ECDC CORPORATE

Data protection governance for EpiPulse

February 2026

Purpose of this document

1. ECDC operates EpiPulse, the digital platform for surveillance referred to in Article 14 of Regulation (EU) 2022/2371[1].
2. This document addresses the data protection governance of the surveillance data provided by the Member States and processed on the platform, including the roles and obligations of ECDC and the Member States pursuant to data protection legislation[2].
3. The document has been discussed with the National Focal Points for Surveillance on behalf of their respective Member States. The document formalises the scope of ECDC and Member State accountability when processing personal data in EpiPulse.
4. The document takes into account the latest draft version of the upcoming delegated acts under Article 14 of the Regulation on Serious Cross-Border Threats to Health (SCBTH) and the principles of data governance shall comply with the final adopted text of these delegated acts. The document may need to be amended once the European Data Protection Board adopts its guidelines on scientific research, or if the legal definition of pseudonymised data changes.

Legal framework: controllership of EpiPulse

5. In data protection, a data controller is the entity that determines the purposes and means of processing of personal data. Controllership entails an overall accountability for the processing of personal data in accordance with data protection legislation.
6. Controllership can be explicitly determined through legislation, or, where such an explicit element is missing, by observing the factual circumstances of a processing operation.
7. Neither ECDC's Founding Regulation nor the SCBTH Regulation include explicit provisions on controllership. However, Annex 1 provides extracts from ECDC's Founding Regulation and from the SCBTH Regulation which include provisions that are relevant for controllership of personal data.
8. From the analysis of ECDC's Founding Regulation and the SCBTH Regulation, the following can be concluded:
   - ECDC is the data controller for the processing operations necessary to operate EpiPulse, in particular for the secure storage of the data. ECDC is also the data controller when using data for European Union/European Economic Area (EU/EEA) surveillance purposes to fulfil its mandate.
   - Member States are controllers for the processing operations occurring before data are uploaded to EpiPulse. This includes ensuring that data are accurate and pseudonymised, and that data subjects are informed of the processing operations. Furthermore, Member States are controllers when using data from EpiPulse for their own surveillance purposes.
9. Situations of joint controllership between ECDC and Member States may arise for specific projects where ECDC and the Member States jointly determine the purpose and means for particular processing operations – for example, with joint analysis of data.

[1] Regulation (EU) 2022/2371 of the European Parliament and of the Council of 23 November 2022 on serious cross-border threats to health and repealing Decision No 1082/2013/EU, hereinafter 'SCBTH'.
[2] Such legislation would be Regulation (EU) 2016/679, 'the GDPR', for the Member States, and Regulation (EU) 2018/1725, 'the EUDPR' for ECDC.

Specific aspects of governance

Operation and management of EpiPulse

10. The technical management of EpiPulse is entrusted to ECDC, which has a legal obligation to operate the platform and is responsible for its development. ECDC is responsible for:
    - ensuring that EpiPulse enables collection of surveillance data from Member States, and access to such data by Member States;
    - ensuring adequate technical and organisational measures to guarantee the security of data in EpiPulse[3];
    - providing training for nominated users.
11. The Member States are responsible for their nominated users. This includes:
    - ensuring that user lists are up-to-date;
    - exercising an overall responsibility to ensure that nominated users only use the data for the original (surveillance) purpose.

Specific provisions relating to data

12. ECDC is responsible for:
    - ensuring the quality of data and information provided and uploaded to EpiPulse by ECDC;
    - enforcing the retention period for personal data related to health processed in EpiPulse (with regard to EpiPulse Cases, the general principle is that ECDC deletes the national ID linked to a case after 10 years[4]; with regard to EpiPulse Events, personal data are deleted six months after the closure of the event they refer to[5]);
    - only processing data for purposes related to the fulfilment of its mandate.
13. Member States are responsible for:
    - ensuring the quality of data uploaded to EpiPulse, as well as the correctness of the information provided in EpiPulse Events;
    - pseudonymisation of data before submission to EpiPulse, when full anonymisation is not possible;
    - implementing appropriate technical and organisational measures to ensure the security of data downloaded from EpiPulse;
    - enforcing legal retention principles for data downloaded from EpiPulse. Data must be deleted as soon as they are no longer necessary to fulfil the surveillance purpose for which they have been processed[6].
14. By default, Member States have access to each other's epidemiological surveillance data in EpiPulse Cases under the principle of reciprocity. Each Member State can decide to restrict such access by making its surveillance data in EpiPulse Cases for selected or all diseases and related special health issues unavailable to users nominated by the other Member States. A Member State that makes its data unavailable to users from other Member States will, in turn, no longer have access to the corresponding data from the other Member States in EpiPulse. Any such opt-out must be communicated to ECDC (surveillance@ecdc.europa.eu) in writing by the country's National Focal Point for Surveillance before ECDC can proceed with the technical implementation and inform the other Member States.
15. When processing data whose source is another Member State, the Member State using the data is responsible for:
    - ensuring that data are used only for reasons of public interest in the area of public health and that processing complies with the GDPR;
    - ensuring that only authorised users have access to personal data originating from another Member State, and that users have undergone adequate training on protection of personal data and are aware of any confidentiality obligations.

