EUROPEAN DATA PROTECTION SUPERVISOR

EDPS SUPERVISORY OPINION ON THE USE OF SOCIAL MEDIA MONITORING FOR EPIDEMIC INTELLIGENCE PURPOSES BY THE EUROPEAN CENTRE FOR DISEASE PREVENTION AND CONTROL ('ECDC')

09/11/2023

(Cases 2021-0712 and 2021-0830)

Summary:

This Supervisory Opinion assesses the lawfulness of the processing operations conducted by the European Centre for Disease Prevention and Control (the 'ECDC') in the context of a pilot project involving the manual and automated monitoring of social media for epidemic intelligence purposes.

The Opinion includes recommendations issued in accordance with Article 58(3)(c) of the Regulation (EU) 2018/1725 ('the Regulation').

EUROPEAN DATA PROTECTION SUPERVISOR
Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30 - B-1000 Brussels
E-mail: edps@edps.europa.eu
Website: edps.europa.eu
Tel.: 32 2-283 19 00 - Fax: 32 2-283 19 50

Contents

1. INTRODUCTION

1. This Supervisory Opinion relates to use of social media monitoring by the European Centre for Disease Prevention and Control (the 'ECDC') for epidemic intelligence purposes within the context of a pilot study.

2. This Supervisory Opinion includes recommendations issued in accordance with Article 58(3)(c) of Regulation (EU) 2018/1725[1] ('the Regulation').

2. FACTS

3. On 12 July 2021, the European Data Protection Supervisor ('EDPS') received a request for prior consultation under Article 40 of the Regulation from the ECDC regarding an ongoing pilot study[2] on the use of social media monitoring for epidemic intelligence purposes (Case 2021-0712).

4. Since the processing had already started at the time of the consultation[3], the EDPS considered the prior consultation as inadmissible. Instead, the EDPS now issues this Supervisory Opinion, which includes recommendations with respect to the pilot project.

2.1. The ECDC'S mission and tasks

5. As part of its activities and under its mandate established by Regulation (EC) No 851/2004 of the European Parliament and of the Council of 21 April 2004 establishing a European Centre for disease prevention and control (the 'ECDC Regulation')[4], the ECDC performs epidemic intelligence: the systematic collection, recording, analysis, interpretation and dissemination of data and analysis on communicable diseases and related special health issues. This processing operation aims to detect potential public health threats early on.

---

[1] Regulation (EU) 2018/1725 of the European Parliament and the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ, L 295, 21.11.2018, pages 39-98.

[2] See Annex 1 to the ECDC's letter to the EDPS of 12 July 2021 - the ECDC's Internal Procedure on the use of social media for epidemic intelligence activities, page 6. The pilot project is planned to end in 2025 (page 10 of the same document)

[3] As indicated by the ECDC in its letter to the EDPS of 12 July 2021.

[4] Article 3(2) of the Regulation (EC) No 851/2004 of the European Parliament and of the Council of 21 April 2004 establishing a European Centre for disease prevention and control.

6. According to Article 3(1) of the ECDC Regulation, the agency is mandated to **identify, assess and communicate current and emerging threats to human health from communicable diseases**. In particular, Articles 3(2)(a), Article 5(1), Article 10(1) and Article 11(1) of the ECDC Regulation authorise the ECDC to collect, evaluate and disseminate relevant scientific and technical data, including to identify emerging health threats and to support the networking activities of the competent bodies recognised by the Member States, through the operation of the dedicated surveillance networks and the provision of technical and scientific expertise.

7. The EDPS notes that, since having received the ECDC's consultation request, the ECDC Regulation has been amended by Regulation (EU) 2022/2370 of the European Parliament and of the Council of 23 November 2022[5] (the 'ECDC Amending Regulation'). Nevertheless, the Articles referenced above have not changed substantially in substance and, therefore, the ECDC's mandate remains the same.

8. According to Article 6(1) of the Decision No. 1082/2013/EU of the European Parliament and of the Council of 22 October 2013, the ECDC operates and coordinates a network of epidemiological surveillance of communicable diseases.

9. The ECDC Strategy 2021-2027[6] includes as a strategic objective[7] the adoption and exploitation of new technologies for prevention and control of infectious diseases.

10. The ECDC Single Programming Document 2021-2023[8] provides that it shall carry out a **pilot study** to assess the benefits of trend analysis of social media sources for epidemic intelligence, in order to improve threat detection through epidemic intelligence screening.[9]

2.2. Manual and automated social media monitoring for epidemic intelligence purposes

11. According to the information provided to the EDPS, the ECDC's monitoring of social media, carried out in the context of the pilot study mentioned above, has been performed either in a manual or in an automated way[10].

---

5 See Regulation (EU) 2022/2370 of the European Parliament and of the Council of 23 November 2022.

6 See the ECDC Strategy 2021-2027.

7 Ibid, under strategic objective 3 action area 3.3. 'Support transformation: Provide leadership and support to countries in adapting, adoption and exploiting new technologies for infectious disease prevention and control'.

8 See the ECDC Single Programming Document 2021-2023.

9 Ibid, page 28.

10 See Annex 1 to the ECDC's letter to the EDPS of 12 July 2021 - the ECDC's Internal Procedure on the use of social media for epidemic intelligence activities, page 6.

2.2.1. Manual social media monitoring

12. Concerning the **'manual' (i.e. non-automated) method** of social media monitoring, which is still ongoing**,** the ECDC has an account on Twitter[11] and on Facebook in order to be able to follow the posts of selected individuals, experts and institutions renowned for providing accurate information on public health events and threats, and more specifically on infectious diseases.[12]

13. The ECDC follows approximately 100 **Twitter** and 40 **Facebook** accounts of official sources (public health agencies, universities, ministries of health, etc.) on the one hand, and of duly selected unofficial sources (journalists, media and active experts within the field of public health and communicable diseases), whose information and data are subsequently verified with official sources (websites of ministries of health or direct contact with the ECDC's national focal points), on the other hand.[13]

14. According to the documentation provided to the EDPS, members of the ECDC's epidemiological intelligence group (the 'ECDC's EI Group'), through the above-mentioned accounts and following specific internal processes, visually screen Facebook and Twitter once or twice per day by checking the latest posts of selected accounts exclusively in view of collecting, collating, storing and evaluating data and information included in Twitter and Facebook posts relating to cases of communicable diseases, which refer to epidemiological figures (confirmed cases, suspected cases, deaths, etc.), situation reports on specific events, and relevant public health campaigns (e.g. vaccination campaigns).[14] In this regard, **only information and data from publicly available sources are used**.[15]

15. Concerning the **categories of data processed in the context of the manual social media monitoring method**, the documentation provided by the ECDC states that, in line with the principle of data minimization, it 'does not collect, store, evaluate or disseminate personal data of the individuals that are suffering from a communicable disease. Neither does the ECDC collect, store, evaluate or disseminate personal data of its sources, meaning the persons who publish and disseminate data or information on social media.'[16]

16. Furthermore, the documentation provided by the ECDC states that data are not systematically stored. However, the ECDC states that on rare occasions, data is

[11] Twitter rebranded to "X" on 23 July 2023. For the sake of clarity, this supervisory opinion consistently refers to "Twitter".
[12] Ibid, page 7.
[13] Ibid.
[14] See Annex 1 to the ECDC's letter to the EDPS of 12 July 2021 - the ECDC's Internal Procedure on the use of social media for epidemic intelligence activities, page 7.
[15] Ibid.
[16] See Annex 1 to the ECDC's letter to the EDPS of 12 July 2021 - the ECDC's Internal Procedure on the use of social media for epidemic intelligence activities, pages 7-8.

included in the **ECDC's Threat Tracking Tool** for the production of the ECDC's outputs, such as reports. However, this is only done if the data are coming from official social media accounts of public health authorities, public health organisations or any other official organisations (e.g. civil protection or government) and their core employees (e.g. president or minister).[17]

17. The ECDC states that 'on a sporadic basis or in *ad hoc* situations, other social media platforms can be manually monitored, such as Telegram, Weibo or YouTube'[18].

2.2.2. Automated social media monitoring (Epitweetr)

18. Concerning the ECDC's **automated method** of monitoring social media, the only social media platform used was Twitter. At the time of the ECDC's consultation, automated social media monitoring was being carried out in the context of the pilot project. However, on 3 October 2023, the EDPS was notified that **as of 19 April 2023, the ECDC's use of epitweetr for its automated social media monitoring was discontinued**, due to X (former Twitter) putting up a paywall to access the tweets.

19. According to the documentation provided to the EDPS, the last tweet collected via automated social media monitoring was on 19 April 2023. There are no raw tweets as indicated in the privacy statement[19] older than 6 months. Due to these changes in possibilities of data access implemented by X, no raw tweets are currently being collected or stored, only aggregated[20], anonymised data of tweets collected before 19 April 2023. Previous raw tweets were deleted when the access to data from Twitter/X was discontinued.

20. Despite the ECDC's discontinuation of Epitweetr, the ECDC has expressed its interest in obtaining the EDPS's guidance, in case the project is resumed in the future, or a similar project is initiated. Therefore, in this Opinion, the EDPS still conducts an assessment of the ECDC's automated social media monitoring using Epitweetr, as operated by the ECDC until 19 April 2023 and based on the information received at the time of the consultation.

