Riktlinjer

Riktlinjer 04/2022 om beräkning av administrativa sanktionsavgifter enligt den allmänna dataskyddsförordningen

Version 2.1

Antagna den 24 maj 2023

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Version 1.0	12.5.2022	Antagande av riktlinjerna inför offentligt samråd
Version 2.0	24.5.2023	Antagande av riktlinjerna efter offentligt samråd
Version 2.1	29.6.2023	Mindre korrigeringar

Europeiska dataskyddsstyrelsen (EDPB) har antagit dessa riktlinjer för att harmonisera de metoder som tillsynsmyndigheterna använder vid beräkningen av sanktionsbeloppet. Dessa riktlinjer kompletterar de tidigare antagna riktlinjerna för tillämpning och fastställande av administrativa sanktionsavgifter i enlighet med förordning 2016/679 (WP 253), som är inriktade på de omständigheter under vilka sanktionsavgifter ska åläggas.

Det står tillsynsmyndigheten fritt att beräkna sanktionsbeloppet, om inte annat följer av bestämmelserna i den allmänna dataskyddsförordningen. I detta sammanhang ska sanktionsbeloppet i varje enskilt fall vara effektivt, proportionellt och avskräckande (artikel 83.1 i dataskyddsförordningen). När tillsynsmyndigheterna fastställer sanktionsbeloppet ska de dessutom ta vederbörlig hänsyn till en förteckning över omständigheter som hänvisar till drag hos överträdelsen (dess allvarlighetsgrad) eller egenskaper hos gärningsmannen (artikel 83.2 i dataskyddsförordningen). Slutligen får sanktionsbeloppet inte överstiga de maximibelopp som anges i artikel 83.4, 83.5 och 83.6 i den allmänna dataskyddsförordningen. Kvantifieringen av sanktionsbeloppet baseras därför på en särskild utvärdering som görs i varje enskilt fall, inom ramen för de parametrar som föreskrivs i dataskyddsförordningen.

Mot bakgrund av ovanstående har EDPB utarbetat följande metod, bestående av fem steg, för beräkning av administrativa sanktionsavgifter för överträdelser av dataskyddsförordningen.

För det första måste uppgiftsbehandlingen i fallet identifieras och tillämpningen av artikel 83.3 i dataskyddsförordningen måste utvärderas (**kapitel 3**). För det andra måste utgångspunkten för ytterligare beräkning av sanktionsbeloppet fastställas (**kapitel 4**). Detta görs genom att utvärdera klassificeringen av överträdelsen i dataskyddsförordningen, bedöma överträdelsens allvarlighet mot bakgrund av omständigheterna i fallet och utvärdera företagets omsättning. Det tredje steget är att utvärdera försvårande och förmildrande omständigheter i samband med den personuppgiftsansvariges/personuppgiftsbiträdets tidigare eller nuvarande beteende och öka eller minska sanktionsavgifterna i enlighet därmed (**kapitel 5**). Det fjärde steget är att fastställa de relevanta lagstadgade maximibeloppen för de olika överträdelserna. Ökningar som tillämpas i föregående eller nästa steg får inte överstiga detta maximibelopp (**kapitel 6**). Slutligen måste det analyseras om det beräknade slutliga beloppet uppfyller kraven på effektivitet, avskräckande effekt och proportionalitet. Böterna kan fortfarande justeras i enlighet med detta (**kapitel 7**), dock utan att överskrida det relevanta lagstadgade maximibeloppet.

I alla ovannämnda steg måste man komma ihåg att beräkningen av sanktionsavgifter inte bara är en matematisk övning. Snarare är omständigheterna i det specifika fallet de avgörande faktorer som leder fram till det slutliga beloppet, vilket i samtliga fall kan vara vilket belopp som helst upp till och med det lagstadgade maximibeloppet.

Dessa riktlinjer och dess metoder kommer att ses över kontinuerligt av EDPB.

Innehållsförteckning

SAMMANFATTNING 3

KAPITEL 1 – INLEDNING 6

1.1 – Rättslig ram 6
1.2 – Mål 6
1.3 – Tillämpningsområde 7
1.4 – Tillämplighet 7

KAPITEL 2 – METOD FÖR BERÄKNING AV SANKTIONSBELOPPET 8

2.1 – Allmänt 8
2.2 – Översikt över metoden 8
2.3 – Överträdelser med fasta belopp 9

KAPITEL 3 – SAMMANFALLANDE ÖVERTRÄDELSER OCH TILLÄMPNING AV ARTIKEL 83.3 I DATASKYDDSFÖRORDNINGEN 9

Diagram 11

3.1 – Ett straffbart beteende 11
3.1.1 – Sammanfallande av överträdelser 13

3.1.2 – Enhetlighet avseende åtgärder – artikel 83.3 i dataskyddsförordningen 14

3.2 – Flera straffbara beteenden 15

KAPITEL 4 – UTGÅNGSPUNKT FÖR BERÄKNING 16

4.1 – Kategorisering av överträdelser enligt artiklarna 83.4–83.6 i dataskyddsförordningen 17
4.2 – Överträdelsens allvarlighetsgrad i varje enskilt fall 17

4.2.1 – Överträdelsens karaktär, svårighetsgrad och varaktighet 17

4.2.2 – Om överträdelsen skett med uppsåt eller genom oaktsamhet 19

4.2.3 – Kategorier av berörda personuppgifter 19

4.2.4 – Klassificering av överträdelsens allvar och fastställande av lämpligt startbelopp 20

4.3 – Företagets omsättning i syfte att ålägga effektiva, avskräckande och proportionella sanktionsavgifter 22

KAPITEL 5 – FÖRSVÅRANDE OCH FÖRMILDRANDE OMSTÄNDIGHETER 25

5.1 – Identifiering av försvårande och förmildrande faktorer 25
5.2 – Åtgärder som vidtas av den personuppgiftsansvarige eller personuppgiftsbiträdet för att minska den skada som de registrerade lidit 25
5.3 – Den personuppgiftsansvariges eller personuppgiftsbiträdets grad av ansvar 25
5.4 – Tidigare överträdelser av den personuppgiftsansvarige eller personuppgiftsbiträdet 26

5.4.1 – Tidsram 26

5.4.2 – Sakfråga 27

5.4.3 – Andra överväganden 27

5.5 – Grad av samarbete med tillsynsmyndigheten för att komma till rätta med överträdelsen och minska dess potentiella negativa effekter 27
5.6 – Sättet på vilket tillsynsmyndigheten fick kännedom om överträdelsen 28
5.7 – Efterlevnad av åtgärder som tidigare beslutats med avseende på samma sakfråga 28
5.8 – Tillämpning av godkända uppförandekoder eller godkända certifieringsmekanismer 29
5.9 – Andra försvårande och förmildrande omständigheter 29

KAPITEL 6 – LAGSTADGAT MAXIMIBELOPP OCH FÖRETAGENS ANSVAR 33

6.1 – Fastställande av det lagstadgade maximibeloppet 33

6.1.1 – Statiska maximibelopp 33
6.1.2 – Dynamiska maximibelopp 33
6.2 – Fastställande av företagets omsättning och företagens ansvar 34
6.2.1 – Fastställande av ett företag och företagens ansvar 34
6.2.2 – Fastställande av omsättningen 36
KAPITEL 7 – EFFEKTIVITET, PROPORTIONALITET OCH AVSKRÄCKANDE EFFEKT 37
7.1 – Effektivitet 38
7.2 – Proportionalitet 38
7.3 – Avskräckande effekt 39
KAPITEL 8 – FLEXIBILITET OCH REGELBUNDEN UTVÄRDERING 40
BILAGA – TABELL FÖR ILLUSTRATION AV RIKTLINJERNA 04/2022 OM BERÄKNING AV ADMINISTRATIVA SANKTIONSAVGIFTER ENLIGT DATASKYDDSFÖRORDNINGEN 41

med beaktande av artikel 70.1 k, 70.1 j och 70.1 e i 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 (nedan kallad *dataskyddsförordningen*),

med beaktande av EES-avtalet, särskilt bilaga XI och protokoll 37, ändrat genom gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018[1],

med beaktande av artiklarna 12 och 22 i arbetsordningen,

med beaktande av artikel 29-arbetsgruppens Riktlinjer för tillämpning och fastställande av administrativa sanktionsavgifter i enlighet med förordning 2016/679, WP 253, som godkändes av Europeiska dataskyddsstyrelsen (nedan kallad *Europeiska dataskyddsstyrelsen*) vid dess första plenarsammanträde.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL 1 – INLEDNING

1.1 – Rättslig ram

1. EU har – med den allmänna dataskyddsförordningen (nedan kallad *dataskyddsförordningen*), som har varit tillämplig sedan den 25 maj 2018 – slutfört en omfattande reform av regleringen av dataskyddet i Europa. Skyddet för fysiska personer med avseende på behandling av personuppgifter är en grundläggande rättighet. Förordningen vilar på flera viktiga komponenter, varav en är starkare verkställighetsbefogenheter för tillsynsmyndigheter. Genom förordningen införs en ny, avsevärt högre bötesnivå samt en harmonisering av bötesnivåerna mellan medlemsstaterna.

2. Personuppgiftsansvariga och personuppgiftsbiträden har större ansvar för att se till att enskildas personuppgifter skyddas effektivt. Tillsynsmyndigheterna har befogenhet att se till att principerna i dataskyddsförordningen och de berörda individernas rättigheter upprätthålls i enlighet med ordalydelsen och andan i dataskyddsförordningen.

3. EDPB har därför tagit fram riktlinjer för att tillhandahålla en tydlig och öppen grund för tillsynsmyndigheternas fastställande av sanktionsavgifter. I de tidigare offentliggjorda riktlinjerna om tillämpning och fastställande av administrativa sanktionsavgifter behandlas de omständigheter under vilka administrativa sanktionsavgifter skulle vara ett lämpligt verktyg, och kriterierna i artikel 83 i dataskyddsförordningen tolkas i detta avseende[2]. I dessa riktlinjer behandlas metoden för beräkning av administrativa sanktionsavgifter. De två uppsättningarna riktlinjer är tillämpliga samtidigt och bör ses som kompletterande.

1.2 – Mål

4. Dessa riktlinjer är avsedda att användas av tillsynsmyndigheterna för att säkerställa en konsekvent tillämpning och ett konsekvent genomdrivande av dataskyddsförordningen och ge uttryck för EDPB:s samlade uppfattning om bestämmelserna i artikel 83 i dataskyddsförordningen.

[1] Hänvisningar till ”medlemsstater” i detta dokument bör förstås som hänvisningar till ”medlemsstater i EES”.
[2] Riktlinjer för tillämpning och fastställande av administrativa sanktionsavgifter i enlighet med förordning 2016/679, (nedan kallade *WP 253-riktlinjerna*). WP 253-riktlinjerna godkändes av EDPB vid dess första plenarsammanträde den 25 maj 2018. Se *Endorsement 1/2018*, finns på internet här.

5. Syftet med dessa riktlinjer är att skapa harmoniserade utgångspunkter för en gemensam inställning, som kan ligga till grund för beräkningen av administrativa sanktionsavgifter i enskilda fall. Enligt fast rättspraxis behöver sådan vägledning dock inte vara så specifik att den personuppgiftsansvarige eller personuppgiftsbiträdet ska kunna göra en exakt matematisk beräkning av de förväntade sanktionsavgifterna [3] . I dessa riktlinjer betonas att det slutliga sanktionsbeloppet beror på alla omständigheter i ärendet. EDPB planerar därför att harmonisera de utgångspunkter och metoder som används för att beräkna sanktionsavgifter i stället för att harmonisera resultatet.

6. Dessa riktlinjer kan anses följa en stegvis strategi, även om tillsynsmyndigheterna inte är skyldiga att följa alla steg om de inte är tillämpliga i ett visst fall, eller att motivera aspekter av riktlinjerna som inte är tillämpliga. Resonemanget bör dock omfatta åtminstone de faktorer som ledde till att allvarlighetsgraden fastställdes, den omsättning som tillämpas och de försvårande och förmildrande faktorer som tillämpades.

7. Utan hinder av vad som sägs i dessa riktlinjer omfattas tillsynsmyndigheterna fortfarande av alla förfarandemässiga skyldigheter enligt nationell lagstiftning och EU-lagstiftning, inbegripet skyldigheten att motivera sina beslut och sina skyldigheter enligt mekanismen med en enda kontaktpunkt. Även om tillsynsmyndigheterna är skyldiga att motivera sina slutsatser i enlighet med nationell lagstiftning och EU-lagstiftning, bör dessa riktlinjer inte tolkas som att tillsynsmyndigheten måste ange det exakta startbeloppet eller kvantifiera den exakta effekten av varje försvårande eller förmildrande omständighet. Enbart hänvisningen till dessa riktlinjer kan inte heller ersätta resonemanget i ett specifikt fall.

8. Riktlinjerna kommer att ses över fortlöpande i takt med att praxis inom EU och EES utvecklas. Det bör noteras att med undantag för Danmark och [4] Estland har tillsynsmyndigheterna rätt att utfärda administrativa sanktionsavgifter, som är bindande om de inte överklagas. Således kommer både administrativ och rättslig praxis att utvecklas ytterligare med tiden.

1.3 – Tillämpningsområde

9. Dessa riktlinjer är avsedda att reglera och lägga grunden för tillsynsmyndigheternas fastställande av sanktionsavgifter på en övergripande nivå. Den vägledning som fastställs gäller för alla typer av personuppgiftsansvariga och personuppgiftsbiträden i enlighet med artikel 4.7 och 4.8 i dataskyddsförordningen, med undantag för fysiska personer när de inte agerar som företag. Detta påverkar inte de nationella myndigheternas befogenheter att bötfälla fysiska personer.

10. Enligt artikel 83.7 i dataskyddsförordningen får varje medlemsstat fastställa regler för huruvida och i vilken utsträckning administrativa sanktionsavgifter får åläggas offentliga myndigheter och organ som är etablerade i den medlemsstaten. Förutsatt att tillsynsmyndigheterna har denna befogenhet på grundval av nationell lagstiftning ska dessa riktlinjer tillämpas på beräkningen av de sanktionsavgifter som ska åläggas offentliga myndigheter och organ, med undantag för kapitel 4.3. Tillsynsmyndigheterna är dock fria att tillämpa en metod som liknar den som beskrivs i detta kapitel. Dessutom är kapitel 6 inte tillämpligt på beräkningen av de sanktionsavgifter som åläggs offentliga myndigheter och organ, om nationell lagstiftning föreskriver olika lagstadgade maximibelopp och den offentliga myndigheten eller det offentliga organet inte fungerar som ett företag enligt definitionen i kapitel 6.2.1.

11. Riktlinjerna omfattar gränsöverskridande och icke-gränsöverskridande ärenden.

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

1.4 – Tillämplighet

[3] Se t.ex. mål C-189/02 P, C-202/02 P, C-205/02 P till C-208/02 P och C-213/02 P, Dansk Rørindustri A/S m.fl./kommissionen, punkt 172 och mål T-91/11, InnoLux Corp./kommissionen, punkt 88.
[4] Se skäl 151 i dataskyddsförordningen.

13. Enligt artikel 70.1 e i dataskyddsförordningen har EDPB befogenhet att utfärda riktlinjer, rekommendationer och bästa praxis för att främja en konsekvent tillämpning av dataskyddsförordningen. I artikel 70.1 k i dataskyddsförordningen anges att styrelsen ska säkerställa en enhetlig tillämpning av dataskyddsförordningen och, på eget initiativ eller, i förekommande fall, på begäran av Europeiska kommissionen, särskilt utarbeta riktlinjer för tillsynsmyndigheter när det gäller tillämpningen av de åtgärder som avses i artikel 58 och fastställandet av administrativa sanktionsavgifter i enlighet med artikel 83.

14. För att uppnå en konsekvent strategi för åläggande av administrativa sanktionsavgifter som på ett tillfredsställande sätt återspeglar alla principer i dataskyddsförordningen har EDPB enats om en gemensam syn på bedömningskriterierna i artikel 83 i dataskyddsförordningen. De enskilda tillsynsmyndigheterna kommer att återspegla denna gemensamma strategi, i enlighet med de lokala administrativa och rättsliga lagar som är tillämpliga på dem.

KAPITEL 2 – METOD FÖR BERÄKNING AV SANKTIONSBELOPPET

2.1 – Allmänt

15. Utan hinder av skyldigheterna i fråga om samarbete och enhetlighet ska tillsynsmyndigheten själv fastställa sanktionsbeloppet. Enligt dataskyddsförordningen ska sanktionsbeloppet i varje enskilt fall vara effektivt, proportionellt och avskräckande (artikel 83.1 i dataskyddsförordningen). När tillsynsmyndigheterna fastställer sanktionsbeloppet ska de dessutom ta vederbörlig hänsyn till en förteckning över omständigheter som hänvisar till drag hos överträdelsen (dess allvarlighetsgrad) eller egenskaper hos gärningsmannen (artikel 83.2 i dataskyddsförordningen). Kvantifieringen av sanktionsbeloppet baseras därför på en särskild utvärdering som görs i varje enskilt fall, med beaktande av de parametrar som föreskrivs i dataskyddsförordningen.

16. För beteenden som bryter mot dataskyddsreglerna föreskriver dataskyddsförordningen inte några lägsta sanktionsavgifter. I dataskyddsförordningen föreskrivs i stället endast maximibelopp i artikel 83.4–83.6 i dataskyddsförordningen, där flera olika typer av beteenden grupperas tillsammans. Ett sanktionsbelopp kan i slutändan endast beräknas genom en avvägning av alla de faktorer som uttryckligen anges i artikel 83.2 a–j i dataskyddsförordningen och som är relevanta för fallet och andra relevanta faktorer, även om de inte uttryckligen anges i nämnda bestämmelser (eftersom artikel 83.2 k kräver att vederbörlig hänsyn tas till alla andra tillämpliga faktorer). Slutligen måste det slutliga sanktionsbeloppet till följd av denna bedömning vara effektivt, proportionellt och avskräckande i varje enskilt fall (artikel 83.1 i dataskyddsförordningen). Alla sanktionsavgifter som utdöms måste i tillräcklig grad beakta alla dessa parametrar, samtidigt som de inte överskrider det lagstadgade maximibeloppet enligt artikel 83.4–83.6 i dataskyddsförordningen.

2.2 – Översikt över metoden

17. Med beaktande av dessa parametrar har EDPB utarbetat följande metod för beräkning av administrativa sanktionsavgifter för överträdelser av dataskyddsförordningen.

Steg 1	Identifiera behandlingarna i fallet och utvärdera tillämpningen av artikel 83.3 i dataskyddsförordningen. **(Kapitel 3)**
Steg 2	Hitta utgångspunkten för ytterligare beräkningar baserat på en utvärdering av **(Kapitel 4)** a) klassificeringen i artikel 83.4–83.6 i dataskyddsförordningen, b) hur allvarlig överträdelsen är enligt artikel 83.2 a, b och g i dataskyddsförordningen, c) företagets omsättning som en relevant faktor att beakta i syfte att ålägga effektiva, avskräckande och proportionella sanktionsavgifter i enlighet med artikel 83.1 i dataskyddsförordningen.

Steg 3	Utvärdera försvårande och förmildrande omständigheter i samband med den personuppgiftsansvariges/personuppgiftsbiträdets tidigare eller nuvarande beteende och öka eller minska sanktionsavgifterna i enlighet därmed. **(Kapitel 5)**
Steg 4	Fastställa de relevanta lagstadgade maximibeloppen för de olika behandlingarna. Ökningar som tillämpas i föregående eller nästa steg får inte överstiga detta belopp. **(Kapitel 6)**
Steg 5	Analys av huruvida det slutliga sanktionsbeloppet uppfyller kraven på effektivitet, avskräckande effekt och proportionalitet, i enlighet med artikel 83.1 i dataskyddsförordningen, och höjning eller sänkning av sanktionsbeloppet i enlighet med detta. **(Kapitel 7)**

2.3 – Överträdelser med fasta belopp

18. Under vissa omständigheter kan tillsynsmyndigheten anse att vissa överträdelser kan bestraffas med sanktionsavgifter på ett förutbestämt, fast belopp. Tillämpningen av ett fast belopp på vissa typer av överträdelser får inte hindra tillämpningen av dataskyddsförordningen, särskilt artikel 83. Tillämpningen av fasta belopp befriar inte tillsynsmyndigheterna från samarbete och enhetlighet (kapitel VII i dataskyddsförordningen).

