# DECISIONS

## COMMISSION IMPLEMENTING DECISION (EU) 2023/975

**of 15 May 2023**

**amending Commission Implementing Decision (EU) 2019/417 laying down guidelines for the management of the European Union Rapid Information System 'RAPEX' established under Article 12 of Directive 2001/95/EC of the European Parliament and of the Council on general product safety and its notification system**

*(notified under document C(2023) 2817)*

**(Text with EEA relevance)**

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety ([1]), and in particular Article 11(1), the third subparagraph, thereof and point 8 of Annex II thereto,

Having regard to Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 ([2]), and in particular Article 20 thereof,

Having regard to Regulation (EU) 2018/1725 of the European Parliament and of 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 ([3]), and in particular Article 28(1) thereof,

Having regard to 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 ([4]), and in particular Article 26(1) thereof,

After consulting the committee established by Article 15(1) of Directive 2001/95/EC,

After consulting the European Data Protection Supervisor in accordance with Article 42 of Regulation (EU) 2018/1725,

Whereas:

(1) Commission Implementing Decision (EU) 2019/417 ([5]) sets out the guidelines for the management of the European Union Rapid Information System 'RAPEX' established under Article 12 of Directive 2001/95/EC and its notification system.

([1]) OJ L 11, 15.1.2002, p. 4.
([2]) OJ L 169, 25.6.2019, p. 1.
([3]) OJ L 295, 21.11.2018, p. 39.
([4]) OJ L 119, 4.5.2016, p. 1.
([5]) Commission Implementing Decision (EU) 2019/417 of 8 November 2018 laying down guidelines for the management of the European Union Rapid Information System 'RAPEX' established under Article 12 of Directive 2001/95/EC on general product safety and its notification system (OJ L 73, 15.3.2019, p. 121).

(2) Article 28 of Regulation (EU) 2018/1725 sets out that where two or more controllers jointly determine the purposes and means of processing, they are to be joint controllers. The respective responsibilities of the joint controllers may be determined by EU law, in particular as regards exercising the rights of the data subject and their respective duties to provide the information referred to in Articles 15 and 16 of Regulation (EU) 2018/1725.

(3) Article 26 of Regulation (EU) 2016/679 sets out that where two or more controllers jointly determine the purposes and means of processing of personal data, they are considered joint controllers. The respective responsibilities of the joint controllers may be determined by EU law, in particular as regards exercising the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14 of Regulation (EU) 2016/679.

(4) The Commission and national authorities act as joint controllers for processing data in the Safety Gate/RAPEX system.

(5) It is necessary to lay down the respective roles, responsibilities and arrangements between the Commission and national authorities as joint controllers under Article 28 of Regulation (EU) 2018/1725 and Article 26 of Regulation (EU) 2016/679.

(6) Implementing Decision (EU) 2019/417 should therefore be amended accordingly.

HAS ADOPTED THIS DECISION:

*Article 1*

Implementing Decision (EU) 2019/417 is amended as follows:

(1) Article 1 is replaced by the following:

"*Article 1*

1. The guidelines for the management of the European Union Rapid Information System 'RAPEX' established under Article 12 of Directive 2001/95/EC and its notification system are set out in the Annex I to this Decision.

2. The joint controllership of the European Union Rapid Information System 'RAPEX' is set out in Annex II to this Decision.";

(2) the Annex is renamed Annex I;

(3) Annex II as set out in the Annex to this Decision is added.

*Article 2*

This Decision is addressed to the Member States.

Done at Brussels, 15 May 2023.

*For the Commission*
Didier REYNDERS
*Member of the Commission*

*ANNEX*

*"ANNEX II*

**JOINT CONTROLLERSHIP OF THE EUROPEAN UNION RAPID INFORMATION SYSTEM 'RAPEX' ESTABLISHED UNDER ARTICLE 12 OF DIRECTIVE 2001/95/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [1] (THE GENERAL PRODUCT SAFETY DIRECTIVE)**

1. ***Subject matter and description of the processing***

The Safety Gate/RAPEX application is a notification system intended for the rapid exchange of information between national authorities of Member States, the 3 European Economic Area/European Free Trade Association (EEA/EFTA) states (Iceland, Liechtenstein and Norway) and the Commission on measures taken against dangerous products found on the Union and/or EEA/EFTA market. The purpose of this notification system is:

— to prevent the supply to consumers of dangerous products in the internal market;

— where necessary, to take corrective measures such withdrawing or recalling such products from the market.