21. Nevertheless, while the recommendations relating to the automated social media monitoring included herein are issued based on the facts as they were prior to the discontinuation of the automated social media monitoring, they would nonetheless remain applicable were the ECDC to resume this processing in the future.

22. The documentation provided to the EDPS states that the ECDC has a Twitter account in order to access, download and store tweets made available by Twitter

---

17 Ibid.
18 Ibid, page 6.
19 See Section 2.2.4. and 3.5.3.
20 See Section 2.2.2.2. and 3.5.2.

through its Standard Search API version 1.1[21], which is a tool used to retrieve relevant and **publicly available tweets** matching a specific query from the previous seven days. The ECDC has developed an R-package[22] and interactive web application called '**epitweetr**'[23] which aims to detect public health threats early on based on Twitter data, at country, regional and global levels.[24]

23. Through Twitter's Standard Search API, epitweetr focuses on monitoring Twitter posts (hereafter referred to as 'tweets') that include any or some of the keywords selected by the ECDC relating to specific and popular nomenclature surrounding infectious diseases (in four languages: English, Spanish, French and Portuguese). These keywords are regularly revised and updated, particularly if new topics need to be added (e.g. COVID-19 in 2020).[25]

2.2.2.1. Categories of data processed

24. Concerning the **categories of data processed in the automated social media monitoring method**, according to the ECDC, the following data is processed[26]:

- Date and time of creation of the tweet;
- Identification number of the tweet;
- Content of the tweet;
- Hashtags, symbols, URLs and mentions to other users included in the content of the tweet;
- Type of the results provided by Twitter (this can be 'popular' or 'recent');
- Language of the content of the tweet user;
- Information about the user who posted the tweet: identification, name, screen name, location, description of his/her Twitter profile, URL, if the account is protected[27] and/or verified, number of followers and friends, number of Twitter lists which includes the user, date and time of the creation of the account, number of favourites, and time zone and language of the account. The same

[21] Twitter Standard Search API supports a maximum of 180 requests for every 15-minute window (450 requests for every 15-minute window when using Twitter developer application credentials), each of these requests containing a maximum of 100 tweets and/or retweets.

[22] R packages are extensions to the R statistical programming language used for data analysis and to develop statistical software

[23] epitweetr GitHub repository

[24] See Annex 1 to the ECDC's letter to the EDPS of 12 July 2021 - the ECDC Internal Procedure on the use of social media for epidemic intelligence activities, page 8.

[25] See Annex 1 to the ECDC's letter to the EDPS of 12 July 2021 - the ECDC Internal Procedure on the use of social media for epidemic intelligence activities, page 8.

[26] Twitter Standard Search API documentation

[27] See Twitter Help Center 'About public and protected Tweets' - 'All the listed data and metadata is also available concerning a person with a private account, whose tweet is replied to, retweeted or quoted. Please note that your followers may download or re-share links to media that you share in protected Tweets. Links to media shared on Twitter are not protected. Anyone with the link will be able to view the content.'

metadata are available for the user of a tweet that has been replied to, retweeted or quoted;
- If the tweet is a reply, these variables indicate the tweet id, user id and/or user screen name of the original tweet that has been replied to;
- Whether the tweet is a quote or retweet of another tweet or not.

25. In the documentation provided to the EDPS, the ECDC explains that raw data collected by epitweetr is stored in comprised 'JavaScript Object Notation' (JSON) files that have to be processed to be read since the data files are not structured by name of the topic.[28] In parallel to collecting tweets, epitweetr attempts to geolocate such tweets using a machine learning process and stores two types of geolocation information: tweet geolocation, based on the information within the text of a tweet (or a retweet or quoted tweet), and user location from the available metadata (user's location at the time of the tweet, user's location at the time of the retweet or quoted tweet, user declared location in the tweet or user declared location in the public profile).[29]

2.2.2.2. Data aggregation

26. According to the documentation provided by the ECDC, **epitweetr automatically aggregates data** through an Epitweetr package/Shiny app[30] to create series for each topic for number of tweets, retweets and quotes per day and per location, including number of tweets and most frequently mentioned words per topic, place and time.[31] The ECDC claims that 'these aggregated data do not contain personal data and are used for data visualization in Epitweetr dashboard.'[32]

27. The ECDC **does not intend to detect individual cases and re-identify the data subjects**, but rather intends to detect potential outbreaks of communicable diseases. With that aim, Epitweetr automatically detects signals in the aggregated data, i.e. number of tweets in the aggregated time series that exceed what is expected.[33] For this detection, Epitweetr uses an extended version of the Early Aberration Reporting System (EARS) algorithm.[34] As a default, it uses a moving window of the past seven

[28] See Annex 1 to the ECDC's letter to the EDPS of 12 July 2021 - the ECDC Internal Procedure on the use of social media for epidemic intelligence activities, page 9.
[29] Ibid.
[30] Shiny apps allow to create data reports and views the user can use to explore a raw data set.
[31] See Annex 1 to the ECDC's letter to the EDPS of 12 July 2021 - the ECDC Internal Procedure on the use of social media for epidemic intelligence activities, page 9.
[32] Ibid.
[33] Ibid, page 10.
[34] The Early Aberration Reporting System is a syndromic surveillance system that uses aberration-detection models to identify deviations in current data when compared with a historic mean. Aberration detection methods allow the quick assessment of changes in health trends and the identification of unusual trends.

days to calculate a threshold. If the number of tweets of the current day exceeds this threshold, a signal is generated for that topic and location.[35]

2.2.3. Data Protection Impact Assessment ('DPIA')

28. In application of Article 39 of the Regulation, the ECDC performed a DPIA assessing only the impact on the protection of personal data of the processing operations envisaged in the context of its automated social media monitoring.[36] In that DPIA, the ECDC did not identify high risks to the data subjects. Nevertheless, in its letter to the EDPS, the ECDC raised concerns due to the fact that '*it is impossible for the ECDC to effectively inform a large amount of data subjects that their data is being processed. Therefore, it would be impossible for data subjects to exercise their rights.*'[37]

2.2.4. Privacy Statement

29. The ECDC published a privacy statement on its website and on the webpage dedicated to epitweetr, as well as on its social media.[38] In this privacy statement, the ECDC states that the legal basis for the processing operations is Article 5(1)(a) of the Regulation, affirming that the processing is necessary for the performance of tasks in the public interest attributed by Union or Member State legislation.

30. According to the privacy statement, the ECDC's retention period for raw data containing personal data is of six months. Thereafter, the data is anonymised or aggregated. However, according to the ECDC's 'Internal Procedure for the use of social media for epidemic intelligence activities', the Twitter data collected by epitweetr will be kept until the pilot project is finalised, i.e. 2025.[39] It is further stated that shorter retention periods will be discussed and applied after the end of the pilot phase.[40] In the same document, the ECDC submits that data is stored in a virtual machine stored on a local server on the ECDC's premises which is only accessible to a restrictive list of users within the ECDC (on a need-to-know basis)[41], including the ECDC's EI Group and 24/7 duty officers, with a double-step credential-based access.[42]

---

35 See Annex 1 to the ECDC's letter to the EDPS of 12 July 2021 - the ECDC Internal Procedure on the use of social media for epidemic intelligence activities, page 10.

36 See Annex 3 to the ECDC's letter to the EDPS of 12 July 2021 - the ECDC DPIA.

37 See the ECDC's letter to the EDPS of 12 July 2021, page 1.

38 See Annex 2 to the ECDC's letter to the EDPS of 12 July 2021 - the ECDC Privacy Statement 'Social Media Monitoring for Epidemic Intelligence Activities'.

39 See Annex 1 to the ECDC's letter to the EDPS of 12 July 2021 - the ECDC's Internal Procedure on the use of social media for epidemic intelligence activities, page 10.

40 Ibid.

41 See Annex 3 to the ECDC's letter to the EDPS of 12 July 2021 - the ECDC DPIA, page 4.

42 See Annex 1 to the ECDC's letter to the EDPS of 12 July 2021 - the ECDC Internal Procedure on the use of social media for epidemic intelligence activities, page 8.

3. LEGAL ANALYSIS AND RECOMMENDATIONS

31. Although the ECDC has indicated that other social media platforms, such as Telegram, Weibo or YouTube, can be manually monitored on a sporadic basis or in *ad hoc* situations[43], this EDPS Opinion relates exclusively to the more organised forms of monitoring, i.e. the ECDC's manual and automated monitoring of **Twitter** and **Facebook**, i.e. the main social media platforms being monitored on a routine basis[44] for epidemic intelligence purposes.

3.1. Processing of personal data

32. According to Article 2(1) of the Regulation, the processing of personal data by all Union institutions and bodies (EUIs) falls within the scope of the Regulation. Therefore, the ECDC as Union agency falls under the scope of the Regulation.

33. In line with Article 3(3) of the Regulation, 'processing' means 'any operation or set of operations which is performed on personal data or on sets of personal data, 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'.

