

Official Journal of the European Union

L 236



English edition

Legislation

Volume 63

22 July 2020

Contents

II *Non-legislative acts*

RULES OF PROCEDURE

- ★ **Decision of the European Investment Fund of 4 June 2020 on internal rules concerning restrictions of certain rights of data subjects in relation to the processing of personal data in the framework of activities carried out by the European Investment Fund** 1
- ★ **Decision No 1/2020 of the Governing Board of the Shift2Rail Joint Undertaking of 26 March 2020 laying down internal rules concerning restrictions of certain rights of data subjects in relation to processing of personal data in the framework of the functioning of the S2R JU** 7

EN

Acts whose titles are printed in light type are those relating to day-to-day management of agricultural matters, and are generally valid for a limited period.

The titles of all other acts are printed in bold type and preceded by an asterisk.

II

(Non-legislative acts)

RULES OF PROCEDURE

DECISION OF THE EUROPEAN INVESTMENT FUND

of 4 June 2020

on internal rules concerning restrictions of certain rights of data subjects in relation to the processing of personal data in the framework of activities carried out by the European Investment Fund

THE EUROPEAN INVESTMENT FUND (EIF),

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

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, repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC ⁽¹⁾ (hereinafter 'the Regulation'), and in particular Article 25 thereof,

Having regard to the opinion ⁽²⁾ of the European Data Protection Supervisor (EDPS),

Whereas:

- (1) EIF Compliance Department may, in the context of its functioning, conduct administrative inquiries, on the basis of the EIB Group Staff Code of Conduct, which implies processing of information including personal data.
- (2) The EIF Data Protection Officer (DPO) may, on his or her own initiative or at the request of the controller or any individual, investigate matters and occurrences directly relating to his or her tasks which come to his or her notice and report back to the person who commissioned the investigation or to the controller, as per Article 45(2) of the Regulation.
- (3) EIF Human and Resources Management Department may, in the context of its functioning, conduct disciplinary proceedings, on the basis of Section 6 of the EIF Staff Regulations, Title IV of the Dignity at Work Policy, and the applicable EIF codes of conduct.
- (4) The members of EIF Board of Directors, the Chief Executive, the Deputy Chief Executive and staff members as well as operation/transaction related parties have the obligation to report to the EIB's Fraud Investigations Division ('IG/IN') any possible prohibited conduct (e.g. fraud or corruption), detrimental to the interests of the EIF and of the Union, or to report to other competent services any conduct relating to the discharge of professional duties which may constitute a serious failure to comply with any applicable obligations. In addition any member of the public, individual, entity can report allegation of Prohibited Conduct to IG/IN.
- (5) Investigations into Prohibited Conduct, as defined in the EIF's Anti-Fraud Policy, are conducted by IG/IN, as data processor, based on the Framework Agreement between the EIF and the EIB concerning provision of services.
- (6) The EIF conducts audits on its activities. This is currently performed through the Internal Audit Directorate of the EIB based on the Framework Agreement between the EIF and the EIB concerning provision of services.

⁽¹⁾ OJ L 295, 21.11.2018, p. 39.

⁽²⁾ EDPS comments and recommendations dated 20 February 2020 (DH/CCP/ALS/D(2020) 0372 C2019-1114).