The information exchange concerns preventive and restrictive measures and actions taken in relation to dangerous consumer and professional products, except food, feed, pharmaceuticals and medical devices. Both measures ordered by national authorities and measures taken voluntarily by economic operators are covered by the Safety Gate/RAPEX system.

2. ***Scope of the Joint Controllership***

The Commission and national authorities act as joint controllers for processing data in the Safety Gate/RAPEX system. 'National authorities' are all Member States authorities and authorities of EFTA/EEA countries acting on product safety and participating in the Safety Gate/RAPEX network, including market surveillance authorities responsible for monitoring the compliance of products with safety requirements and authorities in charge of external border controls.

For the purposes of Article 26 of Regulation (EU) 2016/679 of the European Parliament and of the Council [2] and Article 28 of Regulation (EU) 2018/1725 of the European Parliament and of the Council [3], the following processing activities fall under the responsibility of the Commission as a joint controller of personal data:

(1) The Commission may process information regarding measures taken against products posing serious risks, imported into or exported from the Union and the European Economic Area, in order to transmit it to the RAPEX Contact Points.

(2) The Commission may process information received from third countries, international organisations, businesses or other rapid alert systems about products of EU and non-EU origin posing a risk, in order to transmit such information to the national authorities.

It is the responsibility of the Commission to ensure compliance with the obligations and conditions of Regulation (EU) 2018/1725 regarding these activities.

[1] Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (OJ L 11, 15.1.2002, p. 4).

[2] 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) (OJ L 119, 4.5.2016, p. 1).

[3] Regulation (EU) 2018/1725 of the European Parliament and of 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, p. 39).

The following processing activities fall under the responsibility of the national authorities, as joint controllers of personal data:

(1) National authorities may process information pursuant to Articles 11 and 12 of Directive 2001/95/EC and Article 20 of Regulation (EU) 2019/1020 of the European Parliament and of the Council ([4]) in order to notify such information to the Commission and other Member States and EFTA/EEA countries;

(2) National authorities may process information subsequent to their follow-up activities in relation to Safety Gate/RAPEX notifications in order to notify such information to the Commission and other Member States and EFTA/EEA countries;

It is the responsibility of the national authorities to ensure compliance with the obligations and conditions of Regulation (EU) 2016/679 regarding these activities.

3. ***Responsibilities, roles and relationship of the joint controllers towards data subjects***

3.1. **Categories of data subjects and personal data**

The Joint Controllers jointly process the following categories of personal data:

(a) Contact details of the Safety Gate/RAPEX users.

The following data may be processed:

— Name of the Safety Gate/RAPEX users

— Surname of the Safety Gate/RAPEX users

— email address of the Safety Gate/RAPEX users

— country of the Safety Gate/RAPEX users

— preferred language of the Safety Gate/RAPEX users.

(b) Contact details of the authors and validators of notifications and reactions submitted through the Safety Gate/RAPEX system.

These authors and validators include:

— National Safety Gate/RAPEX contact points and inspectors from the market surveillance authorities of Member States and EFTA/EEA countries or from the national authorities in charge of external border controls, who are involved in the notification procedure

— Commission staff such as officials, temporary agents, contract agents, trainees and external service providers.

The following data may be processed:

— Name of the authors and validators of notifications and reactions submitted through the Safety Gate/RAPEX system

— Surname of the authors and validators of notifications and reactions submitted through the Safety Gate/RAPEX system

— name of the authority authoring or validating notifications and reactions submitted through the Safety Gate/RAPEX system

— address of the authority authoring or validating notifications and reactions submitted through the Safety Gate/RAPEX system

([4]) Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (OJ L 169, 25.6.2019, p. 1).

— email address of the authors and validators of notifications and reactions submitted through the Safety Gate/RAPEX system

— phone number of the authors and validators of notifications and reactions submitted through the Safety Gate/RAPEX system

(c) In addition, two types of personal data can incidentally be included in the system:

(i) When necessary to trace dangerous products, as defined in Article 2 (c) of Directive 2001/95/EC, contact details of economic operators (manufacturers, exporters, importers, distributors or retailers) might contain personal data that will be included in the system. Such data are inserted in the Safety Gate/RAPEX system by national authorities only, based on the information collected during their investigation.

The following data may be processed:

— Name of economic operators

— Address of economic operators

— City of economic operators

— Country of economic operators

— Contact information of economic operators: this field may refer to the physical person representing the manufacturers or authorised representatives. Member States are however asked to avoid entering any personal data and favour non-personal contact details like generic email addresses.