34. Article 3(1) of the Regulation provides that information constitutes personal data where it relates to a natural person and that person is identified or identifiable. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

35. Moreover, according to case-law, the use of the expression 'any information' in the definition of the concept of 'personal data' within Article 3(1) of the Regulation, reflects the aim of the EU legislature to assign a wide scope to that concept, which is not restricted to information that is sensitive or private but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments provided that it 'relates' to the data subject.[45] As regards the latter condition, the Court of Justice of the European Union (CJEU) has

[43] See Annex 1 to the ECDC's letter to the EDPS of 12 July 2021 - the ECDC Internal Procedure on the use of social media for epidemic intelligence activities, page 6.
[44] Ibid.
[45] See CJEU, 20 December 2017, Nowak, C-434/16, EU:C:2017:994, para. 34.

held that it is satisfied where the information, by reason of its content, purpose or effect, is linked to a particular person.[46]

36. According to Article 2(5) of the Regulation, the processing of personal data wholly or partly by automated means, as well as the processing other than by automated means of personal data which form or are intended to form part of a filing system, fall under the scope of the Regulation.

37. Although the processing performed by the ECDC in the context of its manual and automated monitoring of social media does not aim at targeting individuals but at gathering information which may enable an early detection of potential outbreaks and communicable diseases, the EDPS finds that it nevertheless involves the processing of personal data, as is illustrated hereunder.[47]

3.1.1. Manual social media monitoring

38. As already described[48], in the documentation provided to the EDPS, the ECDC states that in the context of its manual social media monitoring it collects, collates, stores and evaluates data and information contained in Twitter and Facebook posts which refer to epidemiological figures of communicable diseases (confirmed cases, suspected cases, deaths, etc.), situation reports on specific events, and relevant public health campaigns (e.g., vaccination campaigns).'[49]

39. In addition, the ECDC explains that while the data collected are not systematically stored, on rare occasions (where data are coming from official social media accounts, including those of core employees of official organisations, and no other official source is available), the data is included in its Threat Tracking Tool for the production of the ECDC's outputs (RT report or CTDR).[50]

40. In this regard, the ECDC states that it does not collect, store, evaluate or disseminate **personal data** of individuals that are suffering from a communicable disease, nor the personal data of its sources, meaning the persons who publish and/or disseminate data and or information on social media.[51]

41. As previously described[52], when members of the ECDC's EI Group visually screen Facebook and Twitter in the context of the ECDC's manual social media monitoring by consulting the contents of the posts and tweets of selected individuals, they

---

46 CJEU, 20 December 2017, Nowak, C-434/16, EU:C:2017:994, para. 35.
47 See Sections 3.1.1. and 3.1.2. of this Opinion.
48 See Section 2.2.1. of this Opinion.
49 See Annex 1 to the ECDC's letter to the EDPS of 12 July 2021 - the ECDC's Internal Procedure on the use of social media for epidemic intelligence activities, page 7.
50 Ibid.
51 See Annex 1 to the ECDC's letter to the EDPS of 12 July 2021 - the ECDC's Internal Procedure on the use of social media for epidemic intelligence activities, pages 7-8.
52 See Section 2.2.1. of this Opinion.

inevitably become aware of the identity of the authors and thus *process* their names or unique identifiers. However, since **the mere consultation of** these **names and unique identifiers** is manual and does not form part of a filing system, nor is intended to form part of a filing system, it **does not fall within the scope of the Regulation**.[53]

42. By contrast, the **collection and storage of the contents of tweets and posts** from the Twitter and Facebook accounts of natural persons **in the ECDC's Threat Tracking Tool** are processing operations which **fall within the scope of the Regulation**, as explained hereinafter.

(i) The information 'relates to' natural persons

43. The EDPS finds that in both cases (Twitter and Facebook), the information (i.e. quotes) collected and further stored by the ECDC, 'relate to' the author of the concerned tweets, when the latter is a natural person, because it is the expression of their thoughts on a given matter and therefore is linked to them by reason of its 'content, purpose or effect'.[54]

(ii) The natural persons are 'identifiable'

44. In accordance with Recital 16 of the Regulation, 'to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person, to identify the natural person directly or indirectly. Moreover, for information to be treated as 'personal data' within the meaning of Article 3(1) of the Regulation, it is not required that all the information enabling the identification of the data subject must be in the hands of one person.[55]

45. In the present case, based on the information made available to the EDPS, the authors who are natural persons can be indirectly identifiable by their own quotes. Indeed, the ECDC has not clearly demonstrated to the EDPS that entire quotes of single tweets / posts of core employees of official organisations, which contain the sought-out data relating to infectious diseases, are not included in the ECDC's Threat Tracking Tool and subsequently quoted in a report or other supporting document. The ECDC only collects information and data from public sources. As such, the mere entering of such a quote into a search engine would lead to a search result displaying the original publication of the quote on the data subject's public social media thereby rendering them identifiable. This constitutes a means that is reasonably likely to be used to identify the data subject.

---

[53] See Article 2(5) of the Regulation.
[54] See para. 35 above and referred case law.
[55] CJEU, 19 October 2016, Breyer, C-582/14, paras. 42-45.

46. Therefore, the EDPS concludes that **means exist that are reasonably likely to lead to the identification of the authors of the tweets/posts.** In addition, under the principle of accountability enshrined in Article 4(2) of the Regulation, the ECDC has not provided sufficient information to satisfactorily demonstrate that it only processes non-identifiable data in the context of its manual social media monitoring.

(iii) Processing forming part or intended to form part of a filing system

47. The processing is done manually by members of the ECDC's EI Group[56] and involves the inclusion of personal data in the ECDC's Threat Tracking Tool. The latter tool constitutes a 'filing system', in line with the definition provided under Article 3(7) of the Regulation, as it is structured in order to allow personal data related to individuals to be easily retrievable[57], in view of its use in the ECDC's output. Consequently, the ECDC's collection of information and data from Twitter and Facebook in the context of its manual social media monitoring constitutes a processing other than by automated means of personal data which form part of a filing system, thus falling under the scope of the Regulation in accordance with Article 2(5) of the Regulation.

3.1.2. Automated social media monitoring

48. In the context of the ECDC's automated social media monitoring, epitweetr searches for and collects data and metadata about Tweets related to public health threats or infectious diseases through the use of keywords selected by the ECDC comprising scientific and popular nomenclature, as well as more generic topics relating to diseases and infections.[58]

49. In this regard, in the documentation provided to the EDPS, the ECDC acknowledges that epitweetr collects and stores a significant amount of **personal data**, not only about Twitter users who have posted a tweet containing the above-mentioned keywords, but also the personal data of any user that has replied to, retweeted or quoted the same tweet. The personal data collected includes, amongst other things, identification, name, screen name and location data, as well as mentions of other users included in the content of the tweet.[59]

50. In the documentation provided to the EDPS, the ECDC does not acknowledge that it processes **special categories of personal data**.[60] However, the ECDC does state that in the context of its automated social media monitoring the content of entire

[56] See Section 2.2.1. of this Opinion.
[57] CJEU, 10 July 2018, Jehovan Todistajat, C-25/17, para. 57.
[58] See Section 2.2.2. of this Opinion. See also Annex 1 to the ECDC's letter to the EDPS of 21 July 2021 - the ECDC's Internal Procedure on the use of social media for epidemic intelligence activities, page 8.
[59] See Section 2.2.2. of this Opinion. See also Annex 1 to the ECDC's letter to the EDPS of 21 July 2021 - the ECDC's Internal Procedure on the use of social media for epidemic intelligence activities, page 9.
[60] See Annex 3 to the ECDC's letter to the EDPS of 21 July 2021 - the ECDC DPIA.

tweets containing selected keywords relating to infectious diseases are collected.[61] In this regard, the ECDC has not provided sufficient information to clearly demonstrate that it does not collect entire tweets which include a selected keyword and also contain special categories of personal data, such as health data - for example, where an individual discloses in a tweet that they have tested positive for COVID-19.

51. Moreover, in the documentation provided to the EDPS, the ECDC states that the data collected by epitweetr also includes the description of Twitter users' profiles (both of the user who posted the tweet containing a selected keyword and of any other user who interacted with the tweet by replying, retweeting or quoting it). Twitter profile descriptions often include special categories of personal data such as racial origin, political opinions, religious beliefs, or sexual orientation, as defined under Article 10 of the Regulation.

52. As such, the EDPS concludes that the ECDC collects special categories of personal data in the context of its automated social media monitoring. In addition, the ECDC has not provided sufficient information to satisfactorily demonstrate that it does not collect special categories of personal data (Article 10 of the Regulation) as it is required to do in accordance with the principle of accountability enshrined in Article 4(2) of the Regulation.

53. Moreover, the processing activities described above involve the use of the ECDC's interactive web application epitweetr[62], thereby constituting processing by wholly automated means. As such, the processing operations carried out by the ECDC in the context of its automated social media monitoring constitute processing of personal data wholly by automated means and, therefore, clearly fall within the scope of the Article 2(5) of the Regulation.

