An Coimisiún um Chosaint Sonraí
Data Protection Commission

DPC Ref: IN-[redacted]

DPC Complaint Ref: C-[redacted]

Date: 27 April 2022

Complainant: [redacted]

Data Controller: Twitter International Company

RE: [redacted] v Twitter International Company

This document is a decision of the Data Protection Commission of Ireland ("**DPC**") in relation to DPC complaint reference, C-[redacted] hereinafter referred to as the ("**Complaint**"), submitted directly to the DPC by Mr. [redacted] ("**Complainant**") against Twitter International Company (the "**Twitter**").

This decision is made pursuant to the powers conferred on the DPC by section 113(2)(a) of the Data Protection Act 2018 ("**the Act**") and Article 60 of the General Data Protection Regulation ("**GDPR**").

Communication of draft decision to "supervisory authorities concerned"

In accordance with Article 60(3) of the GDPR, the DPC was obliged to communicate the relevant information and submit a draft decision, in relation to a complaint regarding cross border processing, to the supervisory authorities concerned for their opinion and to take due account of their views.

In accordance with its obligation, the DPC transmitted a draft decision in relation to the matter to the "supervisory authorities concerned". As Twitter offers services across the EU, and therefore the processing is likely to substantially affect data subjects in every EU member state, the DPC in its role as LSA identified that each supervisory authority is a supervisory authority concerned as defined in Article 4(22) of the GDPR. On this basis, the draft decision of the DPC in relation to this complaint was transmitted to each supervisory authority in the EU and EEA for their opinion.

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Complaint Handling by the DPC – Timeline and Summary

1. The DPC received a complaint on 02 July 2019 via its online web form, in which the complainant alleged that Twitter had failed to comply with an erasure request submitted to it by him. The complainant also provided the DPC with copies of correspondence exchanged between him and Twitter in relation to his request. The complainant stated that on receipt of his erasure request, Twitter had requested that he provide a copy of his photo ID before it would remove his data. The complainant stated that he refused to provide a copy of his ID on the basis that a user can create a Twitter account using only an email address and phone number to verify who you are and therefore the same data should be enough to remove your data. The complainant stated that he had been requesting the erasure of his personal data from Twitter since the middle of May 2019. In the documentation provided by the complainant it appears that the complainant initially submitted an erasure request pursuant to Article 17 of the GDPR to Twitter via email on 13 May 2019.

2. The DPC notified Twitter of receipt of the complaint via email on 10 September 2019. The DPC also provided Twitter with a copy of the complaint and the supporting documentation provided by the complainant.

3. Twitter responded to the DPC by way of letter dated 23 September 2019.

4. The DPC relayed Twitter's response to the complainant via email on 10 October 2019. The complainant responded via emails on 10 & 16 October 2019.

5. The DPC reverted to Twitter via email on 30 October 2019, advising it of the position of the complainant. Twitter responded to the DPC via email dated 13 November 2019.

6. The DPC relayed the response of Twitter to the complainant via email on 04 December 2019.

7. The complainant responded via emails dated 04 December 2019.

8. The DPC informed Twitter of the content of the complainant's reply via email on 10 December 2019.

9. Twitter responded via email dated 23 December 2019.

10. The DPC reverted to Twitter via email dated 24 February 2020 and requested further information.

11. Twitter responded via correspondence dated 06 March 2020.

12. The DPC reverted to Twitter via email on 24 March 2020 requesting further information.

13. Twitter responded via email on 04 April 2020.

14. The complainant contacted the DPC via email dated 07 April 2020.

15. In an attempt to facilitate the amicable resolution of the complaint, the DPC advised the complainant of Twitter's position via email dated 22 April 2020.

16. The complainant responded via email dated 22 April 2020 and 23 April 2020.

17. The DPC notified Twitter, via email dated 03 March 2021, that the attempts to facilitate the amicable resolution of the complaint were unsuccessful and that the DPC was now required to comply with section 113(2) of the Data Protection Act, 2018 which provides that the DPC shall *"make a draft decision in respect of the complaint (or, as the case may be, part of the complaint) and, where applicable, as to the envisaged action to be taken in relation to the controller or processor concerned, and, in accordance with Article 60 [of the GDPR] and, where appropriate, Article 65, adopt its decision in respect of the complaint or, as the case may be, part of the complaint."*

18. In summary, therefore, the DPC was unable to arrange or facilitate within a reasonable time an amicable resolution of the complaint through the mechanism of its complaint handling process and the issues that remained unresolved in relation to this complaint following the DPC's complaint handling process are:

    a) Whether Twitter had a lawful basis for requesting a copy of the data subject's ID in order to verify his identity in circumstances where he had submitted a request for erasure pursuant to Article 17; and

    b) Whether Twitter's handling of the data subject's erasure request was compliant with the GDPR and the Act.

Conduct of Inquiry

19. Acting in its capacity as lead supervisory authority, the DPC commenced an Inquiry in relation to this matter by writing to Twitter on 08 April 2021.

20. The DPC advised Twitter that the Inquiry commenced by the Commencement Notice would seek to examine and assess whether or not Twitter had complied with its obligations under the GDPR and the Act, in particular under Articles 5, 6 and 17 of the GDPR in respect of the relevant processing operations which are the subject matter of the complaint.

21. The DPC advised Twitter that the scope of the Inquiry concerned an examination and assessment of the following:

    a) Whether Twitter had a lawful basis for requesting a copy of the complainant's ID in order to verify his identity in circumstances where he had submitted a request for erasure pursuant to Article 17; and

    b) An examination of whether Twitter's handling of the complainant's erasure request was compliant with the GDPR and the Act.

    The DPC subsequently extended the scope of the Inquiry to include Article 12 and it notified Twitter accordingly.

22. In order to progress the matter the DPC posed specific questions regarding the erasure request and the manner in which it was handled.

23. The DPC also informed the complainant via email dated 08 April 2021 that an Inquiry had commenced in relation to his complaint. The DPC provided the complainant the opportunity to withdraw any information previously provided and asked whether the complainant had any new information he wished to submit regarding the complaint. The complainant replied to the DPC via email on 08 April 2021 stating that he had previously provided all of the relevant information and confirming that all correspondence previously provided in the context of the complaint handling process could be used for the purposes of the Inquiry.

24. On 26 April 2021, Twitter provided the DPC with its response to the questions posed in the DPC's Commencement Notice and did not indicate that it wished to withdraw any information previously provided during the course of the

complaint handling process. In response to the DPC's query as to what legal basis was relied upon for requesting a copy of the complainant's photographic ID, Twitter advised the DPC that it does not require a legal basis to *request* information but rather must have a legal basis tied to the *processing* of information should it be provided. Twitter advised the DPC that it will seek an ID to authenticate an individual to ensure that it is not processing a fraudulent request and if the complainant had provided their ID Twitter would rely on legitimate interests for processing the complainant's ID to fulfil his erasure request. Twitter asserted that authenticating that a requester is who they claim to be (i.e., the owner of a given account) is of paramount importance to the safety, security, and integrity of its services. Twitter explained that, as any person may complete a write-in request by filling out one of its help forms, it must ensure that the requester is in fact authorised to make the request they are making. Twitter advised that, in this instance, the complainant requested the deactivation of the account [redacted] and the removal of the phone number and email address associated with the account. Twitter stated that to complete such a request, it requires corroborating points of identification for the purposes of verifying account ownership - an ID with a corresponding signed statement, along with a confirmation that the request is submitted through the email address associated with the Twitter account. Twitter advised that it does this because, through the operation of its services, it knows that emails may become compromised such that requests from email addresses associated with an account may not in fact be from the owner of the account (e.g., where a partner or friend has been able to gain access to an account holder's email account).Twitter asserted that the request for ID is, therefore, necessary and proportionate, as it allows Twitter to verify that the data subject's identity matches the name on their signed statement in order to prevent:

1) the erasure of accounts submitted by parties other than the account owner; and
2) account takeover, which could occur if parties other than the account holder are able to remove or change a phone number or email address associated with an account that is not theirs.

In terms of the DPC's query as to the reasonable doubts, if any, Twitter had concerning the complainant's identity, Twitter stated that the majority of deactivation requests it receives are through its self-help tools available to logged-in users. Twitter advised that this means the user can login to their account and deactivate their account themselves, which does not require submitting an ID. Twitter stated that as the complainant had been permanently suspended due to repeated violations of its Hateful Conduct Policy the option of using the self-help tool was not available to the complainant. Twitter explained

that when an account is permanently suspended the data subject must submit their request for erasure through Twitter's Office of Data Protection because they cannot access their account, and therefore, cannot use the self-help tools. Twitter advised that this process is in place because of situations where the suspension is due to violations of laws that would also require Twitter to keep information on foot of a valid legal process. Twitter highlighted that this may occur where a user is permanently suspended for violating Twitter's Child Sexual Exploitation Policy. In such a case, Twitter will preserve the account information for law enforcement. However, to ensure compliance with applicable data protection laws, Twitter advised that it still enables an account owner to file their request, which will be reviewed and processed accordingly. Twitter stated that once a request has been manually submitted (i.e., through its help centre forms), it comes under a higher degree of scrutiny so that it can ensure, to the maximum extent possible, that it is not processing fraudulent requests. Twitter again advised the DPC that this is because any person may complete a help form and emails may become compromised such that requests from email addresses associated with an account may not, in fact be from the owner of the account (e.g., where a partner or friend has been able to gain access to an account holder's email account); and, as such, it must exercise significant diligence in processing these requests. On this basis, Twitter asserted that requesting ID verification of an individual seeking to have their account deactivated is a security measure implemented for the safety of all users.

