Beslut 01/2020 om tvisten rörande den irländska tillsynsmyndighetens utkast till beslut om Twitter International Company enligt artikel 65.1 a i den allmänna dataskyddsförordningen

Antaget den 9 november 2020

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Innehållsförteckning

Europeiska dataskyddsstyrelsen

med beaktande av artiklarna 63 och 65.1 a 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 (den allmänna dataskyddsförordningen)[1],

med beaktande av EES-avtalet, särskilt bilaga XI och protokoll 37 till detta, ändrat genom gemensamma EES-kommitténs beslut nr 154/2018 av den 6 juli 2018[2], och

med beaktande av artikel 11 och artikel 22 i arbetsordningen[3],

och av följande skäl:

(1) Den viktigaste uppgiften för Europeiska dataskyddsstyrelsen (nedan även kallad **styrelsen**) är att säkerställa en enhetlig tillämpning av den allmänna dataskyddsförordningen inom hela EES. Det följer därför av artikel 60 i den allmänna dataskyddsförordningen att den ansvariga tillsynsmyndigheten ska samarbeta med övriga berörda tillsynsmyndigheter i en strävan att uppnå samförstånd, att den ansvariga tillsynsmyndigheten och de berörda tillsynsmyndigheterna ska utbyta all relevant information med varandra och att den ansvariga tillsynsmyndigheten utan dröjsmål ska vidarebefordra relevant information i ärendet till övriga berörda tillsynsmyndigheter. Den ansvariga tillsynsmyndigheten ska utan dröjsmål lägga fram ett utkast till beslut för de övriga berörda tillsynsmyndigheterna för deras yttrande och ta vederbörlig hänsyn till deras synpunkter.

(2) Om någon av de berörda tillsynsmyndigheterna har gjort en relevant och motiverad invändning mot utkastet till beslut i enlighet med artikel 4.24 och artikel 60.4 i den allmänna dataskyddsförordningen och den ansvariga tillsynsmyndigheten inte har för avsikt att följa den relevanta och motiverade invändningen eller anser att invändningen inte är relevant och motiverad, ska den ansvariga tillsynsmyndigheten hänskjuta frågan till den mekanism för enhetlighet som avses i artikel 63 i den allmänna dataskyddsförordningen.

(3) Enligt artikel 65.1 a i den allmänna dataskyddsförordningen ska EDPB fatta ett bindande beslut om alla frågor som tas upp i de relevanta och motiverade invändningarna, särskilt om huruvida det föreligger en överträdelse av den allmänna dataskyddsförordningen.

(4) EDPB:s bindande beslut ska antas med två tredjedelars majoritet av EDPB:s ledamöter i enlighet med artikel 65.2 i den allmänna dataskyddsförordningen jämförd med artikel 11.4 i EDPB:s arbetsordning, inom en månad efter att ordföranden och den behöriga tillsynsmyndigheten har beslutat att handlingarna i ärendet är fullständiga. Tidsfristen kan förlängas med ytterligare en månad med beaktande av sakfrågans komplexitet, efter beslut av ordföranden på eget initiativ eller på begäran av minst en tredjedel av EDPB:s ledamöter.

(5) Om EDPB trots en sådan förlängning inte har kunnat fatta ett beslut inom tidsfristen ska den, i enlighet med artikel 65.3 i den allmänna dataskyddsförordningen, fatta ett beslut inom två veckor efter att förlängningen har löpt ut, med enkel majoritet av dess ledamöter.

[1] EUT L 119, 4.5.2016, s. 1.
[2] Alla hänvisningar till ”medlemsstater” i detta beslut bör förstås som hänvisningar till ”EES-medlemsstater”. Hänvisningar till ”EU” bör i relevanta fall förstås som hänvisningar till ”EES”.
[3] Europeiska dataskyddsstyrelsens arbetsordning, antagen den 25 maj 2018, senast ändrad och antagen den 8 oktober 2020.

1 SAMMANFATTNING AV TVISTEN

1. Detta dokument innehåller ett bindande beslut som antagits av EDPB i enlighet med artikel 65.1 a i den allmänna dataskyddsförordningen. Beslutet avser den tvist som uppstått till följd av ett utkast till beslut (nedan kallat **utkastet till beslut**) som utfärdats av den irländska tillsynsmyndigheten (”dataskyddskommissionen”, nedan kallad **IE SA** och i detta sammanhang även kallad **den ansvariga tillsynsmyndigheten**) samt de efterföljande invändningarna från ett antal berörda tillsynsmyndigheter (Österreichische Datenschutzbehörde, nedan kallad **AT SA**; Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit[4], nedan kallad **DE SA**; Datatilsynet, nedan kallad **DK SA**; Agencia Española de Protección de Datos, nedan kallad **ES SA**; Commission Nationale de l'Informatique et des Libertés, nedan kallad **FR SA**; Nemzeti Adatvédelmi és Információszabadság Hatóság, nedan kallad **HU SA**; Garante per la protezione dei dati personali, nedan kallad **IT SA**; Autoriteit Persoonsgegevens, nedan kallad **NL SA**). Det omtvistade utkastet till beslut avser en ”utredning på eget initiativ” som inleddes av IE SA efter **anmälan av en personuppgiftsincident** den 8 januari 2019 (nedan kallad **incidenten**) vid Twitter International Company (nedan kallat **TIC**), ett bolag med säte i Dublin, Irland[5].

2. Incidenten berodde på **ett programfel i Twitters design** som gjorde att om en användare på en Androidenhet ändrade den e-postadress som är kopplad till dennes Twitterkonto blev de skyddade tweetarna oskyddade och därmed tillgängliga för en bredare allmänhet (och inte bara för användarens följare), detta utan användarens vetskap[6]. Felet upptäcktes den 26 december 2018 av den externa uppdragstagare som förvaltar företagets ”bug bounty”-program, som är ett program genom vilket vem som helst kan lämna in en felrapport[7].

3. Under sin undersökning upptäckte Twitter ytterligare användaråtgärder som också skulle leda till samma oavsiktliga resultat. Felet i koden **spårades tillbaka till en kodändring som gjordes den 4 november 2014**[8].

4. TIC informerade IE SA om att, såvitt de kunde identifiera, hade **88 726 användare i EU och EES påverkats** av felet mellan den 5 september 2017 och den 11 januari 2019. Twitter har bekräftat att det daterar buggen till den 4 november 2014 men har även bekräftat att det endast kan identifiera berörda användare från och med den 5 september 2017 på grund av en lagringspolicy som är tillämplig på loggarna[9]. TIC erkände därför möjligheten att fler användare kunde ha påverkats av incidenten[10].

5. IE SA:s beslut att inleda utredningen fattades under omständigheter där TIC i sitt formulär för anmälan av incidenter hade identifierat de **potentiella konsekvenserna för berörda personer som ”betydande”**[11].

[4] Invändningen från tillsynsmyndigheten i Hamburg representerar även ”Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, Berliner Beauftragte für Datenschutz und Informationsfreiheit, Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern och Die Landesbeauftragte für den Datenschutz Niedersachsen”. Invändningen har även samordnats med andra tillsynsmyndigheter i Tyskland.
[5] Utkastet till beslut, punkterna 1.1–1.2.
[6] Utkastet till beslut, punkt 1.9.
[7] Utkastet till beslut, punkterna 2.7 och 4.7.
[8] Utkastet till beslut, punkt 2.10.
[9] Utkastet till beslut, punkt 2.10.
[10] Utkastet till beslut, punkterna 1.10, 2.10, 14.2 och 14.3.
[11] Utkastet till beslut, punkt 2.8.

6. IE SA uppgav i sitt utkast till beslut att den är övertygad om att IE SA är den ansvariga tillsynsmyndigheten, i den mening som avses i den allmänna dataskyddsförordningen, när det gäller TIC, såsom personuppgiftsansvarig för den gränsöverskridande behandling av personuppgifter av TIC som var föremål för incidenten[12].

7. Följande tabell visar en sammanfattande tidsplan för händelserna i förfarandet fram till överlämnandet av ärendet till mekanismen för enhetlighet:

26.12.2018	Twitter, Inc., ett företag som bildats i USA, erhåller en felrapport via sitt ”bug bounty”-program. Rapporten skickades av en tredje part som förvaltade ”bug bounty”-programmet (uppdragstagare 1) till den tredje part som anlitats av Twitter, Inc. för att leta efter och bedöma programfel (uppdragstagare 2).
29.12.2018	Uppdragstagare 2 delar resultatet med Twitter, Inc. via en JIRA-biljett.
2.1.2019	Twitter, Inc.:s informationssäkerhetsteam granskar JIRA-biljetten och beslutar att det inte är en säkerhetsfråga men att det kan vara en dataskyddsfråga.
2.1.2019	Twitter, Inc.:s juridiska team underrättas.
3.1.2019	Twitter, Inc.:s juridiska team beslutar att frågan ska behandlas som en incident.
4.1.2019	Twitter, Inc. utlöser **incidenthanteringsprocessen**, men på grund av ett misstag vid tillämpningen av det interna förfarandet läggs det globala dataskyddsombudet inte till som ”övervakare” på biljetten. Det underrättas därför inte.
7.1.2019	Det globala dataskyddsombudet underrättas om incidenten vid ett sammanträde.
8.1.2019	TIC **anmäler incidenten** till IE SA via IE SA:s formulär för anmälan av gränsöverskridande incidenter.
22.1.2019	Utredningens omfattning och rättsliga grund angavs i det meddelande om inledande av utredningen som sändes till TIC den 22 januari 2019. IE SA inleder utredningen och begär information från TIC.
28.5.2019 till 21.10.2019	Utredningsrapport: ⟩ IE SA utarbetar ett **utkast till utredningsrapport** och lägger fram det för TIC så att TIC kan lämna in synpunkter på detta utkast. ⟩ TIC lämnar in sina synpunkter på utkastet. ⟩ IE SA begär förtydliganden när det gäller TIC:s inlagor. ⟩ IE SA utfärdar sin slutliga utredningsrapport.
21.10.2019	IE SA inleder beslutsprocessen.
11 och 28.11.2019.	IE SA kommunicerar med TIC och uppmanar TIC att inkomma med ytterligare skriftliga inlagor.

[12] IE SA har bekräftat att dess bedömning i detta avseende grundades både på dess fastställande att 1) TIC, såsom leverantör av Twittertjänsten i EU och EES, är den relevanta personuppgiftsansvarige och 2) att TIC:s huvudsakliga verksamhetsställe i EU är beläget i Dublin, Irland, där beslut om behandlingens ändamål och de medel med vilka den utförs när det gäller Twitteranvändares personuppgifter i EU och EES fattas av TIC, i enlighet med artikel 4.16 i den allmänna dataskyddsförordningen. Utkastet till beslut, punkterna 2.2–2.3.

2.12.2019	TIC inkommer med ytterligare inlagor till IE SA som svar på IE SA:s korrespondens av den 11 och 28 november 2019.
14.3.2020	IE SA utfärdar ett **preliminärt utkast till beslut** (nedan kallat **det preliminära utkastet till beslut**) till TIC där man kommer fram till att TIC har överträtt artikel 33.1 och artikel 33.5 i den allmänna dataskyddsförordningen och därför har för avsikt att utfärda en reprimand i enlighet med artikel 52.2 i den allmänna dataskyddsförordningen samt en administrativ sanktionsavgift i enlighet med artikel 58.2 i och artikel 83.2 i den allmänna dataskyddsförordningen.
27.4.2020	TIC inkommer med synpunkter på det preliminära utkastet till beslut till IE SA.
27.4.2020–22.5.2020	IE SA beaktar TIC:s inlagor beträffande det preliminära utkastet till beslut och utarbetar sitt utkast till beslut för inlämning till de berörda tillsynsmyndigheterna i enlighet med artikel 60 i den allmänna dataskyddsförordningen.
22.5.2020–20.6.2020	IE SA delar sitt utkast till beslut med de berörda tillsynsmyndigheterna i enlighet med artikel 60.3 i den allmänna dataskyddsförordningen. Flera berörda tillsynsmyndigheter (AT SA, DE SA [företrädd av den tyska tillsynsmyndigheten i Hamburg], DK SA, ES SA, FR SA, HU SA, IT SA och NL SA) framför **invändningar** i enlighet med artikel 60.4 i den allmänna dataskyddsförordningen.
15.7.2020	IE SA utfärdar ett sammansatt memorandum med sina svar på invändningarna och delar det med de berörda tillsynsmyndigheterna (nedan kallat **det sammansatta memorandumet**). IE SA ber de relevanta berörda tillsynsmyndigheterna att bekräfta huruvida de har för avsikt att vidhålla sina invändningar efter att ha beaktat IE SA:s ståndpunkt i fråga om invändningarna i det sammansatta memorandumet.
27 och 28.7.2020.	Mot bakgrund av argumenten från IE SA i det sammansatta memorandumet ger DK SA besked till IE SA om att den inte vidhåller sin invändning, och ES SA informerar IE SA om att den delvis drar tillbaka sin invändning. De övriga berörda tillsynsmyndigheterna (dvs. AT SA, DE SA, ES SA, FR SA, HU SA, IT SA och NL SA) bekräftar för IE SA att de vidhåller sina återstående invändningar.
19.8.2020	IE SA hänskjuter ärendet till EDPB i enlighet med artikel 60.4 i den allmänna dataskyddsförordningen och inleder därmed tvistlösningsförfarandet enligt artikel 65.1 a.

8. IE SA inledde tvistlösningsförfarandet om IMI den 19 augusti 2020. Efter att den ansvariga tillsynsmyndigheten lämnat in ärendet till EDPB i enlighet med artikel 60.4 i den allmänna dataskyddsförordningen bedömde EDPB:s sekretariat handlingarnas fullständighet på ordförandens vägnar i enlighet med artikel 11.2 i EDPB:s arbetsordning. EDPB:s sekretariat kontaktade IE SA första gången den 20 augusti 2020 och bad om att ytterligare handlingar och information skulle lämnas in i IMI och bad IE SA bekräfta att handlingarna i ärendet var fullständiga. IE SA tillhandahöll handlingarna och informationen och bekräftade att handlingarna i ärendet var fullständiga den 21 augusti 2020. En fråga av särskild betydelse som granskades av EDPB:s sekretariat var rätten att bli hörd, i enlighet med artikel 41.2 a i stadgan om de grundläggande rättigheterna. Den 4 september 2020 kontaktade sekretariatet IE SA med ytterligare frågor för att bekräfta huruvida TIC hade getts möjlighet att utöva

sin rätt att bli hörd avseende alla handlingar som lämnats in till styrelsen för beslut. Den 8 september 2020 bekräftade IE SA att så var fallet och tillhandahöll handlingar för att styrka detta[13].

9. Den 8 september 2020 fattades beslutet om handlingarnas fullständighet, och EDPB:s sekretariat delade det med samtliga ledamöter i EDPB.

10. Ordföranden beslutade, i enlighet med artikel 65.3 i den allmänna dataskyddsförordningen läst tillsammans med artikel 11.4 i EDPB:s arbetsordning, att förlänga den normala tidsfristen för antagande på en månad med ytterligare en månad med tanke på sakfrågans komplexitet.

2 VILLKOR FÖR ANTAGANDE AV ETT BINDANDE BESLUT

11. De allmänna villkoren för styrelsens antagande av ett bindande beslut anges i artikel 60.4 och artikel 65.1 a i den allmänna dataskyddsförordningen[14].

2.1 Invändning(ar) från berörda tillsynsmyndigheter mot ett utkast till beslut

12. EDPB noterar att de berörda tillsynsmyndigheterna framförde invändningar mot utkastet till beslut via det informations- och kommunikationssystem som anges i artikel 17 i EDPB:s arbetsordning, nämligen informationssystemet för den inre marknaden. Invändningarna gjordes i enlighet med artikel 60.4 i den allmänna dataskyddsförordningen.

13. Mer specifikt framfördes invändningar från de berörda tillsynsmyndigheterna beträffande följande frågor:

- Den ansvariga tillsynsmyndighetens behörighet.
- Kvalificeringen av TIC:s respektive Twitter, Inc.:s roller.
- De överträdelser av den allmänna dataskyddsförordningen som identifierats av den ansvariga tillsynsmyndigheten.
- Förekomsten av eventuella ytterligare (eller alternativa) överträdelser av den allmänna dataskyddsförordningen.
- Avsaknaden av en reprimand.
- Beräkningen av den föreslagna sanktionsavgiften.

14. Var och en av dessa invändningar lämnades in inom den tidsfrist som anges i artikel 60.4 i den allmänna dataskyddsförordningen.

[13] Bland de handlingar som skickades in av IE SA fanns e-postmeddelanden från det globala dataskyddsombudet som bekräftade mottagandet av de relevanta handlingarna.

[14] Enligt artikel 65.1 a i den allmänna dataskyddsförordningen ska styrelsen fatta ett bindande beslut när en tillsynsmyndighet har framfört en relevant och motiverad invändning mot ett utkast till beslut från den ansvariga tillsynsmyndigheten eller när den ansvariga tillsynsmyndigheten har avslagit en sådan invändning som icke relevant eller motiverad.

2.2 Den ansvariga tillsynsmyndigheten följer inte de relevanta och motiverade invändningarna mot utkastet till beslut eller anser att invändningarna inte är relevanta eller motiverade

15. Den 15 juli 2020 försåg IE SA de berörda tillsynsmyndigheterna med en detaljerad analys av de invändningar som framförts av de berörda tillsynsmyndigheterna i det sammansatta memorandumet, där den angav huruvida den ansåg att invändningarna var ”relevanta och motiverade” i enlighet med artikel 4.24 i den allmänna dataskyddsförordningen och huruvida den beslutade att följa någon av invändningarna[15].

16. Närmare bestämt ansåg IE SA att endast de invändningar som framförts av de berörda tillsynsmyndigheterna i samband med beräkningen av sanktionsavgiften uppfyller den tröskel som anges i artikel 4.24 i den allmänna dataskyddsförordningen, i den mån de avser förenligheten hos den planerade åtgärden gentemot den personuppgiftsansvarige eller personuppgiftsbiträdet i förhållande till den allmänna dataskyddsförordningen och även anger de risker som uppstår i fråga om de registrerades grundläggande fri- och rättigheter[16]. IE SA kom dock fram till att den inte skulle följa invändningarna på grund av de skäl som anges i det sammansatta memorandumet och nedan.

17. IE SA ansåg att övriga invändningar som framförts av de berörda tillsynsmyndigheterna inte var ”relevanta och motiverade” i den mening som avses i artikel 4.24 i den allmänna dataskyddsförordningen.

2.3 Slutsats

18. Ärendet i fråga uppfyller alla de kriterier som anges i artikel 65.1 a i den allmänna dataskyddsförordningen, eftersom flera berörda tillsynsmyndigheter framförde invändningar mot ett utkast till beslut från den ansvariga tillsynsmyndigheten inom den tidsfrist som anges i artikel 60.4 i den allmänna dataskyddsförordningen och den ansvariga tillsynsmyndigheten inte har följt invändningarna eller har avslagit dem som irrelevanta eller omotiverade.

19. EDPB är därför behörig att anta ett bindande beslut, som ska gälla alla de frågor som är föremål för de relevanta och motiverade invändningarna, särskilt om huruvida det föreligger en överträdelse av den allmänna dataskyddsförordningen[17].

20. Inga resultat i detta beslut påverkar några bedömningar eller bindande beslut av EDPB i andra ärenden, inbegripet med samma parter, beroende på ytterligare och/eller nya rön.

[15] Syftet med dokumentet, så som det anges av IE SA, var att underlätta ytterligare samarbete med de berörda tillsynsmyndigheterna i samband med utkastet till beslut och att uppfylla kravet i artikel 60.1 i den allmänna dataskyddsförordningen på att den ansvariga tillsynsmyndigheten ska samarbeta med de övriga berörda tillsynsmyndigheterna i en strävan att uppnå samförstånd.
[16] Det sammansatta memorandumet, punkt 5.59.
[17] Artikel 65.1 a (slutdelen) i den allmänna dataskyddsförordningen. Vissa berörda tillsynsmyndigheter lämnade synpunkter som i sig inte var invändningar och som därför inte har beaktats av EDPB.

3 RÄTTEN TILL GOD FÖRVALTNING

21. EDPB omfattas av artikel 41 i EU-stadgan om de grundläggande rättigheterna, särskilt artikel 41 (rätt till god förvaltning). Detta återspeglas även i artikel 11.1 i EDPB:s arbetsordning[18].

22. EDPB:s beslut *"ska vara motiverat och riktat till den ansvariga tillsynsmyndigheten och alla berörda tillsynsmyndigheter och ska vara bindande för dem"* (artikel 65.2 i den allmänna dataskyddsförordningen). Syftet är inte att vända sig direkt till någon tredje part. Som en försiktighetsåtgärd för att ta itu med möjligheten att TIC skulle kunna påverkas av EDPB:s beslut bedömde dock EDPB om TIC erbjöds möjlighet att utöva sin rätt att bli hörd i samband med det förfarande som leddes av den ansvariga tillsynsmyndigheten, och i synnerhet om alla handlingar som mottagits i detta förfarande och som EDPB använt för att fatta sitt beslut redan tidigare har delgetts TIC och om TIC har hörts om dem.

23. Med tanke på att TIC redan har hörts av IE SA beträffande all den information som EDPB mottagit och använt för att fatta sitt beslut[19] och den ansvariga tillsynsmyndigheten har delat TIC:s skriftliga synpunkter med EDPB i enlighet med artikel 11.2 i EDPB:s arbetsordning[20], när det gäller de frågor som tas upp i detta specifika utkast till beslut, är EDPB övertygad om att artikel 41 i EU-stadgan om de grundläggande rättigheterna har respekterats.

4 OM KVALIFICERINGEN AV PERSONUPPGIFTSANSVARIG OCH PERSONUPPGIFTSBITRÄDE OCH DEN ANSVARIGA TILLSYNSMYNDIGHETENS BEHÖRIGHET

4.1 Den ansvariga tillsynsmyndighetens analys i utkastet till beslut

24. I utkastet till beslut anges att den utsedda utredaren inom IE SA, när utredningen inleddes, övertygades om att TIC är personuppgiftsansvarig i den mening som avses i artikel 4.7 i den allmänna dataskyddsförordningen när det gäller de personuppgifter som var föremål för incidenten, och att TIC i detta avseende bekräftade att det var den personuppgiftsansvarige i formuläret för anmälan av personuppgiftsincidenter och i korrespondensen med IE SA[21]. I utkastet till beslut anges vidare att TIC också bekräftade att incidenten hade uppstått i samband med behandling som utförts för dess räkning av Twitter Inc., dess personuppgiftsbiträde[22], att TIC är personuppgiftsansvarig för de personuppgifter som är föremål för utredningen samt att TIC har ingått ett avtal med Twitter Inc. (dess personuppgiftsbiträde) om att tillhandahålla databehandlingstjänster[23].