19. Det står tillsynsmyndigheten fritt att fastställa vilka typer av överträdelser som kan bestraffas med ett förutbestämt fast belopp, på grundval av deras karaktär, svårighetsgrad och varaktighet. Tillsynsmyndigheten får inte fatta sådana beslut om detta är förbjudet eller på annat sätt skulle strida mot medlemsstatens nationella lagstiftning.

20. Fasta belopp kan fastställas efter tillsynsmyndighetens gottfinnande, med beaktande av bland annat de sociala och ekonomiska omständigheterna i den medlemsstaten, i förhållande till hur allvarlig överträdelsen är enligt artikel 83.2 a, b och g i dataskyddsförordningen. Det rekommenderas att tillsynsmyndigheten i förväg meddelar beloppen och omständigheterna för tillämpningen.

KAPITEL 3 – SAMMANFALLANDE ÖVERTRÄDELSER OCH TILLÄMPNING AV ARTIKEL 83.3 I DATASKYDDSFÖRORDNINGEN

21. Innan man kan beräkna sanktionsavgifter på grundval av metoden i dessa riktlinjer är det viktigt att först överväga vilket beteende (faktiska omständigheter avseende beteendet) och vilka överträdelser (abstrakta rättsliga beskrivningar av vad som är straffbart) som sanktionsbeloppet baseras på. Ett särskilt fall kan omfatta omständigheter som antingen kan betraktas som ett och samma eller separata straffbara beteenden. Ett och samma beteende skulle också kunna ge upphov till ett antal olika överträdelser där fastställandet av en överträdelse utesluter att en annan överträdelse fastställs eller att de kan fastställas föreligga parallellt. Med andra ord kan överträdelser vara sammanfallande. Beroende på reglerna för sammanfallanden av detta slag kan beräkningen av sanktionsavgifter skilja sig åt.

22. Om man granskar analysen av medlemsstaternas traditioner när det gäller regler för sammanfallande i enlighet med EU-domstolens rättspraxis, [5]
och med tanke på de olika tillämpningsområdena och de rättsliga konsekvenserna, kan dessa principer i stort sett delas in i följande **tre kategorier**:
    - **Sammanfallande av överträdelser (kapitel 3.1.1).**
    - **Enhetlighet avseende åtgärder (kapitel 3.1.2).**
    - **Mångfald avseende åtgärder (kapitel 3.2).**

23. Dessa olika kategorier för sammanfallande står inte i konflikt med varandra, men har olika tillämpningsområden och passar in i ett sammanhängande övergripande system som tillhandahåller ett logiskt testprogram.

[5] Se särskilt den ingående analysen i AG Tanchevs yttrande i mål C-10/18 P, Marine Harvest.

24. Därför är det viktigt att först fastställa följande:

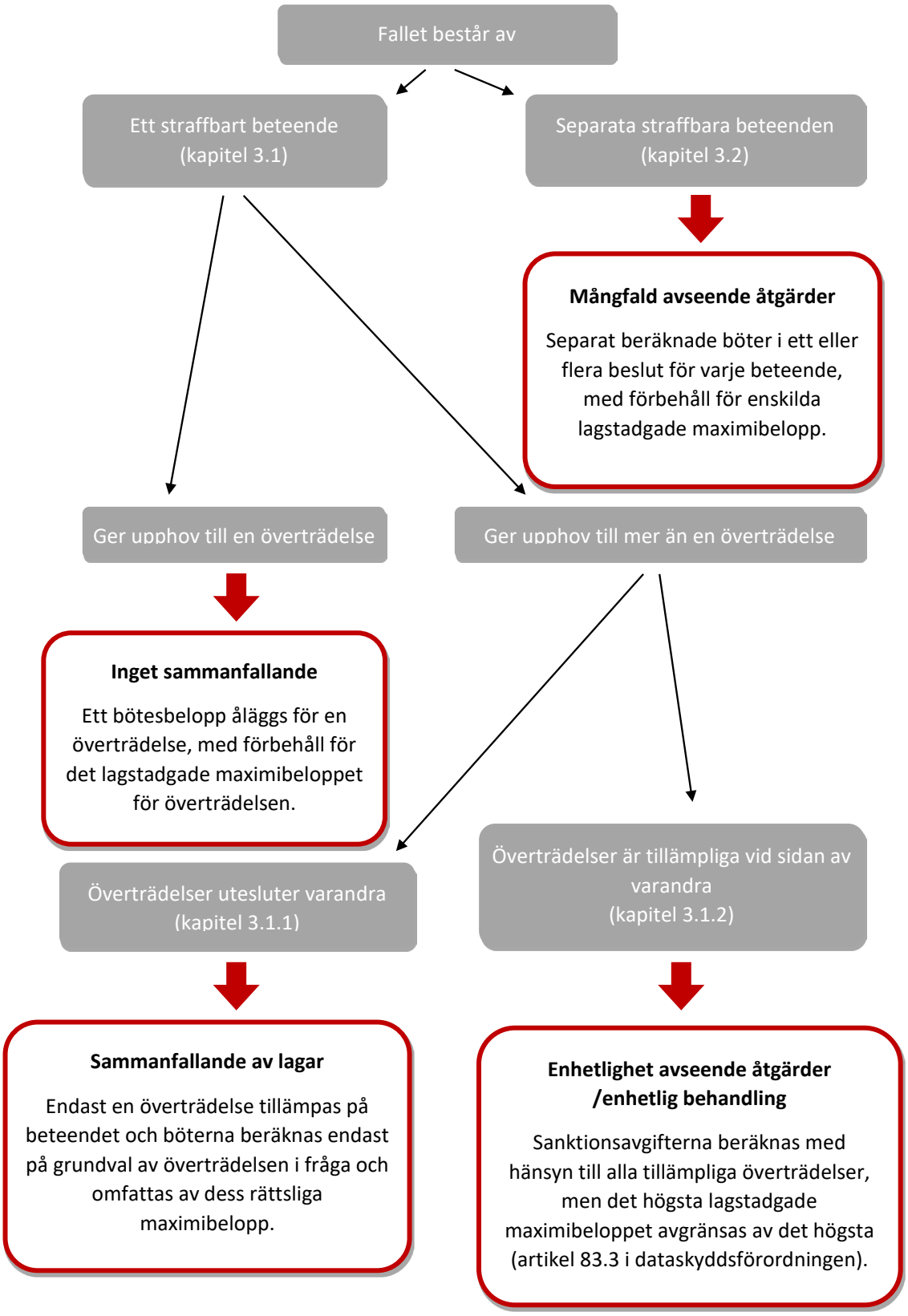
a. Huruvida omständigheterna ska betraktas som ett (**kapitel 3.1**) eller

   flera straffbara beteenden (**kapitel 3.2**).

b. Om det är fråga om ett beteende (**kapitel 3.1**), huruvida detta beteende ger upphov till

   en eller flera överträdelser.

c. När det gäller ett beteende som ger upphov till flera överträdelser, huruvida fastställandet av en överträdelse åsidosätter en annan överträdelse (**kapitel 3.1.1**) eller huruvida de ska fastställas föreligga parallellt (**kapitel 3.1.2**).



3.1 – Ett straffbart beteende

25. Som ett första steg är det viktigt att fastställa om det finns ett och samma straffbara beteende (”idem”) eller om det finns flera sådana beteenden för att fastställa vilket straffbart beteende som ska åläggas sanktionsavgifter. Det är därför viktigt att förstå vilka omständigheter som betraktas som ett och samma beteende, i motsats till flera beteenden. Det relevanta straffbara beteendet måste bedömas och identifieras från fall till fall. I ett visst fall kan t.ex. ”samma eller sammankopplade uppgiftsbehandlingar” utgöra ett och samma beteende.

26. Begreppet *behandling av personuppgifter* tas upp i artikel 4.2 i dataskyddsförordningen där termen *behandling* definieras som varje åtgärd eller serie av åtgärder som vidtas med personuppgifter eller uppsättningar av personuppgifter, vare sig det sker automatiserat eller inte, till exempel insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, hämtning, läsning, användning, utlämnande genom översändande, spridning eller tillhandahållande på annat sätt, sammanställning eller samkörning, begränsning, radering eller förstöring.

27. Vid bedömningen av ”samma eller sammankopplade uppgiftsbehandlingar” bör man komma ihåg att alla skyldigheter som är rättsligt nödvändiga för att behandlingen ska kunna utföras på ett lagligt sätt kan beaktas av tillsynsmyndigheten för dess bedömning av överträdelser, såsom t.ex. öppenhetskrav (t.ex. artikel 13 i dataskyddsförordningen). Detta understryks också av frasen ”för samma eller sammankopplade uppgiftsbehandlingar”, som anger att denna bestämmelses tillämpningsområde omfattar alla överträdelser som rör och kan påverka samma eller sammankopplade uppgiftsbehandlingar.

28. Begreppet ”sammankopplade” avser principen att ett enhetligt beteende kan bestå av flera delar som utförs med en enhetlig föresats och som är kontextuellt (särskilt när det gäller den registrerades identitet, ändamål och karaktär), rumsligt och tidsmässigt förbundna på ett sådant nära sätt att de ur en objektiv synvinkel skulle betraktas som ett likadant beteende. Antagandet om en tillräcklig koppling bör inte ske lättvindigt, för att tillsynsmyndigheten ska undvika överträdelser av principerna om avskräckande verkan och effektiv kontroll av efterlevnaden av EU-lagstiftningen. Dessa aspekter av fastställandet av en tillräcklig koppling måste därför bedömas från fall till fall.

Exempel 1 a – Samma eller sammankopplade uppgiftsbehandlingar
Ett finansinstitut begär en kreditkontroll från ett kreditvärderingsinstitut. Finansinstitutet tar emot denna information och lagrar den i sitt system.

Även om finansinstitutets insamling och lagring av kreditvärdighetsuppgifter var för sig är uppgiftsbehandlingar, utgör de en uppsättning uppgiftsbehandlingar som utförs med en enhetlig föresats och är kontextuellt, rumsligt och tidsmässigt förbundna på ett sådant nära sätt att de ur objektiv synvinkel skulle betraktas som ett enhetligt beteende. De behandlingar som finansinstitutet utför ska därför anses vara ”sammankopplade” och utgöra samma beteende.

Exempel 1 b – Samma eller sammankopplade uppgiftsbehandlingar
En datamäklare beslutar att genomföra en ny behandling enligt följande: Mäklaren beslutar att – som tredje part – samla in information om konsumenttransaktioner från dussintals återförsäljare utan rättslig grund, för att utföra psykometriska analyser för att förutsäga enskilda personers framtida beteende, inklusive politiskt röstbeteende, villighet att säga upp sig med mera. I samma beslut beslutar datamäklaren att inte inkludera detta förfarande i registren över uppgiftsbehandling, att inte informera de registrerade och att ignorera eventuella begäranden om tillgång till uppgifter som rör den nya behandlingen. Uppgiftsbehandlingen i samband med denna behandling utgör en uppsättning behandlingar som utförs med en enhetlig föresats och som är kontextuellt, rumsligt och tidsmässigt relaterade. De ska anses vara ”sammankopplade” och utgöra samma beteende. Detta inbegriper även underlåtenhet att registerföra uppgiftsbehandlingen, att informera de registrerade och att fastställa förfaranden för att ge rätt till åtkomst med avseende på de nya behandlingarna. Dessa skyldigheter har åsidosatts för sammankopplade uppgiftsbehandlingar.

Exempel 1 c – Inte samma eller sammankopplade uppgiftsbehandlingar

i) En byggnadsmyndighet utför en bakgrundskontroll av en arbetssökande. Bakgrundskontrollen omfattar även politisk samhörighet, fackföreningsmedlemskap och sexuell läggning. ii) Fem dagar senare kräver byggnadsmyndigheten att dess leverantörer (enskilda näringsidkare) lämnar överdrivet mycket information om sina affärsavtal med andra enheter, oavsett om de är relevanta för avtalet eller för byggnadsmyndighetens bindande krav. iii) En vecka senare drabbas byggnadsmyndigheten av en personuppgiftsincident. Byggnadsmyndighetens nätverk hackas – trots att lämpliga tekniska och organisatoriska åtgärder har vidtagits – och hackaren får tillgång till ett system som behandlar personuppgifter för medborgare som har lämnat in förfrågningar till byggnadsmyndigheten. Trots att uppgifterna var tillräckligt krypterade enligt tillämpliga standarder kan hackaren bryta sig in med militär dekrypteringsteknik och sälja uppgifterna på darknet. Byggnadsmyndigheten avstår från att underrätta tillsynsmyndigheten, trots att den är skyldig att göra detta. Behandlingen i detta fall, dvs. bakgrundskontrollen, kraven på upplysningar från leverantörer och underlåtenheten att anmäla en personuppgiftsincident, är inte kontextuellt relaterade. De ska därför inte betraktas som ”sammankopplade” utan formar i stället olika beteenden.

29. Om det fastställs att omständigheterna i målet utgör ett och samma agerande och ger upphov till en enda överträdelse kan sanktionsavgifterna beräknas på grundval av överträdelsen och dess lagstadgade maximibelopp. Om omständigheterna i målet emellertid utgör ett och samma beteende, men detta beteende ger upphov till inte bara en utan flera överträdelser, måste det fastställas om fastställandet av en överträdelse utesluter att en annan överträdelse fastställs (kapitel 3.1.1) eller om de kan fastställas föreligga parallellt (kapitel 3.1.2). Om omständigheterna i målet utgör ett flertal beteenden ska de betraktas som en mångfald avseende åtgärder och hanteras i enlighet med kapitel 3.2.

3.1.1 – Sammanfallande av överträdelser

30. Principen om sammanfallande mellan överträdelser (även kallad ”uppenbart sammanfallande”[6] eller ”falskt sammanfallande”) gäller när tillämpningen av en bestämmelse utesluter eller undergräver den andra bestämmelsens tillämplighet. Med andra ord sker sammanfallande redan på den abstrakta nivån i de lagstadgade bestämmelserna. Detta kan antingen grundas på principen om specialitet[7], subsidiaritet eller konsumtion, som ofta tillämpas när bestämmelser skyddar samma rättsliga intressen. I sådana fall skulle det vara olagligt att bestraffa gärningsmannen för samma missgärningar två gånger[8].

31. I ett sådant fall av sammanfallande överträdelser bör sanktionsbeloppet endast beräknas på grundval av den överträdelse som valts ut enligt ovanstående regler (”ersättande överträdelse”)[9].

Specialitetsprincipen[10]

32. Specialitetsprincipen (*specialia generalibus derogant*) är en rättslig princip som innebär att mer specifika bestämmelser (som härrör från samma rättsakt eller olika rättsakter med samma verkan) ersätter en mer allmän bestämmelse, även om båda har samma syfte. Den mer specifika överträdelsen betraktas då ibland som en ”kvalificerad typ” i förhållande till den mindre specifika. En kvalificerad typ av överträdelse kan bli föremål för en högre nivå av sanktionsavgifter, högre lagstadgade maximibelopp eller mer omfattande preskriptionstid.

33. Genom tolkning kan dock specialitet också ibland tillämpas, när en överträdelse på grund av sin karaktär och av systematiska skäl betraktas som en kvalificering av en uppenbart mer specifik sådan, även om dess ordalydelse inte uttryckligen nämner ett ytterligare inslag.

[6] Se t.ex. Österrikes Verwaltungsgerichtshof, Ra 2018/02/0123, punkt 9.
[7] Enligt bedömningen i mål C-10/18 P, Marine Harvest/kommissionen.
[8] Se t.ex. Österrikes Verwaltungsgerichtshof, Ra 2018/02/0123, punkt 7.
[9] Enligt bedömningen i mål C-10/18 P, Marine Harvest/kommissionen.
[10] Enligt bedömningen i mål C-10/18 P, Marine Harvest/kommissionen.

34. Om i stället två bestämmelser har självständiga mål utgör detta en differentierande faktor som motiverar att separata sanktionsavgifter åläggs. Om till exempel en överträdelse av en bestämmelse automatiskt leder till en överträdelse av en annan, men det omvända inte stämmer, har dessa överträdelser självständiga mål.

35. Dessa specialitetsprinciper kan endast tillämpas om och i den mån som de mål som eftersträvas med de berörda överträdelserna faktiskt stämmer överens i det enskilda fallet. Eftersom dataskyddsprinciperna i artikel 5 i dataskyddsförordningen har fastställts som övergripande begrepp kan det finnas situationer där andra bestämmelser konkretiserar en sådan princip, men inte omskriver principen i dess helhet. En bestämmelse definierar med andra ord inte alltid principens fulla räckvidd [11]. Beroende på omständigheterna [12] överlappar principerna i vissa fall varandra på ett samstämmigt sätt och en överträdelse kan därför ersätta den andra, medan överlappningen i andra fall endast är partiell och därför inte helt samstämmig. Såvitt de inte stämmer överens finns inget sammanfallande mellan överträdelserna. I stället kan de tillämpas tillsammans med varandra vid beräkningen av sanktionsavgifterna.

Subsidiaritetsprincipen

36. En annan form av sammanfallande överträdelser kan ofta hänföras till den så kallade subsidiaritetsprincipen. Den gäller om en överträdelse betraktas som underordnad en annan överträdelse. Detta skulle kunna bero på att lagstiftningen formellt fastställer subsidiariteten eller på att subsidiariteten ges av materiella skäl[13]. Det senare kan vara fallet om överträdelserna har samma syfte, men en innehåller en mindre anklagelse om omoral eller oegentlighet (t.ex. kan en administrativ överträdelse vara underordnad ett brott osv.).

Konsumtionsprincipen

37. Konsumtionsprincipen gäller i fall där överträdelsen av en bestämmelse regelbundet leder till överträdelse av den andra, ofta på grund av att den ena överträdelsen är ett preliminärt steg mot den andra.

3.1.2 – Enhetlighet avseende åtgärder – artikel 83.3 i dataskyddsförordningen

38. I likhet med en situation med sammanfallande överträdelser gäller principen om enhetlighet i åtgärder (även kallad ”idealiskt sammanfallande”) i fall där ett beteende omfattas av flera lagbestämmelser, med skillnaden att den ena bestämmelsen varken utesluts eller underordnas av den andra bestämmelsens tillämplighet, eftersom de inte omfattas av principerna om specialitet, subsidiaritet eller konsumtion och till största delen eftersträvar olika mål.

39. Principen om enhetlighet avseende åtgärder specificerades ytterligare på sekundärrättslig nivå i artikel 83.3 i dataskyddsförordningen i form av en ”enhetlig behandling”. Det är viktigt att förstå att artikel 83.3 i dataskyddsförordningen är begränsad när det gäller dess tillämpning och inte tillämpas på varje enskilt fall där det konstateras att flera överträdelser har ägt rum, utan endast på de fall där flera överträdelser har

---

[11] EDPB:s bindande beslut 1/2021 om tvisten som uppstod på grundval av utkastet till beslut från den irländska tillsynsmyndigheten om WhatsApp Ireland enligt artikel 65.1 a i dataskyddsförordningen (nedan kallat *EDPB:s bindande beslut 1/2021*), punkt 192.

[12] EDPB:s bindande beslut 1/2021, punkt 193.

