Datainspektionen

Datainspektionens styrdokument

Dnr: 345-2018
Beslutsdatum: 2018-12-19

Datainspektionens riktlinjer för förebyggande och korrigerande befogenheter samt administrativa sanktionsavgifter enligt brottsdatalagen

Innehåll

1. Inledning

1.1 Bakgrund och syfte

Brottsdatalagen (2018:1177)[1], BDL, är en ramlag och gäller för personuppgiftsbehandling i brottsbekämpande verksamhet[2]. Med brottsbekämpande verksamhet menas allt arbete som sker för att förebygga, förhindra, utreda, avslöja eller lagföra brott. BDL gäller även i verksamhet som sker för att verkställa straffrättsliga påföljder[3] och för upprätthållande av allmän ordning och säkerhet[4]. Datainspektionen är ansvarig för att övervaka att dataskyddsreglerna tillämpas på ett riktigt sätt när personuppgifter behandlas. I syfte att uppnå denna regelefterlevnad ger BDL Datainspektionen förebyggande och korrigerande befogenheter.

Datainspektionens riktlinjer för förebyggande och korrigerande befogenheter samt administrativa sanktionsavgifter enligt brottsdatalagen (riktlinjerna) har till syfte att säkerställa att en enhetlig och likvärdig bedömning sker avseende Datainspektionens befogenheter. Riktlinjerna utgår från BDL och de kompletterande bestämmelserna i brottsdataförordningen (2018:1202), BDF.

Av övergångsbestämmelserna till BDL (punkten 4) framgår att en sanktionsavgift endast får beslutas för överträdelser som har skett efter ikraftträdandet[5].

För myndigheterna i rättskedjan krävs även viss särreglering som regleras i sektorsspecifika författningar. Nya sektorsspecifika författningar för polisen, Tullverket, Kustbevakningen, Skatteverket, åklagarväsendet, domstolarna och kriminalvården träder i kraft den 1 januari 2019. Lagarna gäller utöver BDL och innehåller enbart bestämmelser som innebär preciseringar, undantag eller avvikelser från den lagen. Överträdelser av vissa bestämmelser i de nya sektorsspecifika författningarna kan leda till att en sanktionsavgift tas ut. Enligt övergångsbestämmelserna får en sanktionsavgift inte tas ut om överträdelsen har skett före den 1 januari 2019.

---

[1] Brottsdatalagen införlivar EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF.

[2] Polismyndigheten, Ekobrottsmyndigheten, Åklagarmyndigheten, Tullverket, Skatteverket och Kustbevakningen.

[3] Sådan verksamhet bedrivs till exempel av Kriminalvården (om någon döms till fängelse), Kronofogdemyndigheten (om någon döms till böter), kommunernas socialnämnder (om ungdomar döms till vård inom socialtjänsten) eller sjukhus (om någon döms till psykiatrisk tvångsvård).

[4] Myndigheter som exempelvis Polismyndigheten och Kustbevakningen.

[5] Den 1 augusti 2018.

1.2 Tillämpningsområde och avgränsning

BDL gäller enligt 1 kap. 2 § vid behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga, förhindra eller upptäcka brottslig verksamhet, utreda eller lagföra brott eller verkställa straffrättsliga påföljder. BDL gäller också vid behandling av personuppgifter som en behörig myndighet utför i syfte att upprätthålla allmän ordning och säkerhet.

BDL gäller enligt 1 kap. 4 § inte vid Säkerhetspolisens behandling av personuppgifter som rör nationell säkerhet eller om Polismyndigheten har övertagit en arbetsuppgift som rör nationell säkerhet från Säkerhetspolisen.

Dessa riktlinjer omfattar personuppgiftsbehandling enligt BDL. Vid personuppgiftsbehandling som sker enligt dataskyddsförordningen[6] ska Datainspektionens riktlinjer för korrigerande befogenheter enligt artikel 58.2 dataskyddsförordningen tillämpas.

Det kan noteras att Datainspektionen, utöver sina förebyggande och korrigerande befogenheter, också har undersökningsbefogenheter enligt 5 kap. 5 § BDL. Undersökningsbefogenheter kan till exempel vara att på begäran få tillgång till alla personuppgifter som behandlas, upplysningar om och dokumentation av behandling av personuppgifter samt tillträde till lokaler. Sådana befogenheter faller dock utanför riktlinjernas tillämpningsområde.