- (7) In the context of the tasks described in recitals 1 to 6, the EIF may provide and receive assistance and cooperation to and from other Union institutions, bodies, offices and agencies, as set in relevant service level agreements, memoranda of understanding and cooperation agreements.
- (8) The EIF may provide and receive assistance and cooperation to and from EU Member States' public authorities, upon their request or by its own initiative.
- (9) The EIF may provide and receive assistance and cooperation to and from third countries' national authorities and international organisations, upon their request or by its own initiative.
- (10) In the context of the abovementioned activities, the EIF, acting as data controller, or any of the business partners of EIF referred to in recital 4 above, including the EIB's Fraud Investigations Division, acting as data processor, or any other competent service may collect and process information and personal data, including identification data of a natural person, contact information, professional roles and tasks, information on private and professional conduct and performance, and financial data.
- (11) Adequate safeguards are in place to protect personal data and prevent them from accidentally or unlawfully being accessed or transferred, both if they are stored in a physical or in an electronic environment. After processing, the data are retained in accordance with the applicable EIF retention rules, as defined in data protection records based on Article 31 of the Regulation. At the end of the retention period, the case related information, including personal data, is in line with the principles of the European Data Protection Regulations and related regulatory acts or EIF policies, deleted, fully anonymised or transferred to the historical archives.
- (12) Within this context, the EIF is committed to fulfil its obligation to provide information to the data subjects in relation to the above processing activities and respect the rights of the data subjects, as laid down in the Regulation.
- (13) It may be necessary to reconcile the rights of data subjects pursuant to the Regulation with the needs of the abovementioned activities, while fully respecting fundamental rights and freedoms of other data subjects. To that effect, Article 25 of the Regulation provides, under strict conditions, the possibility to restrict the application of Articles 14 to 20, 35 and 36, as well as Article 4 in so far as its provisions correspond to the rights and obligations provided for in Articles 14 to 20. In this case it is necessary to adopt internal rules under which the EIF may restrict the aforementioned rights of data subjects in line with the same Article of the Regulation.
- (14) This might in particular be the case when providing information about the processing of personal data to the data subject at the preliminary assessment phase of an administrative inquiry or during the inquiry itself, prior to a possible dismissal of the case or a pre-disciplinary stage. In certain circumstances, providing such information might seriously affect the EIF's capacity to conduct the inquiry in an effective way, whenever, for example, there is a risk that the person concerned destroys evidence or interferes with potential witnesses before they are interviewed. Furthermore, the EIF might need to protect the rights and freedoms of other persons involved. It might, in particular, be necessary to protect the privacy of a witness or a whistle-blower who has asked not to be identified. In such a case, the EIF may decide to restrict access to the identity, statements and other data relating to the whistle-blower and/or other persons involved, in order to protect their rights and freedoms.
- (15) When providing or receiving assistance and cooperation to and from other Union institutions, bodies, offices and agencies, EU Member States' public authorities, third countries' national authorities and international organisations in the context of the abovementioned activities, the EIF, in certain circumstances, and subject to the maintenance of the minimum data protection level required by the EDPS, might need to preserve the effectiveness of its inquiries or of those carried out by the entity it cooperates with, and protect, as necessary, persons involved and their rights and freedoms.
- (16) The EIF shall apply restrictions only when they respect the essence of the fundamental rights and freedoms, and are strictly necessary and a proportionate measure in a democratic society. The EIF shall give justifications explaining the grounds for those restrictions.
- (17) Based on the principle of accountability, the EIF shall keep a record of the application of the restrictions.
- (18) When processing personal data exchanged with other organisations in the context of its tasks, the EIF shall consult and shall be consulted by those organisations on the possible relevant grounds for imposing restrictions and the necessity and proportionality of the restrictions, unless this would jeopardise the activities of the EIF.

- (19) Article 25(6) of the Regulation obliges the controller to inform data subjects of the principal reasons on which the application of the restriction is based and of their right to lodge a complaint with the EDPS.
- (20) Pursuant to Article 25(8) of the Regulation, the EIF may defer, omit or deny the provision of information on the reasons for the application of a restriction to the data subject if this would in any way cancel the effect of the restriction. The EIF shall assess on a case-by-case basis whether the communication of the restriction would cancel its effect.
- (21) The DPO may carry out an independent review of the application of the restrictions, with a view to ensuring compliance with the present Decision,

HAS ADOPTED THIS DECISION:

Article 1

Subject matter and scope

The present Decision lays down rules relating to the conditions under which the EIF may restrict the application of Articles 14 to 20, 35 and 36, as well as Article 4 thereof based on Article 25 of the Regulation.

Article 2

Restrictions

1. In accordance with Article 25(1) of the Regulation, the EIF may, on a case by case basis only, restrict the application of Articles 14 to 20, 35 and 36, as well as Article 4 thereof, in so far as its provisions correspond to the rights and obligations provided for in Articles 14 to 20, when:

- (a) conducting administrative inquiries, on the basis of the EIB Group Staff Code of Conduct and other applicable Codes of Conduct;
- (b) conducting investigations related to matters and occurrences directly relating to the DPO tasks, as per Article 45(2) of the Regulation;
- (c) conducting disciplinary proceedings, on the basis of Section 6 of the EIF Staff Regulations, Title IV of the Dignity at Work Policy, the EIB Group Staff Code of Conduct and other applicable EIF codes of conduct;
- (d) ensuring that EIF staff members may confidentially report facts where they believe there are serious irregularities as regulated by the EIB Group Whistleblowing Policy;
- (e) ensuring that EIF staff members may confidentially report facts where they believe there are suspicions of prohibited conduct, including fraud or corruption, detrimental to the interests of the Union, or conduct relating to the discharge of professional duties which may constitute a serious failure to comply with the EIF Staff members' obligations, as regulated by the EIB Group Whistleblowing Policy, the EIF Anti-Fraud Policy, and the relevant EIF Codes of Conduct;
- (f) conducting investigations of Prohibited Conduct, as per the EIF's Anti-Fraud Policy;
- (g) conducting internal audits in relation to all the activities and departments of the EIF;
- (h) providing or receiving assistance and cooperation to and from other Union institutions, bodies, offices and agencies, in the context of the abovementioned activities, as set out in relevant service level agreements, memoranda of understanding and cooperation agreements;
- (i) providing or receiving assistance and cooperation to and from EU Member States' public authorities, upon their request or by its own initiative;
- (j) providing or receiving assistance and cooperation to and from third countries' national authorities and international organisations, upon their request or by its own initiative.

