

LEGAL HELPDESK

Q&A NO. 13

Secondary use of data
coming from Hospitals
and the Austrian
legal landscape

By University of Vienna



Image provided by Med Uni Graz

Question no. 13

Published: January 2025

Subject: **Secondary use of data, national laws on secondary use; data protection**

1. Secondary data use for research purposes in the GDPR

COMMENT

In order to use personal data initially collected at hospitals (presumably for the purpose of providing healthcare) for scientific research purposes (secondary use), a legal basis is required under the European Union (EU) General Data Protection Regulation (GDPR).¹

Personal data collected at hospitals refer to the health of the individual patients (under GDPR called data subjects) and therefore count as sensitive data and require special legal protection. When healthcare professionals collect personal data, they need to have a valid legal basis under Articles 6 and 9 GDPR – usually this happens on the basis of explicit consent, or because the processing is necessary to protect the vital interests of the data subject, or the processing happens for the purpose of preventive or occupational medicine.²

However, the question is what legal basis can be established when a researcher wishes to further process that personal data for their scientific research, for example, research into developing a new form or treatment or to train an AI model for diagnosing specific illnesses.

In general, the GDPR provides some exceptions for further processing of personal data for scientific research. In principle, scientific research is considered a purpose which is not incompatible with the initial purpose of data collection.³ Such processing is allowed where the controller adopts sufficient safeguards to protect the rights of the data subject, for example, pseudonymization or anonymization.⁴ Furthermore, Member States may introduce their own derogations in national law with regards to secondary use of personal data for research purposes. For example, in Austria, the Austrian Data Protection Law (Datenschutzgesetz, DSG)⁵ and the Research Organization Law (Forschungsorganisationgesetz, FOG)⁶ provide for such rules.

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR) OJ L 119/1, art 5(1)(a).

² GDPR, art 9(2).

³ GDPR, art 5(1)(b).

⁴ GDPR, art 89(1).

⁵ Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG).

⁶ Bundesgesetz vom 1. Juli 1981 über die Forschungsorganisation in Österreich (Forschungsorganisationgesetz – FOG).

2. Applicable national regulations on secondary use of data for research purposes

Article 2§7 DSG distinguishes two instances of processing for scientific research purposes:⁷

- 1) Processing for research purposes in the public interest not aimed at achieving personal results,
- 2) Processing for research purposes in the public interest aimed at achieving personal results.

Different safeguards apply for each of these instances. In the first case, the controller can process personal data which:

- (i) 'are publicly accessible;
- (ii) have been lawfully obtained by the controller for other research projects or other purposes; or
- (iii) are pseudonymised and the controller cannot determine the identity of the data subject by legally permissible means.'⁸

The second instance, the controller can only process personal data:

- (i) 'in accordance with special legal provisions (e.g. the provisions contained in the FOG);
- (ii) with the consent of the data subject; or
- (iii) with the approval of the Supervisory Authority.'⁹

The FOG is a general law on research organisation in Austria and a *lex specialis* to the DSG with regards to processing personal data for research purposes. A legal study conducted for the European Data Protection Board (EDPB) on the topic of secondary data sharing in national legal systems, explains that in line with the provisions of the FOG personal data, including sensitive data, may be processed for research purposes in all domains if:

- (i) 'instead of the name, area-specific personal identifiers or other unique identifiers are used for allocation; or (ii) the processing is
- (ii) carried out in pseudonymised form; or
- (iii) the processing is carried out without publishing the data,
- (iv) or publishing the data only in anonymised or pseudonymised form, or publishing the data without names, addresses or photographs; or
- (v) the processing is carried out exclusively for the purpose of anonymisation or pseudonymisation and no disclosure of direct personal data to third parties is involved.'¹⁰

Additionally, the FOG recognizes 'broad consent' as a legal basis.¹¹

Having said this, the GDPR and Austrian law provide for a general legal basis for secondary use of personal data.

However, a valid legal basis is only one of the requirements which need to be met when further processing personal data. Some contractual requirements follow. The controller must comply with and be able to demonstrate the compliance with other provisions of the GDPR. If the controller (for example, a hospital) shares data with third parties (for example, external) – this data can only be shared on the basis of a concluded data sharing agreement.

⁷ Els Kindt and others, 'Study on the appropriate safeguards under Article 89(1) GDPR for the processing of personal data for scientific research' (Final Report) EDPS/2019/02-08, p. 11.

⁸ Kindt and others (n 7), p. 11.

⁹ Ibid, p. 11.

¹⁰ Ibid, p. 11; § 2d FOG.

¹¹ § 2d (3) FOG.



Such a contractual agreement outlines the conditions for data sharing as well as the obligations of the data recipient. Although some of the data subject rights, such as the right to information or right to access might be limited if data is shared with third parties, the data recipient must still maintain appropriate technical and organizational measures for data security. The question of sharing personal data from hospitals to research institutions or repositories outside that hospital is hence also a contractual question.

To conclude, the starting point for finding a legal basis for secondary use of data from hospitals in Austria are GDPR, DSG and FOG – as discussed above. Depending on the circumstances, some further special hospital regulations might apply. The second step would often be contractual if data are to be shared with a data recipient who is a third party – then a data sharing agreement will be necessary.

***Disclaimer:** this commentary aims to provide a summary of the main ethical and legal issues related to the questions put by interested stakeholders and to direct them to the relevant legal provisions that are applicable. It does not, however, preclude from reading the official sources of legislation relating to the subject matters of this document as well as those quoted by the authors and does not constitute legal advice.*