3.2. Controllership

3.2.1. Manual social media monitoring (Twitter and Facebook)

54. While monitoring Twitter and Facebook manually, the ECDC extracts specific categories of data from Twitter and Facebook in order to accomplish its own tasks.[63] The ECDC determines the purpose of this data processing, as well as most of the essential means of the processing, namely, which data will be processed for its specific purpose, from which categories of data subjects, the recipients and the retention policy; and it accomplishes its tasks autonomously. In light of the above elements, the ECDC has actual control and decisive influence over the data it processes which is extracted from Twitter and Facebook. Hence, in the context of its

[61] See Annex 1 to the ECDC's letter to the EDPS of 21 July 2021 - the ECDC's Internal Procedure on the use of social media for epidemic intelligence activities, page 9.
[62] As described in Section 2.2.2. of this Opinion.
[63] As described in Section 2.2.1. of this Opinion.

manual social media monitoring, the ECDC is a **controller on its own**, separate from Twitter and Facebook, under Article 3(8) of the Regulation.

3.2.2. Automated social media monitoring (Twitter developer account)

55. In addition to the contract for the use of the ECDC's Twitter developer account, the ECDC and Twitter entered into a data protection addendum[64], in which they specifically abide to 'Applicable Data Protection Law' which includes, without limitation, the General Data Protection Regulation (Regulation (EU) 2016/679, hereafter the 'GDPR') and any implementing legislation. In this Addendum, the ECDC and Twitter are considered separate controllers for the processing operation.

56. The ECDC has the above-mentioned Twitter developer account[65] in order to access, download and store tweets made available by Twitter through its Standard Search API tool. The Twitter Standard Search API is a tool used to retrieve relevant and publicly available tweets matching a specific query selected by the user.

57. As put forward in the EDPS guidelines on the concepts of controller, processor and joint controllership under the Regulation[66], '... if the parties involved do not jointly determine or converge on the same general objective (or purpose) or do not base their processing operations on jointly determined (essential elements of the) means, their relationship seems to be pointing to a 'separate controllership' situation.'[67]

58. Therefore, the fact that the ECDC benefits from Twitter's data processing through the Standard Search API is not in itself enough to establish joint controllership. Indeed, whilst the ECDC benefits from Twitter's platform, it sets its own parametrisation through the selection of specific keywords related to infectious diseases and it processes personal data autonomously through its own means via epitweetr for its own purposes, i.e. epidemic intelligence purposes. As such, the ECDC has actual control and decisive influence over the data it processes which are extracted from Twitter, and therefore, it is also a **separate controller** in the context of its automated social media monitoring under Article 3(8) of the Regulation.

3.3. Lawfulness of processing and legal basis in Union law

59. The processing of any personal data is only lawful if one of the grounds for lawfulness listed in Article 5 of the Regulation is applicable. In addition, for the processing of special categories of personal data to be lawful, one of the requirements established

---

64 The Twitter Controller-to-Controller Data Protection Addendum.
65 The terms and conditions of Twitter developer account.
66 See EDPS guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725
67 Ibid, page 24.

in Article 10(2) of the Regulation must be fulfilled. As such, it will be successively analysed below whether all of these requirements are met.

3.3.1. Lawfulness of the processing (Art. 5(1)(a) of the Regulation)

60. In its data protection record[68], the ECDC submits that the processing operations carried out in the context of its manual and automated social media monitoring are lawful under Article 5(1)(a) of the Regulation, according to which **processing shall be lawful if it is necessary for the performance of a task carried out in the public interest.**

61. The **pilot study** launched by the ECDC aims to assess the benefits of trend analysis of social media sources for epidemic intelligence, in order to improve threat detection through epidemic intelligence screening.[69] Thus, it aims to test new means for assessing threats to human health. In this respect, it can be considered that the processing resulting from the pilot project enables the ECDC to perform a task carried out in the public interest, i.e. its mission as described in the ECDC Regulation (see in particular Article 3(1) and 10(1): identify, assess and communicate current threats to human health from communicable diseases).

3.3.2. Lawfulness of the processing of special categories of data (Art. 10 of the Regulation)

62. For the processing of special categories of personal data to be lawful, one of the requirements established in Article 10(2) of the Regulation needs to be fulfilled.

63. A relevant ground for the ECDC's processing of special category data is **Article 10(2)(e) of the Regulation**. According to this Article, the processing of special category data is not prohibited when it is 'manifestly made public by the data subject' themselves. This legal basis would be applicable where a Twitter user with a public account makes their health status public by tweeting about it. However, this derogation only applies to data made public by individuals concerning their *own* health status and is not applicable to data concerning persons other than the person who made those data public.[70]

64. According to case law of the CJEU, where social media users (1) on the basis of individual settings selected with full knowledge of the facts, have the clearly made the choice to have the data they enter into the platform made accessible to the general public and (2) have voluntarily entered sensitive personal information onto their public account, they can be regarded as manifestly making such data public, within the meaning of Article 10(2)(e) of the Regulation.[71] The ECDC via epitweetr

[68] See Annex 4 to the ECDC's letter to the EDPS of 12 July 2021 - the ECDC Data Protection Record.
[69] See above para. 6 of this Opinion and the ECDC Single Programming Document 2021-2023, pages 29 f.
[70] CJEU, 4 July 2023, Meta Bundeskartellamt, C-252/21, para. 75.
[71] Ibid, para. 82 and 83.

only collects information and data from publicly available sources on Twitter.[72] In its settings, Twitter provides users with the possibility of using a protected (i.e., private) account rather than a public account, thereby making their data accessible to a more or less limited number of selected persons. As such, Twitter users who tweet about their health status on their public account could be considered as manifestly making this data public (Article 10(2)(e) of the Regulation). Although, it is debateable whether such a Twitter user would reasonably expect that its public post containing special category data would subsequently be further processed by the ECDC via epitweetr for purposes of detecting and preventing potential outbreaks of communicable diseases.

65. Indeed, the fact that a data subject publishes a tweet online does not mean that EUIs can reuse (i.e. further process) that individual's public information without complying with the Regulation, for what must be considered as a new processing operation. Data protection rules still apply, meaning in particular that EUIs need a legal basis for the further processing of that data.

66. Given the ECDC's mission to early detect public health threats relating to infectious or communicable diseases in view of preventing outbreaks through the use of Twitter data at country, regional and global levels, another relevant ground for the ECDC's processing of special category data is **Article 10(2)(i) of the Regulation**. According to this Article, the processing of special category data is not prohibited where it is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health (e.g. COVID-19).

3.3.3. Legal basis in Union law for the processing (Art. 5(2) of the Regulation)

67. Article 5(2) of the Regulation sets a requirement that the basis for the processing of personal data be laid down in Union law.

68. Article 20(4) of the ECDC Regulation in force at the time when the ECDC consulted the EDPS about their pilot project on social media monitoring, expressly states that: '*Personal data shall not be processed or communicated except in cases where this is strictly necessary for the fulfilment of the mission of the Centre. In such cases, Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data shall apply.*'

69. Under the ECDC Amending Regulation[73], Article 20(4) has been deleted and a new Article 20a(2) has been introduced, according to which: '*The Centre shall not process*

[72] See Section 2.2.2. of this Opinion.

[73] Regulation (EU) 2022/2370 of the European Parliament and of the Council of 23 November 2022 amending Regulation (EC) No 851/2004 establishing a European centre for disease prevention and control, OJ 6.12.2022, L 314, page 1.

personal data except in cases where it is necessary for the fulfilment of its mission. Where appropriate, personal data shall be rendered anonymous in such a manner that the data subject is not identifiable.'

70. In the documentation provided to the EDPS, the ECDC references the following legislation detailing its mission[74]:

- The ECDC Regulation[75], namely:
  - Article 3(1), whereby the **ECDC's mission** shall be to **identify**, assess and communicate **current threats to human health from communicable diseases**;
  - Article 3(2)(a), whereby the ECDC, within the field of its mission, shall search for, collect, collate, evaluate and communicate relevant scientific and technical data;
  - Article 10(1), whereby the ECDC shall within the fields of its mission establish procedures for **systematically** collecting, collating and analysing information and data with a view to the identification of emerging health threats;
  - Article 11(1), whereby the ECDC shall coordinate data collection, validation and analysis at Community level;
- Decision No. 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health[76], namely Article 6(1), whereby the ECDC operates and coordinates a network for epidemiological surveillance of communicable diseases;
- The ECDC Single Programming Document 2020-2022[77], whereby the ECDC shall carry out a pilot study to assess the benefits of trend analysis of social media sources for epidemic intelligence, in order to improve threat detection through epidemic intelligence screening;
- The ECDC Strategy 2021-2027[78], namely strategic objective 3 action area 3.3. 'Support transformation: Provide leadership and support to countries

[74] See Annex 1 to the ECDC's letter to the EDPS of 12 July 2021 - the ECDC's Internal Procedure on the use of social media for epidemic intelligence activities, pages 5-6.
[75] As indicated above in para. 7 of this Opinion, the ECDC Amending Regulation did not bring any substantial changes to the ECDC's mission.
[76] See Decision No. 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health.
[77] See the ECDC Single Programming Document 2021-2023, pages 29 f.
[78] See the ECDC Strategy 2021-2027, page 13.

in adapting, adoption and exploiting new technologies for infectious disease prevention and control'.

3.3.3.1. ECDC Regulation and Decision No. 1082/2013/EU

71. The ECDC Regulation and Decision No. 1082/2013/EU constitute **legal acts under EU law** in the formal sense.[79]

72. However, the question that arises is **whether their provisions are capable of constituting, either alone or in combination, 'Union law'** within the meaning of Articles 5(1)(a) and 5(2) of the Regulation, which contains a basis for the processing of personal data carried out by the ECDC through its social media monitoring.