[18] Europeiska dataskyddsstyrelsens arbetsordning, antagen den 25 maj 2018, senast ändrad och antagen den 8 oktober 2020.
[19] IE SA:s preliminära utkast till beslut (14 mars 2020), IE SA:s utkast till beslut (22 maj 2020), de berörda tillsynsmyndigheternas invändningar och synpunkter (18–20 juni 2020), IE SA:s sammansatta memorandum (15 juli 2020) samt övriga synpunkter och invändningar från de berörda tillsynsmyndigheterna (27–28 juli 2020).
[20] Europeiska dataskyddsstyrelsens arbetsordning, antagen den 25 maj 2018, senast ändrad och antagen den 8 oktober 2020.
[21] Utkastet till beslut, punkt 2.2.
[22] Utkastet till beslut, punkt 4.2.
[23] Utkastet till beslut, punkt 4.6.

25. I utkastet till beslut anges dessutom att IE SA även var övertygad om att den var behörig att agera som ansvarig tillsynsmyndighet när det gäller TIC:s gränsöverskridande behandling i samband med de personuppgifter som var föremål för incidenten[24].

26. I detta avseende anges vidare i utkastet till beslut att TIC bekräftade för IE SA när det anmälde incidenten att det var ett irländskt företag och leverantör av Twittertjänster i Europa och att TIC:s integritetspolicy (uppdaterad i januari 2016) informerade användarna av Twittertjänsten i EU om att de hade rätt att ta upp farhågor antingen med sin lokala tillsynsmyndighet eller med TIC:s ansvariga tillsynsmyndighet, IE SA[25].

27. IE SA har dessutom i utkastet till beslut tagit med ett utdrag ur TIC:s årsredovisning och årsredovisningar för det räkenskapsår som avslutades den 31 december 2018, där det anges att den yttersta kontrollerande part och den största företagsgrupp för vilken koncernredovisningar upprättas, och som företaget är medlem i, är Twitter, Inc., ett företag som bildats i Amerikas förenta stater och är noterat på New York-börsen[26].

28. Inledningsvis ställdes IE SA inför osäkerhet på grund av användningen av termerna ”vi” och ”vår” i formuläret för anmälan av personuppgiftsincidenter för att hänvisa omväxlande till TIC och Twitter, Inc. IE SA begärde förtydliganden i detta avseende och TIC angav att anställda vid TIC och Twitter, Inc. vanligtvis använder ”vi” och ”vår” på ett löst sätt för att hänvisa till koncernen med dess namn. Dessutom uppgav TIC att även om TIC är den personuppgiftsansvarige och fattar beslut om uppgiftsbehandlingens ändamål och de medel med vilka den utförs agerar det inte ensamt: ”*TIC och dess anställda ingår i [...] Twittergruppen [...]. Alla anställda i Twittergruppen använder samma datasystem, följer samma allmänna policyer [...] och arbetar tillsammans för att säkerställa det globala stöd dygnet runt som krävs för att hålla Twitterplattformen i drift*”[27].

4.2 Sammanfattning av invändningarna från de berörda tillsynsmyndigheterna

29. I sin invändning hävdar **ES SA** att **utkastet till beslut inte tillräckligt motiverar TIC:s roll som personuppgiftsansvarig**. ES SA betonar att det bör göras en bedömning av vilken enhet som verkligen beslutar om ändamålen och medlen samt en kritisk analys av alla omständigheter som förelegat. Enligt ES SA förefaller de faktorer som ligger till grund för utkastet till beslut tyda på en annan slutsats än den som IE SA dragit. I synnerhet anser ES SA att besluten om de huvudsakliga ändamålen med uppgiftsbehandlingen faktiskt fattas av Twitter, Inc. ES SA stödde sitt resonemang genom att ange vissa faktorer som enligt dess uppfattning skulle kunna tyda på att TIC inte beslutar om ändamålen och medlen. För det första erinrade ES SA om att TIC är ett dotterbolag till Twitter, Inc. och betonade att det därför är svårt att förstå hur TIC skulle kunna ”*utfärda order*” till Twitter, Inc. när det gäller behandlingen av EES-användares personuppgifter. Enligt ES SA var TIC aldrig i stånd att självständigt välja Twitter, Inc. som sitt personuppgiftsbiträde och skulle inte kunna ersätta det. Dessutom hävdade ES SA att Twitter, Inc. inte verkar agera som personuppgiftsbiträde på grund av avsaknaden av en direkt kanal mellan de två företagen när det gäller hanteringen av personuppgiftsincidenter annat än att skicka ett e-postmeddelande med en kopia till det globala dataskyddsombudet. För det tredje uppgav ES SA att det inte stod klart hur TIC självständigt skulle ha kunnat fatta eller påverka de beslut som ledde till korrigeringen av it-felet i det system som förvaltas och kontrolleras av Twitter, Inc. utan att

[24] Utkastet till beslut, punkt 2.3.
[25] Utkastet till beslut, punkt 2.3.
[26] Utkastet till beslut, punkt 2.4.
[27] Utkastet till beslut, punkt 4.5.

det snarare var Twitter, Inc. som fattade beslut om en lösning av incidenten, vars effekter inte var begränsade enbart till europeiska användare.

30. **NL SA** invände också mot den rättsliga kvalificeringen av TIC och Twitter, Inc. som personuppgiftsansvarig respektive personuppgiftsbiträde. Invändningen gäller närmare bestämt det sätt på vilket IE SA har hävdat att TIC är den enda personuppgiftsansvarige i detta fall och att Twitter, Inc. är ett personuppgiftsbiträde som agerar för dess räkning. NL SA anser att bedömningen av personuppgiftsansvar är en grundläggande aspekt i detta fall och att varje eventuell slutsats om rollen som personuppgiftsansvarig, personuppgiftsbiträde eller gemensamma personuppgiftsansvariga därför bör stödjas av rättsliga och faktiska bevis. I sin invändning **hävdar NL SA i huvudsak att utkastet till beslut inte innehåller tillräckliga bevis för att rättsligt och faktiskt fastställa de berörda företagens roller**, i synnerhet för att stödja slutsatsen i) att TIC är (ensam) personuppgiftsansvarig och ii) att Twitter, Inc. endast är ett personuppgiftsbiträde som agerar enligt instruktioner från TIC för driften av den globala Twittertjänsten och/eller de ändamål som är relevanta i detta fall. Enligt NL SA bör den ansvariga tillsynsmyndigheten kontrollera **om organisationens rättsliga förklaringar och/eller dess integritetspolicy överensstämmer med dess faktiska verksamhet**. NL SA begärde att IE SA skulle inkludera mer information om och/eller en beskrivning av de faktorer som ledde till fastställandet av roller i själva utkastet till beslut. NL SA nämner även följande faktorer som exempel på faktorer som bör beaktas: instruktioner från TIC till Twitter, Inc. eller andra objektiva bevis eller praktiska ledtrådar från den dagliga verksamheten, samt exempel från skriftliga register såsom ett databehandlingsavtal.

31. I sin invändning har **DE SA** gjort gällande att **förhållandet mellan Twitter, Inc. och TIC inte är ett förhållande mellan en personuppgiftsansvarig och ett personuppgiftsbiträde**, utan snarare ett förhållande mellan gemensamma personuppgiftsansvariga. Invändningen baseras i första hand på att Twitter, Inc. och TIC inte använder separata databehandlingssystem. Enligt DE SA ändras det grundläggande system som drivs av Twitter, Inc. på grundval av beslut som fattats av TIC och det som gäller för EES-användare, medan det huvudsakliga behandlingssystemet förblir detsamma. DE SA betonade också att alla anställda i gruppen använder samma datasystem och följer samma allmänna policyer.

32. Slutligen invände **FR SA** mot IE SA:s behörighet och hävdade att det verkade som att IE ES drog slutsatsen att befogenheten att fatta beslut om ändamålen och medlen för behandlingen i fråga utövades av TIC. Enligt FR SA **framgår det inte tydligt av utkastet till beslut att andra faktorer än företaget TIC:s uttalanden beaktades av myndigheten för att anse att detta företag hade befogenhet att fatta beslut om behandlingen**. FR SA angav också att det inte tydligt framgår av utkastet till beslut om myndighetens behörighet grundar sig på att företaget TIC bör betraktas som personuppgiftsansvarig eller på att TIC bör betraktas som huvudsakligt verksamhetsställe enligt definitionen i artikel 4.16 i den allmänna dataskyddsförordningen. FR SA kom fram till att utkastet till beslut i sitt nuvarande tillstånd inte förhindrar risken för forumshopping, vilket mekanismen med en enda kontaktpunkt är avsedd att undvika. FR SA uppmanade IE SA att tillhandahålla fler uppgifter som gör det möjligt att bevisa att företaget TIC har befogenhet att fatta beslut om behandlingens ändamål och medel för det sociala nätverket Twitter.

4.3 Den ansvariga tillsynsmyndighetens ståndpunkt avseende invändningarna

33. I sitt sammansatta memorandum ansåg IE SA att en invändning som är baserad på parternas roll eller beteckning som personuppgiftsansvarig och personuppgiftsbiträde och/eller IE SA:s behörighet varken bestrider konstaterandet av en överträdelse eller den planerade åtgärden och därför inte uppfyller definitionen i artikel 4.24, och att den inte omfattas av definitionen av en relevant och motiverad

invändning enligt artikel 4.24[28]. IE SA analyserade dock sådana invändningar och redogjorde därvid för de faktorer som den hade beaktat vid fastställandet av TIC:s status som personuppgiftsansvarig och huvudsakligt verksamhetsställe. I detta avseende redogjorde IE SA (kortfattat[29]) för de fakta och den rättsliga analys som ledde fram till dess slutsats om TIC:s status som personuppgiftsansvarig, i huvudsak följande:

- Twitters tidigare bekräftelse 2015 om att det tänkte göra TIC i Irland till personuppgiftsansvarig för Twitteranvändares personuppgifter i EU[30].
- TIC:s bekräftelse på att det var personuppgiftsansvarig för de personuppgifter som berördes av incidenten, både genom att anmäla incidenten till IE SA och under utredningens gång.
- TIC:s bekräftelse av att det finns ett databehandlingsavtal mellan TIC och Twitter, Inc. som dess personuppgiftsbiträde, vilket inbegriper de bestämmelser som krävs enligt artikel 28 i den allmänna dataskyddsförordningen.
- Interaktionerna mellan TIC och Twitter, Inc. efter den 7 januari 2019, då TIC (genom sitt dataskyddsombud) faktiskt fick vetskap om incidenten, vilket enligt IE SA visar att TIC utövade kontroll och beslutsbefogenheter över Twitter, Inc. när det gäller avhjälpande åtgärder och anmälan av incidenten och i samband med den bakomliggande behandlingen av personuppgifter som påverkats av incidenten.
- Twitter, Inc.:s agerande när det underrättades om incidenten av uppdragstagare 2, vilket enligt IE SA även stöder statusen för förhållandet mellan de två företagen som ett förhållande där TIC utövade befogenheter och bar ansvar som personuppgiftsansvarig.

34. IE SA redogjorde därefter kortfattat[31] för de faktiska omständigheter och den rättsliga analys som ledde till dess slutsats att TIC är huvudsakligt etablerat i Irland, i huvudsak följande (utöver punkterna ovan):

- TIC:s beteckning och förklaring av sig självt som huvudsakligt verksamhetsställe.
- TIC:s bekräftelse i sin integritetspolicy av sin status som relevant personuppgiftsansvarig för Twitteranvändares personuppgifter i EU.
- TIC:s huvudkontor är beläget i Dublin, där det har cirka 170 anställda.
- TIC:s direkta anställning av ett globalt dataskyddsombud i den mening som avses i den allmänna dataskyddsförordningen, rapporteringslinjen för det globala dataskyddsombudet inom TIC samt det globala dataskyddsombudets representation av TIC inom en rad integritets- och databehandlingsrelaterade verksamheter, inbegripet möjligheten att lägga in veto mot databehandling.
- IE SA:s historiska och kontinuerliga övervakning av TIC, under vilken det har varit uppenbart att TIC bestämmer ändamålen och medlen för behandlingen av personuppgifter inom EU.

[28] Det sammansatta memorandumet, punkt 5.39.
[29] Det sammansatta memorandumet, punkt 5.35.
[30] I detta avseende förklaras i det sammansatta memorandumet att TIC den 8 april 2015 informerade IE SA om att den tänkte göra TIC i Irland till personuppgiftsansvarig för sina användares personuppgifter utanför USA och att TIC i maj 2015 anmälde detta till andra tillsynsmyndigheter i EU (punkt 5.15).
[31] Det sammansatta memorandumet, punkt 5.36.

IE SA upprepade att den, trots sitt svar på invändningarna beträffande behörighet och/eller parternas beteckning, inte ansåg att invändningarna i samband med dessa frågor uppfyllde definitionen av en ”relevant och motiverad invändning” enligt artikel 4.24 i den allmänna dataskyddsförordningen. IE SA uppgav att den inte hade för avsikt att följa invändningarna i dessa frågor mot bakgrund av sin bedömning att frågorna inte uppfyllde definitionen i artikel 4.24 i den allmänna dataskyddsförordningen och mot bakgrund av bevisen på att den på ett adekvat sätt hade behandlat frågorna om huvudsakligt verksamhetsställe, behörighet och beteckning av personuppgiftsansvarig och personuppgiftsbiträde i sitt utkast till beslut[32].

4.4 EDPB:s analys

4.4.1 Bedömning av huruvida invändningarna var relevanta och motiverade

35. EDPB inleder sin analys av de framförda invändningarna genom att bedöma huruvida invändningarna ovan ska betraktas som relevanta och motiverade invändningar i den mening som avses i artikel 4.24 i den allmänna dataskyddsförordningen.

36. I artikel 4.24 i den allmänna dataskyddsförordningen definieras ”relevant och motiverad invändning” som en ”*invändning mot ett förslag till beslut avseende frågan huruvida det föreligger en överträdelse av denna förordning eller huruvida den planerade åtgärden i förhållande till den personuppgiftsansvarige eller personuppgiftsbiträdet är förenlig med denna förordning, av vilken invändning det tydligt framgår hur stora risker utkastet till beslut medför när det gäller registrerades grundläggande rättigheter och friheter samt i tillämpliga fall det fria flödet av personuppgifter inom unionen*”[33].

37. Såsom klargörs i riktlinjerna för begreppet relevant och motiverad invändning måste en invändning vara både ”relevant” och ”motiverad”. För att invändningen ska vara ”relevant” måste det finnas en direkt koppling mellan invändningen och utkastet till beslut och det måste antingen röra sig om huruvida det föreligger en överträdelse av den allmänna dataskyddsförordningen eller om huruvida den planerade åtgärden gentemot den personuppgiftsansvarige eller personuppgiftsbiträdet är förenlig med den allmänna dataskyddsförordningen[34].

38. Enligt samma riktlinjer är en invändning ”motiverad” när den är sammanhängande och tydligt, precist och detaljerat tillhandahåller förtydliganden och argument om varför en ändring av beslutet föreslås och hur ändringen skulle leda till en annan slutsats[35], och när den tydligt visar hur betydande riskerna med utkastet till beslut är för de registrerades grundläggande rättigheter och friheter samt, i tillämpliga fall, för det fria flödet av personuppgifter inom Europeiska unionen. Den berörda tillsynsmyndigheten bör således visa vilka konsekvenser utkastet till beslut skulle få för de skyddade värdena genom att lägga fram tillräckliga argument för att visa att sådana risker är betydande och rimliga[36]. Utvärderingen

[32] Det sammansatta memorandumet, punkt 5.40.
[33] Artikel 4.24 i den allmänna dataskyddsförordningen.
[34] Se även EDPB:s riktlinjer 9/2020 för begreppet relevant och motiverad invändning, versionen för offentligt samråd (nedan kallade **riktlinjerna för begreppet relevant och motiverad invändning**), punkt 12, som för närvarande är föremål för offentligt samråd, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-092020-relevant-and-reasoned-objection_en. Riktlinjerna antogs den 8 oktober 2020, efter att IE SA hade inlett utredningen i detta specifika fall.
[35] Riktlinjerna för begreppet relevant och motiverad invändning, punkterna 17 och 20.
[36] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 37.

av riskerna för de registrerades rättigheter och friheter[37] kan bland annat bygga på lämpligheten, nödvändigheten och proportionaliteten hos de planerade åtgärderna[38] och på en eventuell minskning av framtida överträdelser av den allmänna dataskyddsförordningen[39].

39. Vad gäller innehållet kan invändningen, som ett första alternativ, avse förekomst av en överträdelse av den allmänna dataskyddsförordningen. I detta fall bör den förklara varför den berörda tillsynsmyndigheten inte håller med om huruvida den verksamhet som bedrivs av den personuppgiftsansvarige eller personuppgiftsbiträdet har lett till en överträdelse av en viss bestämmelse i den allmänna dataskyddsförordningen, samt specifikt vilken eller vilka överträdelser[40]. Denna invändning kan även omfatta meningsskiljaktigheter beträffande de slutsatser som ska dras av resultaten från undersökningen (t.ex. genom att ange att resultaten utgör en annan överträdelse än dem som redan analyserats eller en överträdelse utöver dessa)[41] eller skulle kunna gå så långt som till att identifiera brister i utkastet till beslut som motiverar ett behov av ytterligare utredning från den ansvariga tillsynsmyndighetens sida[42]. Detta är dock mindre sannolikt när den ansvariga tillsynsmyndighetens skyldighet att samarbeta med de berörda tillsynsmyndigheterna och utbyta all relevant information har uppfyllts på vederbörligt sätt under den tid som föregick utfärdandet av utkastet till beslut[43]. Alternativt kan innehållet i invändningen hänvisa till förenligheten hos den åtgärd gentemot den personuppgiftsansvarige eller personuppgiftsbiträdet (korrigerande eller annan åtgärd) som planeras i utkastet till beslut i förhållande till den allmänna dataskyddsförordningen genom att förklara varför den planerade åtgärden inte är förenlig med den allmänna dataskyddsförordningen[44].

40. EDPB anser att det är möjligt att en invändning som rör förekomst av en överträdelse av den allmänna dataskyddsförordningen avser en frånvaro eller brist på bedömning eller motivering (vilket innebär att slutsatsen i utkastet till beslut inte tillräckligt stöds av den bedömning som gjorts och de bevis som lagts fram, vilket krävs enligt artikel 58 i den allmänna dataskyddsförordningen), så länge hela den tröskel som anges i artikel 4.24 i den allmänna dataskyddsförordningen uppfylls och förutsatt att det finns en koppling mellan den påstått otillräckliga analysen och huruvida det föreligger en överträdelse av den allmänna dataskyddsförordningen eller huruvida den planerade åtgärden är förenlig med den allmänna dataskyddsförordningen[45].

41. EDPB anser att en invändning mot parternas roll eller beteckning kan omfattas av definitionen av ”relevant och motiverad” invändning enligt artikel 4.24 i EDPB, eftersom detta kan påverka fastställandet av huruvida det föreligger en överträdelse av denna förordning eller huruvida den planerade åtgärden i förhållande till den personuppgiftsansvarige eller personuppgiftsbiträdet är förenlig med förordningen. EDPB anser dock att en invändning mot behörigheten hos den

[37] De ”registrerade” vars rättigheter och friheter kan påverkas kan vara både de vars personuppgifter behandlas av den personuppgiftsansvarige eller personuppgiftsbiträdet och de vars personuppgifter kan komma att behandlas i framtiden. Riktlinjerna för begreppet relevant och motiverad invändning, punkt 43.
[38] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 42.
[39] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 43.
[40] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 25.
[41] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 27.
[42] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 28 (där det även anges att det i detta avseende ska göras en åtskillnad mellan, å ena sidan, utredningar på eget initiativ och, å andra sidan, utredningar som utlöses av klagomål eller av rapporter om möjliga överträdelser som delas av berörda tillsynsmyndigheter).
[43] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 27.
[44] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 33. Detta innebär att invändningen bland annat kan ifrågasätta de omständigheter som ligger till grund för beräkningen av sanktionsavgiften (riktlinjerna för begreppet relevant och motiverad invändning, punkt 34).
[45] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 29.

tillsynsmyndighet som agerar som ansvarig tillsynsmyndighet inte bör göras genom en invändning i enlighet med artikel 60.4 i den allmänna dataskyddsförordningen utan faller utanför tillämpningsområdet för artikel 4.24 i den allmänna dataskyddsförordningen[46].

a) Bedömning av invändningen från NL SA

42. Den invändning som framförts av NL SA avser i första hand en avsaknad eller brist på bedömning eller motivering[47] som leder till de slutsatser som IE SA dragit när det gäller den rättsliga kvalificeringen av TIC och Twitter, Inc. Som NL SA påpekar är bedömningen av personuppgiftsansvar en grundläggande aspekt i ärendet. En annan slutsats när det gäller den rättsliga kvalificeringen av TIC och Twitter, Inc. skulle påverka tillsynsmyndighetens slutsatser, både när det gäller fastställandet av en överträdelse av artikel 33 i den allmänna dataskyddsförordningen och det beslut om korrigerande åtgärder som resulterar av utredningen.

43. EDPB erinrar om att varje rättsligt bindande åtgärd som antas av en tillsynsmyndighet måste ange skälen för åtgärden[48]. Fastställandet av huruvida det föreligger en överträdelse av denna förordning eller huruvida den planerade åtgärden gentemot den personuppgiftsansvarige eller personuppgiftsbiträdet är förenlig med förordningen är beroende av en korrekt identifiering av rollerna för de parter som ska bli föremål för åtgärden. Ett utkast till beslut måste därför innehålla tillräckliga rättsliga och faktiska omständigheter till stöd för det föreslagna beslutet[49]. EDPB anser därför att den invändning som framförts av NL SA gäller både huruvida det föreligger en överträdelse av den allmänna dataskyddsförordningen och huruvida den planerade åtgärden är förenlig med den allmänna dataskyddsförordningen.

44. Även om EDPB anser att NL SA:s invändning därför är relevant och inbegriper rättsliga argument till stöd för dess ståndpunkt lägger den inte fram några argument för hur sådana konsekvenser skulle innebära betydande risker för de registrerades rättigheter och friheter och/eller det fria flödet av uppgifter[50]. EDPB erinrar om att skyldigheten att tydligt visa betydelsen av den risk som utkastet till beslut utgör – vilken fastställs i den allmänna dataskyddsförordningen – åligger den berörda tillsynsmyndigheten[51]. Även om möjligheten för de berörda tillsynsmyndigheterna att tillhandahålla sådant bevis även kan bero på detaljnivån i själva utkastet till beslut och på det tidigare informationsutbytet[52] kan en sådan omständighet, i förekommande fall, inte helt befria den berörda tillsynsmyndigheten från skyldigheten att klart ange varför den anser att utkastet till beslut medför betydande risker för enskildas rättigheter och friheter om det lämnas oförändrat.

