euroconsumers
Empower people, improve the market.

ALTROCONSUMO

TO THE IRISH DATA PROTECTION COMMISSION

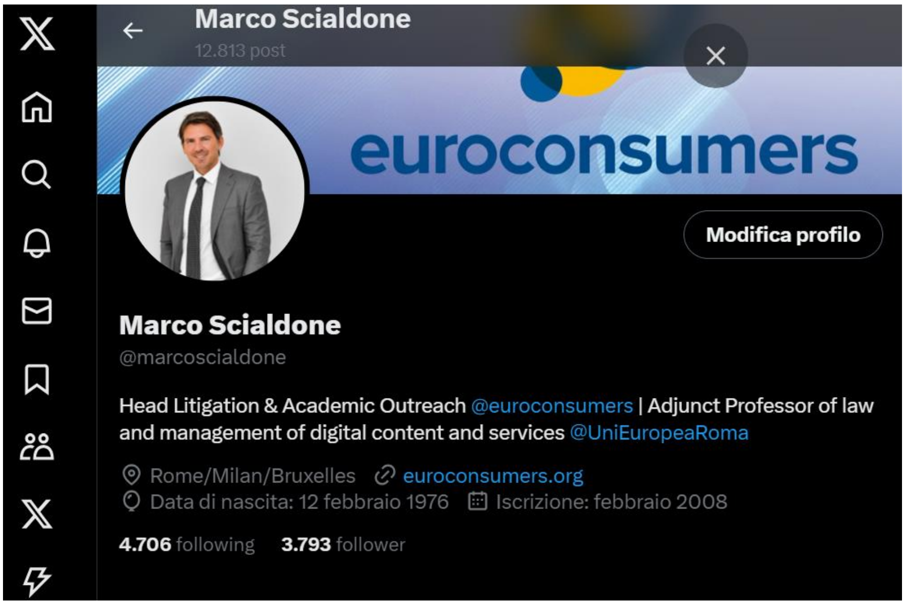
21 FITZWILLIAM SQUARE SOUTH, DUBLIN 2 D02 RD28

Complaint pursuant to art. 77 of Regulation (EU) 2016/679.

The undersigned, Marco Scialdone, *(….omissis ….)*, who for the purposes of this proceeding declares that he wishes to receive any communications at the following address: *(….omissis ….)* states the following:

a) The complainant resides in the Italian Republic and has been the owner of X (formerly known as Twitter) account at https://x.com/marcoscialdone since February 2008 (see image 1)

(Image 1)



Marco Scialdone
12.813 post

Modifica profilo

Marco Scialdone
@marcoscialdone

Head Litigation & Academic Outreach @euroconsumers | Adjunct Professor of law and management of digital content and services @UniEuropeaRoma

Rome/Milan/Bruxelles euroconsumers.org
Data di nascita: 12 febbraio 1976 Iscrizione: febbraio 2008

4.706 following 3.793 follower

b) Twitter International Unlimited Company, based at One Cumberland Place, Fenian Street, Dublin 2, D02 AX07, Ireland, is the data controller for the European Union of the social network X, initially known as Twitter, which allows users to publish and share short messages, video content, create live broadcasts and organize communities.

c) X's privacy policy, updated on September 29, 2023, in section 2 ("How we use information"), paragraph 2.1 ("Operating, improving, and personalizing our services") includes the following statement *"We may use the information we collect and publicly available information to help refine our machine learning or artificial intelligence models for the purposes described in this policy"* (cf. https://x.com/it/privacy).

d) This is, in fact, the only reference that accounts for the possibility of the information collected[1] by the social network being used to train X's artificial intelligence systems.

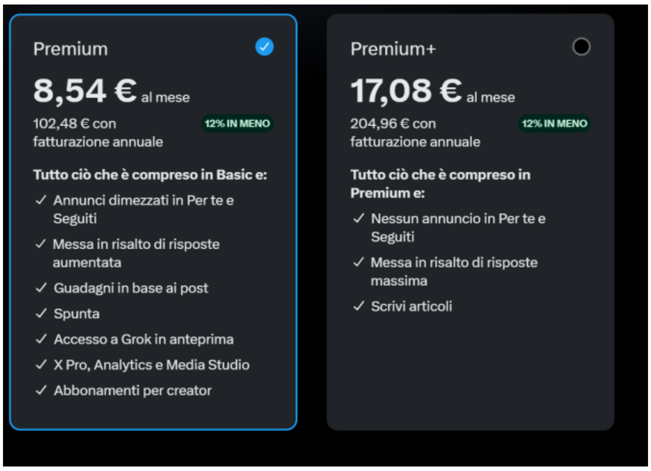
e) This is particularly relevant given that, as of May 16, 2024[2], access to GROK (see image 2, below) is available in Europe as an additional service for Premium and Premium+ users of X, which is described as *"an AI research assistant with a touch of humor and a hint of rebellion. X Premium and Premium+ subscribers have the ability to conduct research and get answers using Grok, as an enhancement to X's search features. Grok is here to help you with search and answers as you entertain and engage."*[3][4]