73. Recital 23 of the Regulation provides that '*The Union law referred to in this Regulation should be **clear and precise** and its application should be **foreseeable** to persons subject to it, in accordance with the requirements set out in the Charter and the European Convention for the protection of Human Rights and Fundamental Freedoms*' [we underline].[80]

74. According to CJEU case law, any legislation which entails interference with the individual rights to privacy and personal data protection must be '***clear** and **precise** rules **governing the scope and application** of the measure in question*'.[81] The law must '*meet quality requirements: it must be accessible to the person concerned and foreseeable as to its* effects' to guarantee that the 'law' permitting for an interference with fundamental rights is compatible with the **rule of law**[82] and that the individuals are protected from arbitrariness of public authorities.[83]

75. A legal base permitting an interference with the fundamental right to personal data protection, as in the present case, must itself **define the scope of the interference** with that right.[84] Hence, in order to serve as a legal basis for the envisaged processing operation, the ECDC needs to rely on a legal basis that, as a bare minimum, **clearly**

---

79 Article 288 TFEU.

80 See also the case law of the CJEU: CJEU, 22 June 2021, Latvijas Republikas Saeima (Penalty Points), C-439/19, ECLI:EU:C:2021:504, para. 105 ('**Penalty Points**'), as well as case General Court judgment of 24 February 2022, SIA, C-175/20, ECLI:EU:C:2022:124 ('**SIA**'), para. 55.

81 Penalty Points, op.cit., para. 105, as well as SIA, op.cit., para. 55.

82 Case no 47143/06, Roman Zakharov v. Russia, 4 December 2015, op.cit., para. 228: The Court notes from its well-established case-law that the wording 'in accordance with the law' requires the impugned measure both to have some **basis in domestic law** and **to be compatible with the rule of law**, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must thus meet **quality requirements**: it must be accessible to the person concerned and foreseeable as to its effects (see, among many other authorities, Rotaru v. Romania [GC], no. 28341/95, § 52, ECHR 2000-V; S. and Marper v. the United Kingdom [GC], nos. 30562/04 and 30566/04, § 95, ECHR 2008; and Kennedy, cited above, § 151).

83 CJEU, 15 February 2016, N., C-601/15 PPU, EU:C:2016:84, para. 81.

84 SIA, para. 54, and CJEU, 6 October 2020, Privacy International, C-623/17, ECLI:EU:C:2020:790, para. 65 ('Privacy International').

and specifically indicates that monitoring of publicly available information are to be used for epidemic intelligence purposes. Without such a clear and precise indication, addressees of the legal acts in question cannot reasonably foresee the applicability of specific rules interfering with their right to personal data protection.

76. Moreover, where a legal basis gives rise to a serious interference with fundamental rights to data protection and privacy, there is a greater need for clear and precise rules governing the scope and the application of the measure as well as the accompanying safeguards. Therefore, **the greater the interference** entailed by the legal basis, **the more robust and detailed the rules and the safeguards should be**.

77. In this regard, the CJEU has advanced several criteria to determine the seriousness of an interference with the right to protection of personal data and the right for respect of private life. Some of the elements to be considered include (1) the nature of the personal data at issue, in particular the processing of any special categories of data[85], (2) the lack of awareness of the data processing on the part of the data subject[86], (3) large-scale processing of personal data[87], (4) public accessibility of the information[88], and (5) automated processing of data involving pre-established models and criteria.[89]

78. A case by case assessment is necessary to assess the seriousness of the interference. In this regard, the criteria developed by the EDPS[90] to determine whether the processing is 'likely to result in a high risk' can also help with this assessment. Some of the criteria relevant to the ECDC's processing include: (1) systematic monitoring through processing used to monitor data subjects in publicly accessible spaces, (2) sensitive data processing, (3) data processed on a large scale based on number of people concerned and geographical coverage, and (4) innovative use of technological solutions that involve novel forms of data collection and usage such as machine learning. In most cases, processing meeting two or more criteria should be considered as likely amounting to a serious interference.

79. As such, to be considered as providing a sufficient ground for lawfulness for the processing, the ECDC Regulation and Decision No. 1082/2013/EU need to be precise, clear and foreseeable enough to allow data subjects to ascertain the processing

---

85 Judgment of the Court of 11 December 2019, Asociaţia de Proprietari bloc M5A-ScaraA; C-708/18, EU:C:2019:1064, para. 57-63

86 Tele2 Sverige and Watson and Others, note 7 and Digital Rights Ireland, note 2.

87 Digital Rights Ireland, note 2, and La Quadrature du Net and Others, note 7.

88 Google Spain and Google, note 14; OT and the Vyriausioji tarnybinės etikos komisija, note 10, para. 99-105.

89 See Opinion 1/15 (EU-Canada PNR Agreement), note 14, and judgment of 21 June 2022, Ligue des droits humains v. Conseil des ministres, Case C-817/19, EU:C:2022:491, para. 194-195.

90 See Annex 1 of the Decision of the EDPS of 16 July 2019 on DPIA lists issued under Articles 39(4) and (5) of the Regulation (EU) 2018/1725.

operation that the ECDC is performing regarding social media monitoring for epidemic intelligence.

80. The ECDC Regulation constitutes the legal basis for establishing the ECDC. However, the ECDC Regulation does not expressly provide for a legal provision authorising the ECDC to conduct the processing of personal data through **monitoring of publicly available information for epidemic intelligence purposes**, or specifically the processing of the (specific) personal data that might result thereof. As such, the EDPS finds that the ECDC Regulation does not sufficiently define the scope of the interference with the fundamental rights of data subjects and is not sufficiently foreseeable to allow the concerned individuals to reasonably anticipate the processing operations entailed by the social media monitoring activities. Failure to specify the use of social media monitoring in this legal act renders it **too generic** to rely on as a legal basis in the present case under Articles 5(1)(a) and 5(2) of the Regulation.

81. With regard to the ECDC Regulation in effect since 26 December 2022, the EDPS takes note of the addition of Recital 31[91], which provides, amongst other things that (1) special categories of personal data are subject to a higher level of protection, (2) that any processing of personal data pursuant to the ECDC Regulation is subject to the GDPR and the Regulation, and that (3) wherever possible data should be anonymised and if impossible, pseudonymised. The EDPS also takes note of the addition of Article 20a(2): '*The Centre shall not process personal data except in cases where it is necessary for the fulfilment of its mission. Where appropriate, personal data shall be rendered anonymous in such a manner that the data subject is not identifiable.*'

82. However, the EDPS notes that the enacting terms of the ECDC Amending Regulation equally remain silent as to the express mentioning of the processing of personal data through monitoring of publicly available information for epidemic intelligence purposes, or the specific processing of personal data that might result thereof. The text still does not set out the categories of data subjects under the scope of the processing, the categories of the personal data actually processed, nor a description of any concrete measures implemented to safeguard the rights and freedoms of the data subjects involved.

[91] Recital 31 of the ECDC Amending Regulation: 'Personal data concerning health are considered to be sensitive data under applicable Union legislation on data protection and therefore enjoy a higher level of protection. Any processing of personal data pursuant to this Regulation by Member States or the Centre is subject to GDPR and EUDPR. Processing of personal data under this Regulation should respect the data protection principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality. Whenever possible, personal data should be anonymised. Where anonymisation would not allow the specific purpose of the processing to be achieved, the personal data should, where possible, be pseudonymised. In the case of cooperation between the health authorities of the Union and third countries, the WHO or other international organisations, transfers of personal data to third countries or international organisations should always comply with the rules laid down in EUDPR.'

83. The EDPS in addition notes that the ECDC Amending Regulation added a new Article 11(2)(d)[92] which states that the ECDC shall '*develop solutions to access relevant health data, whether publicly available or made available or exchanged through digital infrastructure, in order to allow the health data to be used for healthcare, health research, policy-making and regulatory purposes linked to public health; and provide and facilitate controlled and timely access to health data to support public health research.*' While this Article mentions access to 'health data' which is 'made publicly available', it remains silent as to the monitoring of publicly available information for epidemic intelligence purposes. The Article references 'health data' and not personal data (Article 3(1) of the Regulation) or special categories of personal data such as data concerning health (Article 10(1) of the Regulation). Moreover, the Article 11(2)(d) of the ECDC Amending Regulation states that these solutions are to be developed by the ECDC in view of enabling the health data to be used mainly for research purposes rather than for the early detection of emerging health threats through social media monitoring. Indeed, the Article refers back to Article 11(1)[93] of the ECDC Amending Regulation by specifying that the ECDC will develop these solutions for the purposes of 'collection and analysis of data', as opposed to the 'identification of emerging health threats' under Article 10 of the ECDC Amending Regulation.

84. As such, the EDPS finds that the ECDC Regulation, including as amended, remains too generic to be relied upon as a legal basis under Articles 5(1)(a) and 5(2) of the Regulation.

85. The same reasoning applies to Article 6 of Decision No. 1082/2013/EU, which tasks the ECDC to operate and coordinate a network for epidemiological surveillance of the communicable diseases and of the related special health issues, without any explicit reference to social media monitoring.