---

[46] Förfarandet enligt artikel 65.1 b i den allmänna dataskyddsförordningen är tillämpligt i detta fall och kan inledas när som helst (riktlinjerna för begreppet relevant och motiverad invändning, punkt 31).

[47] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 29. En relevant och motiverad invändning om huruvida det föreligger en överträdelse av den allmänna dataskyddsförordningen kan gälla otillräcklig faktisk information om eller beskrivning av det aktuella ärendet eller en oenighet om de slutsatser som ska dras av resultaten från utredningen (riktlinjerna för begreppet relevant och motiverad invändning, punkt 27), eller hänvisa till en avsaknad eller brist på bedömning eller motivering (vilket innebär att slutsatsen i utkastet till beslut inte tillräckligt stöds av den bedömning som gjorts och de bevis som lagts fram, vilket krävs enligt artikel 58 i den allmänna dataskyddsförordningen) (riktlinjerna för begreppet relevant och motiverad invändning, punkt 29).

[48] Skäl 129 i den allmänna dataskyddsförordningen.

[49] Sådan information är även nödvändig för att säkerställa effektiviteten i mekanismen för samarbete och enhetlighet, så att de berörda tillsynsmyndigheterna kan fatta ett informerat beslut om huruvida de ska samtycka till eller uttrycka en relevant och motiverad invändning.

[50] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 19.

[51] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 36, och artikel 4.24 i den allmänna dataskyddsförordningen.

[52] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 36.

45. EDPB anser att NL SA:s invändning inte tydligt visar riskerna för enskildas rättigheter och friheter som sådana. EDPB anser därför att invändningen från NL SA inte uppfyller kraven i artikel 4.24 i den allmänna dataskyddsförordningen.

b) Bedömning av invändningen från ES SA

46. Invändningen från ES SA ifrågasätter också huruvida bedömningen eller motiveringen är tillräcklig för de slutsatser som IE SA dragit beträffande den rättsliga kvalificeringen av TIC respektive Twitter, Inc. Invändningen klargör också att en korrekt kvalificering av TIC och Twitter, Inc. är avgörande för att fastställa deras respektive ansvar samt för IE SA:s behörighet. EDPB anser därför också att den invändning som framförts av ES SA gäller både huruvida det föreligger en överträdelse av den allmänna dataskyddsförordningen och huruvida den planerade åtgärden är förenlig med den allmänna dataskyddsförordningen. I ES SA:s invändning anges även varför den anser att en ändring av utkastet till beslut är nödvändig och hur ändringen skulle leda till en annan slutsats.

47. Även om EDPB anser att ES SA:s invändning därför är relevant och inbegriper rättsliga argument till stöd för dess ståndpunkt anger den inte på ett tydligt sätt varför beslutet, om det inte ändras i detta avseende, skulle innebära betydande risker för de registrerades rättigheter och friheter och, i tillämpliga fall, det fria flödet av personuppgifter. EDPB anser därför att ES SA:s invändning inte uppfyller kraven i artikel 4.24 i den allmänna dataskyddsförordningen.

c) Bedömning av invändningen från DE SA

48. Medan invändningarna från NR SA och ES SA i första hand avser en avsaknad av en motivering till slutsatsen att TIC fungerar som (ensam) personuppgiftsansvarig håller DE SA inte med om vilka slutsatser som ska dras av resultaten från undersökningen[53]. I synnerhet anser DE SA att de faktiska omständigheterna i ärendet är tillräckliga för att motivera slutsatsen att Twitter, Inc. inte kan betraktas som personuppgiftsbiträde, utan snarare ska betraktas som gemensamt personuppgiftsansvarig tillsammans med TIC.

49. I sin invändning anger DE SA även varför parternas kvalificering är relevant för att fastställa huruvida det föreligger en överträdelse. I synnerhet hävdar DE SA att den rättsliga bedömningen av förhållandet mellan Twitter, Inc. och TIC påverkar fastställandet av tidpunkten för när incidenten blev känd. Enligt DE SA måste vetskap i lika hög grad tillskrivas båda (de gemensamt) personuppgiftsansvariga mot bakgrund av artikel 26.1 i den allmänna dataskyddsförordningen. Med hänsyn till detta hävdar DE SA att det relevanta datumet då TIC såsom gemensamt personuppgiftsansvarig fick vetskap (eller borde ha fått vetskap) måste omprövas av IE SA.

50. EDPB anser att invändningen från DE SA tydligt anger varför en ändring av utkastet till beslut anses nödvändig och hur invändningen, om den följs, skulle leda till en annan slutsats. EDPB anser dock inte att invändningen från DE SA innehåller ett tydligt uttalande om de risker som utkastet till beslut innebär när det gäller de registrerades grundläggande rättigheter och friheter i förhållande till parternas kvalificering som sådan. EDPB anser därför att DE SA:s invändning inte uppfyller kraven i artikel 4.24 i den allmänna dataskyddsförordningen.

d) Bedömning av invändningen från FR SA

51. FR SA anser i huvudsak också att utkastet till beslut lider av en avsaknad av eller brist på bedömning eller motivering, eftersom det inte tydligt anger att IE SA beaktade andra faktorer än TIC:s egna uttalanden när den kom fram till att TIC utövade en befogenhet att fatta beslut om behandlingen. I

[53] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 27.

likhet med NL SA och ES SA betonar även FR SA att det är viktigt att den ansvariga tillsynsmyndighetens beslut är tillräckligt motiverat. Till skillnad från NL SA och ES SA fokuserar dock FR SA i sin invändning främst på vikten av att inkludera ett sådant resonemang för att fastställa den ansvariga tillsynsmyndighetens behörighet, i synnerhet för att förhindra forumshopping.

52. EDPB erinrar om att en oenighet om behörigheten för den tillsynsmyndighet som fungerar som ansvarig tillsynsmyndighet att utfärda ett beslut i det specifika fallet inte bör framföras genom en invändning enligt artikel 60.4 i den allmänna dataskyddsförordningen utan faller utanför tillämpningsområdet för artikel 4.24 i samma förordning[54]. EDPB anser att FR SA:s invändning inte innehåller tillräckliga argument för att tydligt visa hur stor risk utkastet till beslut innebär för de registrerades rättigheter och friheter. EDPB anser därför att invändningen från FR SA inte är en relevant och motiverad invändning i den mening som avses i artikel 4.24 i den allmänna dataskyddsförordningen.

4.4.2 Slutsats

53. EDPB anser att invändningarna ovan uppfyller flera av kriterierna i artikel 4.24 i den allmänna dataskyddsförordningen. Till skillnad från IE SA:s slutsats anser EDPB att var och en av dessa invändningar uppfyllde villkoret att hänvisa antingen till huruvida det föreligger en överträdelse av denna förordning, eller till huruvida den planerade åtgärden gentemot den personuppgiftsansvarige eller personuppgiftsbiträdet är förenlig med denna förordning. Dessutom anser EDPB att en invändning som grundar sig på parternas roll eller beteckning i princip kan omfattas av definitionen av en relevant och motiverad invändning i artikel 4.24 i den allmänna dataskyddsförordningen.

54. Såsom anges ovan uppfyller emellertid de ovannämnda invändningarna inte tröskeln när det gäller att på ett tydligt sätt visa betydelsen av riskerna med utkastet till beslut när det gäller de registrerades grundläggande rättigheter och friheter och, i tillämpliga fall, det fria flödet av personuppgifter inom Europeiska unionen.

55. När det gäller den ovannämnda invändningen från FR SA gäller invändningen en oenighet om behörigheten för den tillsynsmyndighet som agerar som ansvarig tillsynsmyndighet; detta utöver att den inte lägger fram tillräckliga argument som på ett tydligt sätt visar betydelsen av den risk som utkastet till beslut innebär för de registrerades rättigheter och friheter. EDPB erinrar om att en sådan oenighet inte bör framföras genom en invändning i enlighet med artikel 60.4 i den allmänna dataskyddsförordningen utan faller utanför tillämpningsområdet för artikel 4.24 i samma förordning[55].

56. EDPB anser därför att invändningarna ovan inte uppfyller kraven i artikel 4.24 i den allmänna dataskyddsförordningen.

57. **EDPB tar därför inte ställning till huruvida några väsentliga frågor som tas upp i dessa invändningar är välgrundade. EDPB upprepar att dess nuvarande beslut inte påverkar eventuella bedömningar som styrelsen kan komma att uppmanas göra i andra fall, även med samma parter, med beaktande av innehållet i det relevanta utkastet till beslut och de invändningar som framförts av de berörda tillsynsmyndigheterna.**

[54] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 31. I riktlinjerna anges vidare att till skillnad från invändningen enligt artikel 60.4 i den allmänna dataskyddsförordningen är förfarandet enligt artikel 65.1 b i samma förordning tillämpligt i alla skeden.
[55] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 31.

5 ÖVERTRÄDELSER AV DEN ALLMÄNNA DATASKYDDSFÖRORDNINGEN SOM IDENTIFIERATS AV DEN ANSVARIGA TILLSYNSMYNDIGHETEN

5.1 Slutsatser om en överträdelse av artikel 33.1 i den allmänna dataskyddsförordningen

5.1.1 Den ansvariga tillsynsmyndighetens analys i utkastet till beslut

58. IE SA kom fram till att TIC inte uppfyllde sina skyldigheter som personuppgiftsansvarig enligt artikel 33.1 i den allmänna dataskyddsförordningen, vilket inte kan betraktas isolerat utan måste förstås mot bakgrund av de mer övergripande skyldigheterna för personuppgiftsansvariga enligt den allmänna dataskyddsförordningen, särskilt ansvarsskyldigheten enligt artikel 5.2, förhållandet mellan personuppgiftsansvariga och personuppgiftsbiträden (artikel 28) och skyldigheten att genomföra lämpliga (och effektiva) tekniska och organisatoriska åtgärder[56].

59. När det gäller den tidpunkt då den personuppgiftsansvarige fick vetskap om incidenten kom man i utkastet till beslut fram till att om personuppgiftsbiträdet drabbas av incidenten får den personuppgiftsansvarige vetskap när personuppgiftsbiträdet underrättar den om incidenten[57], men den personuppgiftsansvarige måste se till att den har tillräckliga åtgärder inrättade för att underlätta sådan vetskap[58]. Eftersom TIC i egenskap av personuppgiftsansvarig var ansvarig för att övervaka den behandling som utförs av dess personuppgiftsbiträde Twitter, Inc.[59] konstaterades i utkastet till beslut att om personuppgiftsbiträdet inte följer förfarandet eller förfarandet misslyckas på annat sätt kan den personuppgiftsansvarige inte ursäkta sin egen försenade anmälan på grundval av personuppgiftsbiträdets fel,[60] eftersom en personuppgiftsansvarigs fullgörande av sin anmälningsskyldighet inte kan vara beroende av att dess personuppgiftsbiträde fullgör sina skyldigheter enligt artikel 33.2 i den allmänna dataskyddsförordningen[61]. IE SA fann att den personuppgiftsansvarige under dessa omständigheter måste anses ha konstruktiv vetskap om incidenten genom sitt personuppgiftsbiträde[62] och att en sådan tolkning speglar den personuppgiftsansvariges ansvar och ansvarsskyldighet enligt den allmänna dataskyddsförordningen[63].

---

[56] Utkastet till beslut, punkt 6.20. Se även utkastet till beslut, punkterna 6.5, 6.7 och 6.13. I utkastet till beslut (punkt 7.129 i) anges även att kravet i artikel 33.1 bygger på att den personuppgiftsansvarige säkerställer att den har interna system och förfaranden (samt i tillämpliga fall system och förfaranden inrättade med externa parter, inbegripet personuppgiftsbiträden) som är konfigurerade och följs, för att underlätta snabb vetskap om och läglig anmälan av incidenter.

[57] Utkastet till beslut, punkt 7.129 iii.

[58] Utkastet till beslut, punkt 7.98.

[59] Utkastet till beslut, punkt 7.129 iv.

[60] Utkastet till beslut, punkt 7.129 iv.

[61] Utkastet till beslut, punkt 7.129 x.

[62] Utkastet till beslut, punkt 7.129 v.

[63] Utkastet till beslut, punkt 7.98. Enligt utkastet till beslut lämnar en alternativ tolkning med slutsatsen att en personuppgiftsansvarig endast har vetskap när den informeras av sitt personuppgiftsbiträde en betydande lucka i det skydd som den allmänna dataskyddsförordningen erbjuder, eftersom det skulle kunna leda till att den personuppgiftsansvarige undgår ansvar även vid större fördröjningar om den visar att den har fullgjort sina skyldigheter när det gäller att välja ett personuppgiftsbiträde och ha lämpliga system inrättade, men personuppgiftsbiträdet har bortsett från dessa system (utkastet till beslut, punkt 7.99). IE SA angav vidare i utkastet till beslut att den alternativa tillämpningen av artikel 33.1, samt den som föreslagits av TIC, enligt vilken

60. Enligt utkastet till beslut fick TIC således faktiskt vetskap om incidenten den 7 januari 2019,[64] men borde ha haft vetskap om den senast den 3 januari 2019, eftersom det var det datumet då Twitter, Inc., såsom personuppgiftsbiträde, först bedömde incidenten som en potentiell personuppgiftsincident och Twitter, Inc.:s juridiska team gav instruktioner om att incidenten skulle öppnas[65]. I utkastet till beslut angavs också att även under de särskilda omständigheterna i denna situation (där tidigare fördröjningar också hade uppstått)[66] borde eventuella arrangemang med Twitter, Inc. ha möjliggjort detta[67]. På grund av förfarandets ineffektivitet under de särskilda omständigheterna i det aktuella fallet och/eller underlåtenheten hos personuppgiftsbiträdets personal att följa sin incidenthanteringsprocess skedde i stället en fördröjning som ledde till att den personuppgiftsansvarige inte fick vetskap förrän den 7 januari 2019[68]. Detta ledde till en överträdelse av artikel 33.1 i den allmänna dataskyddsförordningen, även om mindre än 72 timmar förflöt mellan den tidpunkt då TIC faktiskt fick vetskap om incidenten (7 januari 2019) och anmälan (8 januari 2019).

5.1.2 Sammanfattning av invändningarna från de berörda tillsynsmyndigheterna

61. **FR SA** framförde en invändning om att resultaten inte motsvarar en överträdelse av artikel 33.1 i den allmänna dataskyddsförordningen, utan snarare av artikel 28 eller artikel 32 i samma förordning, vilka anger den personuppgiftsansvariges skyldigheter när den beslutar att anlita ett personuppgiftsbiträde. Detta argument bygger på att konstaterandet av överträdelsen av artikel 33.1 huvudsakligen grundar sig på bristerna i tillämpningen av det förfarande som inrättats mellan TIC och dess personuppgiftsbiträde vid en personuppgiftsincident, medan artikel 33.1 i den allmänna dataskyddsförordningen endast hänvisar till den personuppgiftsansvariges skyldighet att anmäla personuppgiftsincidenter till den behöriga myndigheten.

62. **DE SA:s** invändningar fokuserade i stället på det resonemang som ledde till slutsatsen att artikel 33.1 i den allmänna dataskyddsförordningen hade överträtts, utan att ifrågasätta denna slutsats i sig, och hänvisade mer specifikt till fastställandet av den tidpunkt då tidsfristen på 72 timmar började löpa.

63. DE SA hävdade i sin invändning att frågan om rollfördelningen påverkar fastställandet av tidpunkten för vetskap om incidenten, eftersom vetskapen om en incident i lika hög grad måste tillskrivas båda de gemensamt personuppgiftsansvariga. Enligt DE SA kan detta leda till att den 26 december 2018 betraktas som det datum då TIC såsom gemensamt personuppgiftsansvarig fick vetskap om eller borde ha fått vetskap om incidenten.

---

en personuppgiftsansvarigs fullgörande av sin anmälningsskyldighet väsentligen är beroende av att dess personuppgiftsbiträde fullgör sina skyldigheter enligt artikel 33.2, skulle undergräva effektiviteten av skyldigheterna för personuppgiftsansvariga enligt artikel 33 och att ett sådant tillvägagångssätt skulle strida mot det övergripande syftet med den allmänna dataskyddsförordningen och EU-lagstiftarens avsikt.

[64] Utkastet till beslut, punkt 7.129 vi.

[65] Utkastet till beslut, punkt 7.129 vi.

[66] För att identifiera den 3 januari 2019 som det datum då TIC borde ha känt till incidenten beaktade IE SA även att en tidigare fördröjning hade uppstått under perioden från det att incidenten först anmäldes av den externa uppdragstagaren (uppdragstagare 2) till Twitter, Inc. den 29 december 2018 till den tidpunkt då Twitter, Inc. inledde sin granskning av incidenten, den 2 januari 2019. TIC bekräftade under utredningens gång att detta berodde på vintersemesterschemat.

[67] Utkastet till beslut, punkt 7.129 ix.

[68] Utkastet till beslut, punkt 7.129 vi.

5.1.3 Den ansvariga tillsynsmyndighetens ståndpunkt avseende invändningarna

64. När det gäller invändningen från FR SA anser IE SA att den begär att alternativa bestämmelser i den allmänna dataskyddsförordningen ska beaktas och att de berörda tillsynsmyndigheternas begäran om att överväga alternativa bestämmelser i den allmänna dataskyddsförordningen väsentligen skulle syfta till att omarbeta den utredning som genomförts[69]: IE SA konstaterade att en sådan invändning inte omfattas av definitionen av en relevant och motiverad invändning i den mening som avses i artikel 4.24 i den allmänna dataskyddsförordningen[70]. IE SA betonade även sin uppfattning att en överträdelse av artikel 33.1 i den allmänna dataskyddsförordningen har ägt rum och föreslog inte att man skulle beakta överträdelser av andra bestämmelser i den allmänna dataskyddsförordningen som ett alternativ till artikel 33.1[71], utan underströk att en utvidgning av överträdelserna till andra skyldigheter enligt den allmänna dataskyddsförordningen på begäran av berörda tillsynsmyndigheter skulle äventyra hela utredningen och förfarandet enligt artikel 60 genom att utsätta den för risken för påståenden om processuell orättvisa[72]. IE SA påpekade även att den undersöker om TIC fullgör sina mer omfattande skyldigheter enligt den allmänna dataskyddsförordningen i samband med en annan pågående utredning[73].

65. När det gäller invändningen från DE SA, särskilt fastställandet av tidpunkten för vetskap om incidenten, hävdade IE SA att även om det fanns ett förhållande av gemensamt personuppgiftsansvar (en åsikt som, enligt avsnitt 4.3 ovan, IE SA inte delade) skulle det inte nödvändigtvis innebära att vetskap om incidenten kan tillskrivas båda gemensamt personuppgiftsansvariga i lika hög grad[74].

5.1.4 EDPB:s analys

5.1.4.1 Bedömning av huruvida invändningarna var relevanta och motiverade

66. Såsom erinras om ovan (se avsnitt 4.4.1) är det nödvändigt att bedöma om invändningarna från de berörda tillsynsmyndigheterna uppfyller tröskeln i artikel 4.24 i den allmänna dataskyddsförordningen.

67. Även om **FR SA:s** invändning är relevant, i och med att den anger en oenighet om huruvida en viss överträdelse av den allmänna dataskyddsförordningen har ägt rum i det specifika fallet och inbegriper rättsliga argument till stöd för invändningen, uppfyller den inte normen i artikel 4.24 i den allmänna dataskyddsförordningen, eftersom den inte innehåller motiveringar när det gäller konsekvenserna av att utfärda ett beslut utan de ändringar som föreslås i invändningen och hur sådana konsekvenser skulle innebära betydande risker för de registrerades rättigheter och friheter[75]. Man kan därför inte säga att invändningen tydligt visar betydelsen av de risker som följer av utkastet till beslut (vid ett eventuellt slutgiltigt utfärdande) eftersom den inte anger tillräckliga argument för varför sådana rättigheter och friheter för de registrerade är väsentliga och rimliga, i synnerhet när det gäller konstaterandet av en överträdelse av artikel 33.1 (i stället för artikel 32 eller 28) i den allmänna dataskyddsförordningen[76]. EDPB drar därför slutsatsen att invändningen från **FR SA** inte är relevant

[69] Det sammansatta memorandumet, punkt 5.45.
[70] Det sammansatta memorandumet, punkt 5.45.
[71] Det sammansatta memorandumet, punkt 5.47.
[72] Det sammansatta memorandumet, punkt 5.44 c.
[73] Det sammansatta memorandumet, punkt 5.44 d.
[74] Det sammansatta memorandumet, punkt 5.34 (som även hänvisar till EU-domstolens dom i mål C-210/16, Wirtschaftsakademie, punkt 43).
[75] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 19.
[76] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 37.

och motiverad på grund av att det inte tydligt visas hur stora riskerna är, vilket uttryckligen krävs enligt artikel 4.24 i den allmänna dataskyddsförordningen.

68. När det gäller **DE SA:s** invändning, särskilt fastställandet av den tidpunkt då tidsfristen börjar löpa för överträdelsen av artikel 33.1 i den allmänna dataskyddsförordningen som beroende av parternas kvalificering, vill EDPB dessutom påminna om analysen i avsnitt 4.4 och konstaterar att invändningen inte visar vilka konsekvenser utkastet till beslut med dess nuvarande innehåll skulle få för de skyddade värdena[77] (de registrerades rättigheter och friheter eller, i tillämpliga fall, det fria flödet av personuppgifter), särskilt när det gäller det resonemang som ligger till grund för konstaterandet av en överträdelse av artikel 33.1 i den allmänna dataskyddsförordningen.

5.1.4.2 Slutsats

69. EDPB anser att invändningarna ovan uppfyller villkoret att hänvisa antingen till huruvida det föreligger en överträdelse av denna förordning eller huruvida den planerade åtgärden i förhållande till den personuppgiftsansvarige eller personuppgiftsbiträdet är förenlig med denna förordning, men de visar inte på ett tydligt sätt hur stora risker utkastet till beslut medför när det gäller de registrerades grundläggande rättigheter och friheter samt i tillämpliga fall det fria flödet av personuppgifter inom unionen.

70. FR SA:s och DE SA:s invändningar uppfyller därför inte kraven i artikel 4.24 i den allmänna dataskyddsförordningen[78].

5.2 Slutsatser om en överträdelse av artikel 33.5 i den allmänna dataskyddsförordningen

5.2.1 Den ansvariga tillsynsmyndighetens analys i utkastet till beslut

71. I utkastet till beslut konstaterade IE SA att TIC inte fullgjorde sina skyldigheter enligt artikel 33.5 i den allmänna dataskyddsförordningen att dokumentera incidenten, eftersom den dokumentation som tillhandahölls av TIC under utredningens gång inte ansågs innehålla tillräcklig information och inte ansågs innehålla ett register eller dokument som specifikt rörde en personuppgiftsincident; den utgjorde dokumentation av mer allmän karaktär[79].