25. Twitter advised that where an individual provides a copy of their ID in order to verify their identity for the purposes of processing their request, it is removed from its systems within 30 days of the request being completed. Twitter also advised that this process is still currently being utilised by it given the risks of harm that it seeks to balance.

26. In response to the DPC's request for information relating to Twitter's handling of the complainant's erasure request, Twitter advised the DPC that it first received the complainant's erasure request on 02 June 2019, and provided the DPC with a screenshot of the complainant's request. Twitter stated that it first responded to the complainant's request by way of auto response within a number of hours of receipt and provided the DPC with screenshots of the auto response. Twitter stated that the delay in providing a substantive response to the complainant's request was caused by the litany of near identical complaints filed by the complainant. Twitter stated that this caused duplication of efforts and that the complainant also failed to follow instructions given to him causing delays in processing his request. Twitter advised the DPC that its support team received several reports from the complainant that requested the deactivation of the account [redacted] and more specifically the removal of the phone

number and email address associated with the account. Twitter stated that its support team should have transferred these requests to a different team but failed to do so. Twitter further stated that as a number of different teams were trying to respond to his request, the complainant also contacted Twitter's Office of Data Protection and was asked to confirm his ownership of the account by providing a signed statement with corresponding ID as per its policies. Twitter asserted that, in response to one of the complainant's many requests to its Office of Data Protection, it did deactivate his account. However, it stated that after the deactivation had been triggered, the complainant tried to log into his account, which halted the deactivation process and thus, his account remains active. Twitter again stated that it is its policy to retain basic subscriber information (e.g., email or phone number used to sign up) to protect its platform from known policy violators. Twitter highlighted if it were to delete the complainant's email address or phone number from its systems, he could use that information to create a new account even though he has been identified and permanently suspended from the platform for various policy violations (e.g., hateful conduct). Twitter advised that this is explained to users via information published in its Help Centre.

27. Twitter confirmed the personal data it retains following the complainant's erasure request is:

- The Phone Number associated with the account [redacted]
- The Email address associated with account [redacted]

Twitter stated that it retains this limited information beyond account deactivation indefinitely and in accordance with its legitimate interest to maintain the safety and security of its platform and users as is outlined in its Help Centre[1]. Further, Twitter asserted that its Privacy Policy[2] notifies users that their data may be retained for these purposes as follows:

"Notwithstanding anything to the contrary in this Privacy Policy or controls we may otherwise offer to you, we may preserve, use, or disclose your personal data or other safety data if we believe that it is reasonably necessary to comply with a law, regulation, legal process, or governmental request; to protect the safety of any person; to protect the safety or integrity of our platform, including to help prevent spam, abuse, or malicious actors on our services, or to explain why we have removed content or accounts from our services; to address fraud, security, or technical issues; or to protect our rights or property or the rights or

[1] https://help.twitter.com/en/rules-and-policies/data-processing-legal-bases
[2] https://twitter.com/en/privacy

property of those who use our services. However, nothing in this Privacy Policy is intended to limit any legal defenses [sic] *or objections that you may have to a third party's, including a government's, request to disclose your personal data."*

Twitter stated that it has an obligation to ensure the safety, security and integrity of its services for all users and the public at large and, by allowing people to circumvent suspensions for violating its policies (e.g. hateful conduct, child sexual exploitation) by simply detaching and deleting their phone numbers or email addresses from their account so that they can deactivate the account and create a new account, this would put other people at risk. Twitter asserted that in such a case, the rights of the data subject do not override the legitimate interests (i.e. rights of others) being protected by the continued processing of the limited data.

28. The DPC reverted to Twitter with further queries via email on 11 May 2021 requesting that Twitter clarify the exact date the complainant submitted his request for erasure as Twitter had provided contradictory dates during the complaint handling process.

29. Twitter responded to the DPC's queries via email on 14 May 2021. In its correspondence, Twitter asserted that a formal data erasure request referencing Article 17 of the GDPR from the complainant was received on 02 June 2019 and attached a screenshot. Twitter stated that on 16 May 2019 the complainant submitted a request to remove his phone number and email address from his account, and then to deactivate the account. Twitter asserted that this request did not reference the right to erasure or specifically request deletion of all data associated with the complainant's account (although it did request deletion of his phone number and email address). Twitter again stated that it is its policy to retain basic subscriber information (e.g., email or phone number used to sign up) to protect its platform from known policy violators. Twitter advised that deactivation of an account, which is what the complainant requested on 16 May 2019, also does not result in the automatic deletion of data associated with the account. Twitter stated that, as set out in its publicly available Help Centre article with respect to deactivated accounts, deactivated accounts only have data associated with them deleted if they are not reactivated within 30 days. Twitter again asserted that the complainant filed a litany of near identical complaints causing duplication of efforts, and then failed to follow instructions provided to him causing delays in the processing of his request.

30. The DPC provided both the complainant and Twitter with a copy of its preliminary draft decision on 20 September 2021 and requested their submissions on the content of the preliminary draft decision.

31. The complainant responded via email on 20 September 2021 and confirmed that he had no further submissions to make.

32. Twitter responded via email on 06 October 2021. In its submission, Twitter summarised its position on the facts pertaining to the complaint. Twitter opined that it is questionable whether the complainant's conditional request to delete his Twitter account only after the deletion of his email address and phone number can properly be characterised as an Article 17 request at all. Twitter stated that conditional or contingent requests are not contemplated by the GDPR and it remains unclear how they should be handled or defined under the legislation. Twitter stated that it had addressed both elements of the complainant's request (i.e. the email/phone number erasure request and the account deactivation/deletion request) and reserved its position in this respect.

33. Twitter advised that when a user opens a Twitter account, it requests that the new user provide unique identifiers (email and telephone numbers) so that a user can be uniquely associated with that account, but that these registration details are not intended to be, nor are they in fact, a method to verify the real identity of a new Twitter user. Twitter stated that neither piece of information on its own or in combination verifies a person's identity and consequently, whenever Twitter subsequently has a requirement to verify the identity of a person purporting to be a Twitter user, Twitter must seek ID information at that point in time. In doing so, Twitter is in the same position as a bank or other institution that has a valid reason to verify a person's identity, and the same verification methods (e.g. photographic ID with a signed declaration) are available to Twitter as to those institutions. Twitter stated that the DPC has erred in classifying the email/telephone number provided at account opening as identity verification information, and as a result the DPC has wrongly concluded that these identifiers were valid substitutes to the photographic ID requested by Twitter.

34. Further, Twitter stated that it did not ever in fact collect the complainant's photographic ID, and as such Article 5(1)(c) is not engaged as Twitter did not process the relevant data in question. Twitter further stated that the wording of Article 5(1)(c) states that personal data shall be *"adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"*. Twitter advised that as the photographic ID was not collected in this instance, the data was not processed and therefore it was not possible for Twitter to have

collected data that was not adequate, relevant or limited to what was necessary for the purposes of processing.

35. Twitter stated that if it did process the data in question simply by requesting a copy of the ID, the following points stand. In order to meet the principle of data minimisation, the data controller must meet the three separate parts of Article 5(1)(c) and only process data that is: i) adequate; ii) relevant; and iii) limited to what is necessary in relation to the purposes for which they are processed.

36. Twitter advised the DPC that the purpose of processing the complainant's ID was to make sure that it had received a valid request from the data subject himself and not from someone impersonating the data subject seeking to impact the true account holder's account. Twitter stated that its conduct in pursuing this purpose met all three parts of the data minimisation test.

37. Twitter stated that the request for a copy of ID was adequate as it was necessary for Twitter to ensure that it had sufficient information to make sure that it could identify the individual making the erasure request. Twitter stated that, given the complainant could not log into his account as it had been suspended for breach of Twitter's Hateful Conduct policy, the complainant could not use the self-service tools to deactivate his account and therefore, the complainant's identity could not be verified by simply logging into his account. Twitter again advised that for such account holders, Twitter provides a mechanism to write in to request deactivation and/or the erasure of other personal data. Twitter stated that, while it has a record of the complainant's email address on file, Twitter understands (and has experienced) the relative ease with which email addresses can be hacked and therefore it does not generally consider that a request from an email address linked to the account is adequate on its own as a source of identity information. Twitter stated that this is particularly the case with an individual who has been suspended from Twitter services for breach of Twitter policies including the Hateful Conduct policy. Twitter advised the DPC that such individuals have targeted other Twitter users with hostile, sometimes racist, content, and therefore both the targeted individuals and others who have seen the harmful content would have a motive to seek to remove the individual's data from the platform, either as a form of revenge or to protect themselves and others from similar harm. Further, Twitter stated that the request for a copy of the complainant's ID was relevant to the question of whether the person making the request was who they say they were.

