataskyddsförordningen.
[11] WP 253 s. 5.
[12] Jfr prop. 2017/18:232 s. 295, där det bl.a. framgår att ett beslut om varning enligt BDL, till skillnad från vad Datainspektionen ansåg i sitt remissyttrande, inte ska vara bindande och överklagbart.

3.2 Reprimand

När personuppgiftsansvariga och personuppgiftsbiträden bryter mot bestämmelserna i dataskyddsförordningen, eller kompletterande bestämmelser, kan Datainspektionen tillrättavisa dessa genom att utfärda reprimander.[13] Om det är fråga om en överträdelse som kan föranleda en administrativ sanktionsavgift, får en reprimand utfärdas i stället för sanktionsavgift (i) vid en mindre överträdelse eller (ii) om den sanktionsavgift som sannolikt skulle utdömas skulle innebära en oproportionell börda för en fysisk person.[14] Notera att en enskild firma är en fysisk person. Frågan om det är en mindre överträdelse[15] avgörs genom en bedömning av kriterierna i artikel 83.2 dataskyddsförordningen (se avsnitt 2.2 ovan och 4.3.2 nedan).

En reprimand kan kombineras med samtliga övriga korrigerande åtgärder. I praktiken kommer dock sådana kombinationer att aktualiseras endast i enstaka fall när det gäller juridiska personer. Reprimander utfärdas bara mot juridiska personer vid mindre överträdelser och innehåller i sig en tillrättavisning som tillsynsobjektet (om bristen inte redan har åtgärdats) förväntas rätta sig efter. Mot den bakgrunden bör det, i situationer då det kan finnas behov av att utfärda till exempel ett föreläggande (inklusive förbud), sällan vara fråga om mindre överträdelser. Vidare är en reprimand att betrakta som en mildare sanktion än både förelägganden och sanktionsavgifter, varför den inte heller utgör en förstärkning av övriga korrigerande åtgärder.

3.3 Föreläggande, förbud och återkallelse

Dataskyddsförordningen innehåller en rad olika situationer där den som behandlar personuppgifter kan föreläggas att vidta åtgärder. Datainspektionen kan använda sig av följande förelägganden, inklusive begränsning av och förbud mot behandling samt återkallelse av certifiering:

Artikel	Föreläggande
58.2 c	Förelägga den personuppgiftsansvarige eller personuppgiftsbiträdet att tillmötesgå den registrerades begäran att få utöva sina rättigheter enligt dataskyddsförordningen.

[13] Artikel 58.2 b dataskyddsförordningen.
[14] Skäl 148 dataskyddsförordningen.
[15] Angående ”mindre överträdelser” har Artikel 29-gruppen uttalat att ”resultatet av bedömningen enligt kriterierna i artikel 83.2 kan dock bli att tillsynsmyndighetens 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” och ”i sådana fall kan (men måste inte) sanktionsavgiften ersättas med en reprimand” (WP 253 s. 9).

58.2 d	Förelägga den personuppgiftsansvarige eller personuppgiftsbiträdet att se till att behandlingen sker i enlighet med dataskyddsförordningen och, om så krävs, på ett specifikt sätt och inom en specifik period.
58.2 e	Förelägga den personuppgiftsansvarige att meddela den registrerade att en personuppgiftsincident har inträffat.
58.2 g	Förelägga om rättelse eller radering av personuppgifter samt begränsning av behandling (enligt artiklarna 16–18) och underrätta mottagare till vilka personuppgifterna har lämnats ut om dessa åtgärder (enligt artiklarna 17.2 och 19).
58.2 j	Förelägga om att flödet av uppgifter till en mottagare i tredje land eller en internationell organisation ska avbrytas.

Artikel	**Begränsning och förbud**
58.2 f	Införa en tillfällig eller definitiv begränsning av, inklusive ett förbud mot, behandling.

Artikel	**Återkallelse av certifiering**
58.2 h	Återkalla en certifiering eller beordra certifieringsorganet att återkalla en certifiering (utfärdad enligt artikel 42 eller 43) eller beordra certifieringsorganet att inte utfärda certifiering om kraven för certifiering inte (längre) uppfylls.

Som följer av ovanstående uppräkning är föreläggandena olika till sin karaktär och lämpade för olika situationer.