72. I en annan kommentar medgav IE SA att TIC samarbetade fullt ut under utredningen (även om detta inte betraktades som en förmildrande omständighet)[80].

5.2.2 Sammanfattning av invändningarna från de berörda tillsynsmyndigheterna

73. EDPB tar tillfället i akt att för tydlighetens skull betona att ingen av invändningarna ifrågasatte slutsatsen att TIC brutit mot artikel 33.5 i den allmänna dataskyddsförordningen.

[77] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 37.
[78] EDPB tar därför inte ställning till huruvida några väsentliga frågor som tas upp i dessa invändningar är välgrundade. EDPB upprepar att dess nuvarande beslut inte påverkar eventuella bedömningar som styrelsen kan komma att uppmanas göra i andra fall, även med samma parter, med beaktande av innehållet i det relevanta utkastet till beslut och de invändningar som framförts av de berörda tillsynsmyndigheterna.
[79] Utkastet till beslut, punkt 10.46.
[80] Utkastet till beslut, punkt 14.50.

74. **IT SA** framförde dock en invändning om att konstaterandet av överträdelsen av artikel 33.5 i den allmänna dataskyddsförordningen inte förefaller vara förenligt med den ansvariga tillsynsmyndighetens resonemang eftersom den bristande dokumentation som togs fram under en så omfattande utredning, som grundar sig på flera interaktioner mellan den ansvariga tillsynsmyndigheten och den personuppgiftsansvarige, tyder på ett dåligt samarbete med dataskyddsmyndigheten från den personuppgiftsansvariges sida. Enligt IT SA bör slutsatsen i utkastet till beslut, om att TIC samarbetade fullt ut under utredningsfasen, ses över, eftersom ett sådant fullständigt samarbete endast kan anses föreligga om lämplig, uttömmande dokumentation görs tillgänglig av den personuppgiftsansvarige på ett direkt och uppriktigt sätt.

5.2.3 Den ansvariga tillsynsmyndighetens ståndpunkt avseende invändningarna

75. IE SA anser att skyldigheten enligt artikel 33.5 i den allmänna dataskyddsförordningen gäller oberoende av skyldigheten enligt artikel 31 i den allmänna dataskyddsförordningen att samarbeta med tillsynsmyndigheten och av hur TIC agerade gentemot, och interagerade med, den ansvariga tillsynsmyndigheten när den senare inledde sin tillsynsverksamhet beträffande TIC:s incident[81]. IE SE hävdade att bristerna i hur TIC dokumenterade incidenten inte nödvändigtvis korrelerar med bristande samarbete från TIC:s sida[82]. Dessutom betonade IE SA att TIC samarbetade med IE SA under utredningen genom att besvara alla begäranden om upplysningar och genom att tillhandahålla alla begärda handlingar, utan att försöka störa eller hindra utredningen på något sätt[83]. I vilket fall som helst betraktade IE SA inte TIC:s samarbete som en förmildrande omständighet[84]. Av ovannämnda skäl ansåg IE SA att det var diskutabelt huruvida den invändning som framförts av IT SA är motiverad och relevant, eftersom den visserligen rör en överträdelse av den allmänna dataskyddsförordningen men inte visar hur IE SA:s ståndpunkt om TIC:s grad av samarbete leder till risker för de registrerades grundläggande rättigheter och friheter till följd av utkastet till beslut[85]. IE SA konstaterade att den inte skulle följa denna invändning[86].

5.2.4 EDPB:s analys

5.2.4.1 Bedömning av huruvida invändningarna var relevanta och motiverade

76. IT SA bestrider inte i sin invändning att en överträdelse av artikel 33.5 i den allmänna dataskyddsförordningen har ägt rum. En relevant och motiverad invändning kan ifrågasätta det resonemang som ligger till grund för den ansvariga tillsynsmyndighetens slutsatser i utkastet till beslut endast om resonemanget har en koppling till dessa slutsatser och invändningen är tillräckligt motiverad. I detta fall framgår det inte tydligt av invändningen hur den skulle kunna medföra en ändring av utkastet till beslut om den följs. Invändningen uppfyller dessutom inte de kriterier som anges i artikel 4.24 i den allmänna dataskyddsförordningen, eftersom den inte visar på ett tydligt sätt hur betydande riskerna med utkastet till beslut är, eftersom den inte visar vilka konsekvenser det påstådda felet i utkastet till beslut skulle få för de skyddade värdena.

[81] Det sammansatta memorandumet, punkt 5.87.
[82] Det sammansatta memorandumet, punkt 5.87.
[83] Det sammansatta memorandumet, punkt 5.87.
[84] Det sammansatta memorandumet, punkt 5.87.
[85] Det sammansatta memorandumet, punkt 5.88.
[86] Det sammansatta memorandumet, punkt 5.88.

5.2.4.2 Slutsats

77. Eftersom IT SA:s invändning inte uppfyller kraven i artikel 4.24 i den allmänna dataskyddsförordningen tar styrelsen inte ställning till huruvida de väsentliga frågor som tas upp i invändningen är välgrundade. EDPB upprepar att dess nuvarande beslut inte påverkar eventuella bedömningar som styrelsen kan komma att uppmanas göra i andra fall, även med samma parter, med beaktande av innehållet i det relevanta utkastet till beslut och de invändningar som framförts av de berörda tillsynsmyndigheterna.

6 EVENTUELLA YTTERLIGARE (ELLER ALTERNATIVA) ÖVERTRÄDELSER AV DEN ALLMÄNNA DATASKYDDSFÖRORDNINGEN SOM IDENTIFIERATS AV DE BERÖRDA TILLSYNSMYNDIGHETERNA

6.1 Den ansvariga tillsynsmyndighetens analys i utkastet till beslut

78. På grundval av den information som TIC lämnade in när det anmälde incidenten till IE SA noterade IE SA att det av formuläret för anmälan av personuppgiftsincidenten framgick att en period på mer än 72 timmar hade förflutit från det att TIC (såsom personuppgiftsansvarig) fick vetskap om incidenten[87]. Av detta skäl beslutade IE SA att på eget initiativ inleda en utredning för att undersöka om TIC hade fullgjort sina skyldigheter enligt artikel 33.1 och artikel 33.5 i den allmänna dataskyddsförordningen[88].

79. För att fastställa huruvida TIC fullgör sina skyldigheter enligt artikel 33.1 i den allmänna dataskyddsförordningen beaktade IE SA dem inom ramen för en personuppgiftsansvarigs mer övergripande skyldigheter, inbegripet dess ansvarsskyldighet (artikel 5.2 i den allmänna dataskyddsförordningen), dess skyldighet att anlita ett personuppgiftsbiträde (artikel 28 i den allmänna dataskyddsförordningen) samt dess skyldighet när det gäller säkerheten vid behandling av personuppgifter (artikel 32 i den allmänna dataskyddsförordningen)[89]. Om IE SA övervägde de faktorer och sakförhållanden som ledde till att TIC dröjde med att få vetskap om personuppgiftsbiträdets incident och i slutändan med att anmäla incidenten, övervägde IE SA emellertid inte huruvida TIC fullgjorde någon av eller alla dessa skyldigheter annat än i syfte att bedöma huruvida TIC fullgjorde sina skyldigheter enligt artikel 33.1 och artikel 33.5 i den allmänna dataskyddsförordningen[90].

6.2 Sammanfattning av invändningarna från de berörda tillsynsmyndigheterna

80. DE SA, FR SA, HU SA och IT SA invände mot att TIC bröt mot andra bestämmelser i den allmänna dataskyddsförordningen utöver, eller i stället för, artikel 33.1 och artikel 33.5 i den allmänna dataskyddsförordningen.

6.2.1 Överträdelse av artikel 5.1 f i den allmänna dataskyddsförordningen avseende principen om integritet och konfidentialitet

81. **DE SA** gjorde en invändning om att den underliggande buggen i TIC:s program, som ledde till den incident som anmäldes till IE SA, borde ha beaktats av IE SA i utkastet till beslut, för att fastställa huruvida denna bugg faktiskt utgjorde en betydande kränkning av konfidentialiteten för

[87] Utkastet till beslut, punkt 2.11.
[88] Utkastet till beslut, punkt 2.11.
[89] Utkastet till beslut, punkterna 6.13–6.20, 7.111–7.112 och 7.122–7.124.
[90] Utkastet till beslut, punkterna 6.13, 7.111 och 7.122–7.124.

personuppgifter och i slutändan överträdde artikel 5.1 f i den allmänna dataskyddsförordningen, utöver artikel 33.1 och artikel 33.5 i den allmänna dataskyddsförordningen.

82. **HU SA** gjorde en invändning om att IE SA, med tanke på buggen i TIC:s program under årens lopp och dess allvarliga karaktär som påverkar datasäkerheten, bör undersöka om TIC även bröt mot artikel 5.1 f i den allmänna dataskyddsförordningen om principen om integritet och konfidentialitet.

6.2.2 Överträdelse av artikel 5.2 i den allmänna dataskyddsförordningen avseende principen om ansvarsskyldighet

83. **IT SA** invände mot att överträdelsen av artikel 33.1 i den allmänna dataskyddsförordningen visar på en mycket allvarligare överträdelse av principen om ansvarsskyldighet (enligt artikel 5.2 i den allmänna dataskyddsförordningen), eftersom bristen på företagsstrategier för att hantera säkerhetsincidenter eller underlåtenheten att följa dem visar att de åtgärder som den personuppgiftsansvarige genomfört är otillräckliga för att säkerställa efterlevnad och dokumentera dem. IT SA hävdade att dessa förfarandemässiga brister lyfts fram i utkastet till beslut men att ingen särskild analys av dem görs i utkastet till beslut. Eftersom detta även kan påverka hanteringen av framtida personuppgiftsincidenter bör slutsatserna om huruvida TIC uppfyllde kraven i artikel 5.2 i den allmänna dataskyddsförordningen också ingå i IE SA:s slutliga beslut, enligt IT SA:s uppfattning. IT SA ansåg också att överträdelsen av artikel 5.2 i den allmänna dataskyddsförordningen bekräftas av den personuppgiftsansvariges oförmåga att ange det exakta antalet och arten av de personuppgifter som berörs eller det totala antalet registrerade som berörs.

6.2.3 Överträdelse av artikel 24 i den allmänna dataskyddsförordningen om den personuppgiftsansvariges ansvar

84. **DE SA** invände mot att utkastet till beslut inte är tydligt om varför IE SA inte tog ställning till om den betydande överträdelse av konfidentialiteten för personuppgifter som orsakats av en underliggande bugg beror på en överträdelse av artikel 24 i den allmänna dataskyddsförordningen.

6.2.4 Överträdelse av artikel 28 i den allmänna dataskyddsförordningen om förhållandet till personuppgiftsbiträden

85. **FR SA** invände mot att TIC inte respekterade den personuppgiftsansvariges skyldighet att kontrollera giltigheten för de förfaranden som dess personuppgiftsbiträde inrättat. FR SA anser därför att det inte föreligger någon överträdelse av artikel 33.1 i den allmänna dataskyddsförordningen, utan i stället av artikel 28 i den allmänna dataskyddsförordningen (eller artikel 32 i den allmänna dataskyddsförordningen – se avsnitt 6.2.5 nedan). FR SA hävdade att om TIC:s personuppgiftsbiträde är dess moderbolag var det desto lättare för TIC att kontrollera giltigheten för de förfaranden som fastställts av moderbolaget och vid behov begära korrigeringar.

86. **IT SA** invände mot att TIC:s underlåtenhet att involvera det globala dataskyddsombudet i personuppgiftsbiträdets detektions- och insatsgrupp (Twitter, Inc.), trots att denna praxis ingick i TIC:s interna policy, visar att de skyddsåtgärder som personuppgiftsbiträdet vidtar för att genomföra lämpliga organisatoriska åtgärder enligt artikel 28.1 i den allmänna dataskyddsförordningen inte är tillräckligt omfattande. Dessutom hävdade IT SA i sina invändningar att personuppgiftsbiträdet inte fullgjorde sin skyldighet att bistå den personuppgiftsansvarige enligt artikel 28.3 f i den allmänna dataskyddsförordningen.

6.2.5 *Överträdelse av artikel 32 i den allmänna dataskyddsförordningen om säkerheten vid behandling*

87. **DE SA** invände att IE SA borde ha undersökt om alla lämpliga tekniska och organisatoriska åtgärder (i enlighet med artikel 32 i den allmänna dataskyddsförordningen) hade följts i detta fall och huruvida överträdelser på detta område borde ha blivit föremål för detta förfarande. DE SA hävdar även att utkastet till beslut inte är tydligt om varför IE SA inte bedömde om den betydande överträdelse av konfidentialiteten för personuppgifter som orsakats av en underliggande bugg beror på en överträdelse av artikel 32 i den allmänna dataskyddsförordningen.

88. **FR SA** invände mot IE SA:s rättsliga kvalificering av sakförhållandena och konstaterade att TIC:s underlåtenhet att respektera den personuppgiftsansvariges skyldighet att kontrollera giltigheten för de förfaranden som inrättats av dess personuppgiftsbiträde motsvarar en överträdelse av artikel 32 i den allmänna dataskyddsförordningen (eller artikel 28 i den allmänna dataskyddsförordningen – se avsnitt 6.2.4 ovan), snarare än av artikel 33.1 i den allmänna dataskyddsförordningen. FR SA hävdade att om TIC:s personuppgiftsbiträde är dess moderbolag var det desto lättare för TIC att kontrollera giltigheten för de förfaranden som fastställts av moderbolaget och vid behov begära korrigeringar.

89. **HU SA** invände att IE SA, med tanke på buggen i TIC:s program under årens lopp och dess allvarliga karaktär som påverkar datasäkerheten, bör undersöka om TIC även bröt mot artikel 32 i den allmänna dataskyddsförordningen när det gäller TIC:s skyldigheter avseende säkerhet vid behandling.

6.2.6 *Överträdelse av artikel 33.3 i den allmänna dataskyddsförordningen om innehållet i anmälan av en personuppgiftsincident beträffande säkerhet vid behandling*

90. **DE SA** invände att IE SA:s granskning är bristfällig när det gäller omfattningen av den information som ska lämnas in i samband med en anmälan, vilket fastställs som bindande i artikel 33.3 i den allmänna dataskyddsförordningen. På grundval av TIC:s kommentarer om incidenten som det lämnade i enlighet med artikel 33.5 i den allmänna dataskyddsförordningen samt beskrivningen av utredningen av sakförhållandena i ärendet, uppfyllde TIC uppenbarligen inte fullt ut sin dokumentationsskyldighet när det först rapporterade incidenten den 8 januari 2019. DE SA ansåg därför att det finns många indikationer på att resultatet även skulle kunna utgöra en överträdelse av artikel 33.3 i den allmänna dataskyddsförordningen.

6.2.7 *Överträdelse av artikel 34 i den allmänna dataskyddsförordningen om information om en personuppgiftsincident till den registrerade*

91. **HU SA** invände att IE SA, med tanke på buggen i TIC:s program under årens lopp och dess allvarliga karaktär som påverkar datasäkerheten, var tvungen att undersöka om TIC även bröt mot artikel 34 i den allmänna dataskyddsförordningen när det gäller TIC:s skyldigheter att informera de registrerade om incidenten.

6.3 Den ansvariga tillsynsmyndighetens ståndpunkt avseende invändningarna

92. Den ansvariga tillsynsmyndigheten svarade kollektivt på invändningarna om eventuella ytterligare (eller alternativa) överträdelser av den allmänna dataskyddsförordningen i sitt sammansatta memorandum som delades med de berörda tillsynsmyndigheterna. Den ansvariga tillsynsmyndigheten förklarade att den utövade sin frihet att begränsa utredningens omfattning till att omfatta två separata frågor, nämligen huruvida TIC hade fullgjort sina skyldigheter som personuppgiftsansvarig enligt

artikel 33.1 när det gäller anmälan av incidenten, och huruvida det hade fullgjort sina skyldigheter enligt artikel 33.5 att dokumentera incidenten[91]. Den ansvariga tillsynsmyndigheten hänvisade till avsnitt 110.1 i den irländska dataskyddslagen från 2018, där det föreskrivs att IE SA kan vidta de utredningar som den anser lämpliga att genomföra[92]. Syftet med utredningen, såsom den beskrivs av IE SA, var således endast att undersöka omständigheterna kring TIC:s uppenbart fördröjda anmälan av incidenten och dess dokumentering av densamma, en fråga som IE SA ansåg vara av stor vikt med tanke på att nästan 200 000 incidenter anmäldes under två år i hela EU och att det fanns ett behov av klarhet om vad som krävs enligt anmälnings- och dokumentationskraven i den allmänna dataskyddsförordningen[93].

93. I sitt sammansatta memorandum[94] vidhåller IE SA att invändningar inom ramen för artikel 60.4 i den allmänna dataskyddsförordningen inte kan leda till att omfattningen av en utredning ifrågasätts. I det aktuella fallet påminner den ansvariga tillsynsmyndigheten om att den informerade TIC i början av utredningen om att dess syfte var att kontrollera TIC:s efterlevnad av artikel 33.1 och artikel 33.5 i den allmänna dataskyddsförordningen när det gäller dess anmälan av en incident till den ansvariga tillsynsmyndigheten den 8 januari 2019. Hela utredningsförfarandet, liksom utarbetandet av utkastet till beslut, genomfördes således inom ramen för denna omfattning och TIC gavs rätt att yttra sig i detta avseende i varje skede av förfarandet. Den ansvariga tillsynsmyndigheten vidhåller därför att om den skulle följa de berörda tillsynsmyndigheternas invändningar och inkludera andra överträdelser i sitt slutliga beslut på grundval av endast det material som ingår i utkastet till beslut, skulle detta äventyra hela utredningen och förfarandet enligt artikel 60 genom att utsätta den för risken för påståenden om processuell orättvisa[95].

94. Den ansvariga tillsynsmyndigheten förklarar dessutom att den har en annan pågående utredning i samband med andra personuppgiftsincidenter som TIC anmält till den ansvariga tillsynsmyndigheten före den anmälan som rör ärendet i fråga. I denna andra utredning, som inleddes före den aktuella, betonar den ansvariga tillsynsmyndigheten att utredningens omfattning gäller eventuell bristande efterlevnad av bland annat artiklarna 5, 24, 25, 28, 29 och 32 i den allmänna dataskyddsförordningen[96]. Den ansvariga tillsynsmyndigheten anser att denna parallella utredning verkligen är inriktad på att bedöma huruvida TIC fullgör sina bredare skyldigheter enligt den allmänna dataskyddsförordningen för att avgöra om personuppgiftsincidenterna orsakades av bristande efterlevnad. Den ansvariga tillsynsmyndigheten anser följaktligen att de berörda tillsynsmyndigheterna kommer att ha möjlighet att överväga sådana eventuella överträdelser inom ramen för den andra utredningen, eftersom de kommer att rådfrågas om utkastet till beslut i enlighet med artikel 60.4 i den allmänna dataskyddsförordningen[97].

95. TIC hävdade att eftersom det i utkastet till beslut anges att en ingående granskning av de tekniska och organisatoriska åtgärderna ligger utanför undersökningens räckvidd[98] skulle det inte vara rimligt eller lämpligt, och skulle strida mot väletablerade principer om naturlig rättvisa, om beslutet skulle leda till slutsatser eller sanktioner mot TIC med avseende på skyldigheter och principer som inte ingick i uppgiftsskyddskommissionens utredning, eftersom TIC inte har haft möjlighet att ta upp eventuella

[91] Det sammansatta memorandumet, punkt 1.7.
[92] Det sammansatta memorandumet, punkt 1.5.
[93] Det sammansatta memorandumet, punkt 1.9.
[94] Det sammansatta memorandumet, punkt 5.44.
[95] Det sammansatta memorandumet, punkt 5.44 c.
[96] Det sammansatta memorandumet, punkt 1.10.
[97] Det sammansatta memorandumet, punkt 5.44 d.
[98] Utkastet till beslut, punkt 7.19.

frågor som uppgiftsskyddskommissionen eller berörda tillsynsmyndigheter kan ha om TIC:s processer på dessa områden[99].

6.4 EDPB:s analys

6.4.1 Bedömning av huruvida invändningarna var relevanta och motiverade

6.4.1.1 Överträdelse av artikel 5.1 f i den allmänna dataskyddsförordningen avseende principen om integritet och konfidentialitet

96. EDPB noterar att **DE SA:s** invändning mot artikel 5.1 f i den allmänna dataskyddsförordningen avser huruvida det föreligger en överträdelse av den allmänna dataskyddsförordningen genom att uttrycka en oenighet om de slutsatser som ska dras av resultaten av utredningen. Invändningen innehåller också argument till stöd för slutsatsen att efterlevnaden av artikel 5.1 f i den allmänna dataskyddsförordningen bör bedömas. DE SA:s invändning visar tydligt på betydelsen av de risker som utkastet till beslut innebär för de registrerades rättigheter och friheter, i synnerhet genom att betona att sakförhållandena utgör en betydande och väsentlig kränkning av konfidentialiteten för personuppgifter och att ett stort antal personer berördes under en längre tid. Dessutom hävdade DE SA att det fanns indikationer för att anse att det föreligger ett systemfel, vilket skulle ha krävt en mer djupgående granskning utöver den enskilda specifika buggen i fråga.

97. **HU SA:s** invändning kan också anses vara relevant, eftersom den avser huruvida det föreligger en överträdelse av den allmänna dataskyddsförordningen. Dessutom hänvisar den (endast) kortfattat till faktiska argument till stöd för behovet av att bedöma denna ytterligare bestämmelse (buggens varaktighet och dess allvarliga karaktär som påverkar datasäkerheten), men den visar inte på ett tydligt sätt betydelsen av de risker som utkastet till beslut innebär för enskildas rättigheter och friheter, eftersom den inte lägger fram några argument eller motiveringar beträffande konsekvenserna av att utfärda ett beslut utan de ändringar som föreslås i invändningen[100].

98. EDPB anser därför att invändningen från DE SA om en eventuell ytterligare överträdelse av artikel 5.1 f i den allmänna dataskyddsförordningen är relevant och motiverad i den mening som avses i artikel 4.24 i den allmänna dataskyddsförordningen, men anser att HU SA:s invändning beträffande samma ämne inte uppfyller kraven i artikel 4.24[101].

99. EDPB kommer att bedöma sakförhållandena i de väsentliga frågor som tas upp av DE SA:s invändning i förhållande till en eventuell ytterligare överträdelse av artikel 5.1 f i den allmänna dataskyddsförordningen (se avsnitt 6.4.2 nedan).