[13] Idén om en formell subsidiaritet är också indirekt förankrad i artikel 35.2 i Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (*NIS 2-direktivet*), även om konflikten löses på förfarandemässiga snarare än väsentliga nivåer. Bestämmelsen reglerar att ”[o]m de tillsynsmyndigheter som avses i artikel 55 eller 56 i förordning (EU) 2016/679 påför administrativa sanktionsavgifter enligt artikel 58.2 i) i den förordningen ska de behöriga myndigheterna inte påföra administrativa sanktionsavgifter enligt artikel 34 i [NIS 2-direktivet] för en överträdelse som avses i [artikel 35.1 i NIS 2-direktivet] som följer av samma beteende som det som den administrativa sanktionsavgiften avsåg enligt artikel 58.2 i) i [dataskyddsförordningen]”, i den mån den överträdelse som avses i artikel 35.1 i NIS 2-direktivet indirekt anses vara underställd sanktionsavgifter grundade på dataskyddsförordningen när detta gäller samma beteende.

uppstått till följd av ”samma eller sammankopplade uppgiftsbehandlingar” såsom förklaras ovan[14]. I dessa fall får det totala beloppet för de administrativa sanktionerna inte överstiga det belopp som fastställts för den allvarligaste överträdelsen[15].

40. I vissa särskilda fall kan en enhetlighet avseende åtgärder också antas om en enda åtgärd strider mot samma lagbestämmelse flera gånger. Detta kan särskilt vara fallet om omständigheterna innebär en iterativ och liknande överträdelse av samma lagbestämmelse i nära rumslig och tidsmässig följd.

> ***Exempel 2 – Enhetlighet avseende åtgärder***
> *En personuppgiftsansvarig skickar paket med e-postmeddelanden om marknadsföring till grupper av registrerade i olika omgångar under en dag utan att ha någon rättslig grund, och bryter därmed mot artikel 6.1 i dataskyddsförordningen med en enhet av åtgärder flera gånger.*

41. Ordalydelsen i artikel 83.3 i dataskyddsförordningen verkar inte direkt omfatta detta senare fall av enhetlighet avseende åtgärder, eftersom ”flera bestämmelser” inte överträds. Det skulle dock innebära ojämlik och orättvis behandling om en gärningsman som genom en åtgärd bryter mot olika bestämmelser som syftar till att uppnå olika mål gynnas gentemot en gärningsman som med samma åtgärd flera gånger bryter mot samma bestämmelse som eftersträvar samma mål. För att undvika inkonsekvenser i förhållande till rättsprincipen och för att följa den grundläggande rätten till likabehandling i stadgan ska artikel 83.3 i dataskyddsförordningen i sådana fall tillämpas i tillämpliga delar.

42. I dessa fall av enhetlighet avseende åtgärder får det totala beloppet för de administrativa sanktionerna inte överstiga det belopp som fastställts för den allvarligaste överträdelsen. ”När det gäller tolkningen av artikel 83.3 i dataskyddsförordningen påpekar EDPB att principen om ändamålsenlig verkan kräver att alla institutioner ska ge unionsrätten full kraft och verkan” [16]. I detta avseende får artikel 83.3 i dataskyddsförordningen inte tolkas på ett sätt där ”det inte ha[r] någon betydelse om en personuppgiftsansvarig gjorde sig skyldig till en eller flera överträdelser av dataskyddsförordningen […] vid bedömningen av sanktionsavgifterna”[17].

43. Formuleringen ”totalt belopp” innebär att alla överträdelser som begås måste beaktas vid bedömningen av sanktionsbeloppet[18], och ordalydelsen ”det belopp som anges för den allvarligaste överträdelsen” avser de lagstadgade maximibeloppen för sanktionsavgifter (t.ex. artiklarna 83.4–83.6 i dataskyddsförordningen). ”Även om själva sanktionsavgifterna inte får överskrida den lagstadgade högsta sanktionsavgiftsnivån ska lagöverträdaren fortfarande uttryckligen anses skyldig till att ha överträtt flera bestämmelser och dessa överträdelser måste beaktas vid fastställandet av de slutliga sanktionsavgifter som ska ådömas”[19]. Även om detta inte påverkar skyldigheten för den tillsynsmyndighet som ålägger sanktionsavgifterna att beakta behovet av att sanktionsavgifterna är proportionerliga, kan de andra överträdelser som begåtts inte åsidosättas utan måste beaktas vid beräkningen av sanktionsavgifterna.

3.2 – Flera straffbara beteenden

44. Principen om mångfald avseende åtgärder (även kallad *Realkonkurrenz*, *factual concurrence* eller *coincidental concurrence*) beskriver alla fall som inte omfattas av principerna om sammanfallande överträdelser (kapitel 3.1.1) eller av artikel 83.3 i dataskyddsförordningen (kapitel 3.1.2).

[14] EDPB:s bindande beslut 1/2021, punkt 320.
[15] I artikel 83.3 i dataskyddsförordningen anges följande: ”Om en personuppgiftsansvarig eller ett personuppgiftsbiträde, med avseende på en och samma eller sammankopplade uppgiftsbehandlingar, uppsåtligen eller av oaktsamhet överträder flera av bestämmelserna i denna förordning får den administrativa sanktionsavgiftens totala belopp inte överstiga det belopp som fastställs för den allvarligaste överträdelsen.”
[16] EDPB:s bindande beslut 1/2021, punkt 322.
[17] Ibid, punkt 323.
[18] Ibid, punkt 325.
[19] Ibid, punkt 326.

45. Det enda skälet till att dessa överträdelser hanteras i ett beslut är att tillsynsmyndigheten av en tillfällighet har uppmärksammats på dem samtidigt, utan att de är samma eller sammankopplade uppgiftsbehandlingar i den mening som avses i artikel 83.3 i dataskyddsförordningen. Därför konstateras gärningsmannen ha brutit mot flera lagbestämmelser, och separata sanktionsavgifter åläggs enligt det nationella förfarandet antingen i samma sanktionsbeslut eller i separata sanktionsbeslut. Eftersom artikel 83.3 i dataskyddsförordningen inte är tillämplig får det totala beloppet för de administrativa sanktionsavgifterna dessutom överstiga det belopp som anges för den allvarligaste överträdelsen (*argumentum e contrario*). Fall av mångfald avseende åtgärder medför inga skäl till att ge gärningsmannen privilegier när det gäller beräkningen av sanktionsavgifterna. Detta påverkar dock inte skyldigheten att fortfarande följa den allmänna proportionalitetsprincipen.

Exempel 3 – Mångfald avseende åtgärder
Efter att ha genomfört en dataskyddsinspektion i en personuppgiftsansvarigs lokaler finner tillsynsmyndigheten att den personuppgiftsansvarige har underlåtit att fastställa ett förfarande för granskning och fortsatt förbättring av webbplatsens säkerhet, för att tillhandahålla information enligt artikel 13 till anställda om behandling av personuppgifter och för att informera tillsynsmyndigheten om en nyligen inträffad uppgiftsincident avseende uppgifter från leverantören. Ingen av överträdelserna är utesluten eller underordnad med avseende på specialitet, subsidiaritet eller konsumtion. De uppfyller inte heller kraven för ”samma uppgiftsbehandling” eller ”sammankopplade uppgiftsbehandlingar”: De utgör inte en enhet av åtgärder, utan en mångfald av åtgärder. Tillsynsmyndigheten kommer därför att finna att den personuppgiftsansvarige har överträtt artiklarna 13, 32 och 33 i dataskyddsförordningen. Den kommer i sitt sanktionsbeslut att ålägga enskilda sanktionsavgifter för var och en av dem, utan att det finns ett enda lagstadgat maximibelopp som är tillämpligt på deras belopp.

KAPITEL 4 – UTGÅNGSPUNKT FÖR BERÄKNING

46. EDPB anser att beräkningen av administrativa sanktionsavgifter bör börja från en harmoniserad utgångspunkt[20]. Denna utgångspunkt utgör början för ytterligare beräkning, där alla omständigheter i fallet beaktas och viktas, vilket resulterar i det slutliga sanktionsbelopp som ska åläggas den personuppgiftsansvarige eller personuppgiftsbiträdet.

47. Fastställandet av harmoniserade utgångspunkter i dessa riktlinjer hindrar inte att tillsynsmyndigheterna bedömer varje enskilt fall i sak, vilket inte bör uteslutas Sanktionsbeloppet för en personuppgiftsansvarig/ett personuppgiftsbiträde kan variera från vilket belopp som helst upp till det högsta rättsliga sanktionsbeloppet, förutsatt att sanktionsbeloppet är effektivt, avskräckande och proportionerligt. Förekomsten av en utgångspunkt hindrar inte tillsynsmyndigheten från att sänka eller höja sanktionsavgiften (upp till dess högsta belopp) om omständigheterna i ärendet så kräver.

48. EDPB anser att tre faktorer utgör utgångspunkten för ytterligare beräkningar: kategorisering av överträdelser efter karaktär enligt artiklarna 83.4–83.6 i dataskyddsförordningen, överträdelsens allvarlighet (som diskuteras i avsnitt 4.2 nedan) och företagets omsättning som en relevant faktor att beakta i syfte att ålägga effektiva, avskräckande och proportionella sanktionsavgifter, i enlighet med artikel 83.1 i dataskyddsförordningen. Dessa beskrivs i kapitel 4.1, 4.2 och 4.3 nedan.

[20] Förutsatt att riktlinjerna ger tillräckligt utrymme för att anpassa administrativa sanktionsavgifter till omständigheterna i målet godtar EU-domstolen i allmänhet beräkningar som inleds från en abstrakt utgångspunkt. Särskilt i de förenade målen C-189/02 P, C-202/02 P, C-205/02 P till C-208/02 P och C-213/02 P, Dansk Rørindustri, men också mer nyligen i mål T-15/02, BASF/kommissionen, punkterna 120–121, och 134, mål C-227/14 P, LG Display Co. Ltd/kommissionen, punkt 53 och mål T-26/02, Daiichi Pharmaceutical Co. Ltd/kommissionen, punkt 50.

4.1 – Kategorisering av överträdelser enligt artiklarna 83.4–83.6 i dataskyddsförordningen

49. Nästan alla skyldigheter som personuppgiftsansvariga och personuppgiftsbiträden har enligt förordningen kategoriseras efter sin karaktär i bestämmelserna i artikel 83.4–83.6[21]. Dataskyddsförordningen innehåller två kategorier av överträdelser: överträdelser som är straffbara enligt artikel 83.4 i dataskyddsförordningen, å ena sidan, och överträdelser som är straffbara enligt artikel 83.5 och 83.6 i dataskyddsförordningen, å andra sidan. Den första kategorin överträdelser kan bestraffas med sanktionsavgifter på högst 10 miljoner euro eller 2 % av företagets årsomsättning, beroende på vilket som är högst, medan påföljderna för den andra är sanktionsavgifter på högst 20 miljoner euro eller 4 % av företagets årsomsättning, beroende på vilket som är högst.

50. Med denna åtskillnad har lagstiftaren givit en första indikation på överträdelsens allvarlighetsgrad i abstrakt bemärkelse. Ju allvarligare överträdelsen är, desto högre kommer sanktionsbeloppet sannolikt att bli.

4.2 – Överträdelsens allvarlighetsgrad i varje enskilt fall

51. Enligt dataskyddsförordningen ska tillsynsmyndigheten ta vederbörlig hänsyn till 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 (artikel 83.2 a i dataskyddsförordningen); om överträdelsen skett med uppsåt eller genom oaktsamhet (artikel 83.2 b i dataskyddsförordningen); och de kategorier av personuppgifter som påverkas av överträdelsen (artikel 83.2 g i dataskyddsförordningen). I dessa riktlinjer hänvisar EDPB till dessa faktorer avseende överträdelsens allvarlighetsgrad.

52. Tillsynsmyndigheten måste se över dessa faktorer mot bakgrund av omständigheterna i det specifika fallet, och på grundval av denna analys dra slutsatsen om allvarlighetsgraden i enlighet med punkt 60. I detta avseende kan tillsynsmyndigheten också överväga om uppgifterna i fråga var direkt identifierbara. Även om dessa faktorer diskuteras individuellt i dessa riktlinjer är de i själva verket ofta sammanflätade och bör ses mot bakgrund av fakta i ärendet som helhet.

4.2.1 – Överträdelsens karaktär, svårighetsgrad och varaktighet

53. Artikel 83.2 a i dataskyddsförordningen har ett brett tillämpningsområde och kräver att tillsynsmyndigheten utför en fullständig granskning av alla de faktorer som utgör överträdelsen och som är lämpliga för att skilja den från andra överträdelser av samma slag. Denna bedömning bör därför ta hänsyn till följande specifika faktorer:

a) **Överträdelsens karaktär**, bedömd utifrån de konkreta omständigheterna i ärendet. I det avseendet är denna analys mer specifik än den abstrakta klassificeringen i artikel 83.4–83.6 i dataskyddsförordningen. Tillsynsmyndigheten får se över det intresse som den överträdda bestämmelsen syftar till att skydda och platsen för denna bestämmelse i dataskyddsramen. Dessutom får tillsynsmyndigheten beakta i vilken utsträckning överträdelsen hindrade en effektiv tillämpning av bestämmelsen och uppfyllandet av det mål som den skulle skydda.

b) **Överträdelsens svårighetsgrad**, bedömd på grundval av de särskilda omständigheterna. Såsom anges i artikel 83.2 a i dataskyddsförordningen gäller detta behandlingens art, men även ”den aktuella uppgiftsbehandlingens karaktär, omfattning eller syfte samt antalet berörda registrerade och den skada som de har lidit” kommer att indikera hur allvarlig överträdelsen är.

i. **Uppgiftsbehandlingens karaktär**, inbegripet det sammanhang där behandlingen är funktionellt baserad (t.ex. affärsverksamhet, ideell verksamhet, politiskt parti osv.) och alla behandlingens egenskaper[22]. Om behandlingens karaktär medför högre risker, t.ex.

[21] Se även WP 253-riktlinjerna, s. 9.

[22] Som exempel kan nämnas att när EDPB analyserar den del som rör ”överträdelsens karaktär” i sitt

när syftet är att övervaka, utvärdera personliga aspekter eller fatta beslut eller vidta åtgärder med negativa effekter för de registrerade, beroende på sammanhanget kring behandlingen och den personuppgiftsansvariges eller personuppgiftsbiträdets roll, får tillsynsmyndigheten överväga att tillskriva denna faktor större vikt. Dessutom kan en tillsynsmyndighet lägga större vikt vid denna faktor när det finns en tydlig obalans mellan de registrerade och den personuppgiftsansvarige (t.ex. när de registrerade är anställda, elever eller patienter) eller behandlingen omfattar sårbara registrerade, särskilt barn.

ii. **Uppgiftsbehandlingens omfattning**, med hänvisning till den lokala, nationella eller gränsöverskridande omfattningen av den uppgiftsbehandling som utförs och förhållandet mellan denna information och uppgiftsbehandlingens faktiska omfattning när det gäller den personuppgiftsansvariges resursfördelning. Denna faktor belyser en verklig riskfaktor som är kopplad till de större svårigheterna för den registrerade och tillsynsmyndigheten att begränsa olagliga beteenden i takt med att uppgiftsbehandlingens omfattning ökar. Ju större omfattningen av behandlingen är, desto större vikt kan tillsynsmyndigheten tillskriva denna faktor.

iii. **Uppgiftsbehandlingens syfte** kommer att leda till att tillsynsmyndigheten lägger större vikt vid denna faktor. Tillsynsmyndigheten får också överväga om behandlingen av personuppgifter omfattas av den personuppgiftsansvariges så kallade kärnverksamhet. Ju mer central behandlingen är för den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet, desto allvarligare blir oriktigheterna i denna behandling. Tillsynsmyndigheten får under dessa omständigheter lägga större vikt vid denna faktor. Det kan dock finnas omständigheter där behandlingen av personuppgifter är mer avlägsen från den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet, men påverkar utvärderingen avsevärt (detta är till exempel fallet när det gäller behandling av personuppgifter om arbetstagare där överträdelsen avsevärt påverkar dessa arbetstagares värdighet).

iv. **Antalet registrerade** som konkret men även potentiellt påverkas. Ju fler registrerade som berörs, desto större vikt kan tillsynsmyndigheten tillskriva denna faktor. I många fall kan det också anses att överträdelsen får ”systemiska” konnotationer och därför kan påverka, även vid olika tidpunkter, ytterligare registrerade som inte har lämnat in klagomål eller rapporter till tillsynsmyndigheten. Tillsynsmyndigheten får, beroende på omständigheterna i fallet, beakta förhållandet mellan antalet registrerade som berörs och det totala antalet registrerade i detta sammanhang (t.ex. antalet medborgare, kunder eller anställda) för att bedöma om överträdelsen är systembetingad.

v. **Nivån av skada** som lidits och i vilken utsträckning beteendet kan påverka enskildas rättigheter och friheter. Syftet med hänvisningen till nivån av ”den skada som lidits” är därför att göra tillsynsmyndigheterna uppmärksamma på den skada de lidit, eller som de sannolikt kommer att ha lidit, som en ytterligare separat parameter när det gäller antalet registrerade som berörs (t.ex. i fall där antalet personer som berörs av den olagliga behandlingen är stort men den skada de lidit är marginell). Enligt skäl 75 i dataskyddsförordningen avser skadenivån fysisk, materiell eller immateriell skada. Bedömningen av skadan ska under alla omständigheter begränsas till vad som är funktionellt nödvändigt för att uppnå en korrekt bedömning av överträdelsens svårighetsgrad enligt punkt 60 nedan, utan att överlappa verksamheten för de rättsliga myndigheter vars uppgift är att fastställa de olika formerna av individuell skada.

beslut 01/2020 om tvisten om utkastet till den irländska tillsynsmyndighetens beslut om Twitter International Company enligt artikel 65.1 a i dataskyddsförordningen (nedan kallat *EDPB:s bindande beslut 01/2020*) konstaterades att den berörda uppgiftsbehandlingen omfattade meddelanden från registrerade som avsiktligt valde att begränsa publiken för sådana meddelanden och rekommenderade att denna aspekt skulle beaktas vid bedömningen av behandlingens karaktär. I detta sammanhang se även EDPB:s bindande beslut 01/2020, punkt 186.

c) **Överträdelsens varaktighet**, vilket innebär att en tillsynsmyndighet i allmänhet kan lägga större vikt vid en överträdelse med längre varaktighet. Ju längre överträdelsens varaktighet är, desto större vikt kan tillsynsmyndigheten tillskriva denna faktor. Om ett visst beteende också var olagligt inom det föregående regelverket får, med förbehåll för nationell lagstiftning, både perioden efter dataskyddsförordningens ikraftträdande och den föregående perioden beaktas när sanktionsavgifterna kvantifieras, med beaktande av villkoren i regelverket i fråga.

54. Tillsynsmyndigheten får, beroende på omständigheterna i det enskilda fallet, lägga vikt vid ovannämnda faktorer. Om de inte är av särskild betydelse kan de också betraktas som neutrala.

4.2.2 – Om överträdelsen skett med uppsåt eller genom oaktsamhet

55. I sina tidigare riktlinjer uppgav EDPB att ”[g]enerellt 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”[23]. Oaktsamhet i detta avseende är inte detsamma som icke-frivilligt.

Exempel 4 – Illustrationer av uppsåt och oaktsamhet (från WP 253)[24]
”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.”

56. Överträdelsens uppsåtliga eller oaktsamma karaktär (artikel 83.2 b i dataskyddsförordningen) bör bedömas med beaktande av de objektiva delar av agerandet som samlats in från fakta i ärendet. EDPB betonade att det är allmänt vedertaget att ”uppsåtliga överträdelser som visar lagtrots är allvarligare än oavsiktliga”[25]. Vid en avsiktlig överträdelse kommer tillsynsmyndigheten sannolikt att lägga större vikt vid denna faktor. Beroende på omständigheterna i fallet får tillsynsmyndigheten också fästa vikt vid graden av oaktsamhet. I bästa fall kan oaktsamheten betraktas som neutral.