[3] Includes conducting a data protection impact assessment, as required by the SCBTH Regulation.
[4] It is understood that deleting the national ID in some cases might not ensure full anonymisation if data for several variables are still retained. However, taking into consideration all the reasonable means likely to be used that would be necessary for re-identification, ECDC considers that the measure is sufficient. The alternative would be to delete the entire cases, which seems unnecessary and would undermine the surveillance purposes.
[5] If, for an event that has been closed, personal data must be retained for a period exceeding six months for scientific purposes, these data are no longer available to non-ECDC users.
[6] It is for the Member State that downloaded the data, as controller, to determine the appropriate retention period. For example, when data are downloaded for a specific study or project, data should not be kept for longer than the duration of the study or project, although a longer retention might be possible, if necessary, to validate a scientific output.

Cooperation with the World Health Organization and third countries

16. Certain reporting obligations of Member States to the World Health Organization (WHO) pursuant to the International Health Regulations overlap with their reporting obligations to ECDC pursuant to the SCBTH Regulation. To avoid the burden of double reporting of such data by the Member States, ECDC makes the reported data available to WHO.
    - It is understood that such transfers have been occurring as a service from ECDC under the instructions of the Member States. Each Member State may at any time require ECDC to stop these recurring transfers of their national data to WHO, with ECDC acting as processor for the Member State.
    - To facilitate the transfers and ensure compliance with data protection legislation, ECDC may negotiate a data transfer agreement with WHO on behalf of the Member States.
17. ECDC can transfer data from EpiPulse Cases to WHO (including by granting direct access to specific sets of data) when necessary for joint surveillance activities that come under a formal cooperation framework. In such cases, ECDC ensures that appropriate data protection provisions are in place.
18. Both ECDC and the Member States may have an interest in granting limited access to EpiPulse Events to third countries. For access to EpiPulse Events:
    - ECDC determines which third countries should be granted access to which item;
    - ECDC takes the necessary steps to ensure compliance with legislation. In particular, ECDC ensures that access is granted on the basis of an established cooperation framework with the relevant third country, and that the necessary arrangements to comply with data protection legislation are in place.
19. In some circumstances, third countries might have access to EpiPulse Cases. However, access is limited to their own data, and they will not have access to data from the EU/EEA.

Data sharing with third parties

20. When receiving requests from third parties to transmit or transfer[7] personal data, the following principles apply for ECDC:
    - ECDC can transmit data to other EU institutions and bodies, provided that the data are required for the legitimate performance of tasks within the competence of the recipient and that the recipient has a legal basis for processing data related to health.
    - ECDC can transmit or transfer data to ECDC's institutional partners[8] or contractors, provided that it has a direct and concrete interest in sharing the data[9] and that the necessary legal framework is in place, including for the protection of personal data. If anonymisation is not possible, ECDC ensures that data are duly pseudonymised.
    - If a data request from WHO is neither part of the standard data sharing to avoid double reporting, nor part of a joint project between ECDC and WHO, ECDC analyses the request, proposes a reply and seeks permission from the relevant Member State(s) before disclosing the data. Each Member State decides on whether to authorise the transfer and holds accountability for the decision.
    - With the exception of the cases outlined above, ECDC does not share pseudonymised case-based data with other third parties, only aggregated data.
21. A Member State can decide on the transmission or transfer to third parties of the personal data that it has itself uploaded to EpiPulse. The Member State is the controller for the transmission or transfer.
22. A Member State may transmit or transfer personal data originating from other Member States to third parties under the following conditions:
    - The Member State that transmits or transfers personal data must seek prior permission from the Member State that originally provided the data. The Member States must confer bilaterally to discuss the permission[10]. The Member State that intends to transmit or transfer the data must inform the Member State that originally provided the data of the purposes for which data will be used by the third party; of the technical and organisational measures that the third party has put in place to protect the data, and of the retention period.
    - The Member State that transmits or transfers the data is responsible for ensuring that the necessary processing operations are compliant with the GDPR and with the applicable national legislation, and that the recipient will only use the data for tasks related to public health surveillance.
    - Before sharing data with the recipient, the Member State transmitting or transferring the data shall ensure that any condition set by the Member State that is the source of the data has been satisfied, and that a binding agreement is in place with the third party. This agreement shall describe the purposes for which processing is allowed, the technical and organisational measures required, the retention period, and provisions to ensure that data subjects can exercise their rights.