3.3.3.2. Other grounds put forward by the ECDC

86. The other grounds for lawfulness brought forward by the ECDC, i.e. the ECDC Strategy 2021-2027 and the ECDC Single Programming Document 2020-2022, cannot be considered as 'Union law' within the meaning of Article 5(2) of the Regulation. Firstly, they are internal documents produced by the ECDC under its administrative autonomy. While the EDPS recognises that EUIs may in certain exceptional

[92] Article 11(2)(d) of the ECDC Amending Regulation: 'develop solutions to access relevant health data, whether publicly available or made available or exchanged through digital infrastructure, in order to allow the health data to be used for healthcare, health research, policy-making and regulatory purposes linked to public health; and provide and facilitate controlled and timely access to health data to support public health research.'

[93] Article 11(1) of the ECDC Amending Regulation: '1. The Centre shall: (a) coordinate standardisation of data collection procedures, and validation, analysis and dissemination of data at Union level; (b) seek, where appropriate, the expertise and guidance of the Member States to ensure that there is a correct understanding of the health data made available, their limitations and the national context and information systems.'

circumstances provide for lawful processing in these types of documents, the interference with fundamental rights should be provided for at a level enjoying higher democratic legitimacy. In any event, the former document is, like the legislation analysed above, not precise enough, as it does not reference social media monitoring.

87. While arguably the ECDC Single Programming Document 2020-2022 references a pilot study to assess the benefits of trend analysis of social media sources for epidemic intelligence purposes, the EDPS notes that such a document **is notably not accessible and foreseeable enough to avoid the risk of arbitrariness.** Individuals whose personal data are processed as part of social media monitoring do not have adequate indication, given the unlimited number of data subjects concerned, of the legal rules applicable in their case.

88. In addition, the ECDC Strategy 2021-2027 **does not define precisely enough the scope of the interference** since it does not define its most crucial elements, such as its purpose or the categories of data subjects or personal data. As a consequence, individuals concerned **are not aware of the circumstances and conditions under which their right to personal data protection can be interfered with**.

89. Therefore, the EDPS considers that the acts mentioned in the preceding paragraphs equally **cannot be relied on jointly** to fulfil the conditions of Articles 5(1)(a) and 5(2) of the Regulation.

3.3.3.3. Conclusion

90. It follows that, **at present**, the **ECDC does not have a sufficient 'basis' in 'Union law'** for the social media monitoring activities, which are the object of this Opinion.

91. However, the EDPS acknowledges that the **seriousness of the measures' interference** with the rights to data protection and privacy is **mitigated** considering that the ECDC's social media monitoring activities are in a pilot phase and **do not aim at targeting individuals**, but rather at gathering information which may enable the early detection of potential outbreaks and communicable diseases.

92. The EDPS recognises that the task of monitoring social media with a view to detecting serious cross-border threats to human health at an early stage fits into the ECDC's mission to '*identify* (...) *current and emerging threats to human health from communicable diseases*'[94] and to '*establish procedures for systematically collecting, collating and analysing information and data with a view to the identification of emerging health threats*'[95].

[94] Art. 3(1) of the ECDC Amending Regulation. This task was already included in the initial ECDC Regulation.
[95] Art. 10(1) of the ECDC Amending Regulation. This task was already included in the initial ECDC Regulation.

93. In light of the above, while the ECDC (Amended) Founding Regulation cannot in itself be considered as providing a sufficient basis in Union law for social media monitoring, it can be considered as providing a starting point. In this regard, the ECDC (Amended) Founding Regulation could only meet the requirements of Article 5(2) of the Regulation if complemented by appropriate **internal rules** on social media monitoring activities. These internal rules adopted as a basis for lawful processing operations resulting from the ECDC's social media monitoring will need to meet the 'quality of the law' requirements, i.e., they will need to be precise, accessible and foreseeable.

94. In light of the specific context of the processing operations in question, which involve the **systematic monitoring on a large scale of personal data,** including **special categories of personal data,** through the **use of innovative technological solutions** and in most cases **without data subjects' awareness,** the internal rules adopted by the ECDC will need to meet a **heightened threshold of accessibility and foreseeability**.

95. As such, the EDPS **recommends** that the adopted internal rules be made as widely available as possible, for instance through their publication on the ECDC's website and its social media channels, as well as in the Official Journal of the European Union. In addition, these internal rules should precisely **define the scope of the interference** with the right to personal data, through identification of the purpose of processing, categories of data subjects, categories of personal data, controller, and storage periods, together with a description of the concrete minimum safeguards for the rights of the data subjects.

3.3.4. Legal basis in Union law for the processing of special categories of personal data (Art. 10(2)(i) of the Regulation)

96. As regards special categories of personal data, according to Article 10(2)(i) of the Regulation, in order for the processing to be lawful, it also needs to be performed on the basis of Union law, which provides for suitable and specific measures to safeguard the rights and freedoms of data subjects.

97. **The assessment** carried out above[96] **concluding that the ECDC Regulation needs to be further amended or supplemented by appropriate internal rules**, given that it is not sufficient in itself to be relied on as a legal basis in Union law for the processing operations at hand, is also applicable here. Indeed, the ECDC Regulation, as amended, does not make reference to the processing of special categories of personal data resulting from the ECDC's monitoring of publicly available information on social media for epidemic intelligence purposes. As such, the ECDC Regulation does not meet the 'quality criteria' as detailed above[97].

[96] See Section 3.3.3. of this Opinion.
[97] See Section 3.3.3. of this Opinion.

Recommendation 1: The EDPS deems necessary that a clear legal basis should be provided for the processing entailed by social media monitoring in the legislation. To that purpose, the ECDC could ask the EU legislator to further amend the ECDC Regulation in order for it to meet the criteria of clarity, precision and foreseeability required for rules to be considered as Union law under Articles 5(1)(a),5(2) and 10(2)(i) of the Regulation. This should be done by including a specific reference to the ECDC's monitoring of publicly available information on social media for epidemic intelligence purposes, as well as the personal data processing resulting therefrom.

Recommendation 2: The EDPS deems necessary that pending such an amendment to the ECDC Regulation, or in its absence, in order for the ECDC to have a sufficient basis in Union law for the processing operations resulting from the ECDC's social media monitoring, it will need to **adopt dedicated internal rules** which meet the heightened threshold of clarity, precision and foreseeability, required for such rules to be considered as Union law within the meaning of Articles 5(1)(a)5(2) and 10(2)(i) of the Regulation.

3.3.5. Necessity and proportionality of the processing (Art. 52 of the Charter and 5(1)(a) and 10(2)(i) of the Regulation)

98. According to Article 5(1)(a) of the Regulation, processing of any personal data shall only be lawful if it is **'necessary'** for the performance of a task carried out in the public interest. Moreover, in accordance with Article 10(2)(i) of the Regulation, controllers shall be exempted from the prohibition of the processing of special categories of personal data if the processing is **'necessary'** for reasons of public interest in the area of public health, such as protection against serious cross-border threats to health. Article 20a(2) of the ECDC Regulation also specifies that the ECDC can only process personal data where it is *necessary* for the fulfilment of its mission.

99. According to the EDPS Toolkit on 'Assessing the necessity of measures that limit the fundamental right to the protection of personal data' [98], 'necessity' implies the need for a combined, fact-based assessment of the **effectiveness** of the measure for the objective pursued and of whether it is **less intrusive** compared to other options for achieving the same goal. Once a measure is proved necessary, it should then be examined according to its proportionality. This proportionality test generally involves assessing what **safeguards** should accompany a measure in order to reduce

[98] See EDPS, 'Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit'

the risks posed by the envisaged measure to the fundamental rights and freedoms of the individuals concerned to an acceptable and proportionate level.[99]

100. The necessity Toolkit includes a four-step checklist to assess necessity:

- Step 1 requires that a **detailed factual description** of the measure proposed and its purpose be provided prior to any further assessment;

- Step 2 helps identify whether the proposed measure represents **a limitation** on the rights to the protection of personal data or respect for private life (also called right to privacy), and possibly also on other rights;

- Step 3 considers the **objective of the measure** against which the necessity of a measure should be assessed;

- Step 4 provides guidance on the specific aspects to address when performing the necessity test, in particular that the measure should be **effective** and the **least intrusive.**

101. In this regard, in the documentation provided to the EDPS, the ECDC has failed to provide a sufficiently detailed factual description of the measure proposed and its purpose, as it has not precisely identified what the proposed measure entails in terms of personal data processing. Indeed, in its DPIA, the ECDC's assessment of the necessity of its processing operations is limited to its processing of personal data in the context of its automated social media monitoring. The ECDC's processing of personal data in the context of its manual social media monitoring and its processing of special categories of personal data in the context of its automated social media monitoring have not been assessed.[100]

102. The ECDC has acknowledged that, in addition to a limitation on the rights to the protection of personal data and respect for private life, its processing operations could entail chilling effects on individuals' freedom of expression as they may become more reluctant to express themselves on social media due to social media monitoring. The ECDC has put forward the early detection of public health threats, in particular, potential outbreaks of communicable diseases at a country, regional and global level, as the objective of the processing operations involved in its pilot study.[101]

103. However, even if appropriate, the chosen measure should also be effective and less intrusive than other options for achieving the same goal. The ECDC, in its DPIA, states that the proposed processing operation is effective in achieving its mission of

[99] See EDPS, Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data.
[100] See Annex 3 to the ECDC's letter to the EDPS of 12 July 2021 - the ECDC DPIA.
[101] Ibid.

early detection of public health threats related to infectious diseases and that the alternatives to the processing operation in place would be to keep the manual screening of social media or to access the full dataset of Twitter. The ECDC asserts that the first alternative would reduce the efficiency of early detection in terms of speed and sensitivity and would increase the resources needed, whereas the second alternative would be excessive in relation to the objective pursued.[102] Nevertheless, the EDPS reminds the ECDC, that not everything that 'might prove useful' for a certain purpose is 'desirable or can be considered as a necessary measure in a democratic society'.[103] The ECDC, based on the documentation provided to the EDPS, has not conducted a sufficient analysis to demonstrate that the proposed processing operation is **essential** to meet the identified objective, rather than being the most convenient or cost effective[104], as it is required to do in line with its obligation under the principle of accountability (Article 4(2) of the Regulation). This is particularly the case in light of the sensitivity of the data at stake i.e., sensitive categories of personal data such as health data, for which the threshold is higher.