2. The categories of data may include the identification data of a natural person, contact information, professional roles and tasks, information on private and professional conduct and performance, case involvement data and financial data.

3. The application of the abovementioned restrictions is without prejudice to the possible application of the provisions of Article 16(5) and 17(4) of the Regulation, relating, respectively, to the right of information when data have not been obtained from the data subject, and to the right of access by the data subject.

4. Any restriction shall respect the essence of the fundamental rights and freedoms and be necessary and proportionate in a democratic society, as addressed in the Regulation, corresponding regulatory acts or internal policies of EIF or EIB Group.
5. Any restriction shall be based on an express authorisation in an effective internal EIF policy or procedure and shall affect the rights of the data subject(s) concerned to the least extent possible, as confirmed by the DPO.
6. A necessity and proportionality test shall be carried out on a case-by-case basis and to the satisfaction of the DPO before restrictions are applied. Restrictions shall be limited to what is strictly necessary to achieve the set objectives. Restrictions shall only be established for the time any relevant ground under paragraph 1, which is referred to as motivation for the restriction, so requires, as is evidenced to the satisfaction of the DPO.
7. Where IG/IN restricts, wholly or partly, the provision of information to the data subjects relevant to an investigation (person concerned, witness or informant), it shall record the reasons for the restriction, including an assessment of the necessity and proportionality of the restriction. To that end, the record shall state how the provision of the information would jeopardise the purpose of IG/IN's investigative activities, or of restrictions applied pursuant to Article 2(1)(f), (g) and (h) of this Decision, or would adversely affect the rights and freedoms of other data subjects. The record and, where applicable, the documents containing underlying factual and legal elements shall be registered. They shall be made available to the European Data Protection Supervisor (EDPS) on request.
8. The EIF, shall file, for accountability purposes, a record describing the reasons for the restrictions applied, which grounds among those listed in paragraph 1 apply and the outcome of the necessity and proportionality test. Those records shall be part of an ad hoc register, which shall be made available on request to the EDPS.
9. When processing personal data exchanged with other organisations in the context of its tasks, the EIF shall consult and shall be consulted by those organisations on the possible relevant grounds for imposing restrictions and the necessity and proportionality of the restrictions, unless this would jeopardise the activities of the EIF.

Article 3

Risks to the rights and freedoms of data subjects

The assessment of the risks to the rights and freedoms of data subjects whose personal data may be subject to restrictions, as well as their retention period, are referenced in the record of the relevant processing activities in accordance with Article 31 of the Regulation and, if applicable, in relevant data protection impact assessments based on Article 39 of the Regulation.

Article 4

Storage periods and safeguards

The EIF shall implement safeguards to prevent abuse or unlawful access or transfer of personal data that may be subject to restrictions. These safeguards shall include technical and organisational measures and be detailed, as necessary, in EIF internal decisions, procedures and implementing rules. The safeguards shall include:

- (1) an adequate definition of roles, responsibilities and procedural steps;
- (2) if applicable, a secure electronic environment which prevents unlawful or accidental access or transfer of electronic data to unauthorised persons;
- (3) if applicable, secure storage and processing of paper-based documents;
- (4) due monitoring of restrictions and a periodical revision by the DPO, which shall be done at least every six months. A revision must also be carried out when essential elements of the case at hand change. The restrictions shall be lifted as soon as the circumstances that justify them no longer apply.