[7] Transmission of personal data to recipients established in the EU/EEA pursuant to Article 9 EUDPR and transfers to third countries or international organisations pursuant to Chapter V of the EUDPR.
[8] An institutional partner is an entity with whom ECDC has signed a cooperation agreement.
[9] For ECDC to have a direct interest means that ECDC has a specific interest in an intended data analysis or output to which it contributes. The simple purpose of enhancing cooperation is not covered by the provision.
[10] Member States can create a functional mailbox to facilitate bilateral contact for such purposes and publish details on EpiPulse. ECDC does not have any involvement in the bilateral dialogue between the Member States to decide on data transfer or transmission.

23. There are no restrictions on the sharing of non-personal data. It is up to the entity disclosing the data to determine whether data qualify as personal data.

Rights of data subjects

24. ECDC and the Member States inform the data subjects of the processing operations for which they are the respective controllers. ECDC informs data subjects through a data protection notice on ECDC's website.

25. If data subjects in EpiPulse Cases contact ECDC to exercise their rights, ECDC refers the request to the relevant Member State as ECDC would not be able to verify the identity of the data subject. The Member State and ECDC confer to ensure that the request is processed.

26. In the event of a security incident affecting EpiPulse and compromising personal data, ECDC shall inform the relevant Member States if it considers that the breach poses a high risk for the rights and freedoms of the data subjects.

Situations of joint controllership

27. Joint analysis of personal data by ECDC and Member States commonly occurs, for example in the context of operating disease networks. Such cases may constitute situations of joint controllership, where the purpose and means of the processing operations are jointly determined by ECDC and the Member States.

28. When joint controllership arises, both ECDC and the Member States are responsible for the respective storage and use of data by each entity, which shall be in line with the agreed purpose. The Member States shall inform the data subjects of the joint processing operations[11].

[11] This can be done through a notice on the website, if it is not possible to inform the subjects individually.

Annex 1. Legislation

Applicable legislation: ECDC's Founding Regulation[12]

- Article 5(2)(a) stipulates that ECDC shall 'ensure the continuous development of automated digital platforms and applications, including the digital platform for surveillance established under Article 14 of Regulation (EU) 2022/2371 (…)'
- Article 5(2)(g) stipulates that ECDC shall 'ensure the interoperability of the digital platforms for surveillance with digital infrastructure enabling health data to be used for healthcare, research, policy-making and regulatory purposes (…). The digital platforms and applications referred to in the second subparagraph, point (a), shall be implemented with privacy-enhancing technologies taking into account the state of the art.'
- Article 11(2)(d) stipulates that for the purposes of coordinating standardisation of data collection procedures, and validation, analysis and dissemination of data at Union level, 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.'

Applicable legislation: the SCBTH Regulation[13]

- Article 14(1) stipulates that ECDC 'shall ensure the continued development of the digital platform for surveillance, after conducting data protection impact assessments and having mitigated any risks to the rights and freedoms of the data subjects, as appropriate, through which data are managed and automatically exchanged, to establish integrated and interoperable surveillance systems enabling real-time surveillance where appropriate, for the purpose of supporting communicable disease prevention and control. The ECDC shall ensure that the operation of the digital platform for surveillance is subject to human oversight and shall minimise the risks that may emerge from the transfer of inaccurate, incomplete or ambiguous data from one database to another, as well as establish robust procedures for data quality review. The ECDC, in close cooperation with Member States, shall also ensure the interoperability of the digital platform for surveillance with national systems.'
- Article 14(3) stipulates that 'Member States shall be responsible for ensuring that the integrated surveillance system is fed on a regular basis with timely, complete and accurate information, data and documents transmitted and exchanged through the digital platform. Member States may promote the automation of this process between the national and the Union surveillance systems.'
- Article 14(6) stipulates that the Commission shall adopt implementing acts[14] for the functioning of the digital platform which set out:
  - 14(6)(a) the technical specifications of the digital platform (…);
  - 14(6)(b) the specific rules for the functioning of the digital platform for surveillance, including for the protection of personal data and security of exchange of information;
  - 14(6)(c) contingency arrangements, including secure data backups to be applied in the event of unavailability of any of the functionalities of the digital platform for surveillance;
  - 14(6)(d) arrangements for promoting standardisation of the infrastructure for storage, processing and analysis of data.
- Article 14(7) provides that the Commission shall adopt delegated acts concerning:
  - 14(7)(a) conditions for access to the digital platform by third countries and international organisations;
  - 14(7)(b) cases and conditions under which data and information on epidemiological surveillance (as referred in article 13 SCBTH) are to be transmitted using the digital platform for surveillance, and the list of data, information and documents.

[12] 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.
[13] Regulation (EU) 2022/2371 of the European Parliament and of the Council of 23 November 2022 on serious cross-border threats to health and repealing Decision No 1082/2013/EU.
[14] Member States are involved in the issuing of Implementing Acts. In fact, the Committee on serious cross-border threats to health is required to issue an opinion, pursuant to Article 29(2) SCBTH, which refers to Regulation (EU) No 182/2001. Delegated acts do not require approval from a dedicated Comitology committee.