Som framgår har Datainspektionen (enligt artikel 58.2 d) möjlighet att förelägga om att behandlingen ska ske i enlighet med dataskyddsförordningen och, om så krävs, på ett specifikt sätt och inom en specifik period. I många fall är tillsynsobjektet bättre lämpat att avgöra vad som behöver göras för att behandlingen ska bli författningsenlig. Det kan till exempel vara fråga om vilka tekniska åtgärder som bör vidtas eller vilka säkerhetslösningar som bör väljas. Datainspektionen ska därför endast om det behövs konkret ange vilken åtgärd som ska vidtas.[16] Om det i ett föreläggande anges när åtgärderna ska vara genomförda, är det viktigt att detta inte formuleras som en form av dispens från att följa regelverket innan tiden i föreläggandet har löpt ut. Ett sådant föreläggande kan därför utformas så att inom en specifik period
(i) ska tillsynsobjektet rapportera vidtagna åtgärder till Datainspektionen eller
(ii) kan ärendet komma att följas upp av Datainspektionen.

[16] Jfr prop. 2017/18:232 s. 296.

När Datainspektionen använder sin befogenhet att förelägga om rättelse, radering eller begränsning av behandling (enligt artikel 58.2 g) ska bland annat beaktas att åtgärden inte får strida mot annan lagstiftning, till exempel bestämmelser om bevarande av allmänna handlingar, krav i bokföringslagen, journalföringsplikt m.m.[17]

Med förbud mot behandling avses att någon behandling inte längre får förekomma. Förbud mot behandling ska bara meddelas om den som behandlar personuppgifter på ett allvarligt sätt har åsidosatt sina skyldigheter och bristerna är sådana att de inte kan åtgärdas på annat sätt än att behandlingen upphör. Ett förbud mot behandling bör normalt vara permanent. I vissa fall kan dock ett tillfälligt förbud vara en lämplig åtgärd, till exempel om den personuppgiftsansvarige trots varning från Datainspektionen har påbörjat otillåten personuppgiftsbehandling och Datainspektionen bedömer att bristerna kan rättas till.[18]

I vissa fall kan det vara lämpligt att, i stället för ett förbud, införa en tillfällig eller definitiv begränsning av behandlingen. Att behandlingen begränsas innebär att det sätts upp villkor för hur behandlingen får gå till. En begränsning kan till exempel avse åtkomsten till uppgifterna, behandlingens varaktighet eller att behandling endast får ske för vissa avgränsade syften. Som exempel kan en begränsning ersätta ett förbud när det inte är möjligt att förbjuda behandlingen på grund av lagstadgade skyldigheter rörande exempelvis arkivering och bokföring. Notera att Datainspektionens möjlighet att införa en begränsning av behandling (artikel 58.2 f) ska skiljas från möjligheten att förelägga om begränsning av behandling enligt artikel 18 (artikel 58.2 g).

[17] Jfr prop. 2017/18:232 s. 249.
[18] Jfr prop. 2017/18:232 s. 297.

4. Administrativa sanktionsavgifter

4.1 Allmänt

Administrativa sanktionsavgifter kan påföras för överträdelser av dataskyddsförordningen utöver eller i stället för övriga korrigerande åtgärder som Datainspektionen kan använda enligt artikel 58.2 dataskyddsförordningen.

En administrativ sanktionsavgift som påförs ska alltid vara effektiv, proportionell och avskräckande (se avsnitt 2.1 ovan och 4.3.3 nedan). Det är viktigt att sanktionsavgifter inte behandlas som en sista utväg eller att Datainspektionen tvekar att påföra dem, men de ska inte heller användas på ett sätt som gör att deras effektivitet urholkas.[19]

4.2 Överträdelser som kan leda till sanktionsavgift

I dataskyddsförordningen och dataskyddslagen anges uttryckligen vilka överträdelser som kan leda till administrativa sanktionsavgifter.[20] För att det ska bli aktuellt med sanktionsavgifter måste det därför vara fråga om en överträdelse av någon av följande bestämmelser:

Artikel	**Innehåll**
8, 11, 25–39, 42 och 43	Personuppgiftsansvarigas/personuppgiftsbiträdens skyldigheter
42 och 43	Certifieringsorganets skyldigheter
41.4	Övervakningsorganets skyldigheter
5, 6, 7 och 9	Grundläggande principer, inklusive villkoren för samtycke
12–22	Registrerades rättigheter
44–49	Överföring av personuppgifter till tredjeland m.m.
10[21]	Behandling av personuppgifter som rör lagöverträdelser
3 kap. 10 § dataskyddslagen[22]	Behandling av personnummer/samordningsnummer
58.2 c–h och j[23]	Underlåtenhet att rätta sig efter ett föreläggande från Datainspektionen
58.1[24]	Underlåtelse att ge Datainspektionen tillgång till uppgifter

[19] WP 253 s. 7.
[20] Artikel 83.4–6 dataskyddsförordningen och 6 kap. 3 § dataskyddslagen.
[21] Att artikel 10 dataskyddsförordningen kan föranleda sanktionsavgift följer av 6 kap. 3 § dataskyddslagen. Notera även att artikel 10 inte kan överträdas av myndigheter utan endast av privata subjekt.
[22] Bestämmelsen rör en särskild behandlingssituation och är en sådan skyldighet som följer av nationell lagstiftning som antagits på grundval av dataskyddsförordningens kapitel IX, se artikel 83.5 d.

4.3 Hur sanktionsavgiften ska bestämmas

4.3.1 Maxbelopp

4.3.1.1 Allmänt

I dataskyddsförordningen och dataskyddslagen anges till vilket maxbelopp olika överträdelser ska bestämmas.[25] Bestämmelserna sätter alltså ingen ”prislapp” på specifika överträdelser, utan anger endast en övre beloppsgräns. Detta innebär att skalorna för sanktionsavgifterna går från 0 kronor till i respektive fall angivet maxbelopp.

Maxbeloppen är olika beroende på om överträdelsen har begåtts av företag/andra organisationer eller myndigheter (se avsnitt 4.3.1.2 respektive 4.3.1.3 nedan). För företag gäller att den övre beloppsgränsen ska sättas till, beroende på vilket belopp som är högst, antingen det angivna maxbeloppet eller viss angiven procentsats av företagets totala globala årsomsättning.

4.3.1.2 Företag och andra organisationer[26]

Vid överträdelser av följande bestämmelser (mindre allvarliga överträdelser) är, enligt artikel 83.4 dataskyddsförordningen, maxbeloppet för påförande av administrativa sanktionsavgifter 10 000 000 EUR eller, om det gäller ett företag, på upp till 2 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst:

Artikel	**Innehåll**
8, 11, 25–39, 42 och 43	Personuppgiftsansvarigas/personuppgiftsbiträdens skyldigheter
42 och 43	Certifieringsorganets skyldigheter
41.4	Övervakningsorganets skyldigheter

[23] Artikel 83.5 e och 83.6 dataskyddsförordningen.
[24] Artikel 83.5 e dataskyddsförordningen.
[25] Artikel 83.4–6 dataskyddsförordningen och 6 kap. 2–3 §§ dataskyddslagen.
[26] Ett företag definieras enligt artikel 4.18 dataskyddsförordningen som en fysisk eller juridisk person som bedriver ekonomisk verksamhet, oavsett dess juridiska form, vilket inbegriper partnerskap eller föreningar som regelbundet bedriver ekonomisk verksamhet. Notera att kommunala bolag är att anse som företag vid tillämpningen av dataskyddsförordningen. Observera dock att det inte är denna företagsdefinition – utan den konkurrensrättsliga definitionen som framgår av artikel 150 dataskyddsförordningen – som ska användas vid bestämmande av maxbeloppet för sanktionsavgiften, se vidare nedan.

Vid överträdelser av följande bestämmelser (allvarliga överträdelser) är, enligt artikel 83.5–6 dataskyddsförordningen, maxbeloppet för påförande av administrativa sanktionsavgifter 20 000 000 EUR eller, om det gäller ett företag, på upp till 4 % av den totala globala årsomsättningen under föregående budgetår, beroende på vilket värde som är högst:

Artikel	**Innehåll**
5, 6, 7 och 9	Grundläggande principer, inklusive villkoren för samtycke
12–22	Registrerades rättigheter
44–49	Överföring av personuppgifter till tredjeland m.m.
10[27]	Behandling av personuppgifter som rör lagöverträdelser
3 kap. 10 § dataskyddslagen[28]	Behandling av personnummer/samordningsnummer
58.2 c–h och j[29]	Underlåtenhet att rätta sig efter ett föreläggande från Datainspektionen
58.1 e[30]	Underlåtelse att ge Datainspektionen tillgång till uppgifter