4.2.3 – Kategorier av berörda personuppgifter

57. När det gäller kravet att ta hänsyn till de kategorier av personuppgifter som berörs (artikel 83.2 g i dataskyddsförordningen) belyser dataskyddsförordningen tydligt de typer av uppgifter som förtjänar särskilt skydd och därför striktare åtgärder i fråga om sanktionsavgifter. Detta gäller åtminstone de typer av uppgifter som omfattas av artiklarna 9 och 10 i dataskyddsförordningen och uppgifter utanför tillämpningsområdet för dessa artiklar vars spridning orsakar omedelbar skada eller trångmål för den registrerade [26] (t.ex. lokaliseringsuppgifter, uppgifter om privat kommunikation, nationella identifikationsnummer eller finansiella uppgifter, såsom transaktionsöversikter eller kreditkortsnummer)[27]. I allmänhet kan tillsynsmyndigheten

[23] WP 253-riktlinjerna, s. 11.
[24] Exempel som citeras direkt i WP 253-riktlinjerna, s. 12.
[25] WP 253-riktlinjerna, s. 12.
[26] Ibid, s. 14.
[27] Spridning av privata kommunikations- och lokaliseringsuppgifter kan orsaka omedelbar skada eller trångmål för den registrerade, vilket framhålls av det särskilda skydd som EU-lagstiftaren ger för privat kommunikation i artikel 7 i stadgan

tillskriva denna faktor mer vikt ju fler av dessa kategorier av uppgifter som berörs eller ju känsligare uppgifterna är.

58. Dessutom är mängden uppgifter för varje registrerad relevant, med tanke på att intrånget i rätten till integritet och skydd av personuppgifter ökar med mängden uppgifter för varje registrerad.

4.2.4 – Klassificering av överträdelsens allvar och fastställande av lämpligt startbelopp

59. Bedömningen av faktorerna ovan (kapitel 4.2.1–4.2.3) avgör överträdelsens allvar som helhet. Denna bedömning är ingen matematisk beräkning där ovannämnda faktorer beaktas individuellt, utan snarare en grundlig utvärdering av de konkreta omständigheterna i ärendet, där alla ovannämnda faktorer är sammanlänkade. Vid översynen av hur allvarlig överträdelsen är bör man därför ta hänsyn till överträdelsen som helhet.

60. På grundval av utvärderingen av de faktorer som beskrivs ovan anses överträdelsen vara av i) låg, ii) medelhög eller iii) hög allvarlighetsgrad. Dessa kategorier påverkar inte frågan om huruvida sanktionsavgifter kan åläggas eller inte.

- Vid beräkningen av administrativa sanktionsavgifter för överträdelser med **låg allvarlighetsgrad** kommer tillsynsmyndigheten att fastställa startbeloppet för ytterligare beräkning vid en punkt mellan 0 % och 10 % av det tillämpliga lagstadgade maximibeloppet.

- Vid beräkningen av administrativa sanktionsavgifter för överträdelser med **medelhög allvarlighetsgrad** kommer tillsynsmyndigheten att fastställa startbeloppet för ytterligare beräkning vid en punkt mellan 10 och 20 % av det tillämpliga lagstadgade maximibeloppet.

- Vid beräkningen av överträdelser av administrativa sanktionsavgifter med **hög allvarlighetsgrad** kommer tillsynsmyndigheten att fastställa startbeloppet för ytterligare beräkning vid en punkt mellan 20 % och 100 % av det tillämpliga lagstadgade maximibeloppet.

61. Som en allmän regel är det sannolikt att ju allvarligare överträdelsen är inom sin egen kategori, desto högre är startbeloppet.

62. De intervall inom vilka startbeloppet fastställs granskas fortfarande av EDPB och dess medlemmar och kan anpassas vid behov.

Exempel 5 a – Kvalificering av en överträdelses allvar (hög allvarlighetsgrad)
Efter att ha undersökt ett flertal klagomål om oönskade samtal från kunder i ett telefonföretag fann den behöriga tillsynsmyndigheten att telefonföretaget använde sina kunders kontaktuppgifter för distansmarknadsföring utan giltig rättslig grund (överträdelse av artikel 6 i dataskyddsförordningen). I synnerhet hade telefonföretaget erbjudit sina kunders namn och registrerade telefonnummer till tredje parter i marknadsföringssyfte. Telefonföretaget gjorde detta trots råd från dataskyddsombudet, utan att vidta några åtgärder för att förhindra agerandet eller erbjuda kunderna ett sätt att invända mot det. Faktum är att agerandet hade pågått sedan maj 2018 och fortfarande pågick vid tidpunkten för undersökningen. Telefonföretaget i fråga drevs över hela landet och dess praxis påverkade alla dess 4 miljoner kunder. Tillsynsmyndigheten fann att alla dessa kunder regelbundet hade utsatts för oönskade samtal från tredje part, och att de saknade effektiva medel för att stoppa dem.

Tillsynsmyndigheten fick i uppdrag att bedöma ärendets allvar. Som utgångspunkt noterade tillsynsmyndigheten att en överträdelse av artikel 6 i dataskyddsförordningen ***förtecknas bland överträdelserna av artikel 83.5 i dataskyddsförordningen*** *och därför omfattas av den högre nivån*

om de grundläggande rättigheterna och direktiv 2002/58/EG och av EU-domstolen för lokaliseringsuppgifter i vissa fall, se de förenade målen C-511/18, C-512/18 och C-520/18, La Quadrature du Net m.fl., punkt 117 och där angiven rättspraxis.

i artikel 83 i dataskyddsförordningen. För det andra bedömde tillsynsmyndigheten omständigheterna i ärendet. I detta avseende tillskrev tillsynsmyndigheten ***överträdelsens karaktär*** *betydande vikt, eftersom den överträdda bestämmelsen (artikel 6 i dataskyddsförordningen) underbygger lagligheten i behandlingen av uppgifter som helhet. Bristande efterlevnad av denna bestämmelse undanröjer lagligheten i behandlingen som helhet. Tillsynsmyndigheten tillskrev också* ***överträdelsens varaktighet*** *stor vikt, då den inleddes när dataskyddsförordningen trädde i kraft och inte hade upphört vid tidpunkten för undersökningen. Det faktum att telefonföretaget var verksamt i hela landet ökade betydelsen av* ***behandlingens omfattning****.* ***Antalet berörda registrerade*** *ansågs vara mycket högt (4 miljoner, i förhållande till en total befolkning på 14 miljoner människor), medan* ***nivån på den skada som de lidit*** *ansågs vara måttlig (icke-materiella skador, i form av olägenheter). Den senare bedömningen gjordes med beaktande av de* ***kategorier av uppgifter som berördes*** *(namn och telefonnummer). Överträdelsens allvar ökades dock genom att överträdelsen begicks i strid med ett råd från dataskyddsombudet och därmed ansågs vara* ***uppsåtlig****.*

Mot bakgrund av ovanstående (allvarlig karaktär, lång varaktighet, stort antal registrerade, nationellt tillämpningsområde, uppsåtlig karaktär, måttlig skada) drar tillsynsmyndigheten slutsatsen att överträdelsen anses vara av ***hög allvarlighetsgrad****. Tillsynsmyndigheten kommer att fastställa startbeloppet för ytterligare beräkningar till en punkt mellan 20 och 100 % av det lagstadgade maximibeloppet enligt artikel 83.5 i dataskyddsförordningen.*

Exempel 5 b – Kvalificering av en överträdelses allvar (medelhög allvarlighetsgrad)
En tillsynsmyndighet mottog en anmälan om personuppgiftsincident från ett sjukhus. Av denna anmälan framgick att flera anställda hade kunnat se delar av patienternas hälsojournaler som – med tanke på deras avdelning – inte borde ha varit tillgängliga för dem. Sjukhuset hade arbetat med procedurer för att reglera tillgången till patientfiler och infört strikta åtgärder för begränsad tillgång. Detta innebar att personal från en avdelning endast kunde få tillgång till medicinsk information som var relevant för den specifika avdelningen. Dessutom hade sjukhuset investerat i åtgärder för integritetsmedvetenhet bland sina anställda. Det visade sig dock att det fanns problem med övervakningen av tillstånd. Personal som rörde sig mellan avdelningar kunde fortfarande få tillgång till patientfilerna från sina ”gamla” avdelningar och sjukhuset hade inga rutiner för att matcha de anställdas aktuella befattningar med deras tillstånd. Sjukhusets interna utredning visade att minst 150 anställda (av 3 500) hade felaktiga tillstånd, vilket påverkade minst 20 000 av de 95 000 patientfilerna. Sjukhuset kunde visa att personalen i minst 16 fall hade använt sina tillstånd för att se patientfiler. Tillsynsmyndigheten anser att det har skett en överträdelse av artikel 32 i dataskyddsförordningen.

Vid bedömningen av ärendets allvar noterade tillsynsmyndigheten först att en överträdelse av artikel 32 i dataskyddsförordningen ***förtecknas bland överträdelserna av artikel 83.4 i dataskyddsförordningen*** *och därför omfattas av den lägre nivån i artikel 83 i dataskyddsförordningen. För det andra bedömde tillsynsmyndigheten omständigheterna i ärendet. I detta avseende ansåg tillsynsmyndigheten att även om* ***antalet registrerade som påverkades*** *av överträdelsen endast var 16, kunde det potentiellt ha handlat om 20 000 under omständigheterna i fallet och till och med 95 000 med tanke på ärendets systemiska karaktär. Dessutom kategoriserade tillsynsmyndigheten överträdelsen som* ***oaktsam****, men i låg grad, vilket ansågs vara en neutral faktor under omständigheterna i detta särskilda fall på grund av att sjukhuset underlät att anta riktlinjer för godkännande där det säkerligen borde ha gjort det, men i annat fall hade vidtagit stränga åtgärder för att begränsa tillgången. Denna utvärdering påverkades inte av att annan dataskydds- och säkerhetspolitik genomfördes framgångsrikt, vilket krävs enligt dataskyddsförordningen. Slutligen tillskrev tillsynsmyndigheten ärendet betydande vikt på grund av det faktum att patientjournalerna innehåller hälsouppgifter, som är* ***särskilda kategorier av uppgifter*** *enligt artikel 9 i dataskyddsförordningen.*

Mot bakgrund av ovanstående (uppgiftsbehandlingens karaktär och särskilda kategorier av uppgifter i förhållande till antalet registrerade som faktiskt och potentiellt påverkas) drar tillsynsmyndigheten slutsatsen att överträdelsen anses vara av ***medelhög allvarlighetsgrad****.*

Tillsynsmyndigheten kommer att fastställa startbeloppet för ytterligare beräkningar till en punkt mellan 10 och 20 % av det lagstadgade maximibeloppet enligt artikel 83.4 i dataskyddsförordningen.

Exempel 5 c – Kvalificering av en överträdelses allvar (låg allvarlighetsgrad)
En tillsynsmyndighet har mottagit många klagomål om hur en onlinebutik hanterar de registrerades rätt till åtkomst. Enligt de klagande har hanteringen av deras begäranden om åtkomst tagit mellan 4 och 6 månader, vilket ligger utanför den tidsfrist som medges i dataskyddsförordningen. Tillsynsmyndigheten undersöker klagomålen och konstaterar att onlinebutiken svarar på begäranden om åtkomst högst tre månader för sent i 5 % av fallen. Sammanlagt tog butiken emot omkring 1 000 åtkomstbegäranden på årsbasis och bekräftade att 950 av dessa hanterades i tid. Dessutom hade onlinebutiken riktlinjer för att säkerställa att alla begäranden om åtkomst hanterades korrekt och fullständigt. Tillsynsmyndigheten drog dock slutsatsen att onlinebutiken bröt mot artikel 12.3 i dataskyddsförordningen och beslutade att ålägga sanktionsavgifter.

Vid beräkningen av sanktionsbeloppet fick tillsynsmyndigheten i uppdrag att bedöma ärendets allvar. Som utgångspunkt noterade tillsynsmyndigheten att en överträdelse av artikel 12 i dataskyddsförordningen ***förtecknas bland överträdelserna av artikel 83.5 i dataskyddsförordningen*** *och därför omfattas av den högre nivån i artikel 83 i dataskyddsförordningen. För det andra bedömde tillsynsmyndigheten omständigheterna i ärendet. I detta avseende analyserade tillsynsmyndigheten noggrant* ***överträdelsens karaktär****. Även om rätten till tillgång till personuppgifter i rätt tid är en av hörnstenarna i de registrerades rättigheter ansåg tillsynsmyndigheten att överträdelsen var begränsad i detta avseende, med tanke på att alla begäranden hanterades så småningom och att förseningen var begränsad. Med tanke på* ***syftet med behandlingen*** *fann tillsynsmyndigheten att behandlingen av personuppgifter inte var onlinebutikens kärnverksamhet, men att den fortfarande var en viktig hjälpåtgärd för att uppnå dess mål att sälja varor online. Tillsynsmyndigheten ansåg att detta ökade överträdelsens allvarlighetsgrad. Å andra sidan ansågs den* ***skada som de registrerade lidit*** *vara minimal, eftersom alla begäranden om åtkomst behandlades inom sex månader.*

Mot bakgrund av ovanstående (överträdelsens art, syftet med behandlingen och skadenivån) drar tillsynsmyndigheten slutsatsen att överträdelsen anses vara av ***låg allvarlighetsgrad****. Tillsynsmyndigheten kommer att fastställa startbeloppet för ytterligare beräkningar till en punkt mellan 0 och 10 % av det lagstadgade maximibeloppet enligt artikel 83.5 i dataskyddsförordningen.*

4.3 – Företagets omsättning i syfte att ålägga effektiva, avskräckande och proportionella sanktionsavgifter

63. Enligt dataskyddsförordningen ska varje tillsynsmyndighet säkerställa att administrativa sanktionsavgifter är effektiva, proportionella och avskräckande i varje enskilt fall (artikel 83.1 i dataskyddsförordningen). Tillämpningen av dessa principer i EU-lagstiftningen kan få långtgående konsekvenser i enskilda fall, eftersom de utgångspunkter som dataskyddsförordningen erbjuder för att beräkna administrativa sanktionsavgifter gäller både mikroföretag och multinationella företag. För att ålägga sanktionsavgifter som är effektiva, proportionella och avskräckande i samtliga fall förväntas tillsynsmyndigheterna skräddarsy de administrativa sanktionsavgifterna inom hela det tillgängliga intervallet fram till det högsta lagstadgade maximibeloppet. Detta kan leda till betydande höjningar eller nedsättningar av sanktionsbeloppet, beroende på omständigheterna i ärendet.

64. EDPB anser att det är rimligt att avspegla skillnaden mellan företagens storlek i de utgångspunkter som anges nedan och beaktar därför dess omsättning[28]. EDPB följer kraven i artikel 83 i dataskyddsförordningen,

[28] Se även EDPB:s bindande beslut 1/2021, punkterna 411 och 412: ”[I den mån] ett företags omsättning inte enbart är relevant för fastställandet av det högsta beloppet för sanktionsavgifter i enlighet med artikel 83.4–83.6 i den allmänna dataskyddsförordningen, utan även kan beaktas vid beräkningen av själva sanktionsavgifterna när så är lämpligt för att säkerställa att sanktionsavgifterna är effektiva, proportionella och avskräckande i enlighet med artikel 83.1 i den allmänna dataskyddsförordningen.” Det berörda företagets omsättning beskrivs närmare i kapitel 6.2 i dessa riktlinjer.

dataskyddsförordningen som helhet och EU-domstolens fasta rättspraxis, där det anges att ett företags omsättning kan utgöra en indikation på ett företags storlek och ekonomiska inflytande[29]. Detta utesluter dock inte en tillsynsmyndighet från ansvaret att genomföra en översyn av effektivitet, avskräckande effekt och proportionalitet i slutet av beräkningen (se kapitel 7). Den senare omfattar alla omständigheter i ärendet, t.ex. ackumulering av flera överträdelser, ökningar och minskningar för försvårande och förmildrande omständigheter och finansiella/socioekonomiska omständigheter. Det åligger dock tillsynsmyndigheten att se till att samma omständigheter inte räknas två gånger. I synnerhet bör tillsynsmyndigheterna enligt kapitel 7 inte upprepa höjningar eller nedsättningar i förhållande till företagets omsättning, utan snarare se över sin bedömning av det lämpliga startbeloppet.

65. Av de skäl som anges ovan kan tillsynsmyndigheten överväga att justera startbeloppet som motsvarar överträdelsens allvar i fall där överträdelsen begås av ett företag med en årsomsättning på högst 2 miljoner euro, en årsomsättning på högst 10 miljoner euro eller en årsomsättning på högst 50 miljoner euro[30].

- **För företag med en årsomsättning på ≤ 2 miljoner euro**, kan tillsynsmyndigheterna överväga att göra beräkningar på grundval av ett belopp på mellan 0,2 % och 0,4 % av det fastställda startbeloppet.

- **För företag med en årsomsättning på 2 miljoner euro och upp till 10 miljoner euro** får tillsynsmyndigheterna överväga att göra beräkningar på grundval av ett belopp på mellan 0,3 % och 2 % av det fastställda startbeloppet.

- **För företag med en årsomsättning på 10 miljoner euro och upp till 50 miljoner euro** får tillsynsmyndigheterna överväga att göra beräkningar på grundval av ett belopp på mellan 1,5 % och 10 % av det fastställda startbeloppet.

66. Av samma skäl får tillsynsmyndigheten överväga att justera startbeloppet som motsvarar överträdelsens allvar i fall där överträdelsen begås av ett företag med en årsomsättning på högst 100 miljoner euro, en årsomsättning på högst 250 miljoner euro eller en årsomsättning på högst 500 miljoner euro[31].

- För **företag med en årsomsättning på 50 miljoner euro och upp till 100 miljoner euro** får tillsynsmyndigheterna överväga att göra beräkningar på grundval av ett belopp på mellan 8 % och 20 % av det fastställda startbeloppet.

- För **företag med en årsomsättning på 100 miljoner euro och upp till 250 miljoner euro** får tillsynsmyndigheterna överväga att göra beräkningar på grundval av ett belopp på mellan 15 % och 50 % av det fastställda startbeloppet.

- För **företag med en årsomsättning på 250 miljoner euro och upp till 500 miljoner euro** får tillsynsmyndigheterna överväga att göra beräkningar på grundval av ett belopp på mellan 40 % och 100 % av det fastställda startbeloppet.

- För företag **med en årsomsättning över 500 miljoner euro** får tillsynsmyndigheterna överväga att gå vidare utan att justera det fastställda startbeloppet. Sådana företag överskrider det statiska lagstadgade maximibeloppet och företagets storlek återspeglas därför redan i det dynamiska högsta belopp i lagstiftningen som används för att fastställa startbeloppet för ytterligare beräkning på grundval av en bedömning av överträdelsens allvar.

[29] Detta har fastställts av tribunalen i mål T-25/06, Alliance One International, Inc./kommissionen, punkt 211, med hänvisning till annan rättspraxis, t.ex. mål T-9/99, HFB m.fl./kommissionen, punkterna 528 och 529 och mål T-175/05, Akzo Nobel m.fl./kommissionen, punkt 114.

[30] Dessa omsättningssiffror är inspirerade av kommissionens rekommendation av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag. Vid fastställandet av utgångspunkterna utgår EDPB enbart från företagets årsomsättning (se kapitel 6 nedan).

[31] Dessa siffror läggs till för att överbrygga skillnaden mellan det högsta tröskelvärdet i föregående punkt och det tröskelvärde för omsättning som anges i artikel 83.4–83.6 i dataskyddsförordningen.

67. Som en allmän regel är det sannolikt att ju högre omsättning företaget har inom sin tillämpliga nivå, desto högre är startbeloppet. Det senare gäller särskilt de största företagen, för vilka startbeloppskategorin har störst räckvidd.