[99] Representations in response to objections and comments from CSAs, inlaga av TIC (14 augusti 2020), punkt 4.1. EDPB vill framhålla att de invändningar som framförts av de berörda tillsynsmyndigheterna meddelades TIC av IE SA och TIC utfärdade ovannämnda synpunkter på invändningarna, vilka beaktades av IE SA innan förfarandet enligt artikel 65 inleddes och ingår i de handlingar som beaktas av EDPB inom ramen för detta förfarande. Se även fotnot 19.

[100] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 19.

[101] EDPB tar därför inte ställning till huruvida några väsentliga frågor som tas upp i HU SA:s invändning är välgrundade. EDPB upprepar att dess nuvarande beslut inte påverkar eventuella bedömningar som styrelsen kan komma att uppmanas göra i andra fall, även med samma parter, med beaktande av innehållet i det relevanta utkastet till beslut och de invändningar som framförts av de berörda tillsynsmyndigheterna.

6.4.1.2 Överträdelse av artikel 5.2 i den allmänna dataskyddsförordningen avseende principen om ansvarsskyldighet

100. Den invändning som framförts av **IT SA** ska anses vara ”relevant”, eftersom den om den följs skulle leda till en annan slutsats om huruvida det föreligger en överträdelse av den allmänna dataskyddsförordningen[102]. Mer specifikt innehåller den en ”oenighet om de slutsatser som ska dras av undersökningsresultaten”, eftersom det anges att ”*slutsatserna utgör en överträdelse av en bestämmelse i den allmänna dataskyddsförordningen [...] utöver de som redan analyserats i utkastet till beslut*”[103].

101. Dessutom är invändningen ”motiverad”, eftersom den innehåller förtydliganden om varför ändringen av beslutet föreslås[104]: den föreslagna ändringen bygger på ”*avsaknaden av formaliserade företagsstrategier för hantering av säkerhetsincidenter [...] eller underlåtenhet att följa dessa riktlinjer*”, på det faktum att sådana ”*förfarandemässiga brister uppmärksammas upprepade gånger av [IE SA]*” i utkastet till beslut, och på den personuppgiftsansvariges oförmåga att ange det exakta antalet och arten av de personuppgifter/registrerade som berörs.

102. **IT SA** har tydligt visat betydelsen av de risker som utkastet till beslut medför för de registrerades grundläggande rättigheter och friheter genom att visa ”konsekvenserna som utkastet till beslut skulle ha för de skyddade värdena”[105] och mer specifikt ”inverkan på de registrerades rättigheter och friheter vars personuppgifter kan behandlas i framtiden”[106]: invändningen gjorde det genom att hävda att de nämnda aspekterna är ”*av strukturell karaktär när det gäller den personuppgiftsansvariges organisation” och ”måste ge effekter inte bara på det aktuella fallet utan också på hanteringen av personuppgiftsincidenter som kan inträffa i framtiden*”.

103. Till följd av detta uppfyller IT SA:s invändning mot artikel 5.2 i den allmänna dataskyddsförordningen de krav som anges i artikel 4.24 i den allmänna dataskyddsförordningen. EDPB kommer därför att analysera sakförhållandena i de väsentliga frågor som tas upp i denna invändning[107].

6.4.1.3 Överträdelse av artikel 24 i den allmänna dataskyddsförordningen om den personuppgiftsansvariges ansvar

104. **DE SA:s** invändning hänvisar specifikt till kapitel 5 ”Frågor för avgörande” i utkastet till beslut[108] och invänder mot utkastet till beslut om huruvida även artikel 24 i den allmänna dataskyddsförordningen har överträtts av TIC[109]. Den bygger på de fakta[110] som anges i utkastet till beslut: ”*Om en Twitteranvändare med ett skyddat konto som använder Twitter för Android ändrar sin e-postadress skulle buggen leda till att deras konto inte skyddas.*”[111] Deras skyddade tweetar gjordes därmed tillgängliga för allmänheten via tjänsten. DE SA ifrågasätter närmare bestämt varför IE SA i utkastet till beslut inte undersökte orsakerna till incidenten, särskilt mot bakgrund av artikel 24 i den allmänna

[102] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 13.
[103] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 27.
[104] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 17.
[105] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 37.
[106] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 43.
[107] Se avsnittet 6.4.2 nedan.
[108] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 20.
[109] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 12.
[110] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 14.
[111] Utkastet till beslut, punkt 2.7.

dataskyddsförordningen, och varför IE SA inte förklarade i utkastet till beslut varför den inte gjorde en sådan granskning.

105. DE SA hävdar att eftersom anmälan av incidenten avslöjade ”*brister i efterlevnaden av den allmänna dataskyddsförordningen, ... [a] företag som inte med egna medel och resurser kan inspektera interna eller externa säkerhetsgrupper för att hitta en bugg av denna betydelse och omfattning bör bli föremål för en mer ingående granskning när det gäller dess arrangemang för säkerhet och databehandling, utöver den enda specifika bugg som berörs*”.

106. Enligt DE SA skulle en större granskning av TIC:s databehandlingsinställning ”*i förekommande fall kunna leda till att den personuppgiftsansvarige åläggs att se till att behandlingen överensstämmer med bestämmelserna i den allmänna dataskyddsförordningen. Det aktuella ärendet återspeglar inte denna uppgift. Detta gör det ännu mer angeläget att undersöka de korrigerande befogenheterna enligt artikel 58.2 i den allmänna dataskyddsförordningen i detta sammanhang*”.

107. DE SA påpekade därför vad den ansåg vara en avsaknad av bedömning, med konsekvenserna att de slutsatser som dragits av den ansvariga tillsynsmyndighetens undersökningsresultat skulle kunna vara annorlunda[112].

108. DE SA:s invändning att ”*sanktionsavgifter enligt artikel 83.1 i den allmänna dataskyddsförordningen måste vara ’effektiva, proportionella och avskräckande’ i varje enskilt fall. En sanktion är effektiv och avskräckande om den å ena sidan är lämplig som en allmän förebyggande åtgärd för att avskräcka allmänheten från att begå överträdelser och bekräfta allmänhetens förtroende för unionsrättens giltighet; å andra sidan är den också lämplig som en förebyggande åtgärd för att avskräcka gärningsmannen från att begå ytterligare överträdelser*”. Följaktligen visar DE SA hur den omständighet att inte ändra utkastet till beslut till att omfatta en bedömning av efterlevnaden av artikel 24 i den allmänna dataskyddsförordningen skulle innebära betydande risker för de registrerades grundläggande rättigheter och friheter[113].

109. I sina riktlinjer för begreppet relevant och motiverad invändning godtar EDPB att en invändning kan ifrågasätta den ansvariga tillsynsmyndighetens slutsats genom att anse att den ansvariga tillsynsmyndighetens slutsatser faktiskt leder till slutsatsen att en annan bestämmelse i den allmänna dataskyddsförordningen har överträtts, utöver eller i stället för den bestämmelse som den ansvariga tillsynsmyndigheten identifierat[114]. EDPB anser att detta är kärnan i DE SA:s invändning, och därmed inte hindrar den från att vara relevant och motiverad.

110. Dessutom visar DE SA:s invändning tydligt betydelsen av de risker som utkastet till beslut innebär för de registrerades rättigheter och friheter, bland annat genom att betona att ett stort antal personer berördes under lika lång tid, vilket återspeglar ett systemfel som kräver en djupare granskning som går utöver den enskilda specifika bugg som berörs. Till följd av detta uppfyller DE SA:s invändning mot artikel 24 i den allmänna dataskyddsförordningen det tröskelvärde som anges i artikel 4.24 i den allmänna dataskyddsförordningen.

111. Mot bakgrund av ovanstående bedömning anser EDPB att DE SA:s invändning om en eventuell överträdelse av artikel 24 i den allmänna dataskyddsförordningen är relevant och motiverad i enlighet med artikel 4.24 i den allmänna dataskyddsförordningen. Som en följd av detta bedömer EDPB fördelarna med de väsentliga frågor som tas upp i denna invändning (se avsnitt 6.4.2 nedan).

[112] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 29.
[113] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 19.
[114] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 27.

6.4.1.4 Överträdelse av artikel 28 i den allmänna dataskyddsförordningen om förhållandet till personuppgiftsbiträden

112. **FR SA:s** invändning hänvisar specifikt till punkterna 7.129 iii, iv och v i utkastet till beslut[115] och invänder mot utkastet till beslut om huruvida artikel 28 i den allmänna dataskyddsförordningen har överträtts av TIC i stället för artikel 33.1 i den allmänna dataskyddsförordningen[116]. Den bygger på de fakta[117] som anges i utkastet till beslut och på den ansvariga tillsynsmyndighetens slutsatser att ”TIC inte respekterade den personuppgiftsansvariges skyldighet att kontrollera giltigheten av de förfaranden som personuppgiftsbiträdet inrättat”.

113. Enligt FR SA borde resultaten, eftersom artikel 28.3 h i den allmänna dataskyddsförordningen fastställer den personuppgiftsansvariges skyldigheter när den använder ett personuppgiftsbiträde, ha lett den ansvariga tillsynsmyndigheten till slutsatsen att artikel 28.3 h i den allmänna dataskyddsförordningen har överträtts i stället för artikel 33.1 i den allmänna dataskyddsförordningen. I slutändan innebär det för FR SA att den påföljd som utfärdas som sanktionsavgift bör ta itu med olika överträdelser.

114. I sina riktlinjer för begreppet relevant och motiverad invändning godtar EDPB att en invändning kan ifrågasätta den ansvariga tillsynsmyndighetens slutsats genom att anse att den ansvariga tillsynsmyndighetens slutsatser faktiskt leder till slutsatsen att en annan bestämmelse i den allmänna dataskyddsförordningen har överträtts, utöver eller i stället för den bestämmelse som den ansvariga tillsynsmyndigheten identifierat[118]. EDPB anser att detta är kärnan i FR SA:s invändning, och därmed inte hindrar den från att vara relevant. Invändningen innehåller också tillräckliga argument till stöd för den föreslagna slutsatsen. Samtidigt noterar EDPB att FR SA:s invändning inte tydligt visar de betydande risker som utkastet till beslut innebär för de registrerades grundläggande rättigheter och friheter, särskilt när det gäller underlåtenheten att dra slutsatser om överträdelsen av denna särskilda bestämmelse[119]. Mot bakgrund av denna bedömning anser EDPB att FR SA:s invändning om en eventuell överträdelse av artikel 28 i den allmänna dataskyddsförordningen i stället för artikel 33.1 i den allmänna dataskyddsförordningen inte är relevant eller motiverad i enlighet med artikel 4.24 i den allmänna dataskyddsförordningen[120].

115. IT SA:s invändningar mot utkastet till beslut om huruvida bland annat artikel 28 i den allmänna dataskyddsförordningen överträddes av TIC utöver artikel 33.1 i den allmänna dataskyddsförordningen[121].

116. IT SA förlitar sig på de faktiska omständigheter som anges i utkastet till beslut och på den ansvariga myndighetens slutsatser att även om det globala dataskyddsombudets deltagande i dess personuppgiftsansvariges detektions- och insatsgrupp, Twitter, Inc., planeras ingå i TIC:s interna policy, var det globala dataskyddsombudet i praktiken inte involverat. IT SA noterar också att Twitter, Inc., i egenskap av personuppgiftsansvarig, inte har hjälpt TIC.

---

[115] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 20.
[116] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 12.
[117] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 14.
[118] Invändningsriktlinjer för begreppet relevant och motiverad invändning, punkt 27.
[119] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 29.
[120] EDPB tar därför inte ställning till huruvida några väsentliga frågor som tas upp i dessa invändningar är välgrundade. EDPB upprepar att dess nuvarande beslut inte påverkar eventuella bedömningar som styrelsen kan komma att uppmanas göra i andra fall, även med samma parter, med beaktande av innehållet i det relevanta utkastet till beslut och de invändningar som framförts av de berörda tillsynsmyndigheterna.
[121] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 12.

117. Enligt IT SA, artikel 28.1 i den allmänna dataskyddsförordningen, enligt vilken personuppgiftsansvariga endast får använda personuppgiftsbiträden som ger tillräckliga garantier för att genomföra lämpliga tekniska och organisatoriska åtgärder, och artikel 28.3 f i den allmänna dataskyddsförordningen som kräver att avtalet mellan den personuppgiftsansvarige och personuppgiftsbiträdet föreskriver att personuppgiftsbiträdet ska hjälpa ”den personuppgiftsansvarige att säkerställa att skyldigheterna enligt artiklarna 32–36 fullgörs, med beaktande av behandlingens art och den information som är tillgänglig för personuppgiftsbiträdet”. Resultaten borde ha föranlett den ansvariga tillsynsmyndigheten att dra slutsatsen att även artikel 28.1 och artikel 28.3 f i den allmänna dataskyddsförordningen har överträtts.

118. EDPB anser att IT SA:s invändning avseende artikel 28.1 och artikel 28.3 f i den allmänna dataskyddsförordningen ska anses vara ”relevant”, eftersom den om den följs skulle leda till en annan slutsats om huruvida det föreligger en överträdelse av den allmänna dataskyddsförordningen[122]. Mer specifikt innehåller den en ”oenighet om de slutsatser som ska dras av undersökningsresultaten”, eftersom det anges att ”slutsatserna utgör en överträdelse av en bestämmelse i den allmänna dataskyddsförordningen [...] utöver de som redan analyserats i utkastet till beslut”[123].

119. Enligt EDPB är invändningen dessutom ”motiverad”, eftersom den innehåller förtydliganden om varför ändringen av beslutet föreslås[124]: den föreslagna ändringen förlitar sig på det faktum att den personuppgiftsansvarige inte följde sina interna policyer enligt vilka TIC:s dataskyddsombud skulle involveras. Invändningen gäller dessutom att personuppgiftsbiträdet inte har fullgjort sin avtalsenliga skyldighet att bistå den personuppgiftsansvarige, i enlighet med artikel 28.3 f i den allmänna dataskyddsförordningen.

120. EDPB noterar dock att IT SA:s invändning avseende artikel 28.1 och artikel 28.3 f i den allmänna dataskyddsförordningen inte tydligt visar att utkastet till beslut innebär betydande risker för de registrerades grundläggande rättigheter och friheter[125]. Detta innebär att denna invändning från IT SA inte uppfyller kraven i artikel 4.24 i den allmänna dataskyddsförordningen[126].

6.4.1.5 Överträdelse av artikel 32 i den allmänna dataskyddsförordningen om säkerheten vid behandling

121. **DE SA:s** invändning, om den följs, skulle medföra en ändring som leder till en annan slutsats om huruvida det föreligger en överträdelse av den allmänna dataskyddsförordningen, eftersom den identifierade en ”*oenighet om de slutsatser som ska dras av utredningsresultaten*”[127] genom att påpeka att slutsatserna kan tyda på en överträdelse också av artikel 32 i den allmänna dataskyddsförordningen. EDPB anser därför att det finns ett samband mellan innehållet i invändningen och den eventuella avvikande slutsatsen[128]. Denna invändning rör dessutom det specifika rättsliga och faktiska innehållet i utkastet till beslut[129].

[122] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 13.
[123] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 27.
[124] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 17.
[125] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 29.
[126] EDPB tar därför inte ställning till huruvida några väsentliga frågor som tas upp i dessa invändningar är välgrundade. EDPB upprepar att dess nuvarande beslut inte påverkar eventuella bedömningar som styrelsen kan komma att uppmanas göra i andra fall, även med samma parter, med beaktande av innehållet i det relevanta utkastet till beslut och de invändningar som framförts av de berörda tillsynsmyndigheterna.
[127] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 28.
[128] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 13.
[129] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 14.

122. Dessutom visar DE SA:s invändning tydligt betydelsen av de risker som utkastet till beslut innebär för de registrerades rättigheter och friheter, särskilt genom att betona att sakförhållandena utgör en ”betydande” och ”väsentlig” kränkning av sekretessen för personuppgifter och att ett stort antal personer berördes under en avsevärd tidsperiod. Dessutom hävdade DE SA att det fanns tecken på att det fanns ett ”systemfel”, vilket skulle ha krävt en djupare granskning utöver den enskilda specifika buggen i fråga.

123. Mot bakgrund av ovanstående bedömning anser EDPB att DE SA:s invändning om en eventuell överträdelse av artikel 32 i den allmänna dataskyddsförordningen är relevant och motiverad i enlighet med artikel 4.24 i den allmänna dataskyddsförordningen. Som en följd av detta bedömer EDPB fördelarna med de väsentliga frågor som tas upp i denna invändning (se punkt 6.4.2 nedan).

124. När det gäller **FR SA:s** invändning anser EDPB att den uppfyller kriteriet ”relevant”, eftersom om den ansvariga tillsynsmyndigheten skulle ha följt den skulle slutsatsen ha varit en annan om huruvida det föreligger en överträdelse av den allmänna dataskyddsförordningen[130]. FR SA:s invändning grundar sig på IE SA:s resonemang i utkastet till beslut, och detta resonemang är kopplat till slutsatsen om huruvida en överträdelse av den allmänna dataskyddsförordningen har identifierats korrekt[131]. EDPB erinrar om att den behöriga tillsynsmyndigheten måste lägga fram de fakta som påstås leda till en annan slutsats[132] och noterar att invändningen i det aktuella fallet analyserar de fakta som skulle leda till en överträdelse av artikel 32.1 d i den allmänna dataskyddsförordningen, i stället för en överträdelse av artikel 33.1 i samma förordning, och gör detta på ett konsekvent, tydligt och precist sätt, genom att tydligt ange vilka delar av IE SA:s beslut som den motsätter sig. FR SA:s invändning är tydligt relevant genom att den beskriver en oenighet om huruvida en överträdelse av den allmänna dataskyddsförordningen har ägt rum. FR SA:s invändning förklarar dock endast kortfattat skälen till den föreslagna ändringen och visar inte tydligt hur betydande riskerna med utkastet till beslut är när det gäller de registrerades grundläggande rättigheter och friheter i förhållande till underlåtenheten att konstatera en överträdelse av artikel 32 i den allmänna dataskyddsförordningen. Detta innebär att denna invändning från FR SA inte uppfyller kraven i artikel 4.24 i den allmänna dataskyddsförordningen[133].

125. **HU SA**:s invändning hänvisade också till huruvida det föreligger en överträdelse av den allmänna dataskyddsförordningen och hävdade att ett eventuellt åsidosättande av principen om integritet och konfidentialitet också bör utredas. HU SA:s invändning är tydligt relevant genom att det anges att ytterligare en bestämmelse i den allmänna dataskyddsförordningen (dvs. artikel 32 i den allmänna dataskyddsförordningen) borde ha undersökts. HU SA förklarar dock inte hur utkastet till beslut skulle innebära sådana risker och förklarar inte heller till fullo varför specifika aspekter av beslutet är bristfälliga ur dess synvinkel[134]. HU SA:s invändning uppfyller inte kravet på en välgrundad motivering av sin invändning genom att hänvisa till rättsliga eller faktiska argument. Tvärtom rekommenderar den endast att IE SA också skulle behöva undersöka den personuppgiftsansvariges efterlevnad av artikel 32

[130] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 13.
[131] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 16.
[132] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 18.
[133] EDPB tar därför inte ställning till huruvida några väsentliga frågor som tas upp i dessa invändningar är välgrundade. EDPB upprepar att dess nuvarande beslut inte påverkar eventuella bedömningar som styrelsen kan komma att uppmanas göra i andra fall, även med samma parter, med beaktande av innehållet i det relevanta utkastet till beslut och de invändningar som framförts av de berörda tillsynsmyndigheterna.
[134] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 18.

i den allmänna dataskyddsförordningen. Den invändning som framförts av HU SA uppfyller följaktligen inte kraven i artikel 4.24 i den allmänna dataskyddsförordningen[135].

6.4.1.6 Överträdelse av artikel 33.3 i den allmänna dataskyddsförordningen om innehållet i anmälan av en personuppgiftsincident beträffande säkerhet vid behandling

126. **DE SA** anser att utkastet till beslut anger att artikel 33.3 i den allmänna dataskyddsförordningen kan överträdas utöver andra bestämmelser i den allmänna dataskyddsförordningen. I detta avseende handlar det om ”huruvida det föreligger en överträdelse” av den allmänna dataskyddsförordningen och att den inte har granskats eller behandlats i utkastet till beslut. DE SA anser därför att utkastet till beslut, om det ändras, skulle leda till slutsatsen om ytterligare överträdelser av den allmänna dataskyddsförordningen.

127. DE SA visar dock inte tydligt på de betydande risker som utkastet till beslut innebär för de registrerades grundläggande rättigheter och friheter. Till följd av detta uppfyller inte DE SA:s invändning mot artikel 33.3 i den allmänna dataskyddsförordningen de krav som anges i artikel 4.24 i den allmänna dataskyddsförordningen[136].

6.4.1.7 Överträdelse av artikel 34 i den allmänna dataskyddsförordningen om information om en personuppgiftsincident till den registrerade

128. **HU SA** anser att utkastet till beslut anger att artikel 34 i den allmänna dataskyddsförordningen kan överträdas utöver andra bestämmelser i den allmänna dataskyddsförordningen, särskilt mot bakgrund av att buggen varade under årens lopp och med tanke på den allvarliga karaktär som påverkar den personuppgiftsansvariges säkerhet. I detta avseende handlar det om ”huruvida det föreligger en överträdelse” av den allmänna dataskyddsförordningen och att den inte har granskats eller behandlats i utkastet till beslut. HU SA anser därför att utkastet till beslut, om det ändras, skulle leda till slutsatsen om ytterligare överträdelser av den allmänna dataskyddsförordningen.

129. HU SA visar dock inte tydligt på de betydande risker som utkastet till beslut innebär för de registrerades grundläggande rättigheter och friheter. HU SA:s invändning mot artikel 34 i den allmänna dataskyddsförordningen uppfyller följaktligen inte kraven i artikel 4.24 i den allmänna dataskyddsförordningen[137].

[135] EDPB tar därför inte ställning till huruvida några väsentliga frågor som tas upp i dessa invändningar är välgrundade. EDPB upprepar att dess nuvarande beslut inte påverkar eventuella bedömningar som styrelsen kan komma att uppmanas göra i andra fall, även med samma parter, med beaktande av innehållet i det relevanta utkastet till beslut och de invändningar som framförts av de berörda tillsynsmyndigheterna.

[136] EDPB tar därför inte ställning till huruvida några väsentliga frågor som tas upp i dessa invändningar är välgrundade. EDPB upprepar att dess nuvarande beslut inte påverkar eventuella bedömningar som styrelsen kan komma att uppmanas göra i andra fall, även med samma parter, med beaktande av innehållet i det relevanta utkastet till beslut och de invändningar som framförts av de berörda tillsynsmyndigheterna.