Vid bestämmande av maxbeloppet för sanktionsavgiften ska Datainspektionen använda den definition av begreppet företag som EU-domstolen använder vid tillämpning av artikel 101 och 102 i EUF-fördraget. Detta innebär att begreppet företag omfattar varje enhet som utövar ekonomisk verksamhet, oavsett enhetens rättsliga form och sättet för dess finansiering. Ett företag ska förstås som en ekonomisk enhet, även om enheten i juridisk mening består av flera fysiska eller juridiska personer. Företaget/enheten kan därmed ofta utgöras av en koncern, dvs. ett moderbolag och alla dess dotterbolag.[31] Notera att denna definition av företag (*Eng.* undertaking) – som framgår av skäl 150 och ska användas vid bestämmande av sanktionsavgiftens maxbelopp enligt artikel 83 – skiljer sig från den definition av företag (*Eng.* enterprise) som följer av artikel 4.18 dataskyddsförordningen.

[27] Se fotnot 20.
[28] Se fotnot 21.
[29] Artikel 83.5 e och 83.6 dataskyddsförordningen.
[30] Artikel 83.5 e dataskyddsförordningen.
[31] Skäl 150 dataskyddsförordningen och WP 253 s. 6. Notera att denna fråga även berörs av pågående diskussioner inom Europeiska dataskyddsstyrelsen (EDPB).

4.3.1.3 Myndigheter[32]

Även myndigheter kan påföras administrativa sanktionsavgifter vid överträdelser av dataskyddsförordningen. För myndigheter är det högsta beloppet emellertid lägre än vad som gäller för privata aktörer. I detta sammanhang ska erinras om att en överträdelse av en kompletterande nationell bestämmelse även måste utgöra en överträdelse av en artikel i dataskyddsförordningen för att en sanktionsavgift ska kunna påföras, se avsnitt 1.2 ovan.

Med undantag för att lägre maxbelopp gäller för myndigheter ska dataskydds-förordningen och dessa riktlinjer i övrigt tillämpas på samma sätt för myndigheter som för företag och andra organisationer.

Vid överträdelser av följande bestämmelser (mindre allvarliga överträdelser) är, enligt 6 kap. 2 § dataskyddslagen och artikel 83.4 dataskyddsförordningen, max-beloppet för påförande av administrativa sanktionsavgifter 5 000 000 kronor:

Artikel	**Innehåll**
8, 11, 25–39, 42 och 43	Personuppgiftsansvarigas/personuppgiftsbiträdens skyldigheter
42 och 43	Certifieringsorganets skyldigheter
41.4	Övervakningsorganets skyldigheter

Vid överträdelser av följande bestämmelser (allvarliga överträdelser) är, enligt 6 kap. 2 § dataskyddslagen och artikel 83.5–6 dataskyddsförordningen, max-beloppet för påförande av administrativa sanktionsavgifter 10 000 000 kronor:

Artikel	**Innehåll**
5, 6, 7 och 9	Grundläggande principer, inklusive villkoren för samtycke
12–22	Registrerades rättigheter
44–49	Överföring av personuppgifter till tredjeland m.m.
3 kap. 10 § dataskyddslagen[33]	Behandling av personnummer/samordningsnummer
58.2 c–h och j[34]	Underlåtenhet att rätta sig efter ett föreläggande från Datainspektionen
58.1[35]	Underlåtelse att ge Datainspektionen tillgång till uppgifter

[32] Enligt regeringsformens terminologi, som bör användas även vid tolkningen av dataskydds-förordningen, är alla offentliga organ utom riksdagen och kommun- och landstingsfullmäktige myndigheter, se prop. 2017/18:105, s. 139.
[33] Se fotnot 21.
[34] Artikel 83.5 e och 83.6 dataskyddsförordningen.
[35] Artikel 83.5 e dataskyddsförordningen.