38. Twitter stated that in order to assess the necessity and proportionality of its request for a copy of ID, the specific circumstances of the request must be taken into account, namely that the request was made in relation to the account of a

user who had been suspended for violation of Twitter's Hateful Conduct Policy and the request was made by a user who did not have access to the usual means available to check identity (i.e. the ability to log in to the relevant Twitter account). Twitter also drew the DPC's attention to Recital 64 of the GDPR which states *"The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers."*. Twitter stated that its request for photographic ID was both proportionate and necessary because a higher level of authentication is required where a person is not logged into a Twitter account, which will always be the case with an individual whose account has been suspended, and it is therefore reasonable to ask for further evidence of identity. Twitter advised that where a user has been suspended due to hateful conduct, added caution is required when handling requests from their account, because other Twitter users will have a motivation to try to ensure the individual's data is erased from the platform, both to harm the individual and to protect themselves and others. Further, Twitter advised that the Hateful Conduct which breached Twitter's policy may also violate a law and it is therefore possible that the data will be the subject of valid legal process and Twitter must make sure it has not been accessed or deleted without due authorisation. Twitter opined that Recital 64 of the GDPR specifically recognises that online services may warrant the need to verify identity using *"all reasonable means"*. Twitter stated that a photographic ID is an identification method that is very unlikely to have come into the control of another person and it therefore provides a high level of certainty about someone's real-world identity and the person Twitter is dealing with. Twitter stated that the deactivation and then deletion of an account is a serious step as it is permanent. Twitter advised that as some individuals rely on their Twitter accounts for their livelihoods, the decision to deactivate a user's account can have significant ramifications, and therefore ID generally needs to be confirmed with a high level of certainty when dealing with deletion of account or other erasure requests. Twitter advised that if the user has provided fake details for all the other touchpoints (including name, email address, etc.) then the photographic ID is the only way Twitter can link the account to a real-world person. Twitter advised that this is particularly vital where an individual has been permanently suspended from the platform and may try to open a new Twitter account under another name. Twitter stated that the request for photographic ID is important in a scenario whereby an individual has managed to illegitimately deactivate another person's account, as it provides Twitter with the means of connecting that request to a real person. Twitter advised that the copy of the photographic ID would only be used for the specific purpose of identity verification and would only be retained for a maximum of 30 days, straying neither into disproportionate use nor disproportionate storage of the data.

39. Twitter stated that the fact that it had no record on file of the data subject's photograph against which it could check the veracity of whatever photographic ID the data subject submitted is irrelevant. Twitter advised that it was not requesting the photographic ID for the purpose of checking the photograph against a picture it had on file. Rather, Twitter was collecting the photographic ID as a means of validating a user's real-world identity using a method of verification that is very unlikely to have come within the control of another person, in contrast with an email address or phone number, which can more easily be hacked or used by another individual. Twitter advised that it also verifies the photographic ID against the signed declaration that the account was owned by the declarant. Twitter stated that its request for photographic ID could not be considered disproportionate solely on the basis that the provision of a copy of such data was not a requirement at account opening stage. Twitter stated that such a request for photographic ID from all users of Twitter as a condition for registration would be contrary to the spirit of the data minimisation principle as requesting such ID at account opening stage is neither necessary nor proportionate. Twitter stated that just because a data controller does not request photographic ID at account sign-up stage doesn't mean that conditions may not change such that the photographic ID is needed at a later date for a different purpose.

40. Twitter opined that it is instructive to consider the ID verification methods that are used by other organisations with a requirement to verify their customers' identities. Twitter provided guidance from the Law Society of Ireland on solicitors' KYC (Know your Client) requirements for Anti-Money Laundering checks states that *"In respect of individuals, "identity documents", such as passports and driving licences, are often the best way of being reasonably satisfied as to someone's identity".* Twitter stated that these are examples of photographic IDs that solicitors can validly request from clients (with no related requirement to verify them in person). Twitter argued that its approach is more proportionate than the approach advocated by the Law Society as it only seeks photographic ID in rare scenarios where the person making the request can no longer access the account (either because Twitter has taken action on the account for policy violations, or because they cannot reset their password), rather than requesting the ID from all account holders at the account opening stage.

41. Twitter stated that it has always considered the proportionality of requesting photographic ID for rights requests. Twitter stated that, for requests of this nature, identification is still required, however, where there is a high level of certainty of the user's identity based on other signals (e.g., email of the requester is the same as that on file for the account, the email associated with the account

does not appear to have been recently changed, etc), identification may not be mandated. Twitter informed the DPC that its self-service tool via account login remains the optimal method to minimize risks to data subjects.

42. Twitter advised that it waived the requirement for the provision of photographic ID before acting on the complainant's request to delete his account and the associated email/telephone number. Twitter advised that it acquiesced to the complainant's request to have the notified Twitter account deactivated/deleted (but not the associated email/telephone number), notwithstanding the fact that he had sought to condition that action by the prior deletion of the email/telephone number associated with that account. Twitter stated that this was done on an exceptional basis in an effort to amicably resolve the issue with the data subject and avoid any escalation to the DPC. Notwithstanding the exceptional action taken in this case, Twitter submitted that its insistence on photographic ID and a signed declaration for the purpose of verifying the identification of a person requesting the deletion of a suspended Twitter account and/or the email and telephone number associated with that account is fully justified both in this case and in general for the reasons outlined above.

43. Twitter stated that *'Reasonable doubts'* about the identity of an online user are generally inherent in the nature of online services. Twitter advised that this was particularly the case with regard to the complainant's circumstances, given his Twitter account had been suspended due to hateful conduct in breach of Twitter's policies, meaning there would very likely be individuals who would have been motivated to have the account deleted and the complainant's data erased. Twitter further stated that it did not hold any information about the natural identity of the complainant and his email address could have been used solely for the purpose of his Twitter account, and that his phone number could have been that of a friend or relative, or a temporary number. Twitter stated that given the consequences of deleting the account entirely would have been grave, as the data cannot later be retrieved, Twitter needed to use a process that gave extra assurance that the request was coming from the correct person and so it could show it had taken necessary and proportionate steps to check the identity in case it later turned out the request had not been made by the data subject but by someone else.

44. With regard to its request for a copy of photographic ID, Twitter submitted that a lawful basis is not required to request personal data from a data subject. Twitter stated that Article 6 GDPR provides that "processing" will only be lawful where one of the bases in Article 6 applies. Twitter advised that "Processing" is defined in Article 4(2) as *"any operation or set of operations which is performed*

on personal data or on sets of personal data". Twitter asserted that for an operation to be "performed on" personal data, some action must be carried out "to" or "with" the personal data in question. Twitter stated that the list of "operations" in Article 4(2) notably does not include any activities that are contemplative or speculative, such is the inherent nature of a request. Twitter further stated that there is no reference in Article 4(2) to the fact that "requesting" or "seeking" personal data will amount to "processing". Twitter asserted that, for this reason, to consider the act of asking for personal data is itself a form of collection, does not follow a logical interpretation of the legislative definition, nor does it follow the common-sense meaning of the term "collection". Twitter stated that it cannot be the case that by requesting something, which you never receive, you have in fact collected it.

45. Twitter stated that it never received the complainant's photographic ID and therefore never performed any operation, or set of operations, on the personal data and it did not process the complainant's ID. Twitter submitted that Article 6 of the GDPR is not engaged in the context of this complaint. Twitter stated that irrespective of the fact that provision of ID was stated to be mandatory in order for Twitter to effect the complainant's erasure request (notwithstanding the fact that in this case it took the exceptional step of deactivating the complainant's request based on email authentication), this does not alter the analysis set out above. Twitter stated that it never received a copy of the ID, never performed any operation or set of operations on it, and therefore never collected or processed the personal data.

46. Twitter stated that the DPC may argue that, even if Twitter did not process the complainant's ID in this specific case, it does in limited circumstances collect and process ID from permanently suspended users who submit an erasure request. Twitter submitted that the DPC cannot broaden the scope of its investigation in light of the definition of "complaint" in the Data Protection Act 2018 ("**DPA 2018**"). Twitter stated that the definition of a "complaint" in accordance with Section 107 of the DPA 2018 is conditioned on the complaint being in respect of the processing "*of personal data relating to him or her [the data subject]*" i.e. the data subject making the complaint. Twitter therefore asserted that the DPC cannot extend its examination of this specific complaint to Twitter's general processing of personal data relating to other data subjects who have not submitted a complaint.

47. Twitter stated that, without prejudice to the above, in the event Twitter had collected the complainant's ID it would have processed the data on the basis of legitimate interests in accordance with Article 6(1)(f) of the GDPR. Twitter stated that the collection of ID was necessary to pursue the following legitimate

interests: confirming the identity of the requestor, ensuring that the request was not fraudulent, and by extension protecting the safety, security and integrity of the Twitter platform and other users. Twitter stated that it had explained why the collection of ID is necessary and proportionate in cases involving suspended users and the same analysis supports the legitimate interests pursued by Twitter under Article 6(1)(f) of the GDPR. Twitter stated that, in such circumstances, it does not consider that these legitimate interests are overridden by the rights of the data subject. Twitter asserted that the ID is collected for the specific and sole purpose of handling the data subject's erasure request, verifying the individual's identity and is removed from Twitter's systems within 30 days. Finally, Twitter stated that the legitimate interests pursued are significant and have a direct bearing on the safety and security of other Twitter users and the Twitter platform more broadly. Twitter opined that, taking these factors into account, its legitimate interests in collecting photographic ID for the purposes of handling erasure requests from suspended users are not considered to be overridden by the rights of the data subject supplying the ID.