[1] This expression refers to the set of information indicated in paragraph 1 of X's privacy policy.

[2] https://x.com/GlobalAffairs/status/1790886734898606224

[3] https://help.x.com/en/using-x/about-grok#:~:text=Welcome%20to%20the%20world%20of,enhancement%20of%20X's%20search%20functions.

[4] On July 26, 2024, the online magazine Irish Independent reported on an ongoing investigation by the DPC Ireland regarding this matter (*"Ireland's Data Protection Commissioner says that it is 'surprised' that Elon Musk's X platform has automatically 'opted in' all X users into its Grok AI training program without a choice. The watchdog says that it will now probe the matter further with X to see whether it complies with EU privacy law. The move, which cannot be reversed by those using the mobile app, means that Grok AI is using X users' personal information, including posts, to build its own AI as a rival to ChatGPT and Google Gemini"*), https://m.independent.ie/business/technology/elon-musks-grok-ai-faces-eu-scrutiny-for-opting-in-every-x-users-personal-posts-without-asking/a1525006925.html.



Premium

8,54 € al mese

102,48 € con fatturazione annuale

12% IN MENO

Tutto ciò che è compreso in Basic e:

- ✓ Annunci dimezzati in Per te e Seguiti
- ✓ Messa in risalto di risposte aumentata
- ✓ Guadagni in base ai post
- ✓ Spunta
- ✓ Accesso a Grok in anteprima
- ✓ X Pro, Analytics e Media Studio
- ✓ Abbonamenti per creator

Premium+

17,08 € al mese

204,96 € con fatturazione annuale

12% IN MENO

Tutto ciò che è compreso in Premium e:

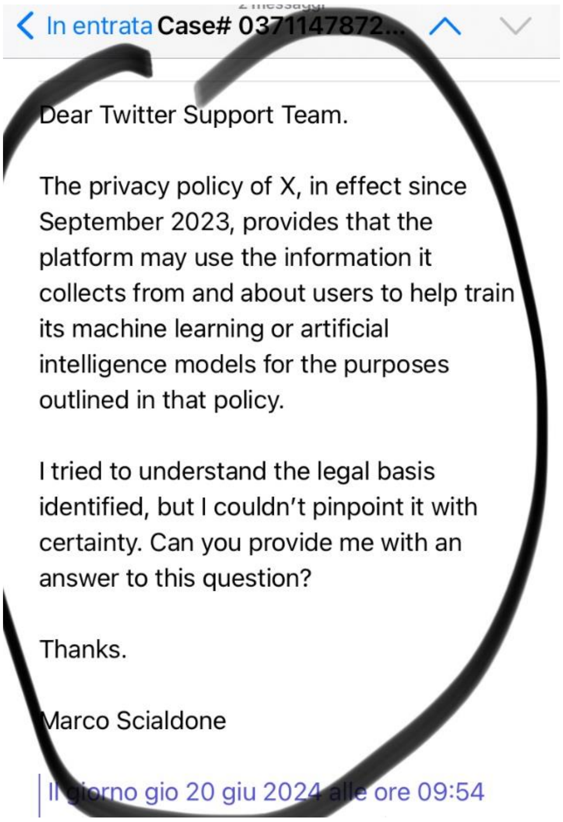
- ✓ Nessun annuncio in Per te e Seguiti
- ✓ Messa in risalto di risposte massima
- ✓ Scrivi articoli

f) From X's privacy policy, it is not possible to understand, in a simple and immediate way, what the legal basis for the processing is with regard to the training of artificial intelligence systems.

g) Only by accessing a subsequent link[5] and scrolling nearly to the end the page can one obtain reasonable certainty that the legal basis is legitimate interest as it is the subject of specific analysis ("*Legitimate interests analysis summary – processing public post data to train machine learning and artificial intelligence models, including generative models*").

h) However, the complainant, in order to further dispel any doubts, on 20 June 2024, asked the data controller [Case# 0371147872] to confirm the legal basis for the aforementioned processing of his personal data (see image 3, below).