4.3.1.4 Flera överträdelser

En och samma behandling eller sammankopplade behandlingar av personuppgifter kan innebära att flera bestämmelser överträds samtidigt. Vid sådan överträdelse av flera bestämmelser ska sanktionsavgiften bestämmas efter de samlade överträdelsernas allvar. Den administrativa sanktionsavgiftens totala belopp får dock inte överstiga maxbeloppet för den allvarligaste överträdelsen.[36]

4.3.2 Bedömningskriterier

I dataskyddsförordningen anges vilka faktorer som ska beaktas (i) vid beslut om administrativa sanktionsavgifter överhuvudtaget ska påföras och (ii) vid bestämmande av avgiftens storlek.[37]

Nedan följer en genomgång av nämnda bedömningskriterier. För ytterligare vägledning hänvisas till Artikel 29-gruppens WP 253 ”Riktlinjer för tillämpning och fastställande av administrativa sanktionsavgifter i enlighet med förordning 2016/679”.

(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)

Nästan alla skyldigheter som personuppgiftsansvariga och personuppgiftsbiträden har enligt dataskyddsförordningen kategoriseras efter sin *karaktär* i artikel 83.4–6. Redan det faktum att dataskyddsförordningen anger två olika högsta belopp för sanktionsavgiften ger därmed en indikation om att det är allvarligare att överträda vissa bestämmelser (artikel 83.5 och 83.6) än andra (artikel 83.4). Överträdelsens karaktär, men också behandlingens omfattning, syfte samt antalet berörda registrerade och den skada som de har lidit ger en indikation om överträdelsens *svårighetsgrad*.[38]

Antalet berörda registrerade bör fastställas för att kunna avgöra om det rör sig om en enstaka händelse eller en mer systematisk överträdelse. Även en enstaka händelse kan dock 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. Generellt gäller att överträdelsen är allvarligare ju fler registrerade som berörs.[39]

---

[36] Artikel 83.3 dataskyddsförordningen.
[37] Artikel 83.2 dataskyddsförordningen.
[38] WP 253 s. 9 f.
[39] Jfr WP 253 s. 10.

Syftet med behandlingen ska också bedömas och beaktas. Personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och får senare inte behandlas på ett sätt som är oförenligt med dessa ändamål. En otillåten behandling som sker i strid med det ursprungliga ändamålet är generellt sett allvarligare än en överträdelse som äger rum inom ramen för detsamma.[40]

Om de registrerade har lidit *skada* ska hänsyn tas till skadans omfattning. Behandling av personuppgifter kan leda till risk för enskildas rättigheter och friheter, vilket kan medföra fysiska, materiella eller immateriella skador, i synnerhet om behandlingen kan resultera i diskriminering, identitetsstöld, bedrägeri, ekonomisk förlust, skadat anseende m.m.[41] Om skadorna har uppstått eller sannolikt kommer att uppstå på grund av en överträdelse av dataskyddsförordningen ska detta beaktas vid valet av korrigerande åtgärd.[42]

Överträdelsens *varaktighet* ska beaktas. Ju längre tid en överträdelse har pågått, desto allvarligare är den som regel. Varaktigheten kan även ge en uppfattning om bland annat (i) den personuppgiftsansvariges uppsåt, (ii) underlåtenhet att vidta lämpliga försiktighetsåtgärder, eller (iii) oförmåga att införa de tekniska och organisatoriska åtgärder som krävs.[43]

(b) Om överträdelsen skett med uppsåt eller genom oaktsamhet

Hänsyn ska tas till om överträdelsen har varit uppsåtlig eller oaktsam. En avsiktlig överträdelse, som visar på nonchalans mot regleringen, är allvarligare än en oavsiktlig sådan. En överträdelse som skett med uppsåt motiverar därmed i större utsträckning att en administrativ sanktionsavgift påförs, och att densamma sätts till ett högre belopp. Att åsidosätta bestämmelserna för att uppnå ekonomisk vinning är exempel på ett uppsåtligt agerande.[44]

I många fall är dock överträdelser resultatet av mer eller mindre oaktsamma förfaranden, till exempel missförstånd om hur regleringen ska tillämpas eller ursäktliga bedömningsfel. Om överträdelsen beror på oaktsamhet bör även graden av oaktsamhet vägas in.[45]

---

[40] Jfr WP 253 s. 11.
[41] Angående riskerna för den enskildes rättigheter och friheter, se vidare skäl 75 dataskyddsförordningen.
[42] WP 253 s. 11.
[43] WP 253 s. 11.
[44] Jfr prop. 2017/18:232 s. 330. Se även WP 253 s. 11 f.
[45] Jfr prop. 2017/18:232 s. 330.