2. Principer för val av befogenhet

Datainspektionens befogenheter bör ses som en trappa som ger möjlighet att successivt använda kraftfullare medel och därigenom stegra påtryckningarna på den som inte självmant rättar sig efter inspektionens anvisningar. De korrigerande åtgärderna är dock inte kopplade till varandra på det sättet att en strängare åtgärd förutsätter att alla mindre ingripande åtgärder redan har prövats.[7]

[6] 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).
[7] Se prop. 2017/18:232 s. 293 f.

3. Förebyggande och korrigerande befogenheter

Förebyggande befogenheter

Bestämmelse	Befogenhet	Karaktär
5 kap. 6 § första stycket BDL	Råd, rekommendationer eller påpekanden	Inte bindande
5 kap. 6 § andra stycket BDL	Varning	Inte bindande

Korrigerande befogenheter

Bestämmelse	Befogenhet	Karaktär
5 kap. 7 § första stycket 1 BDL	Råd, rekommendationer eller påpekanden	Inte bindande
5 kap. 7 § första stycket 2 BDL	Förelägganden	Bindande
5 kap. 7 § första stycket 3 BDL	Förbud mot fortsatt behandling	Bindande
5 kap. 7 § första stycket 4 BDL	Administrativ sanktionsavgift	Bindande

3.1 Förebyggande befogenheter

3.1.1 Allmänt

Om det finns en *risk* för att viss personuppgiftsbehandling kan komma att stå i strid med lag eller annan författning ska de förebyggande befogenheterna i 5 kap. 6 § BDL användas.

3.1.2 Råd, rekommendationer eller påpekanden

Om det finns en risk för att personuppgifter kan komma att behandlas i strid med lag eller annan författning, ska Datainspektionen enligt 5 kap. 6 § första stycket BDL genom råd, rekommendationer eller påpekanden försöka förmå den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att motverka den risken.

En viktig uppgift för Datainspektionen är att lämna råd till personuppgiftsansvariga och personuppgiftsbiträden om deras skyldigheter enligt BDL och att stödja deras strävanden att skapa författningsenliga och integritetssäkra lösningar. Medlen för att motverka risken att behandling av personuppgifter kan komma att strida mot lag

eller annan författning ska främst vara muntliga eller skriftliga råd, rekommendationer och påpekanden. Råden, rekommendationerna eller påpekandena är inte tvingande. På vilket sätt förändringen ska åstadkommas ska i första hand lämnas åt den personuppgiftsansvarige eller personuppgiftsbiträdet att avgöra och i många fall kan det vara tillräckligt att Datainspektionen upplyser om på vilket sätt personuppgiftsbehandlingen riskerar att strida mot regelverket.[8]

Motsvarande uppgift för Datainspektionen att lämna råd till personuppgiftsansvariga och personuppgiftsbiträden finns även i dataskyddsförordningen. I dataskyddsförordningen regleras detta bland annat i artikel 57 om tillsynsmyndighetens uppgifter och inte i artikel 58.2 om tillsynsmyndighetens korrigerande befogenheter.

3.1.3 Varning

Datainspektionen får enligt 5 kap. 6 § andra stycket BDL utfärda en skriftlig varning för att planerad eller pågående behandling av personuppgifter *riskerar* att stå i strid med lag eller annan författning. Med andra ord kan en varning endast utfärdas då någon överträdelse ännu inte har ägt rum.

Varning kan användas för att i ett enskilt fall markera allvaret i en situation och försöka förmå den personuppgiftsansvarige eller personuppgiftsbiträdet att ändra sig i fråga om en kommande behandling. En varning ska utfärdas först när Datainspektionen inte på annat sätt kan förmå den personuppgiftsansvarige eller personuppgiftsbiträdet att följa regelverket.[9] Som exempel kan en varning aktualiseras om det vid förhandssamråd enligt 3 kap. 7 § andra stycket BDL visar sig att det finns risk för att de förändringar som planeras kan göra att den framtida behandlingen inte blir författningsenlig.[10]

En varning ska tydligt ange på vilket sätt den kommande behandlingen riskerar att strida mot regelverket och kan avse vilken form av förändring som helst i behandlingen. En varning är inte bindande och leder inte till något överklagbart beslut.[11]

3.2 Korrigerande befogenheter

3.2.1 Allmänt

De korrigerande befogenheterna i 5 kap. 7 § BDL ska användas när det har *konstaterats* att behandlingen strider mot gällande bestämmelser.