[137] EDPB tar därför inte ställning till huruvida några väsentliga frågor som tas upp i dessa invändningar är välgrundade. EDPB upprepar att dess nuvarande beslut inte påverkar eventuella bedömningar som styrelsen kan komma att uppmanas göra i andra fall, även med samma parter, med beaktande av innehållet i det relevanta utkastet till beslut och de invändningar som framförts av de berörda tillsynsmyndigheterna.

6.4.2 Bedömning av huruvida den eller de väsentliga frågor som tagits upp i de relevanta och motiverade invändningarna och slutsatserna är välgrundade

130. Nämnden analyserar nu de invändningar som konstaterats vara relevanta och motiverade – särskilt DE SA:s invändningar mot artiklarna 5.1 f, 24 och 32 i den allmänna dataskyddsförordningen samt IT SA:s invändning mot artikel 5.2 i den allmänna dataskyddsförordningen – samt den ansvariga tillsynsmyndighetens svar på dessa invändningar och TIC:s inlagor.

131. I enlighet med artikel 65.1 a i den allmänna dataskyddsförordningen ska EDPB inom ramen för ett tvistlösningsförfarande fatta ett bindande beslut om alla frågor som är föremål för de relevanta och motiverade invändningarna, särskilt huruvida det föreligger en överträdelse av den allmänna dataskyddsförordningen. EDPB kan (och måste) fatta ett bindande beslut som när så är möjligt, med beaktande av handlingarna i ärendet och svarandens rätt att bli hörd, ska innehålla en slutlig slutsats om tillämpningen av den allmänna dataskyddsförordningen i det aktuella ärendet. Den ansvariga tillsynsmyndigheten kommer då att vara skyldig att genomföra ändringarna i sitt slutliga beslut.

132. Styrelsen anser att de tillgängliga faktauppgifterna i utkastet till beslut och i invändningarna inte är tillräckliga för att EDPB ska kunna fastställa förekomst av ytterligare (eller alternativa) överträdelser av artiklarna 5.1 f, 5.2, 24 eller 32 i den allmänna dataskyddsförordningen.

133. Styrelsen anser att IE SA:s begränsade utredning – som sedan början endast inriktades på huruvida TIC hade gjort sig skyldig till överträdelser av artikel 33.1 och 33.5 i den allmänna dataskyddsförordningen – har en direkt inverkan på utredningens ansvarsområde och ytterligare faktaresultat samt på de berörda tillsynsmyndigheternas möjlighet att lägga fram tillräckliga uppgifter för att EDPB ska kunna stödja invändningarna.

134. EDPB erinrar om den ansvariga tillsynsmyndighetens skyldighet att ”sträva efter att nå samförstånd” med de berörda tillsynsmyndigheterna (artikel 60.1 i den allmänna dataskyddsförordningen) och att utan dröjsmål förse de berörda tillsynsmyndigheterna med ”relevant information” i frågan (artikel 60.3 i den allmänna dataskyddsförordningen). Även vid en undersökning på eget initiativ anges i riktlinjerna för motiverade och relevanta invändningar att den ansvariga tillsynsmyndigheten ”bör sträva efter samförstånd om förfarandets omfattning (dvs. de aspekter av uppgiftsbehandling som granskas) innan förfarandet inleds formellt”[138], även i samband med ett eventuellt nytt förfarande.

135. EDPB anser visserligen att tillsynsmyndigheterna har ett visst utrymme för skönsmässig bedömning när det gäller att bestämma hur deras utredningar ska utformas, men EDPB påminner om att ett av huvudsyftena med den allmänna dataskyddsförordningen är att säkerställa enhetlighet i hela Europeiska unionen, och att samarbetet mellan den ansvariga tillsynsmyndigheten och de berörda tillsynsmyndigheterna är ett av sätten att uppnå detta. EDPB erinrar också om att det finns en fullständig uppsättning av de samarbetsverktyg som föreskrivs i den allmänna dataskyddsförordningen (inbegripet artiklarna 61 och 62 i den förordningen), med beaktande av målet att nå samförstånd inom samarbetsmekanismen och behovet av att utbyta all relevant information, i syfte att säkerställa skyddet av de registrerades grundläggande fri- och rättigheter.

[138] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 28.

136. EDPB anser att vid fastställandet av utredningens omfattning, även om den kan vara begränsad, bör en ansvarig tillsynsmyndighet utforma den på ett sådant sätt att den gör det möjligt för de berörda tillsynsmyndigheterna att effektivt fullgöra sin roll, tillsammans med den ansvariga tillsynsmyndigheten, vid fastställandet av huruvida det har skett en överträdelse av den allmänna dataskyddsförordningen.

7 OM DE KORRIGERANDE ÅTGÄRDER SOM BESLUTATS AV DEN ANSVARIGA TILLSYNSMYNDIGHETEN – SÄRSKILT INFÖRANDET AV EN REPRIMAND

7.1 Den ansvariga tillsynsmyndighetens analys i utkastet till beslut

137. I utkastet till beslut förklaras att medan de föreslagna korrigerande befogenheterna i det preliminära utkastet till beslut både var en reprimand, i enlighet med artikel 58.2 b i den allmänna dataskyddsförordningen, och en administrativ sanktionsavgift, i enlighet med artikel 58.2 i i den allmänna dataskyddsförordningen, består det slutliga utkastet till beslut endast av en administrativ sanktionsavgift för TIC som personuppgiftsansvarig[139].

138. I sina inlagor avseende det preliminära utkastet till beslut invände TIC mot beslutet att utfärda en reprimand och hävdade att överträdelserna av artikel 33.1 och artikel 33.5 i den allmänna dataskyddsförordningen inte omfattar ”behandlingsverksamhet”, medan artikel 58.2 b i den förordningen ger tillsynsmyndigheterna befogenhet att utfärda reprimander om behandlingsverksamhet har överträtt bestämmelserna i den allmänna dataskyddsförordningen[140]. TIC:s argument grundade sig huvudsakligen på det faktum att varken förseningen av anmälan till tillsynsmyndigheten eller underlåtenheten att föra lämpliga register utgör en behandling i sig[141].

139. I sitt utkast till beslut förklarade IE SA sitt beslut att inte utfärda någon reprimand genom att påminna om TIC:s argument i dess inlagor om det preliminära utkastet till beslut och hävdade att överträdelserna av artikel 33.1 och 33.5 i den allmänna dataskyddsförordningen inte omfattar ”behandlingsverksamhet”, medan artikel 58.2 b i den allmänna dataskyddsförordningen ger tillsynsmyndigheterna befogenhet att utfärda reprimander när behandling har skett i strid med bestämmelserna i den allmänna dataskyddsförordningen[142]. IE SA ansåg att termen ”behandlingsverksamhet(er)” förekommer 50 gånger i den allmänna dataskyddsförordningen och verkar användas för att beteckna behandling eller användning av, med andra ord saker som görs med, personuppgifter som kontrolleras av en personuppgiftsansvarig, men att definitionen av ”behandling” i den allmänna dataskyddsförordningen samtidigt är mycket bred, vilket gör det möjligt att hävda att med tanke på att en incident är något som påverkar eller görs med personuppgifter, följer det att underrättelseskyldigheten (i den mån den till sin natur har samband med undersökningen av vad som har hänt med personuppgifterna eller hur de har påverkats) har samband med en eller flera behandlingsverksamheter[143]. IE ansåg inte att det var nödvändigt att slutgiltigt dra några slutsatser om innebörden eller effekten av termen ”behandlingsverksamhet” i utkastet till beslut, men ”på det hela

[139] Utkastet till beslut, punkt 12.1.
[140] TIC:s argument avseende det preliminära utkastet till beslut, punkt 11.1.
[141] Utkastet till beslut, punkt 12.4.
[142] TIC:s argument avseende det preliminära utkastet till beslut, punkt 11.1.
[143] Utkastet till beslut, punkt 12.5.

taget” ansåg man att TIC:s rättsliga argument var ”märkbart” och beslutade att inte gå vidare med utfärdandet av en reprimand till TIC[144].

7.2 Sammanfattning av invändningarna från de berörda tillsynsmyndigheterna

140. **DE SA** invände mot att endast en sanktionsavgift ingick i utkastet till beslut, trots att både en reprimand och en sanktionsavgift planerades i det preliminära utkastet till beslut. DE SA instämde inte i IE SA:s resonemang om beslutet att inte införa en reprimand. Enligt DE SA är det rättsliga resonemang som den ansvariga tillsynsmyndigheten godtog inte övertygande, eftersom den rättsliga tolkningen inte bara kräver en granskning av bestämmelsens ordalydelse, utan även av dess innebörd och syfte, dess utveckling och dess systematiska integrering i hela lagstiftningskomplexet.

7.3 Den ansvariga tillsynsmyndighetens ståndpunkt avseende invändningarna

141. I sitt sammansatta memorandum ansåg IE SA att medan DE SA:s invändning avser ”huruvida planerade åtgärder i förhållande till en personuppgiftsansvarig eller ett personuppgiftsbiträde är förenliga med [den allmänna dataskyddsförordningen]”, visar den inte hur ett uteblivet utfärdande av en reprimand till TIC skulle kunna leda till betydande risker för de registrerade[145] när det gäller beslutet att inte utfärda en reprimand, inte var relevant eller motiverat i enlighet med artikel 4.24 i den allmänna dataskyddsförordningen.

142. Trots detta tog den ansvariga tillsynsmyndigheten ställning till den/de väsentliga frågorna i invändningarna och förklarade att den beaktade termen ”behandlingsverksamhet” i enlighet med dess innebörd och tillämpning i hela den allmänna dataskyddsförordningen, och noterade att denna term endast används för tillsynsmyndigheternas befogenheter enligt artikel 58 i den allmänna dataskyddsförordningen. Till följd av TIC:s synpunkter i sitt svar på de berörda tillsynsmyndigheternas invändningar på denna punkt beslutade den ansvariga tillsynsmyndigheten, med beaktande av omfattningen på den utredning som fokuserade på den personuppgiftsansvariges skyldigheter i samband med anmälan av incident, att dess utredning ”*inte inbegrep konstaterandet att den bakomliggande ’behandlingsverksamheten’ avseende incidenten stred mot […]* den allmänna dataskyddsförordningen”[146]. Den ansvariga tillsynsmyndigheten ansåg därför att det inte fanns någon anledning att ompröva sitt beslut att inte utfärda någon reprimand mot bakgrund av DE SA:s invändning.

143. Den ansvariga tillsynsmyndigheten noterade att dess ståndpunkt i utkastet till beslut att inte utfärda en reprimand endast är tillämplig på de särskilda omständigheterna i detta fall. Detta påverkar därför inte framtida beslut om reprimander som kan fattas av den ansvariga tillsynsmyndigheten eller någon annan berörd tillsynsmyndighet[147].

[144] Utkastet till beslut, punkt 12.5. TIC:s övriga separata argument om skälen till varför införandet av en reprimand inte ansågs lämpligt (TIC:s synpunkter avseende det preliminära utkastet till beslut, punkterna 11.2–11.4) behandlades inte separat mot bakgrund av ovannämnda beslut (utkastet till beslut, punkt 12.6).
[145] Det sammansatta memorandumet, punkt 5.79.
[146] Det sammansatta memorandumet, punkt 5.78.
[147] Det sammansatta memorandumet, punkt 5.78.

7.4 EDPB:s analys

7.4.1 Bedömning av huruvida invändningarna var relevanta och motiverade

144. **DE SA:s** invändning avser den planerade åtgärdens förenlighet med den allmänna dataskyddsförordningen, eftersom den anger vilka korrigerande åtgärder som enligt dess uppfattning skulle vara lämpliga för den ansvariga tillsynsmyndigheten att inkludera i det slutliga beslutet: det är därför en relevant invändning som på ett tillfredsställande sätt visar den avvikande slutsats som föreslagits. Dessutom innehåller den ett rättsligt resonemang som stöder dess uppfattning och föreslår en alternativ rättslig tolkning. Invändningen visar dock inte tydligt hur stor risk utkastet till beslut innebär för de registrerades rättigheter och friheter och/eller det fria flödet av personuppgifter. I synnerhet ger den ingen motivering till hur underlåtenheten att införa en reprimand i detta specifika fall – där en sanktionsavgift också utdöms – kan utlösa risker för de registrerades grundläggande rättigheter och friheter.

7.4.2 Slutsats

145. EDPB anser att denna invändning inte uppfyller kraven i artikel 4.24 i den allmänna dataskyddsförordningen.

146. EDPB noterar att den ansvariga tillsynsmyndighetens ståndpunkt att inte utfärda en reprimand endast är tillämplig på de särskilda omständigheterna i detta fall. Detta påverkar därför inte framtida beslut om reprimander som kan fattas av den ansvariga tillsynsmyndigheten eller någon annan berörd tillsynsmyndighet[148].

147. Som tidigare nämnts påverkar inte EDPB:s beslut att inte bedöma sakinnehållet i den invändning som gjorts framtida beslut av EDPB i samma eller liknande frågor.

8 OM KORRIGERANDE ÅTGÄRDER – SÄRSKILT BERÄKNINGEN AV DEN ADMINISTRATIVA SANKTIONSAVGIFTEN

8.1 Den ansvariga tillsynsmyndighetens analys i utkastet till beslut

148. I utkastet till beslut förklaras hur IE SA har beaktat kriterierna i artikel 83.2 i den allmänna dataskyddsförordningen när den fattar beslut om huruvida en administrativ sanktionsavgift ska åläggas och hur dess belopp ska fastställas[149].

149. När det gäller beräkningen av sanktionsavgiften analyseras i utkastet till beslut först **överträdelsens karaktär, svårighetsgrad och varaktighet**, i enlighet med artikel 83.2 a i den allmänna dataskyddsförordningen[150]. I utkastet till beslut togs hänsyn till ”*behandlingens karaktär, omfattning eller syfte*” genom att hänvisa till den typ av behandling som utfördes av Twitter (en plattform för mikrobloggning och sociala medier där användarna har möjlighet att dokumentera sina tankar i tweetar), till den typ av behandling som gav upphov till incidenten (till följd av en bugg som ledde till

[148] Det sammansatta memorandumet, punkt 5.78.
[149] Utkastet till beslut, punkterna 14.1–14.62.
[150] I artikel 83.2 a i den allmänna dataskyddsförordningen hänvisas till ”*[ö]verträdelsens 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*”.

att de tidigare ”skyddade” tweetarna blev ”oskyddade” och allmänt tillgängliga – i de fall där Android-användare hade ändrat e-postadressen) och till omfattningen av behandlingen (buggen påverkade minst 88 726 EU-/EES-användare, eftersom fler personer påverkades mellan datumet för buggen den 4 november 2014 och dess fullständiga åtgärdande den 14 januari 2019, men det var inte möjligt att identifiera alla)[151].

150. Utkastet till beslut tog också hänsyn till **antalet registrerade som berördes och omfattningen av den skada som de lidit**[152] genom att dra slutsatsen att antalet registrerade som potentiellt skulle ha kunnat påverkas av det försenade meddelandet och risken för skada för registrerade till följd av tillsynsmyndighetens försenade bedömning var relevanta faktorer att beakta[153]. Det erinrades om att konsekvenserna för enskilda användare och risken för skada till följd av detta kommer att påverka nivån på och arten av de personuppgifter som offentliggörs och att det åtminstone fanns en risk för skada för registrerade i samband med att avhjälpande åtgärder försenades[154]. IE SA:s ståndpunkt i det preliminära utkastet var att ”*även om TIC inte hade bekräftat den exakta karaktären hos de uppgifter som offentliggjordes vid incidenten, var det rimligt att dra slutsatsen att vissa av de personuppgifter som offentliggjordes i samband med incidenten, med tanke på omfattningen av de berörda användarna och arten av den tjänst som TIC erbjuder, skulle åtminstone vissa användare ha omfattat känsliga kategorier av uppgifter och annat särskilt privat material*”[155]. Denna ståndpunkt nyanserades ytterligare i utkastet till beslut mot bakgrund av TIC:s inlagor, eftersom IE SA beslutade att ”*denna faktor bör tillmätas mindre vikt*”, på grundval av det faktum att ”*även om det inte slutgiltigt kan sägas att inga användare som berördes av incidenten påverkades av den försenade anmälan, fanns det inga direkta bevis för att de lidit skada till följd av den försenade anmälan*”[156].

151. När det gäller **överträdelsens art**, framhölls i utkastet till beslut att överträdelserna av artikel 33.1 och 33.5 i den allmänna dataskyddsförordningen inte rör den materiella frågan om incidenten[157]. IE SA ansåg också att skyldigheterna enligt artikel 33.1 och 33.5 i den allmänna dataskyddsförordningen är av sådan art att efterlevnad är av avgörande betydelse för tillsynsmyndighetens övergripande funktion när det gäller både den specifika frågan om personuppgiftsincidenter men även identifieringen och bedömningen av mer omfattande frågor om personuppgiftsansvarigas bristande efterlevnad, och att bristande fullgörande av sådana skyldigheter får allvarliga konsekvenser eftersom det riskerar att undergräva tillsynsmyndigheternas effektiva utövande av sina funktioner enligt den allmänna dataskyddsförordningen[158].

152. När det gäller **hur allvarlig överträdelsen** av artikel 33.1 i den allmänna dataskyddsförordningen var tog utkastet till beslut hänsyn till hur den stred mot det övergripande syftet med att anmäla en personuppgiftsincident till tillsynsmyndigheten, det faktum att ingen materiell skada påvisades för de registrerade, det faktum att TIC:s korrigerande åtgärder begränsades till framåtblickande åtgärder för att stänga buggen (och inte var en bakåtblickande analys för att identifiera riskerna för de registrerade till följd av överträdelsen) och TIC:s uppenbara underlåtenhet att genomföra en formell

[151] Utkastet till beslut, punkt 14.2.
[152] Utkastet till beslut, punkterna 14.3–14.5.
[153] Utkastet till beslut, punkt 14.5.
[154] Punkt 14.5 i utkastet till beslut (i utkastet till beslut konstateras följande: ”Konsekvenserna för enskilda användare och risken för skada till följd av detta kommer att bero på nivån på de personuppgifter som offentliggörs och även på typen av personuppgifter.”).
[155] Utkastet till beslut, punkt 14.5.
[156] Utkastet till beslut, punkt 14.5.
[157] Utkastet till beslut, punkt 14.6.
[158] Utkastet till beslut, punkt 14.11.

riskbedömning[159]. I utkastet till beslut ansågs inte TIC:s påstående att incidenten berodde på ett isolerat misslyckande (vilket ledde till förseningen av anmälan till dataskyddsombudet) vara tillräckligt viktigt för att minska överträdelsens svårighetsgrad (men tog hänsyn till incidentens isolerade karaktär, till skillnad från den preliminära uppfattningen i det preliminära utkastet att incidenten var ett tecken på en bredare, mer systemrelaterad fråga)[160]. När det gäller svårighetsgraden hos överträdelsen av artikel 33.5 i den allmänna dataskyddsförordningen betonades i utkastet till beslut att det krävs ordentlig dokumentation av incidenter för att göra det möjligt för en tillsynsmyndighet att kontrollera den personuppgiftsansvariges efterlevnad av artikel 33 i den allmänna dataskyddsförordningen[161] och att IE SA var skyldig att ta upp flera frågor för att få klarhet om sakförhållandena kring anmälan av incidenten[162], men det medgavs att bristerna i dokumentationen berodde på en felaktig uppfattning av kraven i god tro (som dock tydligt framgår av bestämmelsens lydelse)[163]. I utkastet till beslut drogs slutsatsen att varje överträdelse låg på ”*låg till måttlig nivå*”[164].

153. När det gäller **överträdelsens varaktighet** enligt artikel 33.1 i den allmänna dataskyddsförordningen ansågs i utkastet till beslut att det rörde sig om en period på två dagar och den utvärderades mot bakgrund av den övergripande tidsram som generellt tillåts för anmälningar av incidenter (72 timmar), och det konstaterades att det inte rörde sig om en obetydlig eller oansenlig period[165]. När det gäller överträdelsens varaktighet enligt artikel 33.5 i den allmänna dataskyddsförordningen drogs i utkastet till beslut slutsatsen att den var löpande[166].

154. När det gäller **artikel 83.2 b i den allmänna dataskyddsförordningen** (om överträdelsen skett med uppsåt eller genom oaktsamhet) drog IE SA i sitt utkast till beslut slutsatsen att TIC:s överträdelse av artikel 33.1 i den allmänna dataskyddsförordningen[167] skett genom **oaktsamhet**, och angav att förseningen i anmälan från det globala dataskyddsombudet berodde på att en del av Twittergruppens interna protokoll inte hade slutförts som föreskrivet och på att protokollet inte var så tydligt som det hade kunnat vara[168]. Detta ledde till slutsatsen att förseningen berodde på oaktsamhet från den personuppgiftsansvariges sida, men TIC:s påstående att den försenade anmälan inte var ett tecken på ett bredare systemproblem utan utgjorde en enstaka händelse godtogs[169]. IE SA fann inga bevis för ett uppsåtligt beteende med avseende på överträdelsen av artikel 33.1 i den allmänna dataskyddsförordningen[170]. I utkastet till beslut konstaterades också att TIC:s överträdelse av artikel 33.5 i den allmänna dataskyddsförordningen var oaktsam[171], eftersom det inte fanns någon kunskap eller vilja att orsaka överträdelsen (vilket skulle ha varit liktydigt med uppsåt), men

[159] Utkastet till beslut, punkterna 14.16–14.18.
[160] Utkastet till beslut, punkt 14.19.
[161] Utkastet till beslut, punkt 14.20.
[162] Utkastet till beslut, punkt 14.21.
[163] Utkastet till beslut, punkt 14.24.
[164] Utkastet till beslut, punkt 14.24.
[165] Punkt 14.26 i utkastet till beslut (den inleddes vid utgången av de 72 timmarna från och med den 3 januari 2019 [dvs. den 6 januari 2019] och avslutades vid tidpunkten för TIC:s anmälan av incidenten den 8 januari 2019).
[166] Utkastet till beslut, punkt 14.29.
[167] Utkastet till beslut, punkt 14.34.
[168] Utkastet till beslut, punkterna 14.33–14.34.
[169] Utkastet till beslut, punkt 14.34.
[170] Utkastet till beslut, punkt 14.35.
[171] Utkastet till beslut, punkt 14.38.

dokumentationen var inte tillräcklig för att göra det möjligt att kontrollera efterlevnaden av artikel 33[172].

155. När det gäller **artikel 83.2 c i den allmänna dataskyddsförordningen**, dvs. åtgärder som vidtagits av den personuppgiftsansvarige för att **lindra de skador som de registrerade lidit**, ansågs i utkastet till beslut att korrigerande åtgärder hade vidtagits för att undvika att problemet upprepades och för att rätta buggen, vilket ansågs vara den enda förmildrande omständigheten vid bedömningen av den sanktionsavgift som skulle åläggas[173].