[5] https://help.x.com/en/rules-and-policies/data-processing-legal-bases.



Dear Twitter Support Team.

The privacy policy of X, in effect since September 2023, provides that the platform may use the information it collects from and about users to help train its machine learning or artificial intelligence models for the purposes outlined in that policy.

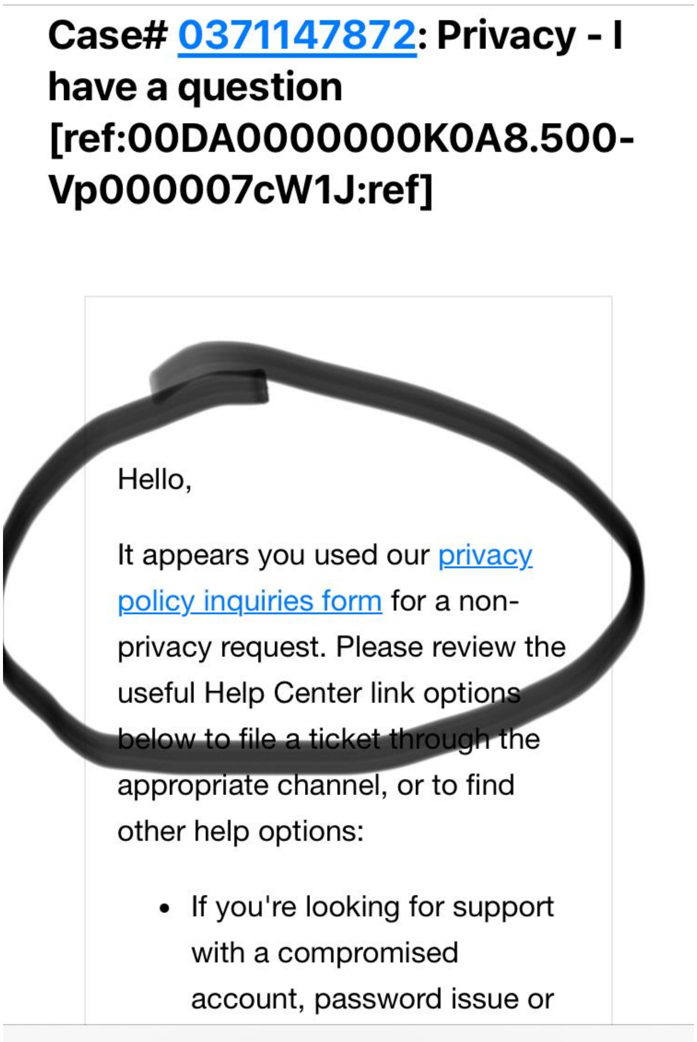
I tried to understand the legal basis identified, but I couldn't pinpoint it with certainty. Can you provide me with an answer to this question?

Thanks.

Marco Scialdone

Il giorno gio 20 giu 2024 alle ore 09:54

i) Incredibly, on July 24, 2024, the complainant received a reply informing him that the question asked did not concern the privacy policy (sic!) (see image 4 below).



Case# 0371147872: Privacy - I have a question [ref:00DA0000000K0A8.500-Vp000007cW1J:ref]

Hello,

It appears you used our privacy policy inquiries form for a non-privacy request. Please review the useful Help Center link options below to file a ticket through the appropriate channel, or to find other help options:

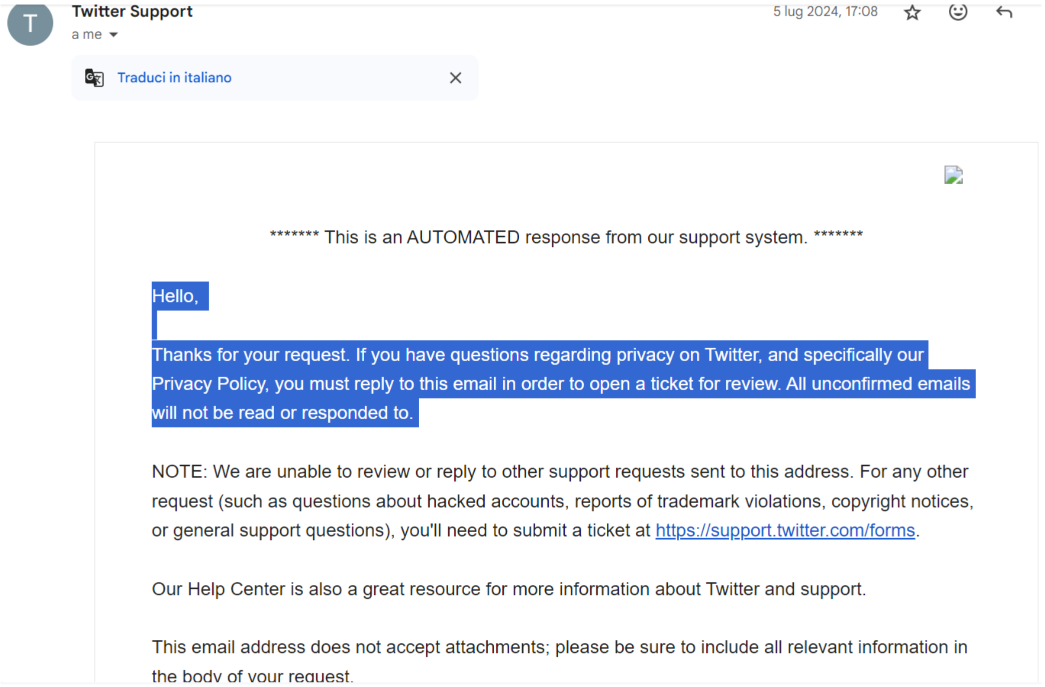
- If you're looking for support with a compromised account, password issue or

j) That said, the complainant, on July 5, 2024, formally exercised [Case# 0372526825] the right to object to the processing of his personal data to help refine X's machine learning or artificial intelligence models.

k) In particular, the complainant requested X to: (1) cease processing of his personal data for the purposes of training and refining machine learning or artificial intelligence models (2) confirm in writing that the request for termination of processing has been implemented.

l) It is useful, preliminarily, to point out the cumbersome and unnecessary complexity of the procedure: firstly, there is no specific form for exercising the right to object. The user can only utilize the generic form for questions regarding X's privacy policy. Furthermore, after filling out and submitting the aforementioned form, the user receives a communication via e-mail, with the assignment of a case number and an additional request: "*Hello, Thanks for your request. If you have questions regarding privacy on Twitter, and specifically our Privacy Policy,* ***you must reply to this email in order to open a ticket for review. All unconfirmed emails will not be read or responded to***".

m) Basically, despite the fact that the complainant had already accessed his account and had correctly submitted the request, it was necessary to reply to the email to confirm the request, otherwise it would not have been processed (see image 5 below).



******* This is an AUTOMATED response from our support system. *******

Hello,

Thanks for your request. If you have questions regarding privacy on Twitter, and specifically our Privacy Policy, you must reply to this email in order to open a ticket for review. All unconfirmed emails will not be read or responded to.

NOTE: We are unable to review or reply to other support requests sent to this address. For any other request (such as questions about hacked accounts, reports of trademark violations, copyright notices, or general support questions), you'll need to submit a ticket at https://support.twitter.com/forms.

Our Help Center is also a great resource for more information about Twitter and support.

This email address does not accept attachments; please be sure to include all relevant information in the body of your request.

n) The data controller has not responded to the request within the terms provided for by art. 12 of the GDPR.

o) The facts, as described above, reveal multiple violations of the GDPR.

p) **VIOLATION OF ARTICLES 5 (1) (a), 12 AND 13 OF THE GDPR FOR FAILURE TO BE TRANSPARENT AND FAIR TO THE DATA SUBJECT**: in general terms, the principle of transparency requires that the data subject be fully aware of the processing of any personal data. Recital 39 of the GDPR contains several explanatory statements regarding the principle of transparency. In particular, *"it should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent personal data are or will be processed"*. Data subjects should be *"informed of the risks, rules, safeguards and rights relating to the processing ... and how to exercise their rights"*. All information communicated should be *"accessible and easy to understand"* and in *"clear and plain language"*. The principle of transparency is closely linked to more detailed provisions. For example, Article 12(1) of the GDPR ensures that information must be provided in a *"concise, transparent, intelligible and easily accessible form, using clear and plain language"*. Paragraph 2 of the same article provides that *"the controller shall facilitate the exercise of the right of the data subject pursuant to Articles 15 to 22"*. Articles 13 and 14 of the GDPR provide for the right to receive information about the processing envisaged, even before the processing takes place. Article 15 of the GDPR provides for the right to access information about the actual processing of the individual's data. In the case at hand, based on the points indicated above, it is quite evident that the data controller failed to adequately inform the complainant and the other users of the X service about the specific processing operations, particularly with reference to the training of its machine learning and generative artificial intelligence systems and, above all, to enable them to effectively exercise their rights. **The legal basis for the aforementioned operations, far from being clearly reported in the privacy policy, is mentioned only in a secondary link and only within the *"Legitimate interests analysis summary"* section, where the average user would certainly not expect to find it given that nowhere else in the document is legitimate interest mentioned as the legal basis for data processing.** In this respect, with reference to the principle of fairness, the EDPB Guidelines 4/2019 have clarified that, for the processing to be "fair", no form of deception is allowed in the processing of data and that all options must be provided in an objective and neutral manner, avoiding any misleading or manipulative language or design. Again, in the present case there are no such elements at all. In addition, the language used does not even allow the user to know if and when the processing of their personal data is carried out. The expression, in fact, alludes to a potential use but it is not known when this possibility materializes or not. Therefore, the lack of information provided to the user is evident.