*Article 5***Information to and review by the Data Protection Officer**

1. The DPO shall be informed without undue delay whenever the rights of any data subject are restricted in accordance with the present Decision and shall be provided full and unrestricted access to all records and any documents containing underlying factual and legal elements, which are relevant for the decision on the restriction and the monitoring of the maintenance of the restriction.
2. The DPO may request to review the application of the restriction.
3. Should the DPO, in the course of his or her own investigations, apply restrictions, he or she will inform the controller without undue delay.
4. The involvement of the DPO in the restrictions process, including information exchanges, shall be documented in the appropriate form and included in the relevant records and registers.
5. In the context of Prohibited Conduct Investigations, the EIB's Fraud Investigations Division will consult the DPO prior to the application of certain grounds for restriction, referred to in Article 25 of the Regulation to data processing operations carried out in the framework of its tasks set out in the EIF's Anti-Fraud Policy, the Fraud Investigations Division's Charter and Investigations Procedures.

*Article 6***Information to data subjects on restrictions to their rights**

1. The EIF shall include in the data protection notices published on its website general information to the data subjects related to the potential restrictions of all data subjects' rights described in Article 2(1). The information shall cover which rights may be restricted.
2. The EIF shall inform data subjects individually on present or future restrictions of their rights without undue delay and in a written form, as further specified in Articles 7, 8 and 9.

*Article 7***Right to information to be provided to data subjects and communication on data breaches**

1. Where in the context of the activities mentioned in the present Decision, the EIF restricts, wholly or partly, their rights of data subjects referred to in Articles 14 to 16 and 35 of the Regulation, data subjects shall be informed of the principal reasons on which the application of the restriction is based, and of their right to lodge a complaint with the EDPS as well as seeking a judicial remedy before the Court of Justice of the European Union. Such restriction shall follow the rules established and the process described in the present Decision.
2. The EIF may defer, omit or deny the provision of information concerning the reasons for the restriction referred to in paragraph 1 to the extent that and for as long as it would jeopardise the purpose of the restriction. This assessment shall take place on a case-by-case basis. Any such deferral or denial must be adequately justified to the satisfaction of the DPO and will be included in the relevant records and registers. For the avoidance of doubt, data subjects concerned shall be informed of their rights to lodge a complaint with the EDPS as well as seeking a judicial remedy before the Court of Justice of the European Union against the decision to defer or deny them the provision of the information referred to under paragraph 1 above.

*Article 8***Data subjects' right of access, rectification, erasure and restriction of processing**

1. Where in the context of the activities mentioned in the present Decision, the EIF restricts, wholly or partly, the right of access to personal data, the right to rectification, erasure, and restriction of processing, as referred to in Articles 17 to 20 respectively of the Regulation, it shall inform the data subject concerned, in its reply to the request, of the principal reasons on which the application of the restriction is based, and of the possibility of lodging a complaint with the EDPS or of seeking a judicial remedy before the Court of Justice of the European Union.

2. Where the right of access is wholly or partly restricted, the EIF, when investigating the request, shall only inform the data subject of whether the data have been processed correctly and, if not, whether any necessary corrections have been made, in accordance with Article 25(7) of the Regulation.

3. The EIF may defer, omit or deny the provision of information concerning the reasons for the restriction referred to in paragraph 1 and 2 to the extent that and for as long as it would jeopardise the purpose of the restriction. This assessment shall take place on a case-by-case basis and shall follow the rules established and the process described in the present Decision.

Article 9

Confidentiality of electronic communication

1. The EIF, under exceptional circumstances, and in line with the provisions and the rationale of Directive 2002/58/EC of the European Parliament and of the Council ⁽³⁾, may restrict the right to confidentiality of electronic communications, as referred to in Article 36 of the Regulation. In this case, the EIF shall detail circumstances, grounds, relevant risks and related safeguards in specific internal rules.

2. Where the EIF restricts the right to confidentiality of electronic communications, it shall inform the data subject concerned, in its reply to their request, of the principal reasons on which the application of the restriction is based, and of the possibility of lodging a complaint with the EDPS or of seeking a judicial remedy before the Court of Justice of the European Union.

3. The EIF may defer, omit or deny the provision of information concerning the reasons for the restriction referred to in paragraph 1 and 2 for as long as it would cancel the effect of the restriction. This assessment shall take place on a case-by-case basis.

Article 10

Entry into force

The present Decision and any amendments thereto shall be approved by the EIF Board of Directors and shall enter into force on the twentieth day after its publication in the *Official Journal of the European Union*.

Done at Luxembourg, 4 June 2020.