156. Utkastet till beslut beaktade **artikel 83.2 d i den allmänna dataskyddsförordningen**, dvs. **graden av ansvar** för den personuppgiftsansvarige eller personuppgiftsbiträdet, genom att notera befintliga och senare förbättrade tekniska och organisatoriska åtgärder som genomförts av TIC i egenskap av personuppgiftsansvarig, inbegripet ändringen av Twittergruppens interna protokoll (som IE SA fann inte var så tydligt som det kunde ha varit) och de personalutbildningsåtgärder som Twitter, Inc. senare vidtog (ytterligare utbildning tillhandahölls internt och betonade vikten av att nämna dataskyddsombudets team – och därmed TIC som personuppgiftsansvarig – i det interna biljettsystemet), liksom förekomsten av interna strukturer och skyddsåtgärder med avseende på ansvaret för informationssäkerhetsfrågor och förekomsten av en återkommande extern tredjeparts expertrevision av Twitter, Inc.:s informationssäkerhetsprogram[174]. Även om de problem som uppkom inte ansågs tyda på ett bredare systemproblem[175] och TIC visade på en allmänt ansvarsfull och ansvarsskyldig strategi för datasäkerhet[176], ansågs det att den personuppgiftsansvarige uppvisade en måttlig till hög ansvarsnivå, eftersom en brist på tydlighet i protokollet också framgick av dess senare ändring[177].

157. **Graden av samarbete** med tillsynsmyndigheten utvärderades i enlighet med **artikel 83.2 f i den allmänna dataskyddsförordningen**, och befanns inte utgöra en förmildrande omständighet[178]. IE SA medgav att TIC samarbetade fullt ut, men noterade att detta var en lagstadgad skyldighet och att TIC inte gick utöver denna skyldighet[179].

158. När det gäller **artikel 83.2 g i den allmänna dataskyddsförordningen** om **de kategorier av personuppgifter som påverkas**, drogs i utkastet till beslut slutsatsen att alla kategorier av personuppgifter kunde ha påverkats av den försenade anmälan och att det inte slutgiltigt kan sägas att det inte förelåg någon skada för registrerade eller inga påverkade kategorier av personuppgifter[180].

159. Det **sätt på vilket överträdelsen blev känd** för IE SA ansågs vara en relevant faktor vid fastställandet av sanktionsavgiften (i enlighet med artikel 83.2 h i den allmänna dataskyddsförordningen), eftersom registren inte gjorde det möjligt för IE SA att kontrollera efterlevnaden av artikel 33 i den allmänna dataskyddsförordningen, trots att TIC skulle tillhandahålla all tillgänglig dokumentation, och den information som ursprungligen lämnades i anmälan till IE SA var otydlig[181].

[172] Utkastet till beslut, punkterna 14.36, 14.38.
[173] Utkastet till beslut, punkterna 14.39–14.42.
[174] Utkastet till beslut, punkterna 14.43–14.47.
[175] Utkastet till beslut, punkt 14.45.
[176] Utkastet till beslut, punkt 14.47.
[177] Utkastet till beslut, punkt 14.47.
[178] Utkastet till beslut, punkt 14.50.
[179] Utkastet till beslut, punkt 14.49.
[180] Utkastet till beslut, punkt 14.54.
[181] Utkastet till beslut, punkt 14.58.

160. Kriterierna i **artikel 83.2 e, i och j i den allmänna dataskyddsförordningen** konstaterades inte vara tillämpliga, och inga ytterligare faktorer identifierades med avseende på **artikel 83.2 k i den allmänna dataskyddsförordningen**[182].

161. IE SA betonade i sitt utkast till beslut att den, i avsaknad av särskilda riktlinjer på EU-nivå för beräkning av sanktionsavgifter, inte var skyldig att tillämpa någon särskild metod eller använda en fast finansiell utgångspunkt[183] och att uttrycket ”vederbörlig hänsyn” ger tillsynsmyndigheterna ett stort utrymme för skönsmässig bedömning när det gäller att väga faktorerna i artikel 83.2 i den allmänna dataskyddsförordningen[184].

162. När det gäller fastställandet av det relevanta företag som ska beräkna det tak som fastställs i **artikel 83.4 i den allmänna dataskyddsförordningen**, underströk IE SA att det faktum att TIC är självständigt i sin kontroll över behandlingen av uppgifter inte innebär att det upphör att vara en del av **en enda ekonomisk enhet** med sitt moderbolag och noterade att utöver Twitters, Inc.:s ägande av TIC, verkar Twitter, Inc.:s chefsjurist vara en av TIC:s tre direktörer[185].

163. Av dessa skäl beräknade den ansvariga tillsynsmyndigheten taket för eventuella sanktionsavgifter med hänvisning till Twitters, Inc.:s omsättning[186]. Eftersom Twitters, Inc.:s årliga omsättning 2018 uppgick till 3 miljarder US-dollar, ansågs taket vara 60 miljoner US-dollar (2 procent av 3 miljarder US-dollar)[187].

164. Vid tillämpningen av principerna om **effektivitet, proportionalitet och avskräckande effekt (artikel 83.1 i den allmänna dataskyddsförordningen**) ansågs i utkastet till beslut att en sanktionsavgift inte kan vara effektiv om den inte har någon betydelse i förhållande till den personuppgiftsansvariges intäkter, att överträdelsen inte behöver betraktas abstrakt, oavsett inverkan på den personuppgiftsansvarige**,** och att framtida överträdelser måste avvärjas[188].

165. IE SA föreslog en administrativ sanktionsavgift inom intervallet 150 000–300 000 US-dollar, dvs. mellan 0,005 procent och 0,01 procent av företagets årsomsättning eller mellan 0,25 procent och 0,5 procent av det högsta belopp som får tillämpas för dessa överträdelser. Detta motsvarar en sanktionsavgift i euro på mellan 135 000 och 275 000 euro[189].

8.2 Sammanfattning av invändningarna från de berörda tillsynsmyndigheterna

166. **AT SA** invände mot det föreslagna beloppet och den omständigheten att den ansvariga tillsynsmyndigheten föreslog ett intervall i stället för ett fast belopp. När det gäller artikel 83.2 a i den allmänna dataskyddsförordningen betonade AT SA att minst 88 726 personer (men förmodligen fler) påverkades av incidenten och att ”*det är mycket sannolikt att känsliga uppgifter lämnades ut till allmänheten*”.

[182] Utkastet till beslut, punkterna 14.48, 14.59, 14.60 och 14.61.
[183] Utkastet till beslut, punkt 15.2.
[184] Utkastet till beslut, punkt 15.1.
[185] Utkastet till beslut, punkt 15.13.
[186] Utkastet till beslut, punkt 15.14.
[187] Utkastet till beslut, punkt 15.19.
[188] Utkastet till beslut, punkt 15.18.
[189] Punkt 15.20 i utkastet till beslut (den övre gränsen för det intervall som föreslås i utkastet till beslut är lägre än i det preliminära utkastet till beslut, för att spegla förändringarna i synen på svårighetsgrad, den personuppgiftsansvariges grad av ansvar och huruvida överträdelserna var systematiska). I punkt 15.21 i utkastet till beslut betonades att för att skydda TIC:s processuella rättigheter föreslogs en sanktionsavgift inom ett intervall i stället för ett fast belopp, och möjligheten erkändes att berörda tillsynsmyndigheter skulle kommentera var i intervallet sanktionen bör ligga.

167. Den invändning som framförts av AT SA var oense om hur den *tidpunkt då den personuppgiftsansvarige bör anses ha fått vetskap om en personuppgiftsincident* analyserades i utkastet till beslut. AT SA hävdade närmare bestämt i sin invändning att TIC borde ha gjort en anmälan av personuppgiftsincident inom 72 timmar efter det att bearbetningsföretaget mottog buggrapporten och därmed fick kännedom om incidenten. AT SA betonade att TIC är ansvarigt för att övervaka den behandling som utförs av dess personuppgiftsbiträde och att en personuppgiftsansvarig inte bör försöka dölja misslyckanden hos det personuppgiftsbiträde med vilket den har ett avtalsförhållande och som valts ut av den personuppgiftsansvarige själv. Detta bidrar till AT SA:s bedömning av överträdelsen av artikel 33.1 i den allmänna dataskyddsförordningen som ”allvarlig”.

168. När det gäller om ”*överträdelsen skett med uppsåt eller genom oaktsamhet*” (artikel 83.2 b i den allmänna dataskyddsförordningen) hävdade AT SA att TIC:s beteende bör betecknas som ”uppsåtligt”, på grundval av de kriterier för kunskap och uppsåt som fastställs i artikel 29-gruppens riktlinjer för tillämpning och fastställande av administrativa sanktionsavgifter (WP253), vilka godkänts av EDPB[190]. När det gäller kriteriet om *åtgärder som vidtagits för att lindra den skada* som de registrerade lidit (artikel 83.2 c i den allmänna dataskyddsförordningen) betonade AT SA att det ”*inledningsvis inte var TIC:s avsikt att underrätta användare som påverkades av incidenten*” och att ”*de åtgärder som vidtagits av Twitter Inc. för att rätta till buggen är den enda förmildrande omständigheten*”. Slutligen anser AT SA att det avgiftsintervall som föreslås av IE SA varken är effektivt, proportionellt eller avskräckande med hänsyn till kriterierna i artikel 83.2 a–k i den allmänna dataskyddsförordningen. Sammanfattningsvis föreslog AT SA att en högre administrativa sanktionsavgift skulle åläggas, vilket skulle kunna uppfylla kravet på effektivitet, proportionalitet och avskräckande effekt (dvs. ”*ett minsta belopp på 1 procent av företagets årsomsättning*”).

169. **DE SA** invände mot att den sanktionsavgift som föreslagits av den ansvariga tillsynsmyndigheten är ”för låg” och ”inte överensstämmer med bestämmelserna i artikel 83.1 i den allmänna dataskyddsförordningen”. Närmare bestämt hävdade DE SA att avgiften inte är avskräckande. I invändningen erinrades om att en sanktion kan anses vara effektiv och avskräckande om den är lämplig både som en allmän förebyggande åtgärd – för att avskräcka allmänheten från att begå överträdelser och för att bekräfta allmänhetens förtroende för unionsrättens giltighet – och som en särskild förebyggande åtgärd – för att avskräcka gärningsmannen från att begå ytterligare överträdelser. Vidare hävdar DE SA att ett företags ekonomiska kapacitet (i fråga om omsättning) kan ge en viktig indikation på de belopp som krävs för att uppnå avskräckande effekt: detta kan innebära att hänsyn tas till den del av omsättningen som genereras av de produkter för vilka överträdelsen har begåtts, vilket kan ge en indikation på överträdelsernas omfattning. DE SA hävdar också att den avskräckande effekten av höga avgifter endast kan uppnås om de utdömda beloppen inte lätt kan betalas på grund av stora tillgångar eller höga inkomster, och betonar att avgiften måste ha en avskräckande effekt, särskilt när det gäller specifik databehandling. Som en följd av detta måste den hotande avgiften vara tillräckligt hög för att uppgiftsbehandlingen ska bli oekonomisk och sakligt ineffektiv. Eftersom Twitters affärsmodell bygger på databehandling, och eftersom Twitter genererar sin omsättning främst genom databehandling, anser DE SA att en avskräckande avgift i detta specifika fall därför måste vara så hög att den olagliga uppgiftsbehandlingen blir olönsam. På grundval av det avgiftsbegrepp som är tillämpligt på DE SA skulle avgiften för den överträdelse som beskrivs i utkastet till beslut uppgå till mellan cirka 7 348 035,00 euro och 22 044 105,00 euro.

[190] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237.

170. **HU SA** hävdade att även om sanktionsavgifter är motiverade för de överträdelser som begåtts är den avgift som anges i utkastet orimligt låg, oproportionell och därmed inte avskräckande med tanke på hur allvarlig överträdelsen är och den personuppgiftsansvariges globala marknadsstyrka.

171. **IT SA** bad den ansvariga tillsynsmyndigheten att ”*se över utkastet till beslut så att det även avsåg kvantifiering av den administrativa sanktionsavgiften, med beaktande av särskilda försvårande omständigheter i ärendet med avseende på den personuppgiftsansvariges art och dataincidentens allvar och varaktighet*”.

8.3 Den ansvariga tillsynsmyndighetens ståndpunkt avseende invändningarna

172. IE SA ansåg att de invändningar som framförts av AT SA, DE SA och HU SA avseende den administrativa sanktionsavgiften var ”relevanta och motiverade” i den mening som avses i artikel 4.24 i den allmänna dataskyddsförordningen. Samtidigt följde inte IE SA dessa invändningar av de skäl som anges i det sammansatta memorandumet[191].

173. När det gäller AT SA:s och DE SA:s invändningar anser IE SA att dess bedömning och tillämpning av faktorerna i artikel 83.2 a och b i den allmänna dataskyddsförordningen, enligt beskrivningen i utkastet till beslut, är lämplig. När det gäller AT SA:s invändning hävdar IE SA att TIC:s överträdelse av artikel 33.1 och artikel 33.5 i den allmänna dataskyddsförordningen berodde på TIC:s försumlighet snarare än på en avsiktlig underlåtenhet[192]. Därför anser IE SA att den sanktionsavgift som föreslås av AT SA inte är proportionell[193]. Dessutom hävdar IE SA att AT SA:s oro över det avgiftsintervall som föreslås i utkastet till beslut, i motsats till ett fast belopp, inte var väl utvecklat eller klargjort av denna berörda tillsynsmyndighet[194]. När det gäller DE SA:s invändning har IE SA noterat DE SA:s invändning om att avgiften måste uppfylla kravet på avskräckande effekt, men anser att den nivå som DE SA föreslår inte är proportionell i detta fall[195]. Av ovannämnda skäl anser IE SA att dessa invändningar är motiverade och relevanta, men föreslår att de inte följs[196].

174. IE SA har tagit vederbörlig hänsyn till AT SA:s ståndpunkt när det gäller tidpunkten för TIC:s vetskap om och anmälan av incidenten, men drog slutsatsen att TIC, trots TIC:s faktiska ”vetskap” om incidenten den 7 januari 2019, borde ha fått vetskap om incidenten senast den 3 januari 2019[197]. IE SA identifierade den 3 januari 2019 som det datum då TIC borde ha fått vetskap om incidenten och beaktade att en tidigare försening hade uppstått under perioden från det att en entreprenör först anmälde händelsen till Twitter, Inc. till den tidpunkt då Twitter, Inc. inledde sin prövning[198]. Dessutom klargörs det av IE SA att den inte antyder att ”*personuppgiftsansvariga automatiskt bör anses ha fått vetskap om personuppgiftsincidenter samtidigt som deras personuppgiftsbiträden får vetskap om överträdelsen*”[199]. IE SA anger också att ”*det vanligtvis är så att ett personuppgiftsbiträde som drabbas av en incident kommer att få vetskap om incidenten vid en tidigare tidpunkt än den personuppgiftsansvarige, och att den personuppgiftsansvarige, förutsatt att den process som överenskommits mellan den personuppgiftsansvarige och personuppgiftsbiträdet är effektiv och/eller*

[191] Det sammansatta memorandumet, punkterna 5.60–5.72.
[192] Det sammansatta memorandumet, punkt 5.62.
[193] Det sammansatta memorandumet, punkt 5.63.
[194] Det sammansatta memorandumet, punkt 5.64.
[195] Det sammansatta memorandumet, punkt 5.68.
[196] Det sammansatta memorandumet, punkterna 5.65 och 5.68.
[197] Det sammansatta memorandumet, punkt 5.48.
[198] Det sammansatta memorandumet, punkt 5.50.
[199] Det sammansatta memorandumet, punkt 5.50.

följs, kommer att få 'vetskap' om incidenten [...] på ett sätt som gör det möjligt för den personuppgiftsansvarige att fullgöra sin skyldighet att anmäla densamma"[200].

8.4 EDPB:s analys

8.4.1 Bedömning av huruvida invändningarna var relevanta och motiverade

175. När det gäller möjligheten att göra relevanta och motiverade invändningar mot huruvida planerade åtgärder mot den personuppgiftsansvarige eller personuppgiftsbiträdet är förenliga med den allmänna dataskyddsförordningen[201] för att bestrida de föreslagna sanktionsavgifterna klargjorde EDPB nyligen att "*det är möjligt att invändningen ifrågasätter de faktorer som ligger till grund för beräkningen av avgiften*"[202]. Detta kan utgöra ett exempel på invändningar om huruvida den planerade åtgärden med avseende på den personuppgiftsansvarige eller personuppgiftsbiträdet är förenlig med den allmänna dataskyddsförordningen.

176. I det aktuella fallet ifrågasätter **AT SA**:s invändning de omständigheter som IE SA har åberopat vid beräkningen av sanktionsbeloppet och avser således huruvida den föreslagna åtgärden gentemot den personuppgiftsansvarige är förenlig med den allmänna dataskyddsförordningen. AT SA klargjorde sambandet mellan sin invändning och utkastet till beslut och visade hur de föreslagna ändringarna skulle leda till en annan slutsats. Dessutom lade den fram argument för varför ändringen av beslutet föreslås, genom att tillhandahålla en alternativ tolkning av tre av de kriterier som förtecknas i artikel 83 i den allmänna dataskyddsförordningen och genom att hänvisa till sakliga och rättsliga argument. AT SA visar tydligt på betydelsen av de risker som utkastet till beslut innebär, för det första genom att hävda att den föreslagna sanktionsavgiften inte är tillräckligt effektiv och avskräckande och genom att påminna om att den i detta syfte måste avskräcka allmänheten från att begå liknande överträdelser och bekräfta allmänhetens förtroende för tillämpningen av unionsrätten samt avskräcka den personuppgiftsansvarige från att begå ytterligare överträdelser. Vid bedömningen av överträdelsens svårighetsgrad avser invändningen också i vilken utsträckning registrerade (i ett antal som sannolikt är högre än det som identifierats) påverkades av incidenten (t.ex. genom att deras tidigare skyddade tweetar, vilka sannolikt innehöll känsliga uppgifter, exponerades för allmänheten). Den påstådda avsiktligheten med överträdelsen innebär enligt AT SA en mycket större inverkan på förmågan att veta vad som är rätt och fel än en oaktsam överträdelse. Mot bakgrund av ovanstående bedömning anser EDPB att AT SA:s invändning är relevant och motiverad i enlighet med artikel 4.24 i den allmänna dataskyddsförordningen. Som en följd av detta kommer EDPB att bedöma fördelarna med de väsentliga frågor som tas upp i denna invändning (se avsnitt 8.4.2 nedan).

177. **DE SA**:s invändning ska också anses vara relevant, eftersom den avser huruvida den planerade åtgärden är förenlig med den allmänna dataskyddsförordningen, genom att bestrida de omständigheter som ligger till grund för beräkningen av sanktionsavgiften. Närmare bestämt hävdar den att den avgift som ålades av IE SA inte är avskräckande och att den beräkning som utförts därför inte är förenlig med artikel 83.1 i den allmänna dataskyddsförordningen. DE SA klargjorde att en sanktion ska anses vara effektiv och avskräckande när den tjänar som en allmän förebyggande åtgärd för att avskräcka allmänheten från att begå överträdelser och för att bekräfta sitt förtroende för unionsrättens giltighet, men även när den avskräcker gärningsmannen från att begå ytterligare överträdelser. Dessutom visar DE SA tydligt på betydelsen av de risker som utkastet till beslut innebär för de registrerades rättigheter och friheter, eftersom underlåtenheten att införa en avskräckande och

[200] Det sammansatta memorandumet, punkt 5.50.
[201] Artikel 4.24 i den allmänna dataskyddsförordningen.
[202] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 34.

effektiv sanktion kanske inte kan avskräcka den personuppgiftsansvarige från att begå ytterligare överträdelser.

178. Ett annat argument från DE SA för att visa på riskernas betydelse är att underlåtenheten att hantera incidenten på lämpligt sätt tyder på ett ”*systemfel*”, som skulle ha krävt en djupare granskning av den personuppgiftsansvarige, utöver den enskilda specifika incidenten. DE SA erinrade också om att ett stort antal personer berördes och att tidsperioden också var lång, och drog slutsatsen att de korrigerande befogenheter som införts på grundval av artikel 58.2 i den allmänna dataskyddsförordningen måste granskas mot bakgrund av dessa faktorer. Sammanfattningsvis anser EDPB att DE SA:s invändning är motiverad och relevant enligt definitionen i artikel 4.24 i den allmänna dataskyddsförordningen. Som en följd av detta kommer EDPB att bedöma fördelarna med de väsentliga frågor som tas upp i denna invändning (se avsnitt 8.4.2 nedan).

179. **HU SA**:s invändning är relevant eftersom den också gäller den planerade åtgärdens förenlighet med den allmänna dataskyddsförordningen genom att hävda att den föreslagna sanktionsavgiften är ”*orimligt låg, oproportionell och därmed inte avskräckande*”. Invändningen avser visserligen ”*buggen i den personuppgiftsansvariges tillämpning under årens lopp*” och ”*dess allvarliga karaktär som påverkar datasäkerheten*”, samt ”*svårighetsgraden hos den begångna överträdelsen*” och ”*den personuppgiftsansvariges globala marknadsinflytande*”, men den visar inte tydligt betydelsen av de risker för de registrerades rättigheter och friheter som sanktionsavgiften innebär som IE SA föreslår. Därför anser EDPB att denna invändning inte uppfyller kraven i artikel 4.24 i den allmänna dataskyddsförordningen[203].

180. Slutligen framgår relevansen av den invändning som framförts av **IT SA** också av dess hänvisning till huruvida den föreslagna åtgärden är förenlig med den allmänna dataskyddsförordningen, eftersom IT SA hävdar att IE SA bör se över utkastet till beslut när det gäller kvantifieringen av den administrativa sanktionsavgiften. Genom att hänvisa till ”*ovanstående invändningar*” och därmed till det faktum att de nämnda aspekterna är ”*strukturella till sin natur när det gäller den personuppgiftsansvariges organisation*” och ”*måste ha effekter inte bara på det aktuella fallet utan även på eventuella framtida personuppgiftsincidenter*”, visar IT SA:s invändning tydligt på betydelsen av riskerna för de registrerades rättigheter och friheter när det gäller kvantifieringen av avgiften.

181. Därför anser EDPB att IT SA:s invändning är motiverad och relevant och uppfyller kraven i artikel 4.24 i den allmänna dataskyddsförordningen. Som en följd av detta kommer EDPB att bedöma fördelarna med de väsentliga frågor som tas upp i denna invändning.