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

Såväl vid valet av korrigerande åtgärd som vid beräkningen av en eventuell sanktionsavgift ska hänsyn tas till vad den personuppgiftsansvarige eller personuppgiftsbiträdet har gjort för att begränsa konsekvenserna av överträdelsen för de enskilda som berörs. Ett ansvarsfullt beteende i form av att vidta åtgärder för att lindra verkningarna ökar möjligheten att inte ta ut någon sanktionsavgift eller leder i vart fall till att sanktionsavgiften blir lägre än den annars skulle ha blivit.[46]

Exempel på åtgärd för att lindra skadorna kan vara att snabbt stoppa överträdelsen från att fortsätta eller utökas till en nivå eller fas som skulle ha gjort följderna mycket allvarligare än de blev.[47]

(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)

Vilka tekniska och organisatoriska åtgärder (enligt artiklarna 25 och 32) som har vidtagits i syfte att undvika överträdelser ska beaktas. Ju fler och effektivare förebyggande åtgärder som vidtagits, desto mindre klandervärt framstår de ansvarigas agerande. Frågan som bör ställas är i vilken grad den personuppgiftsansvarige eller personuppgiftsbiträdet har gjort vad som kunde förväntas, med beaktande av behandlingens karaktär, ändamål och omfattning, i förhållande till sina skyldigheter enligt dataskyddsförordningen. Vid bedömningen ska hänsyn tas till eventuella ”bästa praxis”-koder, dvs. industristandarder och uppförandekoder inom olika områden och yrken.[48]

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

Hänsyn ska också tas till om den personuppgiftsansvarige eller personuppgiftsbiträdet tidigare har gjort sig skyldig till överträdelser. Exempelvis kan den personuppgiftsansvarige eller personuppgiftsbiträdet ha gjort sig skyldig till samma överträdelse tidigare eller ha begått en överträdelse på samma sätt (till exempel – som en följd av otillräcklig kunskap om befintliga rutiner inom organisationen eller olämplig riskbedömning – inte svarat tillräckligt snabbt eller dröjt omotiverat länge med

[46] Jfr WP 253 s. 12 f. Jfr även prop. 2017/18:232 s. 331.
[47] WP 253 s. 13.
[48] WP 253 s. 13. Jfr även prop. 2017/18:232 s. 331.

att svara på begäranden från registrerade). Alla typer av överträdelser av dataskyddsförordningen kan emellertid vara relevanta för bedömningen, även sådana som är annorlunda till sin karaktär än den som utreds för tillfället, eftersom de kan visa att den allmänna kunskapsnivån är för låg eller att dataskyddsreglerna generellt inte beaktas.[49]

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

Om den personuppgiftsansvarige eller personuppgiftsbiträdet har samarbetat med Datainspektionen för att komma till rätta med överträdelsen och minska dess negativa effekter så talar det i förmildrande riktning. Sådant samarbete kan exempelvis vara relevant att beakta om den personuppgiftsansvariges eller personuppgiftsbiträdets insats under Datainspektionens utredning har lett till att de negativa följderna för enskildas rättigheter aldrig uppkom eller blev mer begränsade än de annars skulle ha blivit. I sammanhanget bör hänsyn dock inte tas till sådant samarbete som redan följer av dataskyddsförordningen, såsom skyldigheten att ge Datainspektionen tillträde till lokaler för inspektion.[50]

(g) De kategorier av personuppgifter som påverkas av överträdelsen

Om känsliga personuppgifter (artikel 9) eller andra särskilt integritetskänsliga uppgifter (däribland artikel 10) har behandlats felaktigt, är utrymmet för att avstå från att ta ut sanktionsavgift mindre och beloppet ska generellt sättas högre. Det kan även ha betydelse för bedömningen om personerna är direkt eller indirekt identifierbara och om uppgifterna är direkt tillgängliga utan tekniska eller organisatoriska skydd.[51] Jämför även punkten (d) ovan angående graden av ansvar hos den personuppgiftsansvarige eller personuppgiftsbiträdet med beaktande av de tekniska och organisatoriska åtgärder som genomförts av dem.

[49] WP 253 s. 14.
[50] WP 253 s. 14.
[51] WP 253 s. 14 f. Jfr även prop. 2017/18:232 s. 331.