104. Moreover, in line with Article 20a(2) of the ECDC Regulation, the ECDC should assess in its DPIA whether the data collected could be processed in a such a manner that they are rendered anonymous.

105. As such, based solely on the information provided to the EDPS, **the ECDC has not conducted a sufficiently thorough assessment of the necessity** of the proposed processing operations under Article 5(1)(a) and 10(2)(i) of the Regulation.

106. In accordance with Article 52(1) of the Charter of Fundamental Rights of the European Union ('the Charter'), in order to be lawful, any limitation to the right to privacy (Article 7 of the Charter) and data protection (Article 8 of the Charter), needs not only to be necessary, but also proportionate.[105]

107. Concerning the proportionality assessment, the ECDC, in its DPIA, puts forward that: '*There is an identified need and an explicit mandate to complement and improve epidemic intelligence by using social media. The likelihood of risks to the rights of data subjects is limited. Whilst the amount of the collected tweets is a significant amount of data, it corresponds to less than 1% of all global tweets. Transparency will be ensured through the publication of a privacy statement online and on social media. Data are stored on the premises with very limited access, on a need-to-know basis and authentication is required. The data are compressed and must be processed in order to identify the data subjects. The impact on data subjects is also limited and the remaining*

[102] Ibid.

[103] WP29, Opinion 9/2004 on a Draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services, 9 November 2004, page 4.

[104] WP29, Opinion 3/2012 on developments in biometric technologies of 27 April 2012, page 8.

[105] See EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, page 6.

risks will be mitigated by adopting a retention policy of 6 months. The objective outweighs the limited risks and thus justifies the processing operation.'[106]

108. However, considering that necessity is a pre-condition for proportionality[107], and since it has been established that the ECDC did not conduct a sufficiently thorough assessment of the necessity of its processing operation, the ECDC's assessment of the proportionality of the processing will also need to be re-conducted, with a particular focus on the assessment of the seriousness of the interference based on the criteria advanced by the CJEU.[108] Indeed, this assessment will be important to be able to carry out an effective balancing test in view of demonstrating that the legitimacy and importance of the public interest outweighs the intensity of the interference with the rights to data protection and privacy.[109]

Recommendation 3: In order to demonstrate compliance with the requirements set out under Article 5(1)(a) and 10(2)(i) of the Regulation, as well as under Article 52(1) of the Charter, the ECDC will need to conduct and document a more thorough assessment of the necessity and proportionality of its processing operations in the context of its social media monitoring activities, in line with its obligation under the accountability principle (Article 4(2) of the Regulation). Notably, the ECDC will need to (1) provide a sufficiently detailed factual description of the measure proposed detailing all categories of data processed, (2) demonstrate that the proposed processing operations are 'essential' to meet the identified objective, and (3) conduct a more thorough assessment of the seriousness of the interference of the measure in relation to the benefits brought to the public interests served by the performance of the ECDC's tasks.

3.4. Data Protection Impact Assessment (DPIA)

109. In accordance with Article 39(1) of the Regulation, '*where a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data*'. Under Article 39(4) of the Regulation, the EDPS '*shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data*

[106] See Annex 3 to the ECDC's letter to the EDPS of 12 July 2021 - the ECDC DPIA.
[107] See EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, page 10.
[108] See above paras. 77-78 of this Opinion.
[109] See EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, page 11.

protection impact assessment'. Accordingly, the EDPS adopted its Decision of 16 July 2019 on DPIA Lists (the 'DPIA list decision')[110]

110. According to Article 3 of the DPIA list decision, when assessing whether their planned processing operations trigger the obligation to conduct a DPIA under Article 39 of the Regulation, the controller shall conduct a threshold assessment. Where two or more of the criteria in the template in Annex 1 of the DPIA list decision are applicable, the controller shall in general carry out a DPIA.

111. In this regard, the ECDC's processing operations involve (1) systematic monitoring through processing used to monitor data subjects in publicly accessible spaces, (2) sensitive data processing, (3) data processed on a large scale based on number of people concerned and geographical coverage, and (4) innovative use of technological solutions that involve novel forms of data collection and usage such as machine learning. [111] As such, the ECDC is required to conduct a DPIA.

112. Despite not having mentioned any of the above criteria, the ECDC has carried out a DPIA focusing solely on their use of the Twitter platform for its automated social media monitoring concluding that the risks to the rights of data subjects are limited. Nevertheless, in its letter to the EDPS, the ECDC raises that there might be a high risk to the data subjects' rights due to concerns regarding the possibility of ensuring data subject rights given the high number of persons involved.[112]

113. According to Article 39(7)(a) and (b) of the Regulation, the DPIA should include a systematic description of the envisaged processing operations, as well as an assessment of the necessity and proportionality of the processing operations in relation to the purposes.

114. The ECDC's DPIA does not address the processing of special categories of personal data, nor does it assess the necessity and proportionality of such processing. As such, in order to be compliant with Articles 39(7)(a) and (b) of the Regulation, the EDPS recommends that the ECDC review and complement the DPIA to include the processing of sensitive data, as well as a complete assessment of the necessity and proportionality of the processing.

115. Furthermore, in the documentation provided to the EDPS, the ECDC also indicates that other social media platforms might be used in the context of its manual social media monitoring. Considering that each social media platform entails the processing of various categories of personal data, the EDPS reminds the ECDC that conclusions about Twitter cannot be extrapolated and applied to other social media

[110] See Annex 1 of the Decision of the EDPS of 16 July 2019 on DPIA lists issued under Articles 39(4) and (5) of the Regulation (EU) 2018/1725.
[111] See para. 78 of this Opinion.
[112] See the ECDC's letter to the EDPS of 12 July 2021, page 1.

platforms, and therefore, a separate independent assessment will need to be carried out.

Recommendation 4: Before making its decision to go forward with the pilot project, the ECDC should review and/or complement its DPIA to include the processing of special categories of personal data and should conduct and document a more complete and thorough assessment of the necessity and proportionality of all its processing activities in the context of its manual and automated social media monitoring. Moreover, in the event that the ECDC wishes to perform (automated) processing operations through other social media channels, it should further amend its DPIA accordingly.

3.5. Information to data subjects and exercise of data subject rights

116. The ECDC raises concerns regarding the possibility to ensure data subject rights taking into account the high number of persons involved in the context of its automated and manual social media monitoring activities.

117. Articles 15 and 16 of the Regulation relate to the information to be given to data subjects in order to guarantee a fair and transparent processing of their personal data. When the personal data are not directly obtained from the data subject, the controller must provide them with the information established in Article 16 of the Regulation.

3.5.1. Manual social media monitoring

118. In the case of manual social media monitoring, the personal data (i.e. quotes from public Facebook or Twitter accounts which are subsequently included in the ECDC's output allowing for the indirect identification of the data subject), are manually selected by members of the ECDC's EI Group.[113] Therefore, in principle, **it seems feasible to the EDPS for the ECDC to inform individuals concerned** about this processing operation, by contacting them on their public account at the moment of collection, to inform them e.g. via a standardised message of their data subject rights, such as the right to object to this processing operation (Article 23 of the Regulation), the right of access (Article 17 of the Regulation), the right to rectification and erasure (Article 18 of the Regulation) and all other applicable data subject rights; unless the ECDC can show that one of the exceptions under Article 16(5) of the Regulation applies.

[113] See Annex 1 to the ECDC's letter to the EDPS of 12 July 2021 - the ECDC's Internal Procedure on the use of social media for epidemic intelligence activities, page 7.

3.5.2. Automated social media monitoring

119. In the documentation provided to the EDPS, the ECDC states that, in the context of its automated social media monitoring, the raw data collected by epitweetr is stored in compressed JSON files which are not structured by name of the topic and as such **have to be processed to be read**. Moreover, it is stated that epitweetr automatically aggregates data. These **aggregated data do not contain personal data** and are used for data visualization in the epitweetr dashboard (e.g. trend line reflecting the most frequently used words for a given topic and location).[114] In light of this, in order for ECDC to be able to identify the authors of the tweets collected by epitweetr and be able to inform such data subjects in compliance with Article 16 of the Regulation, it would have to process additional information.