68. Dessutom är tillsynsmyndigheten inte skyldig att tillämpa denna justering om det inte är nödvändigt med tanke på sanktionsbeloppets effektivitet, avskräckande effekt och proportionalitet.

69. Det bör upprepas att dessa siffror är utgångspunkten för ytterligare beräkningar och inte fasta belopp (prismärkningar) för överträdelser av bestämmelserna i dataskyddsförordningen. Tillsynsmyndigheten har rätt att använda hela betalningsintervallet från vilket belopp som helst till dess att det lagstadgade maximibeloppet uppnås, vilket säkerställer att sanktionsavgifterna är skräddarsydda efter omständigheterna i målet, vilket domstolen kräver om en abstrakt utgångspunkt används.

Exempel 6 a – Identifiera startpunkterna för ytterligare beräkning
En stormarknadskedja med en omsättning på 450 miljoner euro har överträtt artikel 12 i dataskyddsförordningen. På grundval av en noggrann analys av omständigheterna i ärendet beslutade tillsynsmyndigheten att överträdelsen var av låg allvarlighetsgrad. För att fastställa utgångspunkten för ytterligare beräkningar fastställer tillsynsmyndigheten först att artikel 12 i dataskyddsförordningen förtecknas i artikel 83.5 b i dataskyddsförordningen och att, baserat på företagets omsättning (450 miljoner euro), det lagstadgade maximibeloppet på 20 miljoner euro ska tillämpas.

Baserat på den allvarlighetsgrad som fastställts av tillsynsmyndigheten (låg) bör ett startbelopp på mellan 0 och 2 miljoner euro beaktas (mellan 0 och 10 % av det lagstadgade maximibeloppet, se punkt 60 ovan).

Tillsynsmyndigheten anser att en justering ned till 90 % av grundbeloppet är motiverad på grundval av företagets storlek, vars omsättning är 450 miljoner euro. Detta belopp utgör grunden för ytterligare beräkningar, vilka bör leda till ett slutligt belopp som inte överstiger det tillämpliga lagstadgade maximibeloppet på 20 miljoner euro.

Exempel 6 b – Identifiera startpunkterna för ytterligare beräkning
En nystartad dejtingapp med en omsättning på 500 000 euro upptäcks ha sålt känsliga personuppgifter om sina kunder till flera datamäklare för analys och har därmed överträtt artiklarna 9 och 5.1 a i dataskyddsförordningen. På grundval av en noggrann analys av omständigheterna i ärendet beslutade tillsynsmyndigheten att överträdelsen var av hög allvarlighetsgrad. För att fastställa utgångspunkten för ytterligare beräkningar fastställer tillsynsmyndigheten först att artiklarna 9 och 5 i dataskyddsförordningen förtecknas i artikel 83.5 a i dataskyddsförordningen och att, baserat på företagets omsättning (500 000 euro), ett lagstadgat maximibelopp på 20 000 000 euro är tillämpligt.

Baserat på den allvarlighetsgrad som fastställts av tillsynsmyndigheten (hög) bör ett startbelopp på mellan 4 000 000 euro och 20 000 000 euro beaktas (mellan 20 % och 100 % av det tillämpliga lagstadgade maximibeloppet, se punkt 60 ovan).

Tillsynsmyndigheten anser att en justering ned till 0,25 % av startbeloppet är motiverad på grundval av företagets storlek, eftersom omsättningen ligger på 500 000 euro. Detta belopp utgör grunden för ytterligare beräkningar, vilka bör leda till ett slutligt belopp som inte överstiger det tillämpliga lagstadgade maximibeloppet på 20 miljoner euro.

KAPITEL 5 – FÖRSVÅRANDE OCH FÖRMILDRANDE OMSTÄNDIGHETER

5.1 – Identifiering av försvårande och förmildrande faktorer

70. Efter att ha utvärderat överträdelsens art, allvar och varaktighet samt dess uppsåtliga eller oaktsamma karaktär och de kategorier av personuppgifter som berörs, måste tillsynsmyndigheten i enlighet med dataskyddsförordningen ta hänsyn till de återstående försvårande och förmildrande faktorer som förtecknas i artikel 83.2 i dataskyddsförordningen.

71. När det gäller bedömningen av dessa faktorer kan höjningar eller nedsättningar av sanktionsavgifter inte förutbestämmas genom tabeller eller procentsatser. Det erinras om att den faktiska kvantifieringen av sanktionsavgifterna kommer att bero på alla de faktorer som samlats in under undersökningens gång och på ytterligare överväganden som också är kopplade till tillsynsmyndighetens tidigare erfarenheter av att betala sanktionsavgifter.

72. För tydlighetens skull bör det noteras att varje kriterium i artikel 83.2 i dataskyddsförordningen – oavsett om det bedöms enligt kapitel 4 eller detta kapitel – endast bör beaktas en gång som en del av den övergripande bedömningen av artikel 83.2 i dataskyddsförordningen.

5.2 – Åtgärder som vidtas av den personuppgiftsansvarige eller personuppgiftsbiträdet för att minska den skada som de registrerade lidit

73. Ett första steg för att avgöra om försvårande eller förmildrande omständigheter har inträffat är att se över artikel 83.2 c, som rör ”[d]e åtgärder som den personuppgiftsansvarige eller personuppgiftsbiträdet har vidtagit för att lindra den skada som de registrerade har lidit”.

74. Såsom erinras om i WP 253-riktlinjerna är personuppgiftsansvariga och personuppgiftsbiträden redan 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”. Vid en överträdelse bör dock den personuppgiftsansvarige eller personuppgiftsbiträdet ”göra vad han eller hon kan för att minska konsekvenserna av överträdelsen för den eller de enskilda som berörs”[32].

75. Antagandet av lämpliga åtgärder för att mildra den skada som de registrerade lidit kan betraktas som en förmildrande faktor som minskar sanktionsbeloppet.

76. De vidtagna åtgärderna måste särskilt bedömas med hänsyn till hur aktuella de är, dvs. när de genomförs av den personuppgiftsansvarige eller personuppgiftsbiträdet, och hur effektiva de är. I detta avseende är det mer sannolikt att åtgärder som genomförs spontant innan tillsynsmyndighetens utredning inleds och blir känd för den personuppgiftsansvarige eller personuppgiftsbiträdet betraktas som en förmildrande faktor än åtgärder som vidtas efter den tidpunkten.

5.3 – Den personuppgiftsansvariges eller personuppgiftsbiträdets grad av ansvar

77. Enligt artikel 83.2 d måste den personuppgiftsansvariges eller personuppgiftsbiträdets grad av ansvar bedömas, med beaktande av de åtgärder som de har vidtagit i enlighet med artiklarna 25 och 32 i dataskyddsförordningen. I enlighet med WP 253-riktlinjerna är ”[d]en fråga tillsynsmyndigheten måste besvara [...] 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[33]”.

78. Särskilt när det gäller detta kriterium måste den kvarstående risken för de registrerades friheter och rättigheter, de negativa effekter som de registrerade åsamkas och den skada som kvarstår efter att den

[32] WP 253-riktlinjerna, s. 12.
[33] Ibid, s. 13.

personuppgiftsansvarige har antagit åtgärderna samt graden av robusthet hos de åtgärder som antagits i enlighet med artiklarna 25 och 32 i dataskyddsförordningen bedömas.

79. I detta avseende får tillsynsmyndigheten också överväga om uppgifterna i fråga var direkt identifierbara och/eller tillgängliga utan tekniskt skydd[34]. Man bör dock komma ihåg att förekomsten av ett sådant skydd inte nödvändigtvis utgör en förmildrande faktor (se punkt 82 nedan). Detta beror på omständigheterna i målet.

80. För att göra en adekvat bedömning av ovanstående faktorer bör tillsynsmyndigheten beakta all relevant dokumentation som tillhandahålls av den personuppgiftsansvarige eller personuppgiftsbiträdet, t.ex. i samband med utövandet av deras rätt till försvar. I synnerhet skulle sådan dokumentation kunna styrka när åtgärderna vidtogs och hur de genomfördes, om interaktioner skedde mellan den personuppgiftsansvarige och personuppgiftsbiträdet (i tillämpliga fall) eller om det förekommit kontakt med uppgiftsskyddsombudet eller registrerade (i tillämpliga fall).

81. Med tanke på den ökade ansvarsskyldigheten enligt dataskyddsförordningen jämfört med direktiv 95/46/EG[35] är det sannolikt att den personuppgiftsansvariges eller personuppgiftsbiträdets grad av ansvar kommer att betraktas som en försvårande eller neutral faktor. Endast i undantagsfall, där den personuppgiftsansvarige eller personuppgiftsbiträdet har överskridit sina skyldigheter, kommer detta att betraktas som en förmildrande faktor.

5.4 – Tidigare överträdelser av den personuppgiftsansvarige eller personuppgiftsbiträdet

82. Tidigare överträdelser är överträdelser som redan konstaterats innan beslutet utfärdas. När det gäller samarbete enligt kapitel VII i dataskyddsförordningen är tidigare överträdelser de som redan fastställts innan utkastet till beslut (i den mening som avses i artikel 60 i dataskyddsförordningen) utfärdas.

83. Enligt artikel 83.2 e i dataskyddsförordningen måste alla relevanta tidigare överträdelser som begåtts av den personuppgiftsansvarige eller personuppgiftsbiträdet beaktas när beslut fattas om huruvida administrativa sanktionsavgifter ska åläggas och om beloppet för de administrativa sanktionsavgifterna. Liknande formulering återfinns i skäl 148 i dataskyddsförordningen.

5.4.1 – Tidsram

84. För det första måste hänsyn tas till den tidpunkt då den tidigare överträdelsen ägde rum, med beaktande av att ju längre tid som förflutit mellan en tidigare överträdelse och den överträdelse som för närvarande utreds, desto mindre är dess betydelse. Ju längre sedan överträdelsen begicks, desto mindre relevans ska alltså tillsynsmyndigheterna tillskriva den. Denna bedömning överlåts åt tillsynsmyndigheten, med förbehåll för tillämplig nationell och europeisk lagstiftning och tillämpliga principer.

85. Eftersom överträdelser som begåtts för länge sedan fortfarande kan vara av intresse vid bedömningen av den personuppgiftsansvariges eller personuppgiftsbiträdets ”spårregister” ska dock fasta preskriptionstider inte fastställas för detta ändamål. Vissa nationella lagar hindrar dock tillsynsmyndigheten från att beakta tidigare överträdelser efter en fastställd tidsperiod. På samma sätt föreskriver vissa nationella lagar en skyldighet att radera registeruppgifter efter en viss tidsperiod, vilket hindrar de tillsynsmyndigheter som agerar från att ta hänsyn till dessa prejudikat.

86. Av samma skäl bör det noteras att överträdelser av dataskyddsförordningen, eftersom de är mer aktuella, måste betraktas som mer relevanta än överträdelser av de nationella bestämmelser som antagits för genomförandet av direktiv 95/46/EG (om nationella lagar tillåter att sådana överträdelser beaktas av tillsynsmyndigheten).

[34] Ibid, s. 14–15.
[35] Ibid, s. 13.

5.4.2 – Sakfråga

87. Vid tillämpning av artikel 83.2 e i dataskyddsförordningen kan tidigare överträdelser av antingen samma eller en annan sakfråga än den som utreds betraktas som ”relevanta”.

88. Även om alla tidigare överträdelser kan ge en indikation om den personuppgiftsansvariges eller personuppgiftsbiträdets allmänna inställning till efterlevnaden av dataskyddsförordningen, måste överträdelser av samma sakfråga ges större betydelse, eftersom de ligger närmare den överträdelse som för närvarande utreds, särskilt när den personuppgiftsansvarige eller personuppgiftsbiträdet tidigare begick samma överträdelse (upprepade överträdelser). Överträdelser av samma sakfråga måste därför anses vara mer relevanta än tidigare överträdelser som rör en annan fråga.

89. Att den personuppgiftsansvarige eller personuppgiftsbiträdet tidigare har underlåtit att inom rimlig tid reagera när registrerade utövar sina rättigheter måste till exempel anses vara mer relevant när den överträdelse som utreds också gäller bristande svar till en registrerad som utövar sina rättigheter, än när det avser en personuppgiftsincident.

90. Dock måste vederbörlig hänsyn tas till tidigare överträdelser av en annan sakfråga, men som begåtts på samma sätt, eftersom de kan tyda på bestående problem inom den personuppgiftsansvarige eller personuppgiftsbiträdets organisation. Detta skulle till exempel vara fallet för överträdelser som uppkommer till följd av att dataskyddsombudet råd har ignorerats.

5.4.3 – Andra överväganden

91. Om tillsynsmyndigheterna beaktar en tidigare överträdelse av de nationella bestämmelser som antagits för genomförandet av direktiv 95/46/EG måste de ta hänsyn till att kraven i direktivet och dataskyddsförordningen kan skilja sig åt (om nationella lagar tillåter att sådana överträdelser beaktas av tillsynsmyndigheten).

92. När tillsynsmyndigheten överväger relevansen av en tidigare överträdelse bör den ta hänsyn till statusen för det förfarande där den tidigare överträdelsen konstaterades, särskilt eventuella åtgärder som vidtagits av tillsynsmyndigheten eller den rättsliga myndigheten, i enlighet med nationell lagstiftning.

93. Tidigare överträdelser kan också beaktas när de påträffades av en annan tillsynsmyndighet avseende samma personuppgiftsansvarig/personuppgiftsbiträde. Till exempel skulle den ansvariga tillsynsmyndighet som hanterar en överträdelse genom samarbetsmekanismen (en enda kontaktpunkt) i enlighet med artikel 60 i dataskyddsförordningen kunna beakta överträdelser som tidigare fastställts i lokala fall av en annan tillsynsmyndighet avseende samma personuppgiftsansvarig/personuppgiftsbiträde. På samma sätt kan överträdelser som tidigare fastställts av den ansvariga tillsynsmyndigheten beaktas när en annan myndighet måste hantera ett klagomål som lämnats in till den i fall med endast lokal påverkan enligt artikel 56.2 i dataskyddsförordningen. Om det inte finns någon ansvarig tillsynsmyndighet (t.ex. om den personuppgiftsansvarige eller personuppgiftsbiträdet inte är etablerat i Europeiska unionen) kan tillsynsmyndigheterna också beakta överträdelser som tidigare fastställts av en annan tillsynsmyndighet avseende samma personuppgiftsansvarig/personuppgiftsbiträde.

94. Förekomsten av tidigare överträdelser kan betraktas som en försvårande faktor vid beräkningen av sanktionsavgifterna. Den vikt som läggs vid denna faktor ska fastställas med hänsyn till de tidigare överträdelsernas karaktär och frekvens. Avsaknaden av tidigare överträdelser kan dock inte betraktas som en förmildrande faktor, eftersom efterlevnad av dataskyddsförordningen är normen. Om det inte förekommit några tidigare överträdelser kan denna faktor betraktas som neutral.

5.5 – Grad av samarbete med tillsynsmyndigheten för att komma till rätta med överträdelsen och minska dess potentiella negativa effekter

95. Enligt artikel 83.2 f ska tillsynsmyndigheten beakta graden av samarbete med den personuppgiftsansvarige eller personuppgiftsbiträdet med tillsynsmyndigheten för att avhjälpa överträdelsen och mildra de eventuella negativa effekterna av överträdelsen.

96. Innan den personuppgiftsansvarige eller personuppgiftsbiträdet ytterligare bedömer graden av samarbete med tillsynsmyndigheten måste det upprepas att en allmän skyldighet att samarbeta åligger den personuppgiftsansvarige och personuppgiftsbiträdet i enlighet med artikel 31 i dataskyddsförordningen, och att bristande samarbete kan leda till att de sanktionsavgifter som föreskrivs i artikel 83.4 a i dataskyddsförordningen tillämpas. Det bör därför anses att den normala samarbetsskyldigheten är obligatorisk och därför bör anses vara neutral (och inte en förmildrande faktor).

97. Om samarbetet med tillsynsmyndigheten inneburit att eventuella negativa konsekvenser för enskilda personers rättigheter har begränsats eller undvikits, får tillsynsmyndigheten dock betrakta detta som en förmildrande faktor i den mening som avses i artikel 83.2 f i dataskyddsförordningen och därigenom minska sanktionsbeloppet. Detta kan till exempel vara fallet när en personuppgiftsansvarig eller ett personuppgiftsbiträde ”genom sin reaktion på tillsynsmyndighetens begäranden under utredningen av det specifika fallet begränsat inverkan på enskildas rättigheter väsentligt”[36].

5.6 – Sättet på vilket tillsynsmyndigheten fick kännedom om överträdelsen

98. Enligt artikel 83.2 h kan det sätt på vilket överträdelsen blev känd för tillsynsmyndigheten vara en relevant försvårande eller förmildrande faktor. Vid bedömningen av detta kan särskild vikt läggas vid frågan om, och i så fall i vilken utsträckning, den personuppgiftsansvarige eller personuppgiftsbiträdet på eget initiativ anmälde överträdelsen innan tillsynsmyndigheten fick kännedom om den, genom till exempel ett klagomål eller en utredning. Denna omständighet är inte relevant när den personuppgiftsansvarige omfattas av särskilda anmälningsskyldigheter (t.ex. vid personuppgiftsbrott enligt artikel 33)[37]. I sådana fall bör denna anmälan betraktas som neutral[38].

99. Om tillsynsmyndigheten fick kännedom om överträdelsen genom t.ex. ett klagomål eller en utredning bör denna faktor i regel också betraktas som neutral. Tillsynsmyndigheten får betrakta detta som en förmildrande omständighet om den personuppgiftsansvarige eller personuppgiftsbiträdet har meddelat överträdelsen på eget initiativ, innan tillsynsmyndigheten har fått kännedom om ärendet.

5.7 – Efterlevnad av åtgärder som tidigare beslutats med avseende på samma sakfråga

100. I artikel 83.2 i i dataskyddsförordningen anges att ”[n]är åtgärder enligt artikel 58.2 tidigare har förordnats mot den berörda personuppgiftsansvarige eller personuppgiftsbiträdet vad gäller samma sakfråga [ska] efterlevnad av dessa åtgärder” beaktas när beslut fattas om huruvida administrativa sanktionsavgifter ska åläggas och om dess belopp ska fastställas.

101. I motsats till artikel 83.2 e i dataskyddsförordningen avser denna bedömning endast åtgärder som tillsynsmyndigheterna själva tidigare har utfärdat till samma personuppgiftsansvarig eller personuppgiftsbiträde i samma sakfråga[39].

102. I detta avseende kan den personuppgiftsansvarige eller personuppgiftsbiträdet ha rimliga förväntningar på att efterlevnaden av tidigare utfärdade åtgärder mot dem skulle förhindra överträdelser av samma sakfråga från att äga rum i framtiden. Eftersom efterlevnad av tidigare beslutade åtgärder är obligatoriskt för den

[36] WP 253-riktlinjerna, s. 14.
[37] Det bör understrykas att en personuppgiftsincident inte nödvändigtvis innebär en överträdelse av dataskyddsförordningen.
[38] Detta betonas i WP 253-riktlinjerna, s. 15.
[39] Ibid.

personuppgiftsansvarige eller personuppgiftsbiträdet bör den dock inte i sig betraktas som en förmildrande faktor. Tvärtom krävs ett starkare åtagande från den personuppgiftsansvariges eller personuppgiftsbiträdets sida när det gäller att uppfylla tidigare åtgärder för att denna faktor ska tillämpas som förmildrande, t.ex. att ytterligare åtgärder vidtas utöver dem som begärts av tillsynsmyndigheten.

103. Däremot kan bristande efterlevnad av tidigare beslutade korrigerande befogenheter betraktas som antingen en försvårande faktor eller som en annan överträdelse i sig i enlighet med artikel 83.5 e och artikel 83.6 i dataskyddsförordningen. Det bör därför noteras att samma beteende där bestämmelser inte efterlevs inte kan leda till en situation där det straffas två gånger.