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

Hur Datainspektionen fick kännedom om överträdelsen ska beaktas. Att den personuppgiftsansvarige eller personuppgiftsbiträdet själv har anmält överträdelsen eller tvärtom försökt dölja den kan beaktas i förmildrande respektive försvårande riktning. När den personuppgiftsansvarige endast uppfyller sin skyldighet att anmäla en personuppgiftsincident enligt dataskyddsförordningen ska det dock inte anses som en förmildrande faktor. Att däremot inte anmäla en personuppgiftsincident bör betraktas som en försvårande omständighet.[52]

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

Om den personuppgiftsansvarige eller personuppgiftsbiträdet inte efterlever de korrigerande åtgärder som Datainspektionen har utfärdat vid ett tidigare tillfälle mot samma personuppgiftsansvarig eller personuppgiftsbiträde ”vad gäller samma sakfråga” ska det beaktas i försvårande riktning.[53] Se även punkten (e) ovan angående eventuella relevanta tidigare överträdelser som den personuppgiftsansvarige eller personuppgiftsbiträdet gjort sig skyldig till.

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

Personuppgiftsansvariga och personuppgiftsbiträden kan visa efterlevnad av dataskyddsförordningen genom att följa godkända uppförandekoder. Vid överträdelse av förordningen kan tillämpningen av en godkänd uppförandekod ge Datainspektionen en uppfattning om hur stort behovet är av att ingripa med en sanktionsavgift eller någon annan korrigerande åtgärd. Datainspektionen kan i sådana fall nöja sig med att den organisation som står bakom koden själv vidtar lämpliga åtgärder[54] mot sin medlem. Datainspektionen kan komma fram till att

[52] WP 253 s. 15 (notera att i den svenska översättningen har ”personal data breach”, dvs. personuppgiftsincident, felaktigt översatts till ”överträdelser rörande personuppgifter”). Jfr även prop. 2017/18:232 s. 331.
[53] Jfr WP 253 s. 15.
[54] Enligt artikel 40.4 dataskyddsförordningen ska en godkänd uppförandekod innehålla mekanismer som gör det möjligt för det (övervakande) organet att utföra den obligatoriska övervakningen av att dess bestämmelser efterlevs. Av artikel 41.2 c och artikel 42.4 dataskyddsförordningen följer att vissa former av sanktioner, såsom avstängning eller uteslutning från uppförandekoden, kan påföras genom övervakningssystemet när skyldigheterna inte uppfylls.

sådana åtgärder är tillräckligt effektiva, proportionella och avskräckande i det enskilda fallet och att det inte behövs några ytterligare åtgärder.[55]

(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

Andra försvårande eller förmildrande faktorer kan beaktas vid beslut om lämpligheten av en administrativ sanktionsavgift. Exempelvis kan information om förtjänst på grund av en överträdelse vara särskilt viktig att ta hänsyn till, eftersom sådan ekonomisk vinning inte kan kompenseras genom (korrigerande) åtgärder som inte har några ekonomiska konsekvenser. Det faktum att en personuppgiftsansvarig har haft vinning av överträdelsen kan i sig utgöra en stark indikation på att en sanktionsavgift bör påföras.[56]

4.3.3 Effektivt, proportionellt och avskräckande

Med hänsyn tagen till aktuell överträdelse, bedömningskriterierna i artikel 83.2, det enskilda objektets ekonomiska situation och harmoniseringen inom EU, ska den beslutade administrativa sanktionsavgiften vara effektiv, proportionell och avskräckande.[57] Det betyder att sanktionsavgiften i varje enskilt fall ska vara kännbar för tillsynsobjektet och verka förebyggande för såväl tillsynsobjektet som andra, men också vara rimlig i förhållande till överträdelsen.

Om det beslutas om en sanktionsavgift för flera överträdelser avseende en och samma behandling eller sammankopplade behandlingar (se avsnitt 4.3.1.4 ovan angående maxbeloppet) ska en avvägning göras så att det totala beloppet blir effektivt, proportionellt och avskräckande.

För det fall ett tillsynsbeslut innehåller flera överträdelser som inte avser en och samma behandling eller sammankopplade behandlingar, och som därför leder till separata sanktionsavgifter, behöver också en helhetsbedömning göras så att den totala reaktionen blir effektiv, proportionell och avskräckande. Det innebär att den totala summan av sanktionsavgifterna behöver ställas i relation till framförallt tillsynsobjektets ekonomiska situation, och en eventuell justering sker då proportionellt avseende respektive sanktionsavgift.