48. With regard to its compliance with Article 17 of the GDPR, Twitter stated that on receipt of the complainant's erasure request, it was in constant correspondence with the complainant in relation to the numerous requests he had filed several of which Twitter claimed included highly abusive language. Twitter stated that the time taken to inform the complainant that certain account information would be retained after his account had been deactivated was the result of a number of different issues such as; i) the back and forth in correspondence; ii) the complainant's refusal to provide his photographic ID; and iii) the complainant's failure to follow instructions on how to deactivate his account. Twitter stated that on account of these factors there was no "undue delay". Twitter stated that it informed the complainant on 31 July 2019 that "*To ensure a safe and secure platform, we currently do not provide a possibility to delete an email address.*" Twitter stated that it is not correct to say that the complainant was first informed on 1 October 2019 that certain account information would be retained. Twitter stated that it is willing to supply a copy of this correspondence to the DPC if requested. Twitter stated that the right under Article 17(1) is to *"obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies".* Twitter stated that where the right to erasure and / or obligation to erase data does not apply, either because an exemption applies or because none of the Article 17 grounds can be established, a data controller cannot be found in breach of failing to erase data (it is not required to erase) "without undue delay". Twitter stated that it has a valid legal basis under Article 6(1)(f) for the retention of the complainant's email address and phone number and, on that basis none of the Article 17(1)

grounds can apply, meaning that Twitter was not subject to the Article 17(1) obligation to erase the complainant's email address and phone number "without undue delay". Twitter asserted that it did not infringe Article 17 in respect of the complainant's request to delete the email address and phone number associated with his account as it had a lawful basis to retain this data, thus it follows that the personal data remains necessary for the purposes for which it was collected and is processed by Twitter. On this basis, Twitter asserted that as the Article 17(1)(a) ground for erasure does not apply, neither can any of the other Article 17 grounds be established based on the facts of the complaint.

49. With regard to its compliance with Article 12(3) of the GDPR, Twitter stated that the time taken for Twitter to inform the complainant: i) that his account had been deactivated; and ii) that certain information would be retained after account deactivation/deletion, resulted primarily from the nature and frequency of the complainant's requests, Twitter's legitimate requirement that users of suspended accounts should provide ID before processing such requests, and the complainant's repeated attempts to halt the deactivation process.

50. Twitter advised the DPC that the complainant submitted several requests (six in total) that were confusing and at times contradictory. Twitter stated that the complainant's primary request appeared to relate to the erasure of the email address and phone number associated with his Twitter account and that the complainant conditioned the deletion of his account (and account content) upon Twitter first deleting the email address and phone number associated with the account, *"under Article 17 of GDPR, please remove my phone number and email. Once you have confirmed that has been done, you may delete the account as I am unable to."* Twitter stated that contingent or conditional erasure requests of this nature are not contemplated by the GDPR and it remains unclear in law how they should be interpreted and handled. Twitter opined that this inherent uncertainty calls into question the very application of the statutory timeframes under Article 12(3) GDPR or whether such requests can even be considered erasure requests under Article 17. Twitter advised the DPC that on a number of occasions the complainant also gave conflicting instructions. Twitter stated that, having reiterated requests for Twitter to delete his email address and phone number, and stating that any account deletion was contingent upon this, on 28 June 2019 he instructed Twitter to remove *"ALL associated data" from the account."* Twitter advised that in correspondence of 01 July 2019 the complainant stated *"REMOVE MY DATA IMMEDIATELY AND CONFIRM ONCE DONE."* Twitter advised the DPC that the contradictory nature and frequency of the requests were such that the complainant was directed through the removal and account deactivation processes by Twitter's support teams due to the complainant's repeated references to deleting his account and the lack of

clarity over the precise scope of his request. Twitter explained that its support teams should have transferred the complainant's requests to a different team but the litany of near identical complaints submitted by the complainant led to a duplication of efforts, which complicated and delayed the support teams' handling of the requests on this specific occasion. Twitter stated that, while it accepted that the support teams should have referred the requests to a different team, it wished to highlight that the complainant received responses from Twitter and was informed several times that Twitter requires ID and a signed statement in order to process account deactivation/deletion requests from suspended users. Twitter advised that on four separate occasions, the 17 and 28 June 2019 and 1 and 2 July 2019, Twitter informed the complainant that he needed to provide a signed statement and an unredacted copy of his ID in order for Twitter to confirm his identity and initiate the deactivation of his account and that it was, therefore, clear to the complainant why further steps were not being taken in respect of his request.

51. Twitter advised the DPC that the complainant's request was passed to the appropriate internal team at Twitter on 26 June 2019. Twitter stated that in light of the complainant's repeated refusal to provide photographic ID, Twitter determined that it would in this exceptional case authenticate the complainant on the basis of his email address. Twitter advised that this decision was also taken in the interests of amicably resolving the request without escalation to the DPC. Twitter informed the DPC that the account deactivation/deletion process was initiated promptly on 5 July 2019 but was halted when the complainant tried to log back into his account. Twitter advised the DPC that the complainant was informed on 31 July 2019 and again on 6 August 2019 that his email address would be retained and that he was specifically informed that, *"To ensure a safe and secure platform, we currently do not provide a possibility to delete an email address. As mentioned in our Help Center, we continue to store your previously used email addresses for safety and security purposes:"*

52. Twitter stated that it accepts that the requests should have been passed to the correct team sooner, it did act promptly on the complainant's request once the correct team had received the reports. In addition, Twitter stated that it informed the complainant that his email address would be retained for safety and security reasons on 31 July 2019 and 6 August 2019. Twitter asserted that the timeframes must also be assessed in the context of Twitter's requirement that users of permanently suspended accounts had to provide ID and a signed statement in order for Twitter to confirm their identity and proceed with an erasure request. Twitter stated that this requirement is proportionate and compliant with the GDPR. Twitter stated that it was not required to take action on the complainant's erasure request until it was in a position to identify him.

Twitter stated that guidance from the DPC on subject access requests specifically states that *"Where the controller does require more information or proof of identity... the time limit for responding to the request begins when they receive the additional information"*. Twitter asserted that pursuant to both the GDPR and the DPC's Guidance, the usual one month time limit for responding to the erasure request (including informing the data subject of the action taken in respect of his request) did not begin to run until Twitter was in a position to confirm the identity of the data subject. Twitter stated that it considered it proportionate and justifiable to request an ID in these circumstances and it was this requirement, and the complainant's refusal to provide his ID, which provide a legitimate explanation as to why Twitter did not immediately deactivate the complainant's account and why he was not immediately informed that certain account information would be retained.

53. Twitter asserted that the complainant gave conflicting instructions as to whether his Article 17 request encompassed a request for the erasure of his Twitter account content. Twitter opined that there are grounds to argue that the account deletion request would not constitute an Article 17 erasure request in view of its conditional nature and because of the way the complainant articulated the request. Twitter stated that, if this is the case, it is not open to the DPC to find that any alleged delay in deactivating the account/deleting its data constitutes an infringement of Article 12(3) and/or Article 17(1) GDPR and that, at the very least, the conditional nature of the complainant's request calls into question the application of the statutory timeframes under Article 12(3) GDPR. Twitter submitted that where a request is made conditional on the controller taking another action, it cannot be correct that the one month timeframe applies in the same way as it would for a 'direct' request as there are additional steps the controller is being asked to take.

54. Twitter stated that it accepted that the complainant made an Article 17 erasure request for the erasure of his email address and telephone number associated with his account. However, Twitter stated that given that it was entitled to refuse to act on this request as it had a legal basis to retain this data, there is no basis for the DPC to find that Twitter has infringed Article 12(3) GDPR. Twitter stated that Article 12(3) GDPR obliges a controller to provide information to a data subject on the "action taken on a request". Twitter submitted that Article 12(3) GDPR is not engaged in circumstances where a controller has decided not to take action in response to an Article 17 erasure request, as was the case here. Twitter asserted that Article 12(3) GDPR does not apply in circumstances where a controller declines to acquiesce to a data subject's erasure request. Further, Twitter stated that in the event the DPC were to make a finding in respect of Article 12(4), Twitter would reiterate that there was no undue delay when

Twitter's authentication procedures and the nature of the complainant's requests are taken into account.

55. The DPC reverted to Twitter requesting clarification in relation to a number of issues.

56. Twitter responded to the DPC via letter dated the 26 November 2021. In its correspondence Twitter confirmed that the complainant's account was deleted on 16 October 2019. Twitter also provided the DPC with a copy of four correspondences issued to the complainant in relation to his erasure request. The correspondences are dated 17 June 2019, 26 June 2019, 01 July 2019 and 02 July 2019. In the correspondence of 17 and 26 June 2019 Twitter requested that the complainant upload the following: a signed request that includes his username and email address associated with the account and a scanned copy of valid government-issued photo ID. Twitter advised the complainant that once it received these documents it could then process his request. In its correspondence to the complainant dated 01 July 2019, Twitter advised the complainant that *"We require 2 factors of identification including a signed statement with a corresponding unredacted ID to confirm your request. These measures are necessary to ensure account security. Please note that your ID will only be used to confirm the request, and will be promptly removed from our system once the request has been completed. If you would still like to proceed with your original request, please upload required[sic] documentation here . . "*

57. In its correspondence to the complainant dated 02 July 2019, Twitter advises the complainant that *"unless we receive a signed statement with a corresponding unredacted ID to confirm your request. These measures are necessary to ensure account security. Rest assured that your ID would only be used to confirm the request, and would be promptly removed from our system once the request is completed. Please note that this case will now be closed."*

58. The DPC reverted to Twitter and requested that it clarify whether it was retaining all personal data relating to the data subject up until the point his account was erased on 16 October 2019, or whether it was only retaining his username and associated mobile phone number.

