EUROPEAN UNIVERSITY INSTITUTE

Un-owned Data Interoperable EU Borders and Transitioning Rights Post Covid-19

MODEL RULES

Principal Investigator of the Project & Supervisor of the Research Team

Prof. Deirdre Curtin

Coordinator of the Model Rules

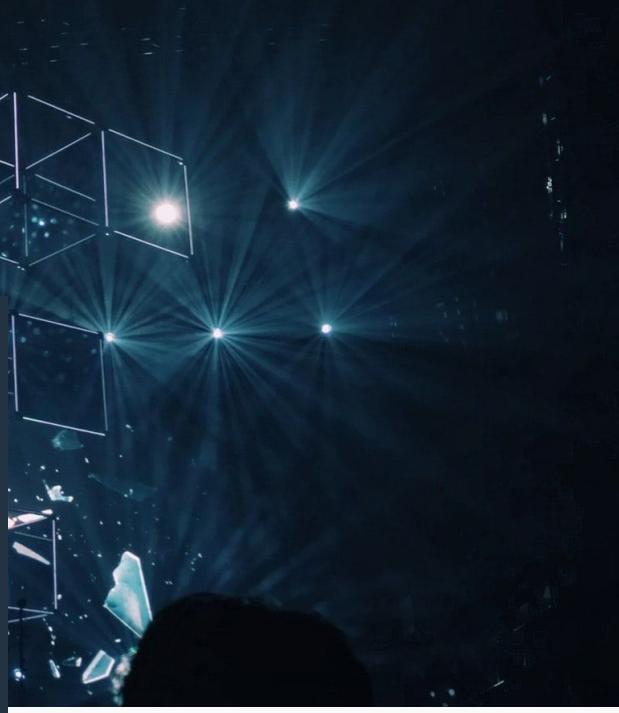
Dr. Mariavittoria Catanzariti

Research Team

Marco Almada
Mariavittoria Catanzariti
Francisco De Abreu Duarte
Francesca Galli
Francesca Palmiotto
Tommaso Fia


“
Interoperability transforms data shared across databases into transitioning rights of individuals

00



Scope of Model Rules

Article 1
Scope

1.These rules apply to personal data which are:

(a) processed in the Entry/Exit System (EES), the Visa Information System (VIS), the European Travel Information and Authorisation System (ETIAS), Eurodac, the Schengen Information System (SIS), and the European Criminal Records Information System for third-country nationals (ECRIS-TCN), or by Europol for the purpose referred to in Article 18(2)(a), (b) and (c) of Regulation (EU) 2016/794;

(b) processed in the interoperability components provided for in Article 1(2) of Regulation (EU) 2019/817 and Article 1(2) Regulation (EU) 2019/818 by the eu-LISA; and

(c) collected for the purposes defined in Articles 1 and 2 of Regulation (EC) No 767/2008, Article 1 of Regulation (EU) 2017/2226, Articles 1 and 4 of Regulation (EU) 2018/1240, Article 1 of Regulation (EU) 2018/1860 and Article 1 of Regulation (EU) 2018/1861

(hereinafter 'interoperable data').

01

Data Ownership

Personal data ownership by public bodies is not based on or justified by national laws or Union primary or secondary legislation.

Article 1
Data ownership. Access by Member State authorities and Union agencies

1.Neither Member State authorities nor Union agencies who originate interoperable data shall restrict access to users of interoperable components or data subjects except if a Union or national legal provision grounding such a restriction applies.

2.Member State authorities and Union agencies shall implement the appropriate organisational and technical measures to comply with Paragraph 1 at the moment when interoperable data is collected by the competent Member State authority or Union agency.

Article 2
Data acess management

1.Member State authorities and Union agencies shall take the necessary measures to ensure interoperable data sharing of personal data amongst the E.U. information systems in compliance with the safeguards provided for in the data protection legislation.

2. The competent Member State authority or Union agency originating interoperable data shall implement
appropriate organisational measures to provide other Member State authorities and Union agencies with access to data shared through the E.U. information systems.