---

[55] WP 253 s. 15 f.

[56] WP 253 s. 16.

[57] Jfr artikel 83.1 dataskyddsförordningen. Notera också att för att kunna påföra sanktionsavgifter som är effektiva, proportionella och avskräckande ska Datainspektionen i sin bedömning använda den konkurrensrättsliga definitionen av begreppet företag, se avsnitt 4.3.1.2 ovan (skäl 150 dataskyddsförordningen och WP 253 s. 6).

Exempel

Datainspektionen har vid en tillsyn konstaterat att ett företag i egenskap av personuppgiftsansvarig (PUA) överträtt flera artiklar i dataskyddsförordningen vid behandling av personuppgifter i sitt kundhanteringssystem. Utöver detta har Datainspektionen funnit olika brister i hur PUA hanterar sina anställdas personuppgifter, däribland vilken övervakning som sker och vilken information som lämnas till de anställda. Överträdelserna gällande kundhanteringssystemet avser en och samma behandling eller sammankopplade behandlingar och ska därför bedömas tillsammans när sanktionsavgiften bestäms. Bristerna vad gäller behandlingen av de anställdas personuppgifter avser också en och samma behandling eller sammankopplade behandlingar och ska på samma sätt bedömas tillsammans vid bestämmande av denna sanktionsavgift. Däremot avser bristerna gällande kundhanteringssystemet och behandlingen av de anställdas uppgifter inte samma behandling och är inte heller att anse som sammankopplade behandlingar. Dessa olika behandlingssituationer ska därför, som utgångspunkt, hanteras var för sig och kommer, om aktuellt, att resultera i två separata sanktionsavgifter. Varje sanktionsavgift i det enskilda fallet ska vara effektiv, proportionell och avskräckande.

Eftersom beslutet avser en och samma PUA behöver dessutom en helhetsbedömning göras för att kontrollera att den sammanlagda summan av sanktionsavgifterna blir effektiv, proportionell och avskräckande i förhållande till främst PUA:s ekonomiska förutsättningar. Då respektive sanktionsavgift redan är bedömd i förhållande till dessa kriterier bör det som regel inte behövas någon ytterligare justering, men om detta krävs för att det totala beloppet i beslutet inte ska bli oproportionerligt, justeras de båda sanktionsavgifterna proportionellt.

Om en administrativ sanktionsavgift åläggs en person som inte är ett företag, till exempel en privatperson eller en ideell förening (se avsnitt 4.3.1.2 ovan) ska Datainspektionen vid övervägandet av lämplig sanktionsavgift, utöver personens ekonomiska situation, ta hänsyn till den allmänna inkomstnivån i Sverige.[58]

4.3.4 Harmonisering

Ett beslut om administrativa sanktionsavgifter ska så långt som möjligt harmoniseras inom EU. Innan ett beslut fattas ska det därför beredas med Datainspektionens EU-sekretariat. Vid denna beredning ska beslut i likartade ärenden i andra medlemsstater och gemensamma vägledningar beaktas.

[58] Skäl 150 dataskyddsförordningen.

4.4 Förfarandebestämmelser

Ett beslut om administrativ sanktionsavgift är en särskilt ingripande åtgärd. En sanktionsavgift får därför inte beslutas om den som anspråket riktas mot inte har fått tillfälle att yttra sig inom fem år från den dag då överträdelsen ägde rum. Vidare ska ett beslut om sanktionsavgift delges den betalningsskyldige enligt delgivningslagen.[59] Sanktionsavgifter tillfaller staten[60] och ska betalas till Kammarkollegiet[61] inom 30 dagar från det att beslutet om att ta ut avgiften har vunnit laga kraft eller inom den längre tid som anges i beslutet.[62] Så snart ett beslut har vunnit laga kraft ska Datainspektionen således skicka detta, tillsammans med besked om laga kraft och delgivning, till Kammarkollegiet för verkställande.

[59] 6 kap. 4 § dataskyddslagen.
[60] 6 kap. 5 § dataskyddslagen.
[61] 9 § förordningen med kompletterande bestämmelser till EU:s dataskyddsförordning (SFS 2018:219).
[62] Prop. 2017/18:105 s. 147.