---

[8] Se prop. 2017/18:232 s. 294.
[9] Se prop. 2017/18:232 s. 295.
[10] Se prop. 2017/18:232 s. 478.
[11] Se prop. 2017/18:232 s. 295.

3.2.2 Råd, rekommendationer eller påpekanden

Om personuppgifter behandlas i strid med lag eller annan författning eller att den personuppgiftsansvarige eller personuppgiftsbiträdet på något annat sätt inte fullgör sina skyldigheter, får Datainspektionen enligt 5 kap. 7 § första stycket 1 BDL genom råd, rekommendationer eller påpekanden, försöka förmå den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig, eller att uppfylla andra skyldigheter.

3.2.3 Förelägganden

Om personuppgifter behandlas i strid med lag eller annan författning eller att den personuppgiftsansvarige eller personuppgiftsbiträdet på något annat sätt inte fullgör sina skyldigheter, får Datainspektionen enligt 5 kap. 7 § första stycket 2 BDL förelägga den personuppgiftsansvarige eller personuppgiftsbiträdet att vidta åtgärder för att behandlingen ska bli författningsenlig eller att uppfylla andra skyldigheter. Enligt 5 kap. 7 § andra stycket BDL ska det av föreläggandet framgå när åtgärderna senast ska vara genomförda och, om det är lämpligt, vilka åtgärder som ska vidtas.

Tillsynsobjektet är oftast bäst lämpat att avgöra vad som ska göras för att behandlingen ska bli författningsenlig. Det kan till exempel vara fråga om vilka tekniska åtgärder som ska vidtas eller vilka säkerhetslösningar som ska väljas. Datainspektionen ska därför endast om det är lämpligt ange vilken åtgärd som ska vidtas.[12] 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.

Datainspektionen har bland annat möjlighet att förelägga om rättelse, radering eller begränsning av behandling. I dessa fall kan det vara lämpligt att ange vilken åtgärd som ska vidtas. När Datainspektionen använder sin befogenhet att förelägga om rättelse, radering eller begränsning av behandling ska inspektionen bland annat beakta att åtgärden inte får strida mot annan lagstiftning, till exempel bestämmelser om bevarande av allmänna handlingar.[13]

Datainspektionen kan även förelägga den behöriga myndigheten att uppfylla andra skyldigheter, till exempel att vidta ytterligare tekniska eller organisatoriska åtgärder

[12] Se prop. 2017/18:232 s. 296.
[13] Se prop. 2017/18:232 s. 249.

för säkerheten vid behandling eller att inrätta en intern ordning för anmälan av överträdelser av bestämmelserna, upprätta konsekvensbedömning eller fullgöra samrådsskyldighet.[14]

3.2.4 Förbud mot fortsatt behandling

Om personuppgifter behandlas i strid med lag eller annan författning eller att den personuppgiftsansvarige eller personuppgiftsbiträdet på något annat sätt inte fullgör sina skyldigheter, får Datainspektionen enligt 5 kap. 7 § första stycket 3 BDL förbjuda fortsatt behandling om bristen är allvarlig.

Med förbud mot fortsatt behandling avses att någon behandling inte längre får förekomma. Förbud mot fortsatt behandling ska bara meddelas om en myndighet på ett allvarligt sätt har åsidosatt sina skyldigheter och bristerna är sådana att de inte kan åtgärdas på annat sätt än att behandlingen upphör. Åtgärden ska på samma sätt som i dag användas restriktivt. Att en personuppgift har behandlats på ett sådant sätt att förbud mot fortsatt behandling aktualiseras behöver inte innebära att all behandling av uppgiften måste upphöra. Förbudet måste därför kopplas till vad som föranledde det. Hur omfattande förbudet blir beror på vilken typ av personuppgifter det är fråga om och hur de har behandlats.[15] När Datainspektionen använder sin befogenhet att förbjuda fortsatt behandling ska inspektionen, som vid förelägganden, beakta att åtgärden inte får strida mot annan lagstiftning.

Ett förbud mot fortsatt behandling ska normalt vara permanent. I vissa fall kan dock ett tillfälligt förbud vara en lämplig åtgärd, till exempel om den personuppgiftsansvarige trots påpekande eller varning från Datainspektionen har påbörjat otillåten personuppgiftsbehandling och myndigheten bedömer att bristerna kan rättas till.[16]

[14] Se prop. 2017/18:232 s. 478.
[15] Se prop. 2017/18:232 s. 297.
[16] Se prop. 2017/18:232 s. 297.