5.8 – Tillämpning av godkända uppförandekoder eller godkända certifieringsmekanismer

104. I artikel 83.2 j i dataskyddsförordningen anges att tillämpningen av uppförandekoder i enlighet med artikel 40 i dataskyddsförordningen eller godkända certifieringsmekanismer i enlighet med artikel 42 i dataskyddsförordningen kan vara en relevant faktor.

105. Så som erinras om i WP 253-riktlinjerna kan tillämpningen av uppförandekoder i enlighet med artikel 40 i dataskyddsförordningen eller godkända certifieringsmekanismer i enlighet med artikel 42 i dataskyddsförordningen under vissa omständigheter utgöra en förmildrande faktor. Godkända uppförandekoder kommer enligt artikel 40.4 i dataskyddsförordningen att innehålla ”mekanismer som gör det möjligt för det [övervakande] organ[et] […]att utföra den obligatoriska övervakningen av att dess bestämmelser efterlevs”. Vissa former av sanktioner mot beteenden som inte uppfyller kraven kan göras genom övervakningssystemet enligt artikel 41.4 i dataskyddsförordningen, inbegripet tillfällig avstängning eller uteslutande av den personuppgiftsansvarige eller personuppgiftsbiträdet från uppförandekoden. Även om tillsynsmyndigheten kan ta hänsyn till tidigare införda sanktioner avseende självregleringssystemet, påverkar övervakningsorganets befogenheter enligt artikel 41.4 i dataskyddsförordningen inte ”den behöriga tillsynsmyndighetens uppgifter och befogenheter”, vilket innebär att tillsynsmyndigheten inte är skyldig att ta hänsyn till några sanktioner från övervakningsorganets sida[40].

106. Om å andra sidan underlåtenheten att efterleva uppförandekoderna eller certifieringen är direkt relevant för överträdelsen, får tillsynsmyndigheten anse att detta är en försvårande omständighet.

5.9 – Andra försvårande och förmildrande omständigheter

107. I artikel 83.2 k i dataskyddsförordningen ges tillsynsmyndigheten utrymme att beakta andra försvårande eller förmildrande faktorer som är tillämpliga på omständigheterna i fallet. I det enskilda fallet kan det finnas många faktorer som inte kan kodifieras eller förtecknas och som måste beaktas för att säkerställa att den sanktion som tillämpas är effektiv, proportionerlig och avskräckande i varje enskilt fall.

108. I artikel 83.2 k i dataskyddsförordningen nämns exempel på ”[e]ventuell annan försvårande eller förmildrande faktor som är tillämplig på omständigheterna i fallet”, dvs. ekonomiska fördelar som erhållits eller förluster som undvikits, direkt eller indirekt, genom överträdelsen. Denna bestämmelse anses vara av grundläggande betydelse för att justera sanktionsbeloppet till det särskilda fallet. I detta avseende anses att den bör tolkas som ett fall av principen om rättvisa och rättsskipning som tillämpas i det enskilda fallet.

109. Tillämpningsområdet för denna bestämmelse, som av nödvändighet är öppet, bör omfatta alla motiverade överväganden om det socioekonomiska sammanhang inom vilket den personuppgiftsansvarige eller personuppgiftsbiträdet bedriver sin verksamhet, de som rör det rättsliga sammanhanget och de som rör marknadssammanhanget[41].

[40] Ibid.

[41] EDPB beslutade i denna fråga i EDPB:s bindande beslut 3/2022 om den tvist som den irländska tillsynsmyndigheten lämnade in om Meta Platforms Ireland Limited och dess Facebook-tjänst (artikel 65 i dataskyddsförordningen) (nedan kallat *EDPB:s bindande beslut 3/2022*), punkt 368.

110. I synnerhet kan den ekonomiska vinsten av överträdelsen vara en försvårande omständighet om ärendet ger information om vinst som erhållits till följd av överträdelsen av dataskyddsförordningen.

111. Exceptionella omständigheter som kan leda till betydande förändringar i det socioekonomiska sammanhanget (t.ex. om en allvarlig pandemikris skulle uppstå som radikalt skulle kunna förändra behandlingen av personuppgifter) kan också övervägas enligt artikel 83.2 k i dataskyddsförordningen.

Observera: Exemplen i detta kapitel är exempel på hur försvårande och förmildrande omständigheter kan påverka sanktionsbeloppet. De höjningar eller nedsättningar som nämns i dessa fantasifall kan inte betraktas som prejudikat eller indikationer på procentandelar som ska användas i verkliga fall.

Exempel 7 a – Viktning av försvårande och förmildrande omständigheter
En idrottsklubb använde kameror med ansiktsigenkänningsteknik vid ingången till en av sina anläggningar för att identifiera sina kunder vid inträdet. Eftersom idrottsklubben gjorde detta i strid med artikel 9 i dataskyddsförordningen (behandling av biometriska uppgifter utan giltigt undantag), beslutade den tillsynsmyndighet som var behörig att utreda överträdelsen att ålägga sanktionsavgifter. Med beaktande av alla relevanta omständigheter i ärendet ansåg tillsynsmyndigheten att denna överträdelse var mycket allvarlig, och eftersom idrottsklubben hade en årsomsättning på 150 miljoner euro ansågs ett startbelopp på 2 000 000 euro (högst upp i kategorin) vara lämpligt.

Samma idrottsklubb bötfälldes dock två år tidigare för att ha använt fingeravtryckstekniк på en annan plats. Tillsynsmyndigheten beslutade att beakta detta som en upprepad överträdelse (artikel 83.2 e i dataskyddsförordningen). Därigenom lade tillsynsmyndigheten vikt vid det faktum att det rörde sig om nästan samma sakfråga och att överträdelsen endast begicks två år tidigare. På grund av denna försvårande faktor beslutade tillsynsmyndigheten att höja sanktionsavgifterna i detta särskilda fall till 2 600 000 euro[42], vilket inte överstiger det tillämpliga lagstadgade maximibeloppet på 20 miljoner euro.

Observera: Exemplen i detta kapitel är exempel på hur försvårande och förmildrande omständigheter kan påverka sanktionsbeloppet. De höjningar eller nedsättningar som nämns i dessa fantasifall kan inte betraktas som prejudikat eller indikationer på procentandelar som ska användas i verkliga fall.

Exempel 7 b – Viktning av försvårande och förmildrande omständigheter
Operatören av en plattform för korttidsuthyrning av bilar drabbades av en dataincident, vilket ledde till att kundernas personuppgifter var sårbara under en kort tid. Med beaktande av alla relevanta omständigheter i ärendet ansåg tillsynsmyndigheten att verksamhetsutövarens brister när det gällde att säkra sin plattform i strid mot artikel 32 i dataskyddsförordningen var en överträdelse av låg allvarlighetsgrad, och eftersom verksamhetsutövaren hade en årsomsättning på 255 miljoner euro ansågs ett startbelopp på 260 000 euro vara lämpligt.

De kompromitterade personuppgifterna omfattade kopior av förarbevis och id-kort. Därför tvingades alla kunder som drabbades av uppgiftsincidenten att ansöka om dessa handlingar på nytt för att begränsa möjligheten till identitetsstöld. Operatören informerade de registrerade om denna incident och erbjöd alla registrerade hjälp att på nytt ansöka om dessa handlingar hos rätt offentliga

[42] Detta visar att kategorierna för startbelopp inte begränsar tillsynsmyndigheternas förmåga att beakta försvårande och förmildrande omständigheter till ett belopp över eller under kategorierna. Såsom upprepas i kapitel 4.3 utgör dessa siffror utgångspunkten för ytterligare beräkningar och inte fasta belopp (prismärkningar) för överträdelser av bestämmelserna i dataskyddsförordningen. Tillsynsmyndigheten behåller friheten att använda hela straffavgiftsintervallet från en punkt över 0 euro till det lagstadgade maximibeloppet, vilket säkerställer att sanktionsavgifterna är skräddarsydda efter omständigheterna i fallet.

institutioner, och skapade ett system för att återbetala eventuella avgifter som betalats för ansökan. Tillsynsmyndigheten ansåg att detta var "åtgärder […] för att lindra den skada som de registrerade har lidit" (artikel 83.2 c i dataskyddsförordningen), vilket hade en mildrande effekt på sanktionsavgifterna. Med tanke på den proaktiva inställningen och effektiviteten hos de åtgärder som vidtagits av operatören beslutade tillsynsmyndigheten att sänka sanktionsavgifterna till 225 000 euro[43], vilket återigen inte överskred det lagstadgade maximibeloppet på 10 miljoner euro.

Exemplen i detta kapitel är exempel på hur försvårande och förmildrande omständigheter kan påverka sanktionsbeloppet. De höjningar eller nedsättningar som nämns i dessa fantasifall kan inte betraktas som prejudikat eller indikationer på procentandelar som ska användas i verkliga fall.

Exempel 7 c – Viktning av försvårande och förmildrande omständigheter
Ett litet kreditvärderingsinstitut befanns ha brutit mot flera bestämmelser som skyddar de registrerades rättigheter, särskilt eftersom det tog ut en avgift från sina kunder för att utöva deras rätt till åtkomst. Institutet gjorde detta för alla begäranden om åtkomst, inte bara dem som nämns i artikel 12.5 a i dataskyddsförordningen. Med beaktande av alla relevanta omständigheter i ärendet ansåg tillsynsmyndigheten att överträdelserna var mycket allvarliga, och eftersom byrån hade en årsomsättning på 35 miljoner euro ansågs ett startbelopp på 100 000 euro vara lämpligt.

Tillsynsmyndigheten ansåg dock att det faktum att byrån kunde dra nytta av överträdelsen var en försvårande omständighet (artikel 83.2 k i dataskyddsförordningen). För att motverka vinsterna från överträdelsen och samtidigt bibehålla effektiva, avskräckande och proportionerliga sanktionsavgifter i detta fall beslutade tillsynsmyndigheten att höja sanktionsavgifterna till 130 000 euro, vilket inte översteg det tillämpliga lagstadgade maximibeloppet på 20 miljoner euro.

Exemplen i detta kapitel är exempel på hur försvårande och förmildrande omständigheter kan påverka sanktionsbeloppet. De höjningar eller nedsättningar som nämns i dessa fantasifall kan inte betraktas som prejudikat eller indikationer på procentandelar som ska användas i verkliga fall.

Exempel 7 d – Viktning av försvårande och förmildrande omständigheter
Ett företag befanns ha överträtt bestämmelserna i dataskyddsförordningen, framför allt på grund av att det sålde sin databas för kommersiell prospektering till partner, vilken innehöll personuppgifter om personer som inte gav sitt samtycke till att bli prospekterade för kommersiella ändamål.

Med tanke på alla relevanta omständigheter i ärendet ansåg tillsynsmyndigheten att överträdelserna var av medelhög allvarlighetsgrad, och eftersom företaget hade en årsomsättning på 45 miljoner euro ansågs ett startbelopp på 150 000 euro vara lämpligt.

Dessutom ansåg myndigheten att detta var en överträdelse som gynnade den personuppgiftsansvarige, eftersom mängden uppgifter som kunde säljas ökade genom det faktum att personernas samtycke till överföringen av deras uppgifter i syfte att sända riktad reklam inte hade inhämtats Tillsynsmyndigheten ansåg därmed att det faktum att byrån kunde dra nytta av överträdelsen var en försvårande omständighet (artikel 83.2 k i dataskyddsförordningen).

För att motverka vinsterna från överträdelsen och samtidigt bibehålla effektiva, avskräckande och proportionerliga sanktionsavgifter i detta fall beslutade tillsynsmyndigheten att höja sanktionsavgifterna till 200 000 euro, vilket inte överskred det tillämpliga lagstadgade maximibeloppet på 20 miljoner euro.

[43] Se föregående fotnot.

KAPITEL 6 – LAGSTADGAT MAXIMIBELOPP OCH FÖRETAGENS ANSVAR

6.1 – Fastställande av det lagstadgade maximibeloppet

112. Som redan anges i WP 253-riktlinjerna fastställer dataskyddsförordningen inte fasta belopp för specifika överträdelser. Dataskyddsförordningen föreskriver i stället generella maximibelopp[44] och följer därmed den allmänna traditionen i EU-lagstiftningen om sanktioner som redan fastställts genom andra rättsakter[45].

113. Beloppen i artikel 83.4–83.6 i dataskyddsförordningen utgör det lagstadgade maximibeloppet och förbjuder tillsynsmyndigheterna att ålägga sanktionsavgifter som när de tillämpas överskrider de tillämpliga maximibeloppen. För att fastställa det korrekta lagstadgade maximibeloppet måste artikel 83.3 i dataskyddsförordningen i tillämpliga fall beaktas[46] (se kapitel 3.1.2). Varje tillsynsmyndighet måste därför se till att dessa maximibelopp inte överskrids vid beräkning av sanktionsavgifter på grundval av dessa riktlinjer. Beroende på det enskilda fallet kan olika maximibelopp bli relevanta.

6.1.1 – Statiska maximibelopp

114. I artikel 83.4–83.6 i dataskyddsförordningen föreskrivs statiska belopp som regel och åtskillnad görs mellan överträdelser av olika kategorier av skyldigheter enligt dataskyddsförordningen. Som förklaras ovan medger artikel 83.4 i dataskyddsförordningen sanktionsavgifter på upp till 10 miljoner euro för överträdelser av de skyldigheter som anges i den, medan artikel 83.5 och 83.6 i förordningen medger sanktionsavgifter på upp till 20 miljoner euro för överträdelser av de skyldigheter som anges i dem.

6.1.2 – Dynamiska maximibelopp

115. När det gäller företag[47] får betalningsintervallet övergå till ett högre omsättningsbaserat[48] maximibelopp. Detta omsättningsbaserade maximibelopp är dynamiskt och individualiserat gentemot respektive företag för att uppnå principerna om effektivitet, proportionalitet och avskräckande effekt.

116. I artikel 83.4 i dataskyddsförordningen föreskrivs ett maximibelopp på 2 % och i artikel 83.5 och 83.6 ett maximibelopp på 4 % av företagets totala årsomsättning för det föregående budgetåret. Formuleringen i dataskyddsförordningen föreskriver att antingen det statiska maximibeloppet eller det dynamiska omsättningsbaserade maximibeloppet ska beaktas, ”beroende på vilket värde som är högst”. Följaktligen gäller dessa omsättningsbaserade maximibelopp endast om de överskrider det statiska maximibeloppet i det enskilda fallet. Så är fallet när företagets totala årsomsättning för föregående räkenskapsår överstiger 500 miljoner euro[49].

Exempel 8 a – Dynamiskt maximibelopp
Ett kreditvärderingsinstitut samlar in och säljer alla uppgifter om alla EU-medborgares kreditvärdighet till reklam- och detaljhandelsföretag utan rättslig grund. Kreditvärderingsinstitutets årliga globala omsättning under föregående år uppgick till 3 miljarder euro. Här åsidosatte kreditvärderingsinstitutet bland annat

[44] Skäl 150 i dataskyddsförordningen, andra meningen: ”Det bör i denna förordning anges vilka överträdelserna är, den övre gränsen för och kriterierna för fastställande av de administrativa sanktionsavgifterna, som i varje enskilt fall bör bestämmas av den behöriga tillsynsmyndigheten med beaktande av alla relevanta omständigheter i det särskilda fallet, med vederbörlig hänsyn bl.a. till överträdelsens karaktär, svårighetsgrad och varaktighet samt till dess följder och till de åtgärder som vidtas för att sörja för fullgörandet av skyldigheterna enligt denna förordning och för att förebygga eller lindra konsekvenserna av överträdelsen.”
[45] I synnerhet artikel 23.2 i förordning (EG) nr 1/2003 av den 16 december 2002 om tillämpning av konkurrensreglerna i artiklarna 81 och 82 i fördraget.
[46] Se även EDPB:s bindande beslut 1/2021, punkt 326.
[47] När det gäller begreppet ”företag”, se kapitel 6.2.1 i dessa riktlinjer.
[48] När det gäller begreppet ”omsättning”, se kapitel 6.2.2 i dessa riktlinjer.
[49] 2 % av 500 miljoner är lika med 10 miljoner (det statiska maximibelopp som avses i artikel 83.4 i dataskyddsförordningen) och 4 % av 500 miljoner är lika med 20 miljoner (det statiska maximibelopp som anges i artikel 83.5 i dataskyddsförordningen).

artikel 6, som kan bestraffas med sanktionsavgifter i enlighet med artikel 83.5 i dataskyddsförordningen. Det statiska maximibeloppet skulle uppgå till 20 miljoner euro. Det dynamiska maximibeloppet skulle uppgå till 120 miljoner euro (4 % av 3 miljarder euro). Böterna kan uppgå till 120 miljoner euro eftersom detta dynamiska maximibelopp är högre än det statiska maximibeloppet på 20 miljoner euro. Böterna får därför överskrida det statiska maximibeloppet på 20 miljoner euro, men får inte överstiga det tillämpliga lagstadgade maximibeloppet på 120 miljoner euro.

Exempel 8 b – Statiskt maximibelopp
En återförsäljare av solglasögon driver en onlinebutik där kunderna kan göra sina beställningar. Genom beställningsformuläret behandlar återförsäljaren även personuppgifter, inklusive bankkontouppgifter. Återförsäljaren underlåter att tillhandahålla en korrekt https-överföringskryptering, vilket innebär att tredje parter potentiellt kan fånga upp personuppgifterna under transaktionen. Återförsäljaren bryter mot artikel 32.1 i dataskyddsförordningen och kan åläggas sanktionsavgifter i enlighet med artikel 83.4 i dataskyddsförordningen. Återförsäljarens årliga globala omsättning under föregående år uppgick till 450 miljoner euro. I detta fall är det statiska maximibeloppet på 10 miljoner euro högre än det dynamiska maximibeloppet på 9 miljoner euro (=2 % av 450 miljoner euro), vilket innebär att maximibeloppet på 10 miljoner euro har företräde. Böterna får därför inte överstiga det lagstadgade maximibeloppet på 10 miljoner euro.

Exempel 8 c – Personuppgiftsansvariga och personuppgiftsbiträden som inte är företag
En kommun har ett onlinesystem genom vilket dess medborgare kan göra tidsbokningar, för att t.ex. ansöka om pass eller äktenskapslicens. Kommunen är den enda personuppgiftsansvarige för detta onlinesystem. Tyvärr konstateras det att systemet också permanent överför insamlade uppgifter till en processors externa servrar i ett olämpligt tredjeland, där de lagras. Det finns inga lämpliga skyddsåtgärder för överföringen till tredjeländer. Med undantag för överföringen samlas uppgifterna in och behandlas på grundval av giltigt samtycke. Kommunen bröt mot artikel 44 i dataskyddsförordningen genom att överföra särskilda kategorier av personuppgifter till ett olämpligt tredjeland utan lämpliga skyddsåtgärder. Den kan därför åläggas sanktionsavgifter i enlighet med artikel 83.5. Eftersom kommunen inte uppfyller definitionen av ett företag gäller det statiska lagstadgade maximibeloppet, vilket innebär att sanktionsbeloppet inte får överstiga 20 miljoner euro. Detta är dock endast fallet om den medlemsstat där denna kommun är belägen inte har fastställt särskilda regler om huruvida och i vilken utsträckning administrativa sanktionsavgifter kan åläggas offentliga myndigheter och organ som är etablerade i den medlemsstaten (artikel 83.7 i dataskyddsförordningen).

6.2 – Fastställande av företagets omsättning och företagens ansvar

117. För att fastställa en korrekt omsättning för det dynamiska lagstadgade maximibeloppet är det viktigt att förstå de begrepp om företag och omsättning som används i artikel 83.4–83.6 i dataskyddsförordningen. I detta avseende måste största möjliga hänsyn tas till skälen i dataskyddsförordningen, som tillhandahålls av den europeiska lagstiftaren för vägledning om tolkning av dataskyddsförordningen.