— Contact address of economic operators.

(ii) When they have been incidentally included in other documents such as test reports, names of persons who have performed the tests on dangerous products and/or authenticated the test reports. These names are included in attachments and are not searchable. Member States are asked to delete such data prior to submission if they are not considered necessary for the purpose of the system.

3.2. **Provision of information to data subjects**

The Commission shall provide the information referred to in Articles 15 and 16 and any communication under Articles 17 to 24 and 35 of Regulation (EU) 2018/1725 in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The Commission shall also take appropriate measures to assist national authorities in providing any information referred to in Articles 13 and 14 and any communication under Articles 19 to 26 and 37 of Regulation (EU) 2016/679 in a concise, transparent, intelligible and easily accessible form, using clear and plain language concerning the following data:

— Data related to Safety Gate/RAPEX users;

— Data related to the authors and validators of notifications and reactions.

Safety Gate/RAPEX users are informed about their rights through the Privacy Statement available in Safety Gate/RAPEX.

National authorities shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 19 to 26 and 37 of Regulation (EU) 2016/679 in a concise, transparent, intelligible and easily accessible form, using clear and plain language concerning the following data:

— information on legal persons identifying a natural person;

— names and other data of persons who have performed the tests on dangerous products and/or authenticated the test reports.

The information shall be provided in writing, including electronically.

National authorities shall use the model for a privacy statement provided by the Commission when complying with their obligations concerning data subjects.

3.3. **Handling of data subjects' requests**

The data subjects may exercise their rights under Regulation (EU) 2018/1725 and Regulation (EU) 2016/679, respectively, in respect of and against each of the Joint Controllers.

The Joint Controllers shall handle the requests of data subjects in accordance with the procedure established by the Joint Controllers for this purpose. The detailed procedure for the exercise of data subjects' rights is explained in the Privacy Statement.

The Joint Controllers shall cooperate and, when so requested, provide each other with swift and efficient assistance in handling any data subject requests.

Should one Joint Controller receive a data subject request, which does not fall under its responsibility, that Joint Controller shall forward the request promptly, and at the latest within seven calendar days of its receipt, to the Joint Controller actually responsible for that request. The responsible Joint Controller shall send an acknowledgment of receipt to the data subject within further three calendar days, while at the same time informing thereof the Joint Controller, which received the request in the first place.

In response to a data subject request for access to personal data, no Joint Controller shall disclose or otherwise make available any personal data processed jointly without first consulting the other relevant Joint Controller.

4. ***Other responsibilities and roles of joint controllers***

4.1. **Security of processing**

Each Joint Controller shall implement appropriate technical and organisational measures designed to:

(a) Ensure and protect the security, integrity and confidentiality of the personal data jointly processed, in line with Commission Decision (EU, Euratom) 2017/46 ([5]) and relevant legal act of the EU Member State/EFTA/EEA country, respectively;

(b) Protect against any unauthorised or unlawful processing, loss, use, disclosure or acquisition of or access to any personal data in its possession;

(c) Not disclose or allow access to the personal data to anyone other than the beforehand agreed recipients or processors.

Each Joint Controller shall implement appropriate technical and organisational measures to ensure the security of processing pursuant to Article 33 of Regulation (EU) 2018/1725 and Article 32 of Regulation (EU) 2016/679, respectively.

The Joint Controllers shall provide a swift and efficient assistance to each other in case of security incidents, including personal data breaches.

4.2. **Management of security incidents, including personal data breaches**

The Joint Controllers shall handle security incidents, including personal data breaches, in accordance with their internal procedures and applicable legislation.

The Joint Controllers shall in particular provide each other with swift and efficient assistance as required to facilitate the identification and handling of any security incidents, including personal data breaches, linked to the joint processing operation.

The Joint Controllers shall notify each other of the following:

(a) any potential or actual risks to the availability, confidentiality and/or integrity of the personal data undergoing joint processing;

(b) any security incidents that are linked to the joint processing operation;

([5]) Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission (OJ L 6, 11.1.2017, p. 40).

(c) any personal data breach (i.e. any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data undergoing joint processing), the likely consequences of the personal data breach, the assessment of the risk to the rights and freedoms of natural persons, and any measures taken to address the personal data breach and mitigate the risk to the rights and freedoms of natural persons;

(d) any breach of the technical and/or organisational safeguards of the joint processing operation.