8.4.2 Bedömning av huruvida de väsentliga frågorna i de relevanta och motiverade invändningarna är välgrundade

182. EDPB anser att de invändningar som anses vara relevanta och motiverade i detta underavsnitt[204] kräver en bedömning av huruvida utkastet till beslut föreslår en sanktionsavgift i enlighet med kriterierna i artikel 83 i den allmänna dataskyddsförordningen och artikel 29-gruppens riktlinjer för tillämpning och

[203] EDPB tar därför inte ställning till huruvida några väsentliga frågor som tas upp i dessa invändningar är välgrundade. EDPB upprepar att dess nuvarande beslut inte påverkar eventuella bedömningar som styrelsen kan komma att uppmanas göra i andra fall, även med samma parter, med beaktande av innehållet i det relevanta utkastet till beslut och de invändningar som framförts av de berörda tillsynsmyndigheterna.
[204] Dessa invändningar är de som framförts av AT SA, DE SA och IT SA.

fastställande av administrativa sanktionsavgifter i enlighet med förordning 2016/679 (WP253) (som godkänts av EDPB)[205].

183. Mekanismen för enhetlighet kan också användas för att främja en konsekvent tillämpning av administrativa sanktionsavgifter[206]: om en relevant och motiverad invändning ifrågasätter de omständigheter som den ansvariga tillsynsmyndigheten har åberopat för att beräkna avgiftsbeloppet, kan EDPB ålägga den ansvariga tillsynsmyndigheten att göra en ny beräkning av det föreslagna beloppet genom att undanröja bristerna i fastställandet av orsakssambandet mellan de aktuella omständigheterna och det sätt på vilket den föreslagna avgiften beräknades på grundval av kriterierna i artikel 83 i den allmänna dataskyddsförordningen och de gemensamma standarder som fastställts av EDPB[207]. En sanktionsavgift bör vara effektiv, proportionell eller avskräckande, i enlighet med artikel 83.1 i den allmänna dataskyddsförordningen, med beaktande av omständigheterna i ärendet[208]. Dessutom ska den ansvariga tillsynsmyndigheten när den beslutar om avgiften ta hänsyn till de kriterier som anges i artikel 83.2 i den allmänna dataskyddsförordningen.

184. När det gäller karaktären, svårighetsgraden och varaktigheten hos den överträdelse som konstaterats i artikel 33.1 och 33.5 i den allmänna dataskyddsförordningen, krävs det enligt **artikel 83.2 a i den allmänna dataskyddsförordningen** att hänsyn tas till bland annat **karaktären, omfattningen och syftet med den aktuella behandlingen** samt **antalet registrerade som påverkas och omfattningen av den skada** som de lidit.

185. EDPB håller med IE SA om att överträdelsen som ska beaktas inte är incidenten som sådan utan efterlevnaden av artikel 33.1 och 33.5 i den allmänna dataskyddsförordningen att anmäla incidenten till den behöriga tillsynsmyndigheten och dokumentera incidenten.

186. EDPB noterar att IE SA tar hänsyn till behandlingens karaktär och antalet registrerade som påverkas. När det gäller **behandlingens karaktär** beskriver IE SA en plattform för ”mikrobloggning” och sociala medier där användarna har möjlighet att dokumentera sina tankar i ”tweetar”. EDPB anser att man vid bedömningen av behandlingens karaktär också måste ta hänsyn till det faktum att ”den aktuella behandlingen” omfattade meddelanden från registrerade som avsiktligt valt att begränsa meddelandenas publik. EDPB noterar att man i utkastet till beslut från IE SA ansåg att ”*konsekvenserna för enskilda användare och risken för skada till följd av detta kommer att bero på nivån på de personuppgifter som offentliggörs och även på dessa personuppgifters art. I detta avseende angav jag i det preliminära utkastet att även om TIC inte hade bekräftat den exakta karaktären hos de uppgifter som offentliggjordes i samband med incidenten, var det rimligt att dra slutsatsen att vissa av de personuppgifter som offentliggjorts avseende åtminstone vissa användare kommer att ha inkluderat känsliga kategorier av uppgifter och annat särskilt privat material, med tanke på omfattningen av de berörda användarna och arten av den tjänst som TIC erbjuder*”[209]. IE SA, grundat på uppgifter från TIC, lade dock mindre vikt vid denna faktor än den gjorde i det preliminära utkastet, eftersom det inte fanns några direkta bevis för skada[210]. EDPB anser dock att IE SA fortfarande borde ha lagt stor vikt vid det faktum att den ”aktuella behandlingen” omfattar meddelanden från registrerade som avsiktligt valt att begränsa dessa meddelandens publik vid bedömningen av behandlingens karaktär. I synnerhet

[205] Artikel 29-gruppens riktlinjer för tillämpning och fastställande av administrativa sanktionsavgifter i enlighet med förordning 2016/679, WP253, antagna den 3 oktober 2017 (godkända av EDPB den 25 maj 2020).
[206] Den allmänna dataskyddsförordningen, skäl 150.
[207] Riktlinjerna för begreppet relevant och motiverad invändning, punkt 34.
[208] EDPB:s riktlinjer om administrativa sanktionsavgifter, s. 7.
[209] Utkastet till beslut, punkt 14.51.
[210] Se punkt 150 ovan.

borde IE SA ha lagt stor vikt vid detta faktum med tanke på att det påpekades av IE SA i utkastet till beslut, där IE SA ansåg att ”*den storskaliga omfattningen av det berörda användarsegmentet ger möjlighet till ett mycket bredare spektrum av skador till följd av incidenten, särskilt med tanke på arten av den tjänst som tillhandahålls av TIC*” och ”*sannolikheten för att många användare kommer att ha förlitat sig på funktionen att hålla tweetar privata för att dela information eller åsikter (i fråga om den privata sektorn)*”[211].

187. När det gäller omfattningen av den berörda behandlingen som sådan verkar IE SA ersätta behandlingens omfattning med antalet berörda registrerade. EDPB anser att **karaktären och omfattningen av den ”behandling”** som ska beaktas vid fastställandet av sanktionsavgiften inte är den behandling som består i (oavsiktligt) utlämnande (personuppgiftsincident) eller orsaken till denna, utan snarare omfattningen av den underliggande behandlingen som utförs av TIC, såsom beskrivs i föregående punkt.

188. Enligt AT SA **påverkar tidpunkten när den personuppgiftsansvarige fick vetskap om incidenten hur allvarlig överträdelsen** är av artikel 33.1 i den allmänna dataskyddsförordningen. Den invändning som framförts av AT SA var oenig om hur den tidpunkt då den personuppgiftsansvarige ska anses ha fått vetskap om en personuppgiftsincident bör fastställas eller bedömas. AT SA hävdade närmare bestämt i sin invändning att TIC borde ha gjort en anmälan av personuppgiftsincident inom 72 timmar efter det att personuppgiftsbiträdet fått vetskap om buggen. Detta bidrar till AT SA:s bedömning av överträdelsen av artikel 33.1 i den allmänna dataskyddsförordningen som ”allvarlig”.

189. I detta avseende erinrar EDPB om att det i riktlinjerna om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679 (WP250)[212], som godkänts av EDPB, anges att ”*[i]ncidenthanteringsplanerna bör vara inriktade på att skydda enskilda och deras personuppgifter. Anmälan av incidenter bör därför ses som ett verktyg för att öka skyddet för personuppgifter*”[213].

190. Enligt riktlinjerna om anmälan av personuppgiftsincidenter bör en personuppgiftsansvarig anses ha fått ”vetskap” när den personuppgiftsansvarige är rimligt säker på att en säkerhetsincident har ägt rum som har medfört att personuppgifter äventyrats[214]. Eftersom den personuppgiftsansvarige använder personuppgiftsbiträdet för att uppnå sina syften bör den personuppgiftsansvarige i princip anses ha fått ”vetskap” så snart personuppgiftsbiträdet har informerat om incidenten[215]. I den allmänna dataskyddsförordningen åläggs dock den personuppgiftsansvarige en skyldighet att snabbt skaffa sig ”vetskap” om eventuella incidenter så att denne kan vidta lämpliga åtgärder[216] och förklara att ”*den personuppgiftsansvarige [får] genomföra en kort undersökning för att fastställa huruvida en incident verkligen har ägt rum. Under denna undersökningsperiod kan den personuppgiftsansvarige inte anses ha fått ’vetskap’ om incidenten*”[217]. I riktlinjerna klargörs dock att denna inledande undersökning bör inledas så snart som möjligt och att en mer ingående undersökning därefter kan följa[218].

[211] Utkastet till beslut, punkt 14.51.
[212] Artikel 29-gruppens riktlinjer om anmälan av personuppgiftsincidenter enligt förordning (EU) 2016/679, WP250 rev.01, som godkänts av EDPB (nedan kallade riktlinjerna om anmälan av personuppgiftsincidenter).
[213] Riktlinjer om anmälan av personuppgiftsincidenter, s. 5.
[214] Riktlinjer om anmälan av personuppgiftsincidenter, s. 10–11.
[215] Riktlinjer om anmälan av personuppgiftsincidenter, s. 13.
[216] Riktlinjer om anmälan av personuppgiftsincidenter, s. 11.
[217] Riktlinjer om anmälan av personuppgiftsincidenter, s. 11 (understrykning tillagd).
[218] Riktlinjer om anmälan av personuppgiftsincidenter, s. 11.

191. I riktlinjerna klargörs således att den personuppgiftsansvarige, och i förlängningen personuppgiftsbiträdet, ska agera skyndsamt. ”I de flesta fall bör dessa preliminära åtgärder slutföras så snart som möjligt efter den inledande varningen (dvs. *när den personuppgiftsansvarige eller personuppgiftsbiträdet misstänker att en säkerhetsincident har ägt rum som kan inbegripa personuppgifter*). Endast i undantagsfall bör detta ta längre tid.”[219]

192. Mot bakgrund av ovanstående instämmer EDPB i IE SA:s bedömning, enligt vilken den personuppgiftsansvarige inte kan förväntas ha fått vetskap om att en säkerhetsincident har inträffat vid den tidpunkt då personuppgiftsbiträdet har insett att en säkerhetsincident har inträffat. I enlighet med artikel 29-gruppens riktlinjer om anmälan av personuppgiftsincidenter, som godkänts av EDPB, måste det finnas en viss säkerhet om att en personuppgiftsincident har ägt rum innan vetskap kan fastställas. Det framgår inte klart av de faktiska omständigheter som anges i utkastet till beslut att så var fallet före den 3 januari 2019. I detta fall kunde AT SA inte bevisa att TIC uppnådde den nödvändiga graden av säkerhet i fråga om att en uppgiftsincident hade inträffat tidigare än när IE SA fann att TIC hade ”vetskap” om incidenten. Följaktligen anser EDPB att bedömningen av överträdelsens allvar inte behöver justeras mot bakgrund av ett annat fastställande av när den personuppgiftsansvarige fick kännedom om uppgiftsincidenten.

193. Dessutom, när det gäller **överträdelsens svårighetsgrad** håller EDPB med IE SA om att efterlevnaden av artikel 33.1 och 33.5 i den allmänna dataskyddsförordningen är av central betydelse för tillsyns- och verkställighetssystemets övergripande funktion.

194. När det gäller den invändning som AT SA framfört om **överträdelsens avsiktliga karaktär** anser EDPB att invändningen inte tillräckligt visar att den personuppgiftsansvarige från och med den tidpunkt då denne fick vetskap avsiktligt åsidosatte sin aktsamhetsplikt.

195. När det gäller överträdelsens försumlighet anser dock EDPB att ett företag för vilket behandlingen av personuppgifter utgör kärnan i dess affärsverksamhet bör ha inrättat tillräckliga förfaranden för dokumentation av personuppgiftsincidenter, inklusive avhjälpande åtgärder, vilket kommer att göra det möjligt för det att även uppfylla anmälningsskyldigheten enligt artikel 33.1 i den allmänna dataskyddsförordningen. Denna omständighet innebär ytterligare en omständighet som ska beaktas vid bedömningen av överträdelsens svårighetsgrad.

196. EDPB erinrar om att EU-domstolen konsekvent har slagit fast att en avskräckande sanktion är en sanktion som har en **verklig avskräckande verkan**[220]. I detta avseende kan åtskillnad göras mellan en allmän avskräckande effekt (som avskräcker andra från att begå samma överträdelse i framtiden) och en specifik avskräckande effekt (att avskräcka den som är föremål för sanktionsavgiften från att på nytt begå samma överträdelse)[221]. Dessutom ska påföljdernas stränghet stå i proportion till hur allvarliga överträdelserna är[222]. Härav följer att sanktionsavgifterna inte får vara oproportionella i förhållande till de eftersträvade målen, det vill säga att reglerna om skydd av personuppgifter iakttas, och att den avgift som åläggs ett företag ska stå i proportion till överträdelsen i dess helhet, med beaktande av bland annat hur allvarlig överträdelsen är[223].

---

[219] Riktlinjer om anmälan av personuppgiftsincidenter, s. 12 (understrykning tillagd).

[220] Se generaladvokaten Geelhoeds förslag till avgörande av den 29 april 2004 i mål av den 12 juli 2005, C-304/02, kommissionen mot Frankrike, EU:C:2005:444, punkt 39.

[221] Se bland annat dom av den 13 juni 2013, Versalis Spa mot kommissionen, C-511/11, ECLI:EU:C:2013:386, punkt 94.

[222] Domstolens dom av den 25 april 2013, Asociaţia Accept, C-81/12.

[223] Tribunalens dom av den 26 oktober 2017 i mål T-704/14, Marine Harvest mot kommissionen.

197. Den ansvariga tillsynsmyndigheten hänvisade i sitt utkast till beslut till kravet på att ärendet måste vara **avskräckande och proportionellt**, men EDPB anser att den ansvariga tillsynsmyndigheten inte tillräckligt underbyggde hur den föreslagna avgiften uppfyller dessa krav. EDPB noterar särskilt att den ansvariga tillsynsmyndigheten övergår från att beräkna det högsta beloppet (fastställt till 60 miljoner US-dollar) till att ange det föreslagna avgiftsintervallet (fastställt till mellan 150 000 och 300 000 US-dollar), utan någon närmare förklaring av vilka faktorer som ledde till att den ansvariga tillsynsmyndigheten fastställde detta specifika intervall[224]. Utöver den allmänna hänvisningen till relevanta faktorer i artikel 83.2 i den allmänna dataskyddsförordningen finns det ingen tydlig motivering till valet av den föreslagna procentandelen (mellan 0,25 procent och 0,5 procent) av det högsta tillämpliga avgiftsbeloppet enligt artikel 83.4 i den allmänna dataskyddsförordningen.

198. I detta avseende har EDPB ovan redogjort för skälen till varför den ansvariga tillsynsmyndigheten i sitt utkast till beslut borde ha lagt större vikt vid den aspekt som rör överträdelsens karaktär, omfattning och försumlighet och anser därför att det föreslagna avgiftsbeloppet bör justeras i enlighet med detta.

8.4.3 Slutsats

199. EDPB anser därför att den administrativa sanktionsavgift som föreslås i utkastet till beslut är för låg och inte fyller sitt syfte som korrigerande åtgärd, i synnerhet inte kraven i artikel 83.1 i den allmänna dataskyddsförordningen på att vara effektiv, avskräckande och proportionell.

200. EDPB begär således att IE SA ska göra en ny bedömning av de omständigheter som den förlitar sig på för att beräkna det fasta avgiftsbelopp[225] som ska åläggas TIC för att säkerställa att det är lämpligt med hänsyn till de faktiska omständigheterna i ärendet.

201. EDPB noterar att analysen av invändningarna är begränsad till sakinnehållet i de invändningar som ska betraktas som relevanta och motiverade. Omfattningen av EDPB:s analys av beräkningen av sanktionsavgiften är därför begränsad till en analys av beräkningsmetoden för avgifterna som sådan. Det utgör inte en implicit eller explicit validering av EDPB, av den ansvariga tillsynsmyndighetens analys av överträdelsen av artikel 33.1 eller artikel 33.5 i den allmänna dataskyddsförordningen eller av den rättsliga kvalificeringen av Twitter Inc. respektive TIC. EDPB upprepar att dess nuvarande beslut inte påverkar eventuella bedömningar som styrelsen kan komma att uppmanas göra i andra fall, även med samma parter, med beaktande av innehållet i det relevanta utkastet till beslut och de invändningar som framförts av de berörda tillsynsmyndigheterna.

9 BINDANDE BESLUT

202. Mot bakgrund av ovanstående och i enlighet med dataskyddsstyrelsens uppgift enligt artikel 70.1 t i den allmänna dataskyddsförordningen att utfärda bindande beslut i enlighet med artikel 65 i den allmänna dataskyddsförordningen utfärdar styrelsen följande bindande beslut i enlighet med artikel 65.1 a i den allmänna dataskyddsförordningen:

[224] Utkast till beslut, punkterna 15.19 och 15.20.
[225] Detta bör helst redan anges i utkastet till beslut enligt artikel 60 i den allmänna dataskyddsförordningen.

203. Om invändningarna avseende den personuppgiftsansvariges och personuppgiftsbiträdets kvalifikationer och den ansvariga tillsynsmyndighetens behörighet:

- EDPB beslutar att IE SA inte är skyldig att ändra sitt utkast till beslut på grundval av de invändningar som framförts, eftersom de inte uppfyller kraven i artikel 4.24 i den allmänna dataskyddsförordningen.

204. Om invändningarna avseende de överträdelser av artikel 33.1 och 33.5 i den allmänna dataskyddsförordningen som den ansvariga tillsynsmyndigheten konstaterat:

- När det gäller FR SA:s invändning om att det inte föreligger någon överträdelse av artikel 33.1 i den allmänna dataskyddsförordningen, DE SA:s invändning mot fastställandet av att överträdelsen av artikel 33.1 i den allmänna dataskyddsförordningen ska upphöra och IT SA:s invändning avseende överträdelsen av artikel 33.5 i den allmänna dataskyddsförordningen, beslutar EDPB att IE SA inte är skyldig att ändra sitt utkast till beslut på grundval av de invändningar som gjorts eftersom de inte uppfyller kraven i artikel 4.24 i den allmänna dataskyddsförordningen.

205. Om invändningarna avseende eventuella ytterligare (eller alternativa) överträdelser av den allmänna dataskyddsförordningen som identifierats av de berörda tillsynsmyndigheterna:

- När det gäller DE SA:s invändning mot eventuella överträdelser av artikel 5.1 f, artikel 24 och artikel 32 i den allmänna dataskyddsförordningen, och mot IT SA:s invändning mot en eventuell överträdelse av artikel 5.2 i den allmänna dataskyddsförordningen, beslutar EDPB att IE SA, trots att den uppfyller kraven i artikel 4.24 i den allmänna dataskyddsförordningen, inte är skyldig att ändra sitt utkast till beslut, eftersom de tillgängliga faktauppgifterna i utkastet till beslut och i invändningarna inte är tillräckliga för att göra det möjligt för EDPB att fastställa förekomst av överträdelser av artiklarna 5.1 f, 5.2, 24 och 32 i den allmänna dataskyddsförordningen.

- När det gäller DE SA:s invändning om en eventuell överträdelse av artikel 33.3 i den allmänna dataskyddsförordningen, FR SA:s invändning om en eventuell överträdelse av artikel 28 och artikel 32 i den allmänna dataskyddsförordningen, HU SA:s invändning avseende en eventuell överträdelse av artikel 5.1 f, artikel 32 och artikel 34 i den allmänna dataskyddsförordningen och IT SA:s invändning avseende en eventuell överträdelse av artikel 28 i den allmänna dataskyddsförordningen, beslutar EDPB att IE SA inte behöver ändra sitt utkast till beslut på grundval av de invändningar som framförts eftersom de inte uppfyller kraven i artikel 4.24 i den allmänna dataskyddsförordningen.

206. Angående invändningen mot den ansvariga tillsynsmyndighetens beslut att inte utfärda någon reprimand:

- När det gäller DE SA:s invändning mot IE SA:s beslut att inte utfärda en reprimand, beslutar EDPB att IE SA inte behöver ändra sitt utkast till beslut på grundval av invändningen eftersom den inte uppfyller kraven i artikel 4.24 i den allmänna dataskyddsförordningen.

207. Angående invändningen mot beräkningen av den sanktionsavgift som föreslagits av den ansvariga tillsynsmyndigheten:

- När det gäller HU SA:s invändning om att sanktionsavgiften inte är tillräckligt avskräckande beslutar EDPB att IE SA inte är skyldig att ändra sitt utkast till beslut på grundval av invändningen eftersom den inte uppfyller kraven i artikel 4.24 i den allmänna dataskyddsförordningen.

- När det gäller AT SA:s invändning, DE SA:s invändning och IT SA:s invändning om att sanktionsavgiften inte är tillräckligt avskräckande, beslutar EDPB att de uppfyller kraven i artikel 4.24 i den allmänna dataskyddsförordningen och att IE SA är skyldig att göra en ny bedömning av **de delar som den förlitar sig på för att beräkna det fasta avgiftsbelopp** som ska åläggas TIC, och ändra sitt utkast till beslut genom att höja avgiftsnivån för att säkerställa att den uppfyller sitt syfte som en korrigerande åtgärd och uppfyller kraven på ändamålsenlighet och proportionalitet och artikel 83.1 i den allmänna dataskyddsförordningen och med hänsyn till kriterierna i artikel 83.2 i den allmänna dataskyddsförordningen.

10 AVSLUTANDE ANMÄRKNINGAR

208. Detta bindande beslut riktar sig till IE SA och de berörda tillsynsmyndigheterna. IE SA ska anta sitt slutliga beslut på grundval av detta bindande beslut i enlighet med artikel 65.6 i den allmänna dataskyddsförordningen.

209. När det gäller de invändningar som inte anses uppfylla kraven i artikel 4.24 i den allmänna dataskyddsförordningen tar EDPB inte ställning till huruvida några väsentliga frågor som dessa invändningar ger upphov till är välgrundade. EDPB upprepar att dess nuvarande beslut inte påverkar eventuella bedömningar som styrelsen kan komma att uppmanas göra i andra fall, även med samma parter, med beaktande av innehållet i det relevanta utkastet till beslut och de invändningar som framförts av de berörda tillsynsmyndigheterna.

210. Enligt artikel 65.6 i den allmänna dataskyddsförordningen ska IE SA meddela sitt slutliga beslut till ordföranden inom en månad efter mottagandet av det bindande beslutet.

211. När ett sådant meddelande har lämnats av IE SA kommer det bindande beslutet att offentliggöras i enlighet med artikel 65.5 i den allmänna dataskyddsförordningen.

212. I enlighet med artikel 70.1 y i den allmänna dataskyddsförordningen ska IE SA:s slutgiltiga beslut som meddelats EDPB upptas i registret över beslut som har varit föremål för mekanismen för enhetlighet.

För Europeiska dataskyddsstyrelsen

Ordförande

(Andrea Jelinek)