6.2.1 – Fastställande av ett företag och företagens ansvar

118. När det gäller begreppet ”företag” ger den europeiska lagstiftaren ytterligare förtydliganden. Skäl 150 i dataskyddsförordningen har följande lydelse: ”Om de administrativa sanktionsavgifterna åläggs ett företag, bör ett företag i detta syfte anses vara ett företag i den mening som avses i artiklarna 101 och 102 i EUF-fördraget”

119. Därför förlitar sig artikel 83.4–83.6 i dataskyddsförordningen, mot bakgrund av skäl 150, på begreppet företag i enlighet med artiklarna 101 och 102 i EUF-fördraget[50], utan att det påverkar tillämpningen av artikel 4.18 i dataskyddsförordningen (som definierar ett företag) och artikel 4.19 i dataskyddsförordningen (som definierar en koncern). Det förstnämnda begreppet används främst i kapitel V i dataskyddsförordningen,

[50] Såsom redan klargjorts i WP 253 och senare bekräftats av EDPB i godkännande 1/2018 den 25 maj 2018. Se även EDPB:s bindande beslut 1/2021, punkt 292, och den regionala domstolen LG Bonn, mål 29 OWi 1/20, 11 november 2020, punkt 92.

avseende företag som bedriver gemensam ekonomisk verksamhet. Dessutom tillämpas termen i allmän bemärkelse, inte avseende rättssubjektet som en bestämmelse eller förpliktelse gäller.

120. I fall där den personuppgiftsansvarige eller personuppgiftsbiträdet är (en del av) ett företag i den mening som avses i artiklarna 101 och 102 i EUF-fördraget kan därför den sammanlagda omsättningen för ett sådant företag som helhet användas för att fastställa den dynamiska övre gränsen för sanktionsavgifterna (se kapitel 6.2.2) och för att säkerställa att de sanktionsavgifter som blir följden är förenliga med principerna om effektivitet, proportionalitet och avskräckande effekt (artikel 83.1 i dataskyddsförordningen)[51].

121. EU-domstolen har utvecklat en omfattande rättspraxis om begreppet *företag*. Begreppet *företag* ”omfattar varje enhet som utövar ekonomisk verksamhet, oavsett enhetens rättsliga form och sättet för dess finansiering”[52]. I konkurrenslagstiftningen identifieras därför ”företag” med ekonomiska enheter snarare än med juridiska enheter. Olika företag inom samma koncern kan bilda en ekonomisk enhet och därmed ett företag i den mening som avses i artiklarna 101 och 102 i EUF-fördraget[53].

122. I linje med EU-domstolens fasta rättspraxis kan begreppet företag i artiklarna 101 och 102 i EUF-fördraget hänvisa till en enda ekonomisk enhet, även om den ekonomiska enheten består av flera fysiska eller juridiska personer. Huruvida flera enheter bildar en enda ekonomisk enhet beror till stor del på om det enskilda företaget har frihet att fatta beslut eller om ett ledande företag, nämligen moderbolaget, utövar ett avgörande inflytande över de andra[54]. Kriterierna för att fastställa detta bygger på de ekonomiska, rättsliga och organisatoriska kopplingarna mellan moderbolaget och dess dotterbolag, t.ex. storleken på deltagandet, personalen eller organisatoriska kopplingar, instruktioner och förekomsten av företagskontrakt[55].

123. I linje med doktrinen om en enda ekonomisk enhet följer artikel 83.4–83.6 i dataskyddsförordningen principen om direkt företagsansvar, vilket innebär att ansvaret för alla handlingar som utförs eller försummas av fysiska personer som är bemyndigade att handla för företagens räkning kan tillskrivas dessa och betraktas som en handling och överträdelse som företaget självt har begått[56]. Det faktum att vissa anställda inte följde en uppförandekod räcker inte för att störa denna tillskrivning av ansvar[57]. Detta störs endast om den fysiska personen agerar uteslutande för sina egna privata syften eller för en tredje parts syften och därmed blir en separat personuppgiftsansvarig (dvs. den fysiska personen har agerat utöver sitt tillåtna ansvarsområde)[58]. Denna EU-rättsprincip och omfattningen av företagens ansvar har företräde och får inte undergrävas genom att begränsas till vissa befattningshavares (t.ex. huvudansvarigas) handlingar genom att den strider mot den nationella lagstiftningen. Det är inte relevant vilken fysisk person som agerade för vilka av enheterna.

[51] Se EDPB:s bindande beslut 1/2021, punkterna 412 och 423 samt även målen C-286/13 P, Dole food och Dole Fresh Fruit Europe/kommissionen, punkt 149 och C-189/02 P, Dansk Rørindustri m.fl./kommissionen, punkt 258.

[52] Mål C-41/90, Klaus Höfner och Fritz Elser/Macrotron GmbH, punkt 21. Se även de förenade målen C-159 och 160/91, Poucet och Pistre/Assurances Générales de France, punkt 17; mål C-364/92, SAT Fluggesellschaft mbH/Eurocontrol, punkt 18; de förenade målen C-180–184/98, Pavlov m.fl., punkt 74; samt mål C-138/11, Compass-Datenbank GmbH/Republik Österreich, punkt 35.

[53] Mål C-516/15 P, Akzo Nobel m.fl./kommissionen, punkt 48.

[54] För att förtydliga; den ”beslutsförmåga” som ska bedömas i syfte att fastställa om ett moderbolag utövar ett avgörande inflytande över andra i koncernen avser beslutsförmågan i förhållande till dotterbolagets beteende ”på marknaden”. Detta skiljer sig från, och är helt separat från, det inflytande som ett moderbolag kan ha över behandlingen i fråga och i synnerhet över förmågan att fatta beslut om ändamålen och medlen för behandlingen. Sådana frågor ska bedömas som en del av varje undersökning av den personuppgiftsansvariges identitet och är inte relevanta för bedömningen av avgörande inflytande i syfte att fastställa en enda ekonomisk enhet.

[55] Se mål C-90/09 P, General Química m.fl./kommissionen. Huvudkriteriet för att fastställa detta är ”avgörande inflytande”, som bör bygga på faktiska bevis (ekonomiska, organisatoriska och rättsliga kopplingar). Det finns dessutom en motbevisbar presumtion om inflytande när det gäller helägda dotterbolag. Se mål C-97/08 P, Akzo Nobel m.fl./kommissionen och de förenade målen C-293/13 och 294/13 P, Fresh Del Monte.

[56] Se de förenade målen C-100–103/80, SA Musique Diffusion française m.fl./kommissionen, punkt 97 och mål C-338/00 P, Volkswagen/kommissionen, punkterna 93–98.

[57] Mål C-501/11 P, Schindler Holding m.fl./kommissionen, punkt 114. Därför är det viktigt för företagen att deras system för hantering av efterlevnad inte bara är en ”pappersskold”, utan i praktiken är effektiv.

[58] Se särskilt riktlinjerna 07/2020 om begreppen personuppgiftsansvarig och personuppgiftsbiträde i dataskyddsförordningen (nedan kallade *EDPB:s riktlinjer 07/2020*), punkt 19.

Tillsynsmyndigheten och de nationella domstolarna får därför inte vara skyldiga att fastställa eller identifiera en fysisk person i utredningarna eller i betalningsbeslutet[59].

124. I det särskilda fall där ett moderbolag innehar 100 % av aktierna eller nästan 100 % av aktierna i ett dotterbolag som har brutit mot artikel 83 i dataskyddsförordningen och därför kan utöva ett avgörande inflytande över sitt dotterbolags beteende, kan det antas att moderbolaget faktiskt utövar detta avgörande inflytande över sitt dotterbolags beteende (den så kallade Akzo-presumtionen)[60]. Detta gäller även om moderbolaget inte direkt innehar aktierna i det totala kapitalet, utan indirekt genom ett eller flera dotterbolag[61]. Det kan till exempel också finnas en kedja av dotterbolag, där ett företag innehar 100 % eller nästan 100 % av aktierna i ett förmedlande företag som innehar 100 % eller nästan 100 % av aktierna i ett annat företag, och så vidare. Ett moderbolag kan också inneha 100 % eller nästan 100 % av aktierna i två enheter som var och en innehar omkring 50 % av ett företag, vilket ger moderbolaget ett avgörande inflytande över alla. Under dessa omständigheter räcker det att tillsynsmyndigheten kan bevisa att dotterföretaget direkt eller indirekt ägs helt eller nästan helt av moderbolaget för att – som en regel från praktisk erfarenhet – anta att moderbolaget utövar ett avgörande inflytande.

125. Akzos antagande är dock inte absolut, utan kan motbevisas av andra bevis[62]. För att motbevisa presumtionen måste företaget eller företagen tillhandahålla bevis avseende organisatoriska, ekonomiska och rättsliga kopplingar mellan dotterbolaget och dess moderbolag som kan visa att de inte utgör en enda ekonomisk enhet trots att de innehar 100 % eller nästan 100 % av aktierna. För att fastställa om ett dotterbolag självt agerar självständigt måste hänsyn tas till alla relevanta faktorer som rör de förbindelser som knyter dotterbolaget till moderbolaget, vilka kan variera från fall till fall och därför inte kan anges i en uttömmande förteckning.

126. Om moderbolaget däremot inte innehar hela eller nästan hela kapitalet måste tillsynsmyndigheten styrka ytterligare fakta för att motivera förekomsten av en enda ekonomisk enhet. I ett sådant fall måste tillsynsmyndigheten visa inte bara att moderbolaget har möjlighet att utöva ett avgörande inflytande över dotterföretaget, utan också att det faktiskt har utövat ett sådant avgörande inflytande så att det när som helst kan blanda sig i dotterbolagets valfrihet och bestämma dess beteende. Instruktionens karaktär eller typ är irrelevant vid fastställandet av moderbolagets inflytande.

127. Sanktionerna åläggs[63] (gemensamma) personuppgiftsansvariga/personuppgiftsbiträden, och den behöriga tillsynsmyndigheten har möjlighet att hålla moderbolaget solidariskt ansvarigt[64] för betalningen av sanktionsavgifterna.

6.2.2 – Fastställande av omsättningen

128. Omsättningen tas från ett företags årsredovisning, som upprättas med avseende på dess verksamhetsår och ger en översikt över det senaste räkenskapsåret för ett företag eller en företagsgrupp (konsoliderade räkenskaper). Omsättning definieras som summan av alla sålda varor och tjänster. Nettoomsättning avser

[59] Mål C-338/00 P, Volkswagen/kommissionen, punkterna 97 och 98. All nationell lagstiftning som står i strid med dataskyddsförordningen är oförenlig med dataskyddsförordningen och principen om ändamålsenlighet, och ska därmed inte tillämpas.
[60] Mål C-97/08 P, Akzo Nobel m.fl./kommissionen, punkterna 59 och 60.
[61] Mål T-38/05, Agroexpansión/kommissionen och C-508/11 P, Eni/kommissionen, punkt 48.
[62] Se bland annat mål C-595/18 P, The Goldman Sachs Group/kommissionen, ECLI: EU: C: 2021:73, punkt 32, citerad mål C 611/18 P, Pirelli & C./kommissionen, ej offentliggjord, punkt 68, och där angiven rättspraxis.
[63] Det beslut i vilket sanktionsavgifter åläggs riktas och överlämnas till de personuppgiftsansvariga/personuppgiftsbiträdena samt gärningsmannen/gärningsmännen som begått överträdelsen och kan dessutom riktas och överlämnas till andra rättsliga enheter som ingår i den enda ekonomiska enheten som är solidariskt ansvariga för sanktionsavgifterna.
[64] EDPB:s bindande beslut 1/2021, punkt 290.

det belopp som erhållits genom försäljning av varor och tillhandahållande av tjänster efter avdrag av försäljningsrabatter och mervärdesskatt samt andra skatter som direkt relateras till omsättningen[65].

129. Omsättningen tas från presentationen av resultaträkningen[66]. Nettoomsättningen omfattar intäkter från försäljning, uthyrning och leasing av produkter och intäkter från försäljning av tjänster minus försäljningsavdrag (t.ex. avdrag, rabatter) och mervärdesskatt.

130. Om företaget omfattas av skyldigheten att upprätta koncernredovisningar[67] är dessa koncernredovisningar för koncernens moderbolag relevanta för att återspegla företagets sammanlagda omsättning[68]. Om sådana redovisningar inte finns, ska alla andra handlingar inhämtas och användas som kan påverka företagets årliga omsättning i hela världen under det aktuella verksamhetsåret.

131. I artikel 83.4–83.6 i dataskyddsförordningen anges att den totala globala årsomsättningen för det föregående budgetåret ska användas. När det gäller frågan om vilken händelse termen ”föregående” avser ska EU-domstolens rättspraxis inom konkurrensrätten också tillämpas på sanktionsavgifter enligt dataskyddsförordningen, så att den relevanta händelsen är det beslut om sanktionsavgifter som utfärdats av tillsynsmyndigheten och inte varken tidpunkten för överträdelsen eller domstolsbeslutet [69] . Vid gränsöverskridande bearbetning är det relevanta beslutet om avräkning inte utkastet till beslut, utan snarare det slutliga beslut som fattats av den ansvariga tillsynsmyndigheten[70]. Om utkastet till beslut går in i medbeslutandeförfarandet enligt artikel 60 i slutet av ett kalenderår, så att det slutliga beslutet sannolikt inte kommer att antas inom samma kalenderår, kommer den ansvariga tillsynsmyndigheten att beräkna eventuella föreslagna sanktionsavgifter med hänvisning till den mest aktuella finansiella information som finns tillgänglig den dag då utkastet till beslut vidarebefordras till de berörda tillsynsmyndigheterna för deras synpunkter. Denna information kommer därefter att uppdateras vid behov innan den ansvariga tillsynsmyndigheten färdigställer och antar det slutliga nationella beslutet.

KAPITEL 7 – EFFEKTIVITET, PROPORTIONALITET OCH AVSKRÄCKANDE EFFEKT

132. De administrativa sanktionsavgifter som åläggs för överträdelser av dataskyddsförordningen som avses i artikel 83.4–83.6 ska i varje enskilt fall vara effektiva, proportionella och avskräckande. Med andra ord är sanktionsbeloppet skräddarsytt för den överträdelse som begåtts i dess specifika sammanhang. EDPB anser att det åligger tillsynsmyndigheterna att kontrollera om sanktionsbeloppet uppfyller dessa krav eller om ytterligare justeringar av beloppet är nödvändiga.

133. Såsom förklaras i kapitel 4 omfattar den utvärdering som görs i detta kapitel hela sanktionsbeloppet och alla omständigheter i ärendet, t.ex. ackumulering av flera överträdelser, höjningar och nedsättningar för försvårande och förmildrande omständigheter och finansiella/socioekonomiska omständigheter. Det åligger dock tillsynsmyndigheten att se till att samma omständigheter inte räknas två gånger.

---

[65] Se t.ex. artikel 2.5 i Europaparlamentets och rådets direktiv 2013/34/EU av den 26 juni 2013 om årsbokslut, koncernredovisning och rapporter i vissa typer av företag, om ändring av Europaparlamentets och rådets direktiv 2006/43/EG och om upphävande av rådets direktiv 78/660/EEG och 83/349/EEG (nedan kallat *direktiv 2013/34/EU*), som är tillämplig på företag med begränsat ansvar, eller liknande tillämplig lagstiftning och artikel 5.1 i rådets förordning (EG) nr 139/2004 om kontroll av företagskoncentrationer (nedan kallad *EG:s koncentrationsförordning*).

[66] Se t.ex. bilagorna V eller VI till artikel 13.1 i direktiv 2013/34/EU under rubriken ”nettoomsättning” eller liknande tillämplig lagstiftning.

[67] Se t.ex. artikel 21 ff. i direktiv 2013/34/EU eller liknande tillämplig lagstiftning.

[68] C-58/12 P Groupe Gascogne SA/kommissionen, ECLI:EU:C:2013:770, punkterna 54–55.

[69] Regionala domstolen LG Bonn, mål 29 OWi 1/20, 11 november 2020, punkt 95, med hänvisning till mål C-637/13 P, Badezimmerkartell Laufen Austria, punkt 49 och mål C-408/12 P, YKK m.fl., punkt 90.

[70] EDPB:s bindande beslut 1/2021, punkt 298.

134. Om dessa justeringar kräver en höjning av sanktionsavgifterna kan en sådan höjning per definition inte överstiga det lagstadgade maximibeloppet som anges i kapitel 6 ovan.

7.1 – Effektivitet

135. Generellt sett kan sanktionsavgifter betraktas som effektiva om de uppnår de mål med vilka de ålades. Detta skulle kunna vara att återupprätta efterlevnaden av reglerna och straffa olagligt beteende, eller bådadera[71]. I skäl 148 i dataskyddsförordningen betonas dessutom att administrativa sanktionsavgifter bör åläggas ”[f]ör att stärka verkställigheten av denna förordning”. Sanktionsavgiftsbeloppet som baserats på dessa riktlinjer bör därför vara tillräckligt för att uppnå dessa mål.

136. Enligt artikel 83.2 i dataskyddsförordningen måste tillsynsmyndigheten utvärdera sanktionsavgiftens effektivitet i varje enskilt fall. I detta syfte måste vederbörlig hänsyn tas till omständigheterna i ärendet, särskilt till den bedömning som gjorts ovan[72], med tanke på att sanktionsavgifterna också bör vara proportionerliga och avskräckande enligt nedan.

7.2 – Proportionalitet

137. Proportionalitetsprincipen kräver att de vidtagna åtgärderna inte överskrider gränserna för vad som är lämpligt och nödvändigt för att uppnå de mål som legitimt eftersträvas genom lagstiftningen i fråga. Om flera åtgärder kan vara lämpliga måste de minst betungande väljas, och de nackdelar som orsakas får inte vara oproportionerliga i förhållande till de eftersträvade målen[73].

138. Av detta följer att sanktionsavgifterna inte får vara oproportionerliga i förhållande till de mål som eftersträvas (dvs. efterlevnad av reglerna om skydd för fysiska personer med avseende på behandling av personuppgifter och regler om fri rörlighet för personuppgifter), och att det ålagda sanktionsbeloppet måste stå i proportion till överträdelsen, betraktad som en helhet, särskilt med hänsyn till hur allvarlig överträdelsen är[74].

139. Tillsynsmyndigheten ska därför kontrollera att sanktionsbeloppet är **proportionerligt** både till överträdelsens allvar och till storleken på det företag som den enhet som begick överträdelsen tillhör[75], och att sanktionsbeloppet därmed inte överstiger vad som är nödvändigt för att uppnå de mål som eftersträvas i dataskyddsförordningen.