q) **VIOLATION OF THE PRINCIPLE OF DATA MINIMIZATION PURSUANT TO ART. 5 (1) (c) GDPR.**

The EDPB (cf. Guidelines 4/2019) has had the opportunity to state that the obligation to minimise data applies to the amount of personal data collected, the scope of processing, the retention period and the accessibility of the data. With particular reference to the quantity, "*data controllers should take into account both the volume of personal data and the types, categories and level of detail of personal data required for the purposes of the processing. Their design choices should take into account the higher risks to the principles of integrity and confidentiality, data minimisation and storage limitation associated with the collection of large amounts of detailed personal data, compared to the lower risks associated with the collection of smaller amounts of data and/or less detailed information about data subjects. In any case, the default settings must not include the collection of personal data that is not necessary for the specific purpose of the processing.* ***In other words, if certain categories of personal data are superfluous or if detailed data is not needed, because less granular data is sufficient, then the excess data is not collected***".

In the present case, X does not restrict the processing of personal data in any way, including by anonymization, pseudonymization or other privacy-preserving technologies. It only refers to the concept of "information collected" which, as highlighted in the previous points, is extremely broad[6].

r) VIOLATION OF ART. 9 OF THE GDPR FOR THE INCLUSION IN THE PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA WITHOUT ADEQUATE LEGAL BASIS.

As mentioned above, X identifies the legal basis for the processing of personal data in the legitimate interest pursuant to Art. 6 (1) (f) of the GDPR. Without prejudice to the inapplicability of this legal basis, it should be pointed out at the outset that it cannot be invoked with reference to the special categories of personal data pursuant to Article 9.

Nor could the data controller invoke the applicability of letter e) of the aforementioned regulatory provision ("*the processing concerns personal data manifestly made public by the data subject*") given that, as clarified by the Court of Justice of the European Union (cf. C-252/21, Meta Platforms v. Bundeskartellamt), "*Article 9(2)(e) of the GDPR must be interpreted as meaning that a user of an online social network, when consulting websites or applications related to one or more of the categories referred to in Article 9(1) of the GDPR, does not manifestly make public, within the meaning of the first of those provisions, the data relating to this consultation, collected by the operator of said online social network through cookies or similar recording technologies*".

[6] Nel Legitimate interests analysis summary – processing public post data to train machine learning and artificial intelligence models, including generative models si dice "*X may use information that individuals provide and data that it receives (as described in X's Privacy Policy) to train machine learning and artificial intelligence models, including generative models*".

On this point, the Opinion of the Advocate General of the CJEU in Case C-446/21 Maximilian Schrems v. Meta Platforms Ireland Limited should not escape this esteemed Authority, where it is stated that the objective of the protection conferred by Article 9(1) is to prevent the data subject from being exposed to detrimental consequences (such as, in particular, public contempt or discriminatory acts) resulting from, in particular, by a negative perception, from a social or economic point of view, of the situations listed therein. That provision therefore provides for a special protection of those personal data by means of a prohibition which is not in principle absolute, the application of which in the present case is subject to the assessment of the data subject, who is the one who is best able to assess the harmful consequences that could result from the disclosure of the data in question and who, where appropriate, may waive that protection or not avail itself of it, in full knowledge of the facts, by making manifestly public, within the meaning of Article 9(2)(e) of that regulation, its situation.