Each Joint Controller is responsible for all security incidents, including personal data breaches, that occur as a result of an infringement of that Joint Controller's obligations under this Decision, Regulation (EU) 2018/1725 and Regulation (EU) 2016/679, respectively.

The Joint Controllers shall document the security incidents (including personal data breaches) and notify each other without undue delay and at the latest within 48 hours after becoming aware of a security incident (including a personal data breach).

The Joint Controller responsible for a personal data breach shall document that personal data breach and notify it to the European Data Protection Supervisor or the competent national supervisory authority. It shall do so without undue delay and, where feasible, no later than 72 hours after having become aware of the personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. The Joint Controller responsible shall inform the other Joint Controllers of such notification.

The Joint Controller, responsible for the personal data breach, shall communicate that personal data breach to the data subjects concerned if the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. The Joint Controller responsible shall inform the other Joint Controllers of such communication.

4.3. **Localisation of personal data**

Personal data collected for the purpose of the notification process through the Safety Gate/RAPEX system shall be stored and collected in the Safety Gate/RAPEX application operated by the Commission in order to ensure that the access to the application is limited only to clearly identified persons and thus that data stored in the application are well protected.

Personal data collected for the purpose of the processing operation shall only be processed within the territory of the EU/EEA and shall not leave that territory, unless they are in compliance with Articles 45, 46 or 49 of Regulation (EU) 2016/679 or with Articles 47, 48 or 50 of Regulation (EU) 2018/1725.

According to Article 12(4) of Directive 2001/95/EC, access to Safety Gate/RAPEX is open to applicant countries, third countries or international organisations, within the framework of agreement between the EU and those countries or international organisations, according to arrangements defined in these agreements. Selected information from the Safety Gate/RAPEX system may be exchanged. Such information shall not contain personal data.

4.4. **Recipients**

Access to personal data shall only be allowed to authorised staff and contractors of the Commission and national authorities for the purposes of administering and operating the Safety Gate/RAPEX system, which facilitates the processing operation. This access shall be subject to identity and password requirements as follows:

— Safety Gate/RAPEX shall only open to the Commission and to users specifically appointed by the EU Member State's authorities and by EFTA/EEA countries, as well as UK authorities in respect of Northern Ireland users.

— Access to the collected personal data on Safety Gate/RAPEX shall only be granted to the nominated and authorised users of the application who have a User Id/Password. Access to the application and granting of a password shall be possible only if this is requested by the competent national authority under the general supervision of the Safety Gate/RAPEX Commission team..

— Access to the collected personal data shall be provided to the Commission staff responsible for carrying out this processing operation and to authorised persons according to the 'need to know' principle. Such staff shall abide by statutory, and, when required, additional confidentiality agreements.

The persons who shall have access to the collected personal data are:

(a) staff and contractors of the Commission;

(b) identified contact points and inspectors from the market surveillance authorities of EU Member States and EFTA/EEA countries as well as UK authorities in respect of Norther Ireland users;

(c) identified inspectors from the authorities in charge of external border controls of EU Member States and EFTA/EEA countries.

The persons who shall have access to all collected personal data and who shall have the possibility to modify them upon request are:

(a) members of the Commission's Safety Gate/RAPEX Team;

(b) members of the Commission's Safety Gate/RAPEX Helpdesk.

A list of all Safety Gate/RAPEX contact points (users nominated by the national authorities in the EU/EEA countries), containing their contact details (surname, name, name of authority, address of authority, phone, fax, email) shall be available on the public Europa website Safety Gate ([6]). User management at national level shall be controlled by the Safety Gate/RAPEX national contact points through the Safety Gate/RAPEX application.

All users shall have access to the content of notifications with an 'EC validated' status. Only national Safety Gate/RAPEX users shall have access to the draft of their notifications (before submission to EC). Commission staff and authorized persons shall have access to notifications with an 'EC submitted status'.

Each Joint Controller shall inform all other Joint Controllers about any transfers of personal data to the recipients in third countries or international organisations.

5. ***Specific responsibilities of Joint Controllers***

The Commission shall ensure and be responsible for:

(a) Deciding on the means, requirements and purposes of processing;

(b) Recording of the processing operation;

(c) Facilitating the exercise of the rights of data subjects;

(d) Handling of data subjects' requests;

(e) Deciding to restrict the application of or derogate from data subject rights, where necessary and proportionate;

(f) Ensuring privacy by design and privacy by default;

(g) Identifying and assessing the lawfulness, necessity and proportionality of transmissions and transfers of personal data;

(h) Carrying out a prior consultation with the European Data Protection Supervisor, where needed;

(i) Ensuring that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(j) Cooperating with the European Data Protection Supervisor, on request, in the performance of his or her tasks.