3. Access to interoperable data:
a. shall be granted to duly authorised officials in charge of processing data based on their functions and job profile;
b. shall be implemented through appropriate data access policies to demonstrate compliance with paragraph (a);
c. shall be ensured through appropriate security measures, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

02

Originator Control Principle

Once data becomes interoperable, its status changes: data is then shared and no longer exclusively under the control of the body or actor that has included it into one of the six databases.

Article 1
Limits to the ORCON principle

1. Only before data is input into the Interoperable Information System, data originators may*:*

a. retain control over the release of information to third parties;
b. grant or deny access to data;
c. limit the usage of information by third parties.

2. Data originators who input personal data in the E.U. Interoperable Information Systems can only track those users that access interoperable data.

3. Data originators are not the owners of interoperable data by virtue of any entitlement, covenant or agreement with third parties or data subjects.

03

Transparency Requirements

The contestability of decisions can be hampered by lack of access to information on EU information systems, who accessed data and for what purpose.

Article 1

Transparency of data-based decision-making

1.Where a decision is taken using data stored in E.U. information systems, the competent authority shall provide to the subject:
a. the grounds supporting the decision;
b. the personal data at the basis of the decision;
c. the log files updated at the moment the decision is taken;
d. the technologies used to process the data at the basis of the decision.

2.The information shall be uploaded in the web portal provided for in Article 49 of Regulation (E.U.) 2019/817 and Regulation (E.U.) 2019/818. The competent authority shall provide to the data subject the instructions on how to access the web portal in a readable format, using clear and plain language the person concerned can reasonably understand or access

Article 2

Transparency of evidence in judicial proceedings

1. When information shared by the interoperable components is used as evidence in an administrative or a criminal proceeding, the automated processing related to such use must be transparent.

2. Transparency of evidence includes:
a. access to the technical documentation on the design of the system and technologies used, including, when applicable, the training data set;
b. access to the data used to provide the evidence;
c. access to the log files.

04

Technology Neutrality

Technology neutrality mandates that technology facilitating interoperability of databases should not be dependent on proprietary technology/software.

Article 1

Technological Neutrality

1. The design of European Union interoperable information systems shall not be dependent on the imposition of specific technological solutions, such as file types, software applications or hardware.

2.The choice for technologies that enable users to use interoperable components might not entail any detrimental effect to the sharing of information, in accordance with the principle of sincere cooperation.

05

Covid-19 Interoperable Data Sharing

The aim of this Covid-19 rule is to provide specific grounds to challenge decisions based on health data shared by EU information systems in response to Covid-19.

Article 1

Health Data Processing

1.Interoperable data may also include health data processed for reasons of public interest in the area of public health, such as contrasting and monitoring the spread of the Pandemic Covid-19 as well as therapeutical purposes related to Covid-19.

2.Where a decision to refuse the entry of a third-country national (TCN) is based on the processing of health data related to them, including that are also shared EU information systems, in compliance with Art. 9 GDPR, the competent authority shall provide the following information to the data subject:

a. the purposes of data processing;
b. the legal and factual ground supporting the decision;
c. the personal data accessed; and
d. the log entries associated with the decision.

3.Sharing of health data shall not be subject to any imposed technological measure either for data subjects and for users of EU interoperable information systems.

4.The temporary incorporation of new categories of data, such as health data, as interoperable data shall be accompanied by technical specifications that:

a. establish a readable format as well as specific purpose for processing of health data that are interoperable in their technical design;
b. provide the measures that are required to deal with data from third countries; and
c. in the case of data incorporated for the purposes of responding to an emergency, include a plan for ensuring that the data remains accessible only for the duration of the emergency that motivates its incorporation.

05

Covid-19 Interoperable Data Sharing

The aim of this Covid-19 rule is to provide specific grounds to challenge decisions based on health data shared by EU information systems in response to Covid-19.

Article 2

Contact Tracing Data

1.Under the conditions laid down by Article 2(1), data generated by means of contact tracing can be shared into interoperable components as far as access to them is not subject to any restriction or limitation by users of interoperable components.

2.Data generated by means of contact tracing that are shared into interoperable components can be only accessed by national health authorities for the purpose laid down by Article 2(1).