In the present case, such an assessment is, *ex ante*, precluded because the data subject is not even properly informed of the existence of such processing: hence the inapplicability of the exception referred to in letter e).

s) **VIOLATION OF ART. 6 (1) (f) OF THE GDPR DUE TO THE INADEQUACY OF LEGITIMATE INTEREST AS A LEGAL BASIS.**

Article 6(1)(f) of the GDPR provides that processing of personal data is lawful if it is *"necessary for the purposes of the legitimate interests pursued by the controller or by a third party, provided that the interests or fundamental rights and freedoms of the data subject which require the protection of personal data do not prevail, in particular if the person concerned is a minor"*.

As established by ECJ case-law, that provision lays down three cumulative conditions for the lawful processing of personal data: first, the pursuit of a legitimate interest by the controller or a third party; second, the necessity of processing personal data for the achievement of the legitimate interest pursued; and third, that the interests or fundamental rights and freedoms of the data subject do not override the legitimate interest of the controller or third party.

Regarding the necessity of the processing, it must be demonstrated that the legitimate interest pursued cannot reasonably be achieved as effectively by other means less prejudicial to the fundamental rights of the data subjects, particularly the rights to respect for private life and the protection of personal data.

In this context, it should also be borne in mind that the condition relating to the necessity of processing must be examined in conjunction with the principle of minimization set out in Article 5(1)(c) of the GDPR.

In the case at hand, it is evident that this condition is not met. Since the data concern only users registered on the social network and the processing is not necessary for the provision of the service, the same purpose can be pursued in a more reasonable and effective way by using another legal basis, namely the consent of the data subject.

Indeed, it is reasonable to suspect that X's choice, far from aligning with the GDPR, was motivated solely by the desire to "harvest" as much data as possible, without risking denial by the data subjects.

Additionally, the Legitimate Interests analysis published by X is wholly inadequate and contains misleading and untruthful information.. The data controller claims that *"... To safeguard the rights of those who use our services, users can easily "protect" (limit to a followers-only audience) their posts, or delete their posts at any time, thereby removing their posts and related metadata from being used"*. However, scientific literature has long highlighted that the mere deletion of data is ineffective once the model has been trained with it[7].

t) **VIOLATION OF ART. 21 OF THE GDPR FOR INADEQUATE MANAGEMENT OF THE RIGHT TO OBJECT.**

Without prejudice to the violations outlined in the preceding points, should this esteemed Authority consider those violations to be non-existent, there remains, nonetheless, a clear violation of Article 21 of the GDPR due to the controller's inadequate handling of the complainant's right to object.

As indicated in point n) above, the data controller, in response to the request made by the complainant, has not provided any response. On the contrary, the data controller should have taken steps to demonstrate the existence of compelling legitimate reasons for continuing the processing that outweigh the interests, rights, and freedoms of the data subject, or for the establishment, exercise, or defense of a right in court.

[7] See, Joshua A. Goland, *Algorithmic disgorgement: destruction of artificial intelligence models as the ftc's newest enforcement tool for bad data*, in Richmond Journal of Law & Technology Volume XXIX, Issue 2, available at https://jolt.richmond.edu/files/2023/03/Goland-Final.pdf (*"Professor Tiffany Li argues that even if data is deleted, an "imprint from the individual users" still remains as an "algorithmic shadow" in the algorithms trained on the data. The persistence of this shadow means that "**some measure of privacy loss cannot be undone" by simply deleting the data while allowing the algorithm to remain**. Once an algorithm has been trained on a user's data, Professor Li argues that the continued use of that algorithm poses some privacy harm to the user, even if their individual data is no longer distinguishable or in active use by the algorithm; only the deletion of the algorithm ensures that this privacy harm is removed*).

All of the above considered, the undersigned:

REQUESTS

The Data Protection Authority, after examining the complaint and finding it well-founded, to take all appropriate measures, and in particular:

I. to address Twitter International Unlimited Company, with registered office at One Cumberland Place, Fenian Street, Dublin 2, D02 AX07, Ireland, with warnings or reprimands under Article 58(2)(a) and (b) of the GDPR, highlighting the unlawfulness of the processing;

II. to order Twitter International Unlimited Company, with registered office at One Cumberland Place, Fenian Street, Dublin 2, D02 AX07, Ireland, to cease the processing of personal data of the affected users for artificial intelligence purposes, pursuant to Article 58(2)(d) and (f) of the GDPR;

III. In any case, to order Twitter International Unlimited Company, with registered office at One Cumberland Place, Fenian Street, Dublin 2, D02 AX07, Ireland, to comply with the requests for the exercise of rights under Article 21 of the Regulation.

Rome, 05/08/2024

Signature