4. Administrativa sanktionsavgifter

4.1 Överträdelser som kan leda till sanktionsavgift

Enligt 6 kap. 1 § BDL får en sanktionsavgift tas ut av en personuppgiftsansvarig vid överträdelse av följande bestämmelser.

Bestämmelse	**Innehåll**
2 kap. 1–5, 7–12 eller 14–18 §§, 19 § andra stycket eller 22 § BDL	Grundläggande krav på behandling, längsta tid som personuppgifter får behandlas, automatiserade beslut samt behandling för ändamål utanför BDL:s tillämpningsområde
3 kap. 2–8 §§ BDL	Tekniska och organisatoriska åtgärder, tillgången till personuppgifter, konsekvensbedömning och förhandssamråd samt säkerhetsåtgärder
8 kap. 1–6 §§ eller 8 § BDL	Överföring av personuppgifter till tredje land och internationella organisationer
3 kap. 9 § första stycket BDL	Anmälan av personuppgiftsincident
3 kap. 14 § BDF	Dokumentation av personuppgiftsincidenter
5 kap. 5 § BDL	Undersökningsbefogenheter
5 kap. 7 § första stycket 2 eller 3 BDL	Om den personuppgiftsansvarige inte följer Datainspektionens beslut

Enligt 6 kap. 2 § BDL får en sanktionsavgift tas ut av ett personuppgiftsbiträde vid överträdelse av följande bestämmelser.

Bestämmelse	**Innehåll**
3 kap. 5, 6 eller 8 §§ BDL	Loggar, tillgången till personuppgifter och säkerhetsåtgärder
5 kap. 5 § BDL	Undersökningsbefogenheter
5 kap. 7 § första stycket 2 eller 3 BDL	Om personuppgiftsbiträdet inte följer Datainspektionens beslut

4.2 Hur sanktionsavgiften ska bestämmas

4.2.1 Maxbelopp

I 6 kap. 3 § BDL regleras sanktionsavgiftens storlek. För mindre allvarliga överträdelser (3 kap. 6 eller 7 §§ eller av 3 kap. 14 § BDF) ska avgiften bestämmas till

högst 5 000 000 kronor och för allvarliga överträdelser (övriga bestämmelser som anges i 6 kap. 1 och 2 §§ BDL) till högst 10 000 000 kronor.

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.

4.2.2 Bedömningskriterier

I 6 kap. 4 § BDL finns en uppräkning av omständigheter som ska beaktas vid bedömningen av om någon sanktionsavgift ska tas ut och när storleken på sanktionsavgiften ska bestämmas. Uppräkningen är inte uttömmande utan anger de omständigheter som är särskilt viktiga. Det finns därför ett utrymme för att beakta andra försvårande eller förmildrande omständigheter.[17]

Vid bedömningen ska särskild hänsyn tas till följande omständigheter.
1. Om överträdelsen varit uppsåtlig eller berott på oaktsamhet,
2. den skada, fara eller kränkning som överträdelsen inneburit,
3. överträdelsens karaktär, svårhetsgrad och varaktighet,
4. vad den personuppgiftsansvarige eller personuppgiftsbiträdet gjort för att begränsa verkningarna av överträdelsen, och
5. om den personuppgiftsansvarige eller personuppgiftsbiträdet tidigare ålagts att betala en sanktionsavgift.

Första punkten anger att särskild hänsyn ska tas till om överträdelsen varit uppsåtlig eller berott på oaktsamhet. En avsiktlig överträdelse visar tydligt på nonchalans mot regleringen och utrymmet att underlåta att ta ut avgift eller att bestämma avgiften till ett lågt belopp är litet. Avsiktliga överträdelser talar tvärtom för att sanktionsavgift ska tas ut och att den ska sättas högt. I vissa 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 ska även graden av oaktsamhet vägas in.[18]

Den andra punkten anger att den skada, fara eller kränkning som överträdelsen inneburit ska beaktas. Utrymmet att avstå från att ta ut en sanktionsavgift eller att

[17] De omständigheter som ska beaktas överensstämmer till stor del med uppräkningen i artikel 83.2 dataskyddsförordningen och ska tolkas på samma sätt Se prop. 2017/18:232 s. 329 f.
[18] Se prop. 2017/18:232 s. 330.