59. Twitter responded to the DPC via correspondence dated 09 December 2021. Twitter stated that, with respect to the complainant's request to deactivate his account and have his associated personal data deleted, prior to deletion of the account, Twitter retained all data associated with complainant's account. Twitter advised that, ordinarily, Twitter users can simply deactivate and delete their information from within their account. Twitter advised that the process is

described in detail in its Help Centre article *"How to Deactivate Your Account."* Twitter stated that this was not applicable to the complainant because he had been suspended for violating Twitter's Hateful Conduct Policy and that once an account has been suspended the individual cannot access it, and therefore, cannot use the account as means to deactivate it and thereby delete the data associated with it. Twitter advised that, as a result, the complainant had to engage with Twitter's Office of Data Protection in order to request deletion. Twitter again stated that the complainant repeatedly failed to follow the instructions provided by Twitter on how to deactivate his account. Further, Twitter asserted that the complainant gave Twitter conflicting instructions regarding deletion of his personal data, in which he sought both the deletion of his Twitter account and the deletion of information Twitter needs to retain for safety and security purposes. Twitter stated that it nevertheless took the step to deactivate the complainant's account based on email authentication, deviating on an exceptional basis, from the normal procedure of ID verification for violators of Twitter's policies with suspended accounts.

60. By email to DPC dated 17 December 2021, Twitter stated that, with respect to the complainant's request to delete his data, the specific demands and nature of these requests were exceptional and odd. Twitter stated that the complainant requested deletion of his email and phone number, then confirmation of this deletion, followed by deletion of the rest of his information. Twitter asserted that complying with the complainant's request in this way would allow the complainant to side-step the disciplinary actions taken by Twitter against him for violating Twitter's Hateful Conduct Policy, by allowing him to create a new account with the same email and phone number. Twitter stated that alternatively, such a request from an individual who was not the owner of the account, if Twitter followed through with it, would enable the individual to delete the data of the true account holder and impersonate them with a new account using the same email and phone number. Twitter stated that requesting deletion in this specific sequence raised doubts and concerns that the requester had intentions of pernicious behaviour.

61. Twitter further stated that Recital 64 of the GDPR requires online services and online identifiers, such as Twitter, to use all reasonable measures to verify the identity of data subjects who request access. Twitter stated that in this instance, a higher level of scrutiny and authentication was reasonable because of the account being suspended and the potential for impersonation. Twitter advised that as a consequence of this, it requested to authenticate the complainant with a photographic ID to protect the interest of its users and the health and integrity of its platform. Twitter stated that, while such photo ID is not something Twitter already has in its possession and so is unable to use it for actual authentication,

its provision nevertheless significantly lessens the likelihood of the requester impersonating the data subject by ensuring they have access to an officially-issued document bearing the data subject's name. Twitter asserted that, accordingly, it believes it was a proportionate approach in these particular unusual circumstances.

62. The DPC has carefully considered Twitter's submissions in making this decision.

Summary of Relevant and Reasoned Objections and opinions received from "supervisory authorities concerned"

63. The DPC received formal relevant and reasoned objections in relation to the draft decision, pursuant to Article 60 (4) of the GDPR, from two supervisory authorities concerned:
    - Personal Data Protection Office (Polish DPA); and
    - Comissão Nacional de Protecção de Dados (Portuguese DPA).

64. The DPC also received opinions, which were not expressed as formal objections, in relation to the draft decision from two other supervisory authorities concerned;
    - Tietosuojavaltuutetun Toimisto (Finnish DPA); and
    - Garante Per La Protezione Dei Dati Personali (Italian DPA).

65. While the Polish DPA agreed with the DPC's findings, in its relevant and reasoned objection the Polish DPA opined that the DPC's draft decision failed to reference the right of an effective legal remedy. The Polish DPA referred to recital 129 of the GDPR in that regard. In the Polish DPA's opinion, the draft decision risks violating the rights and freedoms of data subjects, including the rights under the Charter of Fundamental Rights of the EU, the right to the protection of personal data (Article 8) and the right to an effective remedy and to a fair trial (Article 47) and that leaving the draft decision unchanged would significantly limit the possibilities of data subjects to assert their rights, as this would hinder or prevent the use of an effective remedy in the form of an appeal against the settlements contained in the decision with which the party does not agree. The DPC has carefully considered this matter and makes the following observations. With respect to a draft decision submitted to the Article 60 procedure by the lead supervisory authority, Article 60(6) of the GDPR states that *"Where none of the other supervisory authorities concerned has objected to the draft decision submitted by the lead supervisory authority within the period referred to in paragraphs 4 and 5, the lead supervisory authority and the*

supervisory authorities concerned shall be deemed to be in agreement with that draft decision and shall be bound by it.". Further, Article 60(7) of the GDPR states that *"The lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller or processor, as the case may be and inform the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged shall inform the complainant on the decision."* As the concerned supervisory authority with whom the complaint was lodged is bound by the decision and is responsible for notifying it to the data subject, data subjects may in some cases have the right to a judicial remedy in respect of the supervisory authority in the country where they have lodged their complaint. On this basis, in the ordinary course when issuing a final decision, the DPC notifies the parties of their right to an effective judicial remedy in the cover letter that issues with the final decision. However, in this instance as the complaint was lodged directly with the DPC, and on this basis the complainant's right to an effective judicial remedy will be in respect of the DPC's final decision, the DPC has now included in this decision a notice relating to the judicial remedies (see paragraph 122 below).

66. In its relevant and reasoned objection the Portuguese DPA disputed the DPC's conclusion in the draft decision, for a number of reasons as outlined by the Portuguese DPA, that there is a valid legal basis for the data controller to keep, indefinitely, the email address and telephone number of the user who has the account suspended for violation of Twitter's terms of use, conditions or conduct policies (e.g. hateful Conduct Policy), despite the request for erasure and deactivation of account. The Portuguese DPA stated that it considers that a reasonable maximum period for data retention should be imposed, which, it stated, would reflect in fact a balance of interests. The DPC has carefully considered this matter and has inserted a new paragraph in this decision (see paragraph 116 below).

67. In its opinion, the Finnish DPA opined that the DPC's reasoning in the draft decision could be elaborated by duly taking into account whether the data being retained by Twitter are relevant, adequate and limited to what is necessary in relation to the purposes for which they are processed in terms of the data minimisation principle and whether such data are retained for no longer than is necessary for the purposes for which the personal data are processed, that is, the temporal requirement inherent in the storage limitation principle. The Finnish DPA opined that the draft decision might create, by way of accepting certain data being retained indefinitely, a new industry standard and unjustly normalise indefinite data storage, and would, thus, entail risks for the rights and freedoms

of data subjects. In its opinion, the Finnish DPA asked the DPC to take its remarks into account and consider revising the reasoning of the draft decision accordingly regarding Twitter's retention practice as regards to Twitter retaining email addresses and phone numbers of its suspended users, who have asked for the removal of their personal data, indefinitely and it opined that, perhaps, the draft decision would benefit from elaborating why the thresholds of data minimisation and data storage principles are satisfied in this case/instance.

68. In its opinion, the Italian DPA opined, regarding the data controller's failure to erase the phone number and email associated with the Complainant's account due to security reasons, that the balancing test of the interests at issue would appear to require some further elaboration in the draft decision and that it invites the DPC to consider supplementing the draft decision by further detailing the reasons why the data controller's interests override the rights and freedoms of the data subject. The Italian DPA stated that it harbours some doubts as to whether the processing in question complies with the storage limitation principle set out in Article 5 (1) (e) of the GDPR, insofar as no information is available on the retention periods applying to email and phone number data and that this is why it invites the DPC to consider this element either by amending the draft decision or, if the information and findings in the complaint file are not enough for that purpose, by initiating a new inquiry in that respect.

69. Further, the Italian DPA noted that the inquiry at issue concerns a single complaint, that the DPC did not initiate an own volition inquiry and it observed that the data controller was not ordered under Article 58 (2) (d) of the GDPR to bring the processing into compliance with the GDPR, in particular by undertaking to no longer require the users that do not submit their erasure requests via the self – help tool to provide their I.D. and photograph in order to be able to exercise their rights; it invited the DPC to consider whether this element should be taken into account in deciding on the exercise of its corrective powers.

70. Further to the above, the Portuguese DPA also provided an opinion in relation to the DPC's draft decision. The Portuguese DPA stated that it further considers to convey to the DPC its view as to whether it is necessary to add a corrective measure, under Article 58 (2) (d) of the GDPR, ordering Twitter to revise its internal policies and its procedures for handling requests for data erasure, ensuring that the DPC's conclusion regarding the infringement of Article 5 (1) (c) and Article 6 (1) of the GDPR by Twitter has a general application/effect in the future action of the data controller and does not relate solely/specifically to this complaint. The Portuguese DPA opined, thus, that unless that matter is clearly explained in the draft decision, it should be applied by the DPC as

corrective measure, under Article 58 (2) (d) of the GDPR, ordering Twitter to review its internal policy and its procedures with respect to requests for data erasure, in the circumstances where the accounts are suspended, provisional or permanently, using only email and telephone number as authentication factors for the data subjects. The DPC has carefully considered these opinions and it has now included a further corrective measure at paragraph 126 below.