([6]) https://ec.europa.eu/safety/consumers/consumers_safety_gate/menu/documents/Safety_Gate_contacts.pdf

The national authorities shall ensure and be responsible for:

(a) Recording of the processing operation;

(b) Ensuring that the personal data undergoing processing are adequate, accurate, relevant and limited to what is necessary for the purpose;

(c) Ensuring a transparent information and communication to data subjects of their rights;

(d) Facilitating the exercise of the rights of data subjects;

(e) Using only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing meets the requirements of Regulation (EU) 2016/679 and ensure the protection of the rights of the data subject;

(f) Govern the processor's processing by a contract or legal act under Union or member State law in accordance with Article 28 of Regulation (EU) 2016/679;

(g) Carrying out a prior consultation with the national supervisory authority, where needed;

(h) Ensuring that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(i) Cooperating with the national supervisory authority on request, in the performance of their tasks.

6. ***Duration of processing***

Joint Controllers shall not retain or process personal data longer than necessary to carry out the agreed purposes and obligations as set out in this Decision, i.e. for the time necessary to fulfil the purpose of collection or further processing. In particular:

(a) Contact details of the users of the Safety Gate/RAPEX application shall be kept in the system as long as they are users. Contact details shall be deleted from the application immediately after the receipt of information that a certain person is no longer a user of the system;

(b) Contact details of the inspectors from the market surveillance authorities of Member States and EFTA/EEA countries, as well as from the inspectors from the authorities in charge of external border controls, provided in notifications and reactions shall be kept in the system for a period of five years after the validation of the notification or reaction.

(c) Personal data of other natural persons possibly included in the system shall be kept in a form that permits identification for 30 years from the moment of the insertion of the information in Safety Gate/RAPEX, which corresponds to the estimated maximum lifecycle of categories of products such as electrical appliances or motor vehicles.

Legitimate requests from data subjects to have their data blocked, adjusted or erased shall be complied with by the Commission within one month from receipt of the request.

7. ***Liability for non-compliance***

The Commission shall be liable for non-compliance in line with Chapter VIII of Regulation (EU) 2018/1725.

The EU Member State(s)' authorities shall be liable for non-compliance in line with Chapter VIII of Regulation (EU) 2016/679.

8. ***Cooperation between Joint Controllers***

Each Joint Controller, when so requested, shall provide a swift and efficient assistance to the other Joint Controllers in execution of this Decision, while complying with all applicable requirements of Regulation (EU) 2018/1725 and Regulation (EU) 2016/679, respectively, and other applicable data protection rules.

9. ***Settlement of disputes***

The Joint Controllers shall endeavour to settle amicably any dispute arising out or relating to the interpretation or application of this Decision.

If at any time a question, dispute or difference arises between the Joint Controllers, in relation to or in connection with this Decision, the Joint Controllers shall use every endeavour to resolve it by a process of consultation.

The preference is that all disputes are settled at the operational level as they arise, and that they are settled by the contact points referred to in point 10 of this Annex and listed on the public Europa website Safety Gate.

The purpose of the consultation shall be to review and agree so far as is practicable the action taken to solve the problem arisen and the Joint Controllers shall negotiate with each other in good faith to that end. Each Joint Controller shall respond to a request for amicable settlement within 7 working days of such request. The Period to reach an amicable settlement shall be 30 working days from the date of the request.

If the dispute cannot be settled amicably, each Joint Controller may submit for mediation or/and judicial proceedings in the following manner:

(a) in case of mediation, the Joint Controllers shall jointly appoint a mediator acceptable by each of them, who will be responsible for facilitating the resolution of the dispute within two months from the referral of the dispute to him/her,

(b) in case of judicial proceedings, the matter shall be referred to the Court of Justice of the European Union in accordance with Article 272 of the Treaty on the Functioning of the European Union.

10. ***Contact points for cooperation between the Joint Controllers***

Each Joint Controller nominates a single point of contact, whom other Joint Controllers shall contact in respect of queries, complaints and provision of information within the scope of this Decision.

A detailed list of all contact points nominated by the Commission and the national authorities in the EU/EEA countries, containing their contact details (surname, name, name of authority, address of authority, phone, fax, email) shall be available on the public Europa website Safety Gate."