bestämma avgiften till ett lågt belopp blir mindre ju större skadan, faran eller kränkningen är.[19]

Enligt den tredje punkten ska överträdelsens karaktär, svårhetsgrad och varaktighet beaktas. Det spelar roll vilken typ av personuppgifter som har behandlats, hur många uppgifter som har behandlats, för vilka syften och hur länge uppgifterna har behandlats. Om känsliga personuppgifter eller andra särskilt integritetskänsliga uppgifter har behandlats felaktigt, är utrymmet för att avstå från att ta ut sanktionsavgift mindre och beloppet ska generellt sättas högre. Att en överträdelse vid en samlad bedömning anses vara ringa talar för att någon sanktionsavgift inte ska tas ut eller att den i vart fall ska sättas lågt.[20]

Enligt den fjärde punkten ska hänsyn tas till vad den personuppgiftsansvarige eller personuppgiftsbiträdet gjort för att begränsa verkningarna av överträdelsen. Omständigheter som att kraftfulla åtgärder vidtagits för att lindra verkningarna ökar möjligheten att avstå från att ta ut sanktionsavgift eller i vart fall leda till att sanktionsavgiften blir lägre än den annars skulle ha blivit. Även tekniska och organisatoriska åtgärder som vidtagits i syfte att undvika överträdelser ska beaktas. Ju fler och effektivare åtgärder som vidtagits, desto mindre klandervärt framstår de ansvarigas agerande. Även hur överträdelsen kom till Datainspektionens kännedom kan beaktas. Om den personuppgiftsansvarige eller personuppgiftsbiträdet själv anmält överträdelsen eller försökt att dölja den, kan det beaktas i förmildrande respektive försvårande riktning.[21]

När den personuppgiftsansvarige endast uppfyller sin skyldighet att anmäla en personuppgiftsincident enligt BDL ska det dock inte anses som en förmildrande faktor. Att däremot inte anmäla en personuppgiftsincident bör betraktas som en försvårande omständighet.

Enligt den femte punkten ska det beaktas om den personuppgiftsansvarige eller personuppgiftsbiträdet tidigare ålagts att betala en sanktionsavgift. Det är särskilt graverande om den personuppgiftsansvarige eller personuppgiftsbiträdet trots påpekanden fortsatt att agera i strid med regleringen. Om den personuppgiftsansvarige eller personuppgiftsbiträdet däremot samarbetat med Datainspektionen för att komma till rätta med överträdelser och minska dess negativa effekter talar det i förmildrande riktning.[22]

---

[19] Se prop. 2017/18:232 s. 330.
[20] Se prop. 2017/18:232 s. 331.
[21] Se prop. 2017/18:232 s. 331.
[22] Se prop. 2017/18:232 s. 331.

Sanktionsavgiften får enligt 6 kap. 5 § BDL sättas ned helt eller delvis om överträdelsen är ursäktlig eller om det annars med hänsyn till omständigheterna skulle vara oskäligt att ta ut en avgift. Så kan vara fallet om den personuppgiftsansvarige eller personuppgiftsbiträdet också blir skadeståndsskyldig. Det är då möjligt att jämka beloppet för att undvika att den samlade reaktionen på överträdelsen blir oproportionerlig. Ett annat exempel är om regelverket överträtts på ett sådant sätt att det varit närmast omöjligt för den personuppgiftsansvarige att upptäcka överträdelsen. Möjligheten att helt sätta ned avgiften ska tillämpas restriktivt och endast användas i undantagsfall. Det ska enbart aktualiseras om det skulle vara oskäligt att ta ut en sanktionsavgift.[23]

4.3 Förfarandebestämmelser

Enligt 6 kap. 6 § BDL är det Datainspektionen som beslutar om sanktionsavgift och sanktionsavgiften tillfaller staten. Vidare framgår det av 6 kap. 7 § BDL att en sanktionsavgift inte får beslutas om den som avgiften ska tas ut av inte har fått tillfälle att yttra sig inom fem år från den dag då överträdelsen ägde rum samt att ett beslut om sanktionsavgift ska delges.

Av 6 kap. 8 § BDL och 6 kap. 1 § BDF framgår att en sanktionsavgift ska betalas till Kammarkollegiet inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet. 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.

Datainspektionens beslut enligt 5 kap. BDL får inte verkställas omedelbart.

[23] Se prop. 2017/18:232 s. 331 f.