140. Som en särskild följd av proportionalitetsprincipen kan tillsynsmyndigheten, i enlighet med nationell lagstiftning, överväga att ytterligare sänka sanktionsavgifterna på grundval av principen om betalningsoförmåga. En sådan minskning kräver exceptionella omständigheter. I enlighet med Europeiska kommissionens riktlinjer för beräkning av sanktionsavgifter[76] måste det finnas objektiva bevis för att ett åläggande av sanktionsavgifter oåterkalleligen skulle äventyra det berörda företagets ekonomiska lönsamhet. Dessutom måste riskerna analyseras i ett specifikt socialt och ekonomiskt sammanhang.

a) **Ekonomisk bärkraft:** Företaget ska lämna detaljerade finansiella uppgifter (för de senaste fem åren samt prognoser för innevarande och kommande två år) så att tillsynsmyndigheten kan undersöka den sannolika framtida utvecklingen av nyckelfaktorer som solvens, likviditet och lönsamhet. EU-

[71] WP 253-riktlinjerna, s. 6.
[72] I skäl 148 i dataskyddsförordningen anges också följande: ”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”.
[73] Mål T-704/14, Marine Harvest/kommissionen, punkt 580, mål T-332/09, Electrabel/kommissionen, punkt 279.
[74] Ibid.
[75] Se i detta avseende mål C-387/97, kommissionen/Grekland, punkt 90, och mål C-278/01, kommissionen/Spanien, punkt 41, där det fastslås att sanktionsavgifterna måste vara lämpliga för omständigheterna och stå i proportion både till den konstaterade överträdelsen och till den berörda medlemsstatens betalningsförmåga.
[76] Se t.ex. kommissionens riktlinjer för beräkning av sanktionsavgifter enligt artikel 23.2 a i förordning nr 1/2003 (2006/C 210/02).

domstolarna har slagit fast att endast omständigheten att ett företag befinner sig i en dålig ekonomisk situation, eller kommer att göra det efter att ha ålagts stora sanktionsavgifter, inte uppfyller kravet eftersom ”[g]odtagandet av en sådan skyldighet skulle […] medföra att de företag som var minst anpassade till marknadsvillkoren gavs en oberättigad konkurrensfördel” [77]. I bedömningen av företagets förmåga att betala sanktionsavgifter beaktas även eventuella omstruktureringsplaner och deras genomförandestatus, förbindelser med externa finansiella partner/institutioner såsom banker och förbindelser med aktieägare[78].

b) **Bevis på värdeförlust:** En nedsättning av sanktionsavgifterna får endast beviljas om ett åläggande av sanktionsavgifterna skulle äventyra ett företags ekonomiska bärkraft och leda till att dess tillgångar förlorar hela eller större delen av sitt värde [79]. Ett direkt orsakssamband mellan sanktionsavgifterna och den betydande värdeminskningen måste redovisas. Det finns ingen automatisk acceptans för att konkurs eller insolvens nödvändigtvis kommer att leda till en betydande förlust av tillgångarnas värde. Det kan inte heller råda något tvivel om att sanktionsavgifterna har hotat ett företags ekonomiska lönsamhet om företaget självt hade beslutat att avsluta sin verksamhet och sälja alla sina tillgångar. Företaget måste bevisa att det sannolikt kommer att behöva lämna marknaden och att dess tillgångar kommer att avvecklas eller säljas till kraftigt rabatterade priser utan några alternativ för att företaget (eller dess tillgångar) ska kunna fortsätta sin verksamhet. Detta innebär att tillsynsmyndigheten bör kräva att företaget bevisar att det inte finns några tydliga tecken på att företaget (eller dess tillgångar) kommer att förvärvas av ett annat företag/ägare och fortsätta sin verksamhet.

c) **Särskilda sociala och ekonomiska förhållanden:** Den särskilda ekonomiska situationen kan beaktas om den berörda sektorn genomgår en konjunkturkris (t.ex. lider av överkapacitet eller sjunkande priser) eller om företag har svårt att få tillgång till kapital eller kredit till följd av de rådande ekonomiska förhållandena. Det specifika sociala sammanhanget kommer sannolikt att råda i samband med hög och/eller ökande arbetslöshet på regional eller mer omfattande nivå. Det kan också bedömas med hänsyn till de konsekvenser som betalningen av sanktionsavgifterna kan få i form av ökad arbetslöshet eller försämring av de ekonomiska sektorerna i upp- och nedströms[80].

141. Om kriterierna är uppfyllda får tillsynsmyndigheterna beakta företagets oförmåga att betala och minska sanktionsavgifterna i enlighet därmed.

7.3 – Avskräckande effekt

142. Slutligen har ett avskräckande sanktionsbelopp en verklig avskräckande effekt[81]. I detta avseende kan man skilja mellan allmänt avskräckande (som avskräcker andra från att begå samma överträdelse i framtiden) och individuellt avskräckande (som avskräcker mottagaren av sanktionsavgifterna från att begå samma överträdelse igen)[82]. När tillsynsmyndigheten ålägger sanktionsavgifter tar den hänsyn till både allmänt och individuellt avskräckande.

[77] Se de förenade målen C-189/02 P, C-202/02 P, C-205/02 P till C-208/02 P och C-213/02 P, Dansk Rørindustri m.fl./kommissionen, punkt 327, och de citerade förenade målen 96/82–102/82, 104/82, 105/82, 108/82 och 110/82, NV IAZ International Belgium m.fl./kommissionen, punkterna 54 och 55. Detta upprepades mer nyligen i mål C-308/04 P, SGL Carbon/kommissionen, punkt 105, och mål T-429/10 (de förenade målen T-426/10, T-427/10, T-428/10, T-429/10, T-438/12, T-439/12, T-440/12, T-441/12), Global Steel Wire/kommissionen, punkterna 492–493.

[78] Se mål T-429/10 (gemensamma målen T-426/10, T-427/10, T-428/10, T-429/10, T-438/12, T-439/12, T-440/12, T-441/12), Global Steel Wire/kommissionen, punkterna 521–527.

[79] Se de förenade målen T-236/01, T-239/01, T-244/01–T-246/01, T-251/01 och T-252/01, Tokai Carbon m.fl./kommissionen, punkt 372 och mål T-64/02, Heubach/kommissionen, punkt 163. Se mål T-393/10, INTP, Westfälische Drahtindustrie m.fl./kommissionen, punkterna 293 och 294.

[80] Se mål C-308/04 P, SGL Carbon/kommissionen, punkt 106.

[81] Se AG Geelhoeds yttrande i mål C-304/02, kommissionen/Frankrike, punkt 39.

[82] Se bl.a. mål C-511/11 P, Versalis Spa/kommissionen, punkt 94.

143. Ett sanktionsbelopp är avskräckande om det hindrar en individ från att inkräkta på de mål och regler som fastställs i unionsrätten. Det avgörande i detta avseende är inte bara sanktionsavgiftens karaktär och nivå utan också sannolikheten för att den åläggs. Alla som begår en överträdelse måste frukta att sanktionsavgifterna faktiskt kommer att åläggas dem. Det finns här en överlappning mellan kriteriet om avskräckande effekt och kriteriet om effektivitet[83].

144. Tillsynsmyndigheterna får överväga att höja sanktionsavgifterna om de inte anser att beloppet är tillräckligt avskräckande. Under vissa omständigheter kan det vara motiverat att införa en avskräckande multiplikator[84]. Denna multiplikator kan fastställas efter tillsynsmyndighetens gottfinnande för att återspegla de mål för avskräckande effekt som anges ovan.

KAPITEL 8 – FLEXIBILITET OCH REGELBUNDEN UTVÄRDERING

145. I kapitlen ovan beskrivs en allmän metod för beräkning av sanktionsavgifter, vilket ska underlätta ytterligare harmonisering och insyn i tillsynsmyndigheternas praxis när det gäller sanktionsavgifter. Denna allmänna metod bör dock inte missförstås som en form av automatisk eller aritmetisk beräkning. Det individuella fastställandet av sanktionsavgifter måste alltid grundas på en mänsklig bedömning av alla relevanta omständigheter i ärendet och måste vara effektivt, proportionerligt och avskräckande i det specifika fallet.

146. Man bör komma ihåg att dessa riktlinjer inte kan förutse varje enskilt fall och i detta avseende inte kan ge tillsynsmyndigheterna någon uttömmande vägledning. Dessa riktlinjer ses därför över regelbundet för att utvärdera om tillämpningen av dem verkligen uppfyller de mål som efterfrågas i dataskyddsförordningen. EDPB får se över dessa riktlinjer på grundval av tillsynsmyndigheternas ytterligare erfarenheter av den dagliga praktiska tillämpningen och kan när som helst i framtiden upphäva, ändra, begränsa, ändra eller ersätta dessa riktlinjer.

[83] AG Kokotts yttrande i de förenade målen C-387/02, C-391/02 och C-403/02, Silvio Berlusconi m.fl., punkt 89.
[84] Se särskilt mål C-289/04 P, Showa Denko/kommissionen, punkterna 28–39.

BILAGA – TABELL FÖR ILLUSTRATION AV RIKTLINJERNA 04/2022 OM BERÄKNING AV ADMINISTRATIVA SANKTIONSAVGIFTER ENLIGT DATASKYDDSFÖRORDNINGEN

Läsguide

- Denna tabell ska läsas tillsammans med riktlinjerna i sin helhet och är inte avsedd att tjäna som en fullständig sammanfattning av riktlinjerna eller som ett alternativ till att betrakta riktlinjerna som helhet.
- Denna tabell är endast avsedd för illustrativa ändamål och utgör varken en fullständig eller en slutlig återgivning av EDPB:s ståndpunkt vid beräkningen av administrativa sanktionsavgifter.
- Tabellen har två steg: i det ena illustreras intervallet för startbeloppet baserat på allvar och i det andra illustreras intervallet för startbeloppet efter justering för företagets storlek.
- De siffror som används som startbelopp motsvarar å ena sidan kommissionens rekommendation om små och medelstora företag och hur omsättningen som nämns i den rekommendationen avser omsättningen enligt artikel 83 i dataskyddsförordningen [85]. Å andra sidan, när det gäller överträdelsens allvar, baseras siffrorna på insikter från nuvarande metoder för utfärdande av sanktionsavgifter och omfattande interna tester med sanktioneringsmodeller under flera år. EDPB är övertygad om att dessa utgångspunkter gör rättvisa åt principerna om effektivitet, proportionalitet och avskräckande verkan, i enlighet med artikel 83.1 i dataskyddsförordningen.
- Som alltid är EDPB emellertid medvetet om att beräkningen av administrativa sanktionsavgifter inte är någon rent matematisk övning och att verkliga fall och praxis oundvikligen kommer att leda till en ytterligare skärpning av utgångspunkterna i denna tabell. I riktlinjerna anges därför att tabellen och siffrorna i den fortfarande granskas noggrant av EDPB och kommer att anpassas vid behov.
- Det bör också upprepas att dessa siffror är utgångspunkten för ytterligare beräkningar och inte fasta belopp (prismärkningar). Tillsynsmyndigheten har rätt att använda hela betalningsintervallet från ett belopp upp till och med det lagstadgade maximibeloppet.
- I det första steget gäller att ju allvarligare överträdelsen är inom sin egen kategori, desto högre är sannolikt startbeloppet.
- I det andra steget leder procentsatserna till att det slutliga startbeloppet fastställs, medan justeringar kan göras till en viss procentandel av det startbelopp som anges i steg 1. Detta innebär att den

[85] Kommissionens rekommendation av den 6 maj 2003 om definitionen av mikroföretag samt små och medelstora företag (delgivet med nr K(2003) 1422), (2003/361/EG).

procentsats som väljs i steg 2 ska användas som multiplikator till det startbelopp som fastställs i steg 1. Ju högre omsättningen i företaget är inom sin tillämpliga nivå, desto högre är startbeloppet sannolikt i steg 2.

- Beloppen i det andra steget illustrerar endast de allra lägsta och högsta tal som kan tillämpas i kategorin. Det slutliga startbeloppet kommer att falla någonstans inom dessa extremvärden. Dessa intervall i det andra steget fungerar därför som en sundhetskontroll för handläggaren.
- Observera att det inte görs någon justering i steg 2 för företag med en omsättning på 500 miljoner euro eller mer, eftersom dessa företag kommer att överskrida det statiska lagstadgade maximibeloppet och företagets storlek därför redan återspeglas i det dynamiska lagstadgade maximibelopp som används för att fastställa startbeloppet för ytterligare beräkningar i steg 1.
- Tillämpningen av metoden, inklusive användningen av tabellerna, illustreras av två exempel i slutet av denna bilaga.

Steg 1: Beräkning av grundbeloppet utifrån allvarlighetsgrad

Anm.: I det första steget gäller att ju allvarligare överträdelsen är inom sin egen kategori, desto högre är sannolikt startbeloppet.

	Låg allvarlighetsgrad		**Medelhög allvarlighetsgrad**		**Hög allvarlighetsgrad**	
	Statiskt intervall	*Dynamiskt intervall* vid omsättning > 500 m	*Statiskt intervall*	*Dynamiskt intervall vid omsättning > 500 m*	*Statiskt intervall*	*Dynamiskt intervall vid omsättning > 500 m*
Artikel 83.4 i dataskyddsförordningen	0–1m	0–0,2 % av årsomsättningen	1 m–2 m	0,2 %–0,4 % av årsomsättningen	2m–10m	0,4 %–2 % av årsomsättningen
Artikel 83.5.6 i dataskyddsförordningen	0–2m	0–0,4 % av årsomsättningen	2m–4m	0,4 %–0,8 % av årsomsättningen	4m–20m	0,8 %–4 % av årsomsättningen

Steg 2: Justering av grundbeloppet på grundval av företagets storlek (gäller endast företag som omfattas av den statiska rättsliga ramen)

Ju högre omsättningen i företaget är inom sin tillämpliga nivå, desto högre är startbeloppet sannolikt i detta andra steg.

Artikel 83.4 i dataskyddsförordningen

	Låg allvarlighetsgrad	**Medelhög allvarlighetsgrad**	**Hög allvarlighetsgrad**
Företag med en omsättning på 250	40–100 % av startbeloppet		

	Låg allvarlighetsgrad	Medelhög allvarlighetsgrad	Hög allvarlighetsgrad
miljoner euro och upp till 500 miljoner euro	0–1m	400 000–2m	800 000–10m
Företag med en omsättning på 100 miljoner euro och upp till 250 miljoner euro	15–50 % av startbeloppet		
	0–500 000	150 000–1m	300 000–5m
Företag med en omsättning på 50 miljoner euro och upp till 100 miljoner euro	8–20 % av startbeloppet		
	0–200 000	80 000–400 000	160 000–2m
Företag med en omsättning på 10 miljoner euro och upp till 50 miljoner euro	1,5–10 % av startbeloppet		
	0–100 000	15 000–200 000	30 000–1m
Företag med en omsättning på 2 miljoner euro och upp till 10 miljoner euro	0,3–2 % av startbeloppet		
	0–20 000	3 000–40 000	6 000–200 000
Företag med en omsättning på upp till 2 miljoner euro	0,2–0,4 % av startbeloppet		
	0–4 000	2 000–8,000	4 000–40 000

Artikel 83.5.6 i dataskyddsförordningen

	Låg allvarlighetsgrad	**Medelhög allvarlighetsgrad**	**Hög allvarlighetsgrad**
Företag med en omsättning på 250 miljoner euro och upp till 500 miljoner euro	40–100 % av startbeloppet		
	0–2m	800 000–4m	1,6m–20m
Företag med en omsättning på 100 miljoner euro och upp till 250 miljoner euro	15–50 % av startbeloppet		
	0–1m	300 000–2m	600 000–10m
Företag med en omsättning på 50 miljoner euro och upp till 100 miljoner euro	8–20 % av startbeloppet		
	0–400 000	160 000–800 000	320 000–4m
Företag med en omsättning på 10 miljoner euro och upp till 50 miljoner euro	1,5–10 % av startbeloppet		
	0–200 000	30 000–400 000	60 000–2m
Företag med en omsättning på 2 miljoner euro och upp till 10 miljoner euro	0,3–2 % av startbeloppet		
	0–40 000	6 000–80 000	12 000–400 000
Företag med en omsättning på upp till 2 miljoner euro	0,2–0,4 % av startbeloppet		
	0–8 000	4 000–16 000	8 000–80 000

Steg för steg för tillämpning av kapitel 4 i riktlinjerna för finansiering, inklusive tabellerna

Exempel A

Ett företag inom sociala medier med en omsättning på 200 miljoner euro upptäcks ha sålt känsliga uppgifter om sina användare till flera datamäklare. I detta exempel har företaget endast överträtt artikel 9 i dataskyddsförordningen. Efter att ha analyserat alla relevanta omständigheter i ärendet enligt artikel 83.2 a, b och g beslutade tillsynsmyndigheten att överträdelsen var av hög allvarlighetsgrad.

Därefter måste tillsynsmyndigheten besluta om startbeloppet för ytterligare beräkning. Artikel 9 förtecknas i artikel 83.5 a i dataskyddsförordningen, där det anges att det lagstadgade maximibeloppet antingen är 20 miljoner euro eller 4 % av årsomsättningen. I detta fall är företagets omsättning mindre än 500 miljoner euro, vilket innebär att det statiska taket och intervallet är tillämpliga. Därför bör ett startbelopp på mellan 20 och 100 % av det tillämpliga lagstadgade maximibeloppet, dvs. 4 och 20 miljoner euro, övervägas. Med tanke på att ju allvarligare överträdelsen är inom sin egen kategori, desto högre kommer startbeloppet sannolikt att bli, beslutar tillsynsmyndigheten att startbeloppet baserat på överträdelsens allvarlighetsgrad enligt steg 1 bör vara 10 miljoner euro.

I steg 2 kommer det startbelopp som anges i steg 1 att justeras utifrån företagets storlek. Företaget har en årsomsättning på 200 miljoner euro och ligger därför inom intervallet 100–250 miljoner euro. Detta innebär att startbeloppet kommer att justeras till ett belopp på mellan 15 % och 50 % av startbeloppet. Med tanke på att eftersom ju högre företagets omsättning är inom dess tillämpliga nivå, desto högre är sannolikt startbeloppet, beslutar tillsynsmyndigheten att en justering ned till 40 % av det startbelopp som fastställs i steg 1 är motiverad på grundval av företagets storlek. Startbeloppet efter justeringen kommer då att vara 4 miljoner euro i detta fall.

För att säkerställa att detta startbelopp överensstämmer med riktlinjerna är det möjligt att dubbelkontrollera beloppet mot de intervall som anges i den tillämpliga tabellen. Med tanke på att artikel 83.5 i dataskyddsförordningen är tillämplig, att företaget har en omsättning på mellan 100 och 250 miljoner euro och allvarlighetsgraden är hög, bör startbeloppet vara mellan 600 000 och 10 miljoner euro. Tillsynsmyndigheten drar slutsatsen att ett startbelopp på 4 miljoner euro ligger mellan 600 000 och 10 miljoner euro. Startbeloppet är därför i linje med riktlinjerna.

Därefter beräknar tillsynsmyndigheten sanktionsavgifterna på grundval av återstoden av riktlinjerna.

Exempel B

En hotellkedja med en omsättning på 2 miljarder euro har överträtt artikel 12 i dataskyddsförordningen. Efter att ha analyserat omständigheterna i ärendet enligt artikel 83.2 a, b och g beslutade tillsynsmyndigheten att överträdelsen var medelstor.

Därefter måste tillsynsmyndigheten besluta om startbeloppet för ytterligare beräkning. Tillsynsmyndigheten fastställer först att artikel 12 i dataskyddsförordningen förtecknas i artikel 83.5 b i dataskyddsförordningen. Företagets omsättning är 2 miljarder euro, vilket är mer än 500 miljoner euro och därför gäller det dynamiska maximibeloppet. Detta innebär att det lagstadgade maximibeloppet är 4 % av företagets årsomsättning, vilket motsvarar 80 miljoner euro. Allvarlighetsgraden är medelhög och därför bör det beaktade startbeloppet ligga mellan 10 och 20 % av det tillämpliga lagstadgade maximibeloppet, dvs. 0,4 % och 0,8 % av årsomsättningen, vilket motsvarar ett startbelopp på mellan 8 och 16 miljoner euro.

Med tanke på att ju allvarligare överträdelsen är inom sin egen kategori, desto högre är startbeloppet sannolikt, anser tillsynsmyndigheten att startbeloppet, på grund av överträdelsens allvarlighetsgrad, bör vara 12 miljoner euro, dvs. 15 % av det tillämpliga lagstadgade maximibeloppet och 0,6 % av företagets årsomsättning.

Eftersom företaget har en årsomsättning på över 500 miljoner euro och det dynamiska lagstadgade maximibeloppet gäller, återspeglas företagets storlek redan i det dynamiska lagstadgade

maximibelopp som används för att fastställa startbeloppet. Till följd av detta tillämpas ingen ytterligare justering.

Därefter beräknar tillsynsmyndigheten sanktionsavgifterna på grundval av återstoden av riktlinjerna.