Communication of revised draft decision to the data controller

71. In light of the opinions received from the supervisory authorities concerned, the DPC revised its draft decision to include a summary and analysis of the opinions expressed by the supervisory authorities concerned, as detailed in paragraphs 63 to 70 above.

72. The DPC provided the data controller with a copy of both the revised draft decision and the opinions of the supervisory authorities concerned by way of email on 10 March 2022. The DPC invited the data controller to provide any final submissions in relation to the matter by close of business 24 March 2022.

73. Twitter responded via email dated 24 March 2022. In its submission, Twitter stated that where it receives a request for the erasure of personal data and the requester is able to verify the email address or telephone number associated with the account, it is Twitter's policy to action the request without the requester additionally needing to provide photographic ID. However, Twitter stated that in a significant proportion of the data subject rights' requests Twitter receives, one of the following issues arises regarding the legitimacy of the request:

a)

b)

c)

d)

[redacted]

74. Twitter stated that where any of the above circumstances apply, if Twitter actioned the erasure request without asking for further proof of identity, it runs the risk of doing so at the request of someone other than the relevant data subject. Twitter advised that, accordingly, it is Twitter's policy to require the provision of photographic ID before an erasure request will be actioned in these cases, so that Twitter has a greater level of confidence that it is acting at the request of the appropriate data subject. Twitter stated that by obtaining the relevant ID, it acquires an additional level of assurance regarding the identity of the requester. Twitter advised that in many cases it can check that information on the ID matches the information that Twitter already holds for that account. However, Twitter advised that even in cases where the name does not match information already held by Twitter, the very fact of requiring provision of the ID reduces the risk of a false, fraudulent and potentially malicious request being pursued in the first place.

75. Twitter stated that it believes that its use of photographic ID in these circumstances, where the ID is not used for any purpose other than to provide additional protection to the data subject, and where the data is deleted after 30 days, is a legitimate and proportionate use of the data. Twitter wished to draw this point to the attention of the DPC and the CSAs to demonstrate why it considered that neither a reprimand nor a change of practice is warranted in these circumstances.

76. Twitter stated that if the DPC and CSAs are still of view that Twitter's request for photographic ID is not proportionate, it would be grateful if, as part of the DPC's final decision or via separate correspondence with Twitter, the DPC would confirm to Twitter that where it receives an erasure request and one of the above scenarios (a)-(d) apply, Twitter may either:
    a) reject the request, or;
    b) action the request confident in the knowledge that the DPC does not require it to obtain any further identity verification.

77. Twitter requested that if the DPC is not able to provide such confirmation, that it provides guidance as to how Twitter should proceed when circumstances (a)-(d) apply.(E.g. Would mere confirmation of the email address associated with the account (rather than verification via a link) be sufficient in scenario (b)?).

78. With regard to the indefinite retention of the user's email address and telephone number Twitter advised that, as stated in its policies on platform integrity and authenticity, Twitter is committed to combating abuse motivated by a variety of conducts, such as hatred, violence, prejudice or intolerance, particularly abuse

that seeks to silence the voices of those who have been historically marginalized and others. Twitter stated that, for this reason, it prohibits behaviours that are outlined in those policies. Twitter advised that where a Twitter user persistently breaches these policies, or commits a particularly serious breach, Twitter has taken the legitimate business decision that it will permanently suspend the user's account, to prevent further harm to the targets of the hateful conduct. Twitter stated that in order to enforce a permanent, lifetime ban, Twitter needs to be able to recognise when the owner of the suspended account attempts to set up a new account using the same credentials. Twitter advised that, as users must provide their email address and telephone number when setting up their account, Twitter needs to retain the email address and telephone number of banned users indefinitely, to prevent them from using such details to open up another account at any point in the future - i.e. to enforce the lifetime ban.

79. The DPC has carefully considered the above submissions of Twitter. Having done so, it does not propose to amend any of the findings as communicated to Twitter in the revised draft decision. Furthermore, it is not the purpose of a decision on a complaint to provide advices to a data controller. In light of Twitter's submissions it is, however, important to emphasise that Article 12(6) of the GDPR sets out the path that a controller may follow in the event that it has reasonable doubts concerning the identity of a natural person making a request such as an erasure request. This decision informs Twitter that in the circumstances of this particular case, its requirement for the data subject to verify his identity by way of submission of a copy of his photographic ID infringed the principle of data minimisation. It is a matter for the controller to find an alternative method of confirming the identity of the data subject in a manner that does not infringe the principle of data minimisation or any other provisions of the GDPR. With regard to Twitter's position that it needs to retain the email address and telephone number of banner users indefinitely, Article 5(1)(e) obliges controllers to keep personal data for no longer than is necessary for the purposes for which they are processed. Indefinite retention of personal data is not an option for data controllers and therefore it falls to Twitter as the controller in this instance to determine an appropriate specific retention period based on its business needs and legitimate interests.

Communication of revised draft decision to the CSAs

80. The DPC communicated its revised draft decision to the CSAs on 07 April 2022.

81. The DPC received a comment from both the Polish DPC and the Portuguese DPA.

82. The Polish DPA advised that it was grateful to the DPC for taking its relevant and reasoned objection into account and informed the DPC that it accepted the content of the revised draft decision.

83. The Portuguese DPA thanked the DPC for accommodating its point of view and advised that it was now in agreement with the DPC's proposed revised decision and had no further objections.

Applicable Law

84. For the purposes of its examination and assessment of this complaint, the DPC has considered the following Articles of the GDPR:

- Article 5
- Article 6
- Article 12
- Article 17

Findings of Inquiry

Issue A - The complainant's allegation that Twitter did not have a lawful basis for requesting a copy of his ID in order to verify his identity in circumstances where he had submitted a request for erasure pursuant to Article 17

85. The complainant asserted that, on submitting a request for erasure pursuant to Article 17 of the GDPR, Twitter requested that he provide a signed statement and a copy of his photographic ID in order to verify his identity. The complainant contends that Twitter did not have a legal basis to request a copy of his photographic ID in circumstances where a user can create an account using just an email address and phone number to verify their identity and therefore the same data should be enough to verify his identity when exercising his right to erasure.

86. Throughout the handling of the complaint, Twitter asserted that it does not require a legal basis to request information but rather must have a legal basis tied to the processing of information should it be provided, but that the

complainant had not provided any such data in this case. Twitter has stated that, had the complainant provided a copy of his photographic ID, the legal basis relied upon for processing a copy of his ID was in pursuit of its legitimate interest. Twitter stated that, as the complainant had been permanently banned from the platform due to repeated violations of Twitter's Hateful Conduct Policy the complainant did not have access to self-help tools, which are ordinarily available to users. Twitter advised the DPC that these self-help tools enable users to deactivate their account without the necessity to provide ID. Twitter informed the DPC that, in this case, the complainant had been permanently suspended from the platform due to repeated violations of Twitter's Hateful Conduct Policy [3]. Twitter advised the DPC that when an account is permanently suspended the data subject must submit their request for erasure through Twitter's "Office of Data Protection" because they can no longer access their account, and therefore, cannot use the self-help tools associated with the account. Twitter advised that this process is in place because of situations where the suspension of the account may be due to violations of laws that would also require Twitter to keep information on foot of a valid legal process. Twitter explained that these manual requests are in place as requests from permanently banned users come under a higher level of scrutiny. Furthermore, Twitter advised the DPC that this process for banned users is ongoing in these scenarios given the risks of harm they wish to balance and to prevent these account holders returning.

87. Twitter stated that, in circumstances where a request has been manually submitted (i.e., through its help centre forms), it comes under a higher degree of scrutiny so that Twitter can ensure, to the maximum extent possible, that it is not processing fraudulent requests. Twitter informed the DPC that this process is in place as any person may complete a help form and email accounts may become compromised such that requests from email addresses associated with an account may not, in fact be from the owner of the account. As such, Twitter asserted that it must exercise significant diligence in processing these requests. On this basis, Twitter asserted that requesting ID verification of an individual seeking to have their account deactivated is a security measure implemented for the safety of all users of the platform. Further, Twitter stated that its request for photographic ID was both proportionate and necessary because a higher level of authentication is required where a person is not logged into a Twitter account, which will always be the case with an individual whose account has been suspended, and it is therefore reasonable to ask for further evidence of identity.

88. Article 4(2) of the GDPR defines "processing" as *"any operation or set of operations which performed on personal data or on sets of personal data,*

[3] https://help.twitter.com/en/rules-and-policies/hateful-conduct-policy

whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.".

89. Article 5(1)(c) of the GDPR states that *"Personal data shall be adequate, relevant and limited to what is necessary in relation to the specific purposes for which they are processed.".* Article 6(1)(f) of the GDPR states that the processing of personal data shall be lawful only if and to the extent the *"processing is necessary for the purposes of the legitimate interest pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.".* Further, Article 12(6) of the GDPR states that, *"Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject."*

90. The DPC notes that Twitter has stated that it does not require a legal basis to request information, but rather it must have a legal basis tied to the processing of information should it be provided. The DPC disagrees with Twitter on this point. The DPC considers that making the provision of photographic ID a mandatory requirement in order for the data subject in this case to exercise his rights pursuant to Article 17 of the GDPR constitutes the collection of personal data. This is processing as per the definition set out in Article 4(2) of the GDPR. In this case, Twitter has not identified any lawful basis under Article 6 for that specific data processing activity.