3.5.2.1. Processing which does not require identification (Art. 12(1) of the Regulation)

120. Article 12(1) of the Regulation provides that if the purposes for which a controller processes personal data do not or no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation. Article 12(2) of the Regulation goes on to say that, in this situation, where the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 17 to 22 on data subject rights shall not apply, except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.

121. Considering that the ECDC does not need to know the authors' identities in order to achieve the aim of the processing (i.e. the early detection of public health threats), the ECDC should be able to perform the processing operation without identifying data subjects. Therefore, in principle, the ECDC does not have data enabling them to inform individually the users whose posts will be monitored.

122. In view of the above, in accordance with Article 12(1) of the Regulation, **requiring that the ECDC collect and process identification data** for the sole purpose of informing data subjects individually **would run counter to the principle of data minimisation** and would be disproportionate.[115]

---

[114] See Annex 1 to the ECDC's letter to the EDPS of 12 July 2021 - the ECDC's Internal Procedure on the use of social media for epidemic intelligence activities, page 9.

[115] See EDPS' Prior Checking Opinion on the data processing for social media monitoring at the European Central Bank, page 9.

3.5.2.2. Exemption from the obligation to provide individual information to data subjects (Art. 16(5) of the Regulation), Transparency (Art. 14 of the Regulation) and response to data subject requests (Art. 12(2) of the Regulation)

123. In these circumstances, the ECDC could rely on Article 16(5) of the Regulation according to which a controller is **exempted from the obligation of providing the individual information** included under Article 16(1) to (4) where the provision of such information '*proves impossible or would involve disproportionate effort, in particular for the processing for (...) scientific (...) research purposes*', or '*in so far as it is likely to render impossible or seriously impair the achievement of the objectives of the processing*', provided that it is able to demonstrate that the conditions of the exemption are fulfilled.

124. Even though the ECDC is exempted from the obligation to provide individual information to data subjects, it is still required to **publish a privacy statement** on its website, in line with the transparency obligation of Article 14(1) of the Regulation.[116]

125. Were the ECDC to receive a **data subject request to exercise their data subject rights**, the ECDC could inform the data subject that it is not - or is no longer - in a position to identify them and that Articles 17-22 of the Regulation do not apply, unless the data subject provides additional information enabling the ECDC to identify them.[117]

3.5.3. The ECDC's Privacy Statement

126. As indicated in the previous Section, the ECDC has a duty under Article 14 of the Regulation to provide any information referred to in Article 16 in a concise, transparent, intelligible and easily accessible form. The ECDC states in its DPIA that 'transparency will be ensured through the publication of a privacy statement online and on social media'.

127. Under Article 16(1)(c) and (d) of the Regulation, the ECDC is required to provide data subjects with information on the legal basis for processing, as well as the categories of personal data concerned. As previously explained[118], the EDPS is of the view that in the context of its automated social media monitoring, the ECDC processes special category data as defined under Article 10 of the Regulation. As such, the EDPS recommends that the ECDC include a mention of its **processing of special categories of personal data** in its privacy statement and that it clarifies

[116] See Section 3.5.3. of this Opinion.
[117] Article 12(2) of the Regulation.
[118] See Section 3.1.2. of this Opinion.

which legal basis is relied upon for the processing of this data, for example, Article 10(2)(e) and (i) of the Regulation.

128. Moreover, again in relation to the automated social media monitoring, in light of the application of Article 12(2) of the Regulation and in order to ensure fairness and transparency, the EDPS recommends that the ECDC indicate in their privacy statement that it is **impossible or** it would involve a **disproportionate effort to inform data subjects individually** of their rights under Article 16 of the Regulation, since, in principle, the ECDC does not have the information needed to contact them.

129. In addition, in accordance with Article 16(2)(a), the ECDC is required to inform data subjects of the period for which their personal data will be stored. According to the ECDC's privacy statement, the **retention period** for raw data collected containing personal data is of six months. Thereafter, the data is anonymised or aggregated. However, according to the ECDC's 'Internal Procedure for the use of social media for epidemic intelligence activities', the Twitter data collected by epitweetr will be kept until the pilot project is finalised, i.e. 2025, and that shorter retention periods will be discussed and applied after the end of the pilot phase.[119] This is not included in the privacy statement. As such, the EDPS recommends that the ECDC update its privacy statement to reflect the retention period referenced in its internal procedure document.

Recommendation 5: In view of ensuring the respect of data subject rights enshrined in the Regulation and of transparency obligations under Article 14 of the Regulation, as well as compliance with the requirements set out in Article 16 of the Regulation, the ECDC should:

(1) require employees conducting its **manual social media monitoring** to inform the data subjects involved, at the time of collection, about the processing of their personal data and about their rights as data subjects, e.g. by sending them a standardised direct message on their public account which is being monitored, unless the ECDC can show that one of the exceptions under Article 16(5) of the Regulation applies;

(2) adapt its **privacy statement** as follows:

- mention the processing of special categories of personal data in the context of its automated social media monitoring and the legal basis relied upon for this processing;

[119] See Annex 1 to the ECDC's letter to the EDPS of 12 July 2021 - the ECDC's Internal Procedure on the use of social media for epidemic intelligence activities, page 10.

- indicate, where appropriate, its reliance on Articles 12(1)-(2) and 16(5) of the Regulation as regards individual information and other data subject rights, and

- clarify the applicable retention period.

4. CONCLUSION

130. In this Opinion, the EDPS has assessed the lawfulness of the processing operations conducted by the ECDC in the context of its pilot project involving the manual and automated monitoring of social media for purposes of epidemic intelligence.

131. In this regard, in order to ensure the compliance of the processing with the Regulation, the EDPS deems the following necessary for ECDC to undertake:

- **Recommendation 1:** A clear legal basis should be provided for the processing entailed by social media monitoring in the legislation. To that purpose, the ECDC should ask the EU legislator to amend the ECDC Regulation in order to for it to meet the criteria of clarity, precision and foreseeability required for rules to be considered as Union law under Articles 5(1)(a), 5(2) and 10(2)(i) of the Regulation. This should be done by including a specific reference to the ECDC's monitoring of publicly available information on social media for epidemic intelligence purposes, as well as the processing of personal data and special categories of personal data resulting therefrom.

- **Recommendation 2:** Pending an amendment to the ECDC Regulation, or in its absence, in order for the ECDC to have a sufficient basis in Union law for the processing operations resulting from the ECDC's social media monitoring, it will need to adopt dedicated internal rules which meet the heightened threshold of clarity, precision and foreseeability required for such rules to be considered as Union law within the meaning of Articles 5(1)(a),5(2) and 10(2)(i) of the Regulation.

132. Moreover, the EDPS issues the following recommendations to the ECDC:

- **Recommendation 3:** In order to demonstrate compliance with the requirements set out under Article 5(1)(a) and 10(2)(i) of the Regulation, as well as under Article 52(1) of the Charter, the ECDC will need to conduct and document a more thorough assessment of the necessity and proportionality of the processing operations in the context of its manual and automated social media monitoring, in line with its obligations under the accountability principle (Article 4(2) of the Regulation). Notably, the

ECDC will need to (1) provide a sufficiently detailed factual description of the measure proposed, detailing all categories of data processed, (2) demonstrate that the proposed processing operations are 'essential' to meet the identified objective, and (3) conduct a more thorough assessment of the seriousness of the interference of the measure in relation to the benefits brought to the public interests served by the performance of the ECDC's tasks.

- **Recommendation 4:** Before making its decision to go forward with the pilot project, the ECDC should review/complement its DPIA to include the processing of special categories of personal data and should conduct and document a more complete and thorough assessment of the necessity and proportionality of all its processing activities in the context of its manual and automated social media monitoring. Moreover, in the event that the ECDC wishes to perform (automated) processing operations through other social media channels, it should further amend its DPIA accordingly.

- **Recommendation 5:** In view of ensuring the respect of data subject rights enshrined in the Regulation and of transparency obligations under Article 14 of the Regulation, as well as compliance with the requirements set out in Article 16 of the Regulation, the ECDC should

  (1) require employees conducting its manual social media monitoring to inform the data subjects involved, at the time of collection, about the processing of their personal data and about their rights as data subjects, by sending them a standardised direct message on their public account which is being monitored, unless the ECDC can show that one of the exceptions under Article 16(5) of the Regulation applies,

  (2) adapt its privacy statement as follows:
  - mention the processing of special categories of personal data in the context of its automated social media monitoring and the legal basis relied upon for this processing,
  - indicate, where appropriate, its reliance on Article 12(1)-(2) of the Regulation in its privacy statement as regards individual information and other data subject rights, and
  - clarify the applicable retention period.

133. The EDPS expects that the ECDC will implement recommendations 1 through 5 and will provide documentary evidence of this implementation within **three months** of this Opinion.

134. This Supervisory Opinion is without prejudice to any follow-up or other actions the EDPS might undertake in the future in order to allow it to verify any factual assertions made by the ECDC in the context of this matter or for the supervision of the ECDC generally.

Done at Brussels on 09 November 2023

[e-signed]

Wojciech Rafał WIEWIÓROWSKI