91. The DPC notes that Twitter has claimed a legitimate interest in verifying a user's identity prior to complying with an erasure request, especially in circumstances where the request was submitted through a help centre form that is readily accessible to any member of the public and from a data subject whose Twitter account was suspended at the time of the erasure request. However, in this instance Twitter has not sufficiently demonstrated to this inquiry that the request for a copy of an individual's photographic ID was either necessary or proportionate in circumstances where Twitter required the complainant to submit a copy of a photographic ID in order to process his erasure request even though the provision of a copy of such data was not a requirement at account opening stage. Therefore, if the data subject had submitted a copy of photographic ID in response to Twitter's request Twitter had no record on file of the data subject's photograph against which it could check the veracity of whatever photographic

ID the data subject submitted. Instead Twitter asserted that the request for ID allowed it to verify that the data subject's identity matches the name on their signed statement (made at the same time as the photographic ID was submitted). Other solutions were available to Twitter at the time that would not have necessitated the seeking of photographic ID. It was, for example, in possession of his email address (which Twitter has not claimed it had any concerns that it may have been compromised) and his mobile telephone number. There is nothing to suggest that Twitter used these tools that were already in its possession to assist it in verifying the data subject's identity.

92. The DPC notes that Twitter has advised that any person may complete a help form and has highlighted that email accounts may become compromised such that requests from email addresses associated with an account may not, in fact be from the owner of the account. The DPC also notes that Twitter stated that its request for photographic ID was both proportionate and necessary because a higher level of authentication is required where a person is not logged into a Twitter account, which will always be the case with an individual whose account has been suspended, and it is therefore reasonable to ask for further evidence of identity.

93. Further, the DPC notes that Twitter advised, in its submission of 24 March 2022 that, in a significant proportion of the rights requests it receives, one of the issues outlined at paragraph 73(a-d) above arises regarding the legitimacy of the request such that, if Twitter actioned the request without asking for further proof of identity, it would run the risk of doing so at the request of someone other than the relevant data subject. However, the DPC notes that none of those specific issues highlighted apply with respect to this complaint as, in this case, the complainant was suspended by Twitter and he was unable to access his account as Twitter had restricted his access.

94. The DPC considers that Twitter has not sufficiently demonstrated to this inquiry that it had reasonable doubts in this case as to the complainant's identity nor has it shown that it had any reason to believe that his email address had become compromised, such as would have justified it requesting the provision of additional information to confirm his identity in the form of photographic ID or otherwise. Further, the DPC does not consider that the request for ID is either necessary or proportionate in circumstances where a user's account has been suspended and they cannot log in to utilise the self-help tools, as it is Twitter who has deprived the user of the ability to log in to their account and as such this does not demonstrate a reasonable doubt as to the user's identity in accordance with Article 12(6). Further, the DPC considers that Twitter could have utilised the information already available to it, such as the complainant's

telephone number, to verify his identity and ownership of the account such as either (i) by requesting that he verify the phone number associated with the account or (ii) by contacting the complainant via the telephone number he had provided at account opening stage to verify that it was he who had submitted the erasure request.

95. **The DPC finds that Twitter's requirement that the complainant verify his identity by way of submission of a copy of his photographic ID constituted an infringement of the principle of data minimisation, pursuant to Article 5(1)(c) of the GDPR. This infringement occurred in circumstances where no such requirement for photographic ID was in place at the time the complainant opened his Twitter account, and a less data-driven solution to the question of identity verification (namely by way of confirmation of email address or verification of telephone number) was available to Twitter.**

96. **The DPC finds that Twitter has not demonstrated that reasonable doubts existed concerning the complainant's identity that would have necessitated the application of Article 12(6) of the GDPR.**

97. **The DPC finds that Twitter has not identified a valid lawful basis under Article 6(1) of the GDPR for seeking a copy of the complainant's photographic ID in order to process his erasure request.**

Issue B - An examination of whether Twitter's handling of the complainant's erasure request was compliant with the GDPR and the Act.

98. The data subject also complained about Twitter's handling of his erasure request. He asserted that Twitter had failed to properly comply with an erasure request submitted by him to it. He asserted that Twitter had not responded to his request within the statutory period and that it was retaining his phone number and email address associated with his account without a legal basis to do so.

Compliance with statutory timeframe

99. During the handling of the complaint, Twitter advised the DPC that the complainant did not submit a formal data erasure request referencing Article 17 of the GDPR until 02 June 2019 and it attached a screenshot. Twitter stated that, while the complainant submitted a request to remove his phone number and email address from his account on 16 May 2019, and to deactivate his

account once this data had been removed, this request did not reference the right to erasure or specifically request deletion of all data associated with the complainant's account. Twitter also provided the DPC with a copy of four correspondence issued to the complainant in relation to his erasure request. The correspondence is dated 17 June 2019, 26 June 2019, 01 July 2019 and 02 July 2019. In response to the DPC's request for confirmation as to when the complainant's personal data had been deleted in accordance with his erasure request, Twitter advised the DPC that the complainant's account information was deleted on 16 October 2019. However, the data subject's email address and telephone number were not deleted and Twitter informed this inquiry that the complainant was specifically notified of this in email correspondence on 01 October 2019 and 16 October 2019. Twitter stated that the email address and phone number associated with accounts held by permanently suspended users are retained indefinitely for the purposes of maintaining the safety and security of the Twitter platform and that this corresponds to the need to prevent permanently suspended policy violators from creating new Twitter accounts. The notification of 1 October 2019 told the data subject that *"when an account is suspended, depending on the violation we may keep certain information to prevent bad actors from regaining access to our platform. This is described in our Help Center. If you wish that Twitter deactivates the account on your behalf, please let us know."* The notification of 16 October, 2019 told the data subject that *"as requested, we deactivated the account on your behalf. Please note that when an account was suspended, depending on the violation, we may keep certain information to prevent bad actors from regaining access to our platform. This is described in our Help Center. This ticket will now be closed."*

100. In his initial correspondence with the DPC, the complainant provided the DPC with a number of screenshots and copies of correspondence he had previously had with Twitter in relation to his request. In this correspondence, the complainant provided the DPC with a copy of an email sent by him to Twitter on 13 May 2019 at 21.11. In that email to Twitter the complainant stated:

"under Article 17 of GDPR, please remove my phone number and email from the [redacted] *Twitter account. Once you have confirmed that has been done, you may delete the account as I am unable to. Do NOT delete the account until you have confirmed to ME that my personal data has been removed from that account."*

The DPC considers that the data subject's email to Twitter of 13 May 2019 as described above constitutes a valid request for erasure pursuant to Article 17 of the GDPR.

101. In accordance with Article 17 of the GDPR, a data subject is entitled to obtain the erasure of personal data concerning him or her from a data controller without undue delay.

102. Article 12(3) of the GDPR states that *"The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject."* Further, Article 12(4) of the GDPR states that *"If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy."*

103. The DPC notes that the complainant made a valid erasure request pursuant to Article 17 of the GDPR to Twitter on 13 May 2019. The complainant also received an automated email response to this request from Twitter on 14 May 2019.

104. In its correspondence to the DPC of 26 April 2021 Twitter stated that the delay in responding to the complainant's request was caused by the litany of near identical complaints filed by him and that this caused a duplication of efforts. Twitter also asserted that the complainant failed to follow instructions given to him, causing further delays in processing his request. Twitter advised the DPC that its support team received several reports from the complainant and requested the deactivation of the account [redacted] and more specifically the removal of the phone number and email address associated with the account. Twitter stated that its support team should have transferred these requests to a different team but failed to do so.

105. In summary, therefore, the erasure request was submitted on 13 May 2019; Twitter first requested that the complainant provide a copy of his ID and a signed statement on 17 June 2019; the requester was first told on 01 October 2019 that "certain information" would be kept by Twitter; the requester was told for a second time on 16 October, 2019 that "certain information" would be kept by Twitter; and the data subject's Twitter account information was deleted on 16 October 2019. Twitter continues to indefinitely retain the data subject's email

address and mobile telephone number (the matter of retention is dealt with further below).

106. While the DPC notes that the complainant issued a number of separate complaints to Twitter in relation to the matter of his erasure request, Twitter failed to provide the complainant with information on action taken in relation to his request within one month of receipt of the request.

107. **Based on the facts and analysis outlined above, the DPC finds that Twitter infringed Article 17(1) of the GDPR, as there was an undue delay in handling the complainant's request for erasure.**

108. **The DPC finds that Twitter infringed Article 12(3) of the GDPR by failing to inform the data subject within one month of the action taken on his request pursuant to Article 17 of the GDPR.**

Retention of Data following Erasure Request

109. Throughout the handling of his complaint, the complainant asserted that Twitter was retaining his personal data, namely his phone number and email address associated with Twitter account [redacted], without a legal basis to do so. The complainant informed the DPC that he had submitted an erasure request to Twitter pursuant to Article 17 of the GDPR, requesting that it erase his phone number and email address associated with his account. The complainant advised the DPC that he was aware that Twitter had retained this data as each time he tried to create a new account with this data it was immediately banned.

110. During the handling of this complaint Twitter advised the DPC that it retains following personal data relating to the complainant following the completion of his erasure request:

- The Phone Number associated with the account [redacted]
- The Email address associated with account [redacted]

Twitter stated that it retains this limited information beyond account deactivation indefinitely in accordance with its legitimate interest to maintain the safety and security of its platform and users. Twitter stated that it is its policy to retain basic subscriber information (e.g. email or phone number used to sign up) to protect its platform from known policy violators.

111. Twitter has asserted that, on three separate occasions between 26 April 2019 and 06 May 2019, Tweets from the complainant's account were found to be in

violation of its Terms of Service and specifically its "Hateful Conduct Policy". Twitter advised the DPC that the Hateful Conduct Policy prohibits users from promoting *"violence against or directly attack or threaten other people on the basis of race, ethnicity, national origin, sexual orientation, gender, gender identity, religious affiliation, age, disability, or serious disease."*. Twitter stated that, after each violation, the complainant was reminded of the Hateful Conduct Policy. Twitter informed the DPC that the complainant's third violation led to the permanent suspension of his account. Twitter advised the DPC that the complainant was aware of these violations as, when a Tweet is found to be in violation of its Terms of Service, the user is notified and is required to go through the process of removing the violating Tweet themselves before regaining access to their account or, alternatively, has the option of appealing Twitter's review if they believe Twitter has made an error. Further, Twitter advised the DPC that, if an account gets suspended after multiple violations of its Terms of Service, a user can appeal the account suspension by submitting a help centre form to Twitter for review. Twitter advised the DPC that the account [redacted] was not reinstated in response to the account holder's appeals as the suspension was confirmed valid after a second review.

112. Twitter asserted that if it were to delete the complainant's email address or phone number from its systems, he could then use that information to create a new account even though he has been identified and permanently suspended from the platform for various violations of its Hateful Conduct Policy. Twitter advised the DPC that the retention of this data in these circumstances is explained to user's via information published in its Help Centre and its Privacy Policy which notifies users that their data may be retained for these purposes as follows:

"Notwithstanding anything to the contrary in this Privacy Policy or controls we may otherwise offer to you, we may preserve, use, or disclose your personal data or other safety data if we believe that it is reasonably necessary to comply with a law, regulation, legal process, or governmental request; to protect the safety of any person; to protect the safety or integrity of our platform, including to help prevent spam, abuse, or malicious actors on our services, or to explain why we have removed content or accounts from our services; to address fraud, security, or technical issues; or to protect our rights or property or the rights or property of those who use our services. However, nothing in this Privacy Policy is intended to limit any legal defenses [sic] *or objections that you may have to a third party's, including a government's, request to disclose your personal data."*

Twitter stated that it has an obligation to ensure the safety, security and integrity of its services for all users and the public at large and that by allowing people to circumvent suspensions for violating its policies by simply detaching and deleting their phone numbers or email addresses from their account so that they can deactivate the account and create a new account, would put other users at risk. Twitter asserted that in such a case, the rights of the data subject do not override the legitimate interests of Twitter or other individuals.

113. Article 5(1)(c) of the GDPR states that *"Personal data shall be adequate, relevant and limited to what is necessary in relation to the specific purposes for which they are processed."*. Article 6(1)(f) of the GDPR states that the processing of personal data shall be lawful only if and to the extent the *"processing is necessary for the purposes of the legitimate interest pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."*

114. The DPC considers that Twitter has identified a valid legal basis for the retention of the complainant's personal data. It also considers that Twitter has sufficiently demonstrated that its legitimate interest in ensuring the integrity of its platform and protecting the safety and security of its users overrides the complainant's legitimate interests. Further, as Twitter has retained and is processing personal data limited to the complainant's email address and phone number that was associated with his account, the DPC considers that Twitter is processing personal data that is necessary for the purposes of pursuing its legitimate interest.

115. **Therefore, the DPC finds that Twitter has a valid legal basis in accordance with Article 6(1)(f) for the retention of the complainant's email address and phone number that were associated with his account. Furthermore, and without prejudice to its finding above concerning the data minimisation principle with regard to photo ID, the DPC finds that Twitter is compliant with the data minimisation principle set out in Article 5(1)(c) as the processing of this data (i.e. email address and phone number) is limited to what is necessary in relation to the purposes for which they are processed.**

116. However, in order to comply with the principle of storage limitation under Article 5(1)(e) the data controller is obliged to keep personal data for no longer than is necessary. This means, in this case, that the complainant's email address and phone number cannot be retained indefinitely by Twitter. The onus lies on Twitter as the data controller to determine, based on its business needs and

legitimate interests, the appropriate specific retention period to apply in this case.

Decision on infringements of the GDPR

117. Following the investigation of the complaint against Twitter International Company, the DPC is of the opinion that Twitter International Company infringed the General Data Protection Regulation as follows:

118. **Article 5(1)(c) of the GDPR**
The DPC finds that Twitter's requirement that the complainant verify his identity by way of submission of a copy of his photographic ID constituted an infringement of the principle of data minimisation, pursuant to Article 5(1)(c) of the GDPR. This infringement occurred in circumstances where no such requirement for photographic ID was in place at the time the complainant opened his Twitter account, and a less data-driven solution to the question of identity verification (namely by way of confirmation of email address or verification of telephone number) was available to Twitter.

119. **Article 6(1) of the GDPR**
The DPC finds that Twitter has not identified a valid lawful basis under Article 6(1) of the GDPR for seeking a copy of the complainant's photographic ID in order to process his erasure request.

120. **Article 17(1) of the GDPR**
The DPC finds that Twitter infringed Article 17(1) of the GDPR, as there was an undue delay in handling the complainant's request for erasure.

121. **Article 12(3) of the GDPR**
The DPC finds that Twitter infringed Article 12(3) of the GDPR by failing to inform the data subject within one month of the action taken on his erasure request pursuant to Article 17 of the GDPR.

Judicial remedies with respect to decision of the DPC

122. In accordance with Article 78 of the GDPR, each natural or legal person has the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them. Pursuant to Section 150(5) of the Act,

an appeal to the Irish Circuit Court or the Irish High Court may be taken by a data subject or any other person (this includes a data controller) affected by a legally binding decision of the DPC within 28 days of receipt of notification of such decision. An appeal may also be taken within 28 days of notification by a data controller: under Section 150(1) against the issuing of an enforcement notice and/or information notice by the DPC against the data controller; and under Section 142, against any imposition upon it of an administrative fine by the DPC.

Remedial measures undertaken by Twitter International Company

123. In respect of the complainant's request for erasure of personal data submitted on 13 May, 2019 pursuant to Article 17(1) of the GDPR, it is noted that Twitter has erased the complainant's personal data associated with his Twitter account, aside from his email address and phone number, albeit it did not confirm the deletion of the complainant's data until 12 November 2019 when the complainant's account was permanently deactivated.

Exercise of Corrective Power by the DPC

124. In deciding on the corrective powers that are to be exercised in respect of the infringements of the GDPR outlined above, I have had due regard to the Commission's power to impose administrative fines pursuant to Section 141 of the 2018 Act. In particular, I have considered the criteria set out in Article 83(2)(a) – (k) of the GDPR. When imposing corrective powers, I am obliged to select the measures that are effective, proportionate and dissuasive in response to the particular infringements. The assessment of what is effective, proportionate and dissuasive must be made in the context of the objective pursued by the corrective measures, for example re-establishing compliance with the GDPR or punishing unlawful behaviour (or both)[4]. I find that an administrative fine would not be necessary, proportionate or dissuasive in the particular circumstances in relation to the infringements of the Articles of the GDPR as set out above. In coming to this finding, I have had particular regard to the fact that Twitter does not generally seek a copy of photographic ID in respect of the processing of erasure requests from data subjects. This case falls into an exceptional category (account permanently suspended). Furthermore, I have had regard to the fact that the delay in handling the erasure request in this case does not appear to have arisen from a systemic set of issues but was

[4] See the Article 29 Data Protection Working Party 'Guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679, at page 11.

particular in the circumstances of this case to factors such as the data subject filing multiple requests and not following instructions. For the reasons outlined, I find that no administrative fine should be imposed in respect of these infringements. Given that the data subject's personal data has been erased, I find that no order to the data controller is required to comply with the data subject's erasure request.

125. **In light of the extent of the infringements identified above, the DPC hereby issues a reprimand to Twitter International Company, pursuant to Article 58(2)(b) of the GDPR.**

126. **In light of the infringement of Article 5(1)(c) in the case of this data subject, it is necessary that the data controller bring its data processing operations into compliance with Article 5(1)(c) to prevent similar infringements occurring with regard to data subjects in the future in similar circumstances. Accordingly, the DPC hereby orders Twitter to revise its internal policies and procedures for handling erasure requests to ensure that data subjects are no longer required to provide a copy of photographic ID when making data erasure requests, unless it can demonstrate a legal basis for doing so. This order is made pursuant to Article 58(2)(d) of the GDPR and Twitter is requested to provide details of its revised internal policies and procedures to the DPC by 30 June 2022.**

Signed: Tony Delaney

Tony Delaney

Deputy Commissioner

On behalf of the Data Protection Commission