⁽³⁾ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

**DECISION No 1/2020 OF THE GOVERNING BOARD OF THE SHIFT2RAIL JOINT UNDERTAKING
of 26 March 2020**

**laying down internal rules concerning restrictions of certain rights of data subjects in relation to
processing of personal data in the framework of the functioning of the S2R JU**

THE GOVERNING BOARD OF THE SHIFT2RAIL JOINT UNDERTAKING (hereafter referred as 'the S2R JU'),

Having regard to the Treaty on the Functioning of the European Union ⁽¹⁾,

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 ⁽²⁾, and in particular Article 25 thereof,

Having regard to Council Regulation (EU) No 642/2014 of 16 June 2014 establishing the Shift2Rail Joint Undertaking ⁽³⁾, and in particular Article 8 of the Statutes annexed to that Regulation,

Having regard to the European Data Protection Supervisor Guidance on Article 25 of the new Regulation and internal rules,

After having consulted the EDPS on 12 November 2019, in accordance with Article 41(2) of Regulation (EU) 2018/1725,

Having regard to the recommendations of the European Data Protection Supervisor ('EDPS') of 18 December 2019,

After having consulted the S2R JU Staff Committee,

Whereas:

- (1) Only legal acts adopted on the basis of the Treaties provides for a restriction of data subject rights. Where these restrictions cannot be based on legal acts adopted on the basis of the Treaties, Regulation (EU) 2018/1725 provides that, in matters relating to the operations of S2R JU, restrictions may be provided for by internal rules, including its provisions on the assessment of the necessity and proportionality of a restriction.
- (2) In accordance with Article 25(1) of Regulation (EU) 2018/1725 restrictions of the application of Articles 14 to 22, 35 and 36, as well as Article 4 of that Regulation in so far as its provisions correspond to the rights and obligations provided for in Articles 14 to 22 should be based on internal rules to be adopted by the S2R JU.
- (3) Within the framework of its administrative functioning, the S2R JU may conduct administrative inquiries, disciplinary proceedings, carry out preliminary activities related to cases of potential irregularities reported to OLAF, process whistleblowing cases, process (formal and informal) procedures of harassment, process internal and external complaints, conduct internal audits, carry out investigations by the Data Protection Officer in line with Article 45(2) of Regulation (EU) 2018/1725 and internal (IT) security investigations.
- (4) The S2R JU processes several categories of personal data, such as identification data, contact data, professional data, administrative details, data received from specific sources, electronic communications and traffic data, and data related to the case (such as reasoning, behavioural data, appraisals, performance and conduct data and data related to or brought forward in connection with the subject matter of the procedure or activity) ⁽⁴⁾.
- (5) The S2R JU, represented by its Executive Director, acts as the data controller.

⁽¹⁾ OJ C 202, 7.6.2016, p. 47.

⁽²⁾ OJ L 295, 21.11.2018, p. 39.

⁽³⁾ OJ L 177, 17.6.2014, p. 9.

⁽⁴⁾ In cases of joint controllership data shall be processed in line with the means and purposes established in the relevant agreement among the joint controllers as defined in Article 28 of Regulation (EU) 2018/1725.

- (6) The personal data are stored securely in an electronic environment or on paper preventing unlawful access or transfer of data to persons who do not have a need to know. The personal data processed are retained for no longer than necessary and appropriate for the purposes for which the data are processed for the period specified in the data protection notices, privacy statements or records of the S2R JU.
- (7) The internal rules should apply to all processing operations carried out by the S2R JU in the performance of administrative inquiries, disciplinary proceedings, preliminary activities related to cases of potential irregularities reported to OLAF, whistleblowing procedures, (formal and informal) procedures for cases of harassment, processing internal and external complaints, internal audits, the investigations carried out by the Data Protection Officer in line with Article 45(2) of Regulation (EU) 2018/1725, (IT) security investigations handled internally or with external involvement (e.g. CERT-EU).
- (8) They should apply to processing operations carried out prior to the opening of the procedures referred to above, during these procedures and during the monitoring of the follow-up to the outcome of these procedures. It should also include assistance and cooperation provided by the S2R JU to national authorities and international organisations outside of its administrative investigations.
- (9) In cases where these internal rules apply, the S2R JU must provide justifications explaining why the restrictions are strictly necessary and proportionate in a democratic society and respect the essence of the fundamental rights and freedoms.
- (10) Within this framework the S2R JU is bound to respect, to the maximum extent possible, the fundamental rights of the data subjects during the above procedures, in particular, those relating to the right of provision of information, access and rectification, right to erasure, restriction of processing, right of communication of a personal data breach to the data subject or confidentiality of communication as enshrined in Regulation (EU) 2018/1725.
- (11) However, the S2R JU may be obliged to restrict the information to data subject and other data subject's rights to protect, in particular, its own investigations, the investigations and proceedings of other public authorities, as well as the rights of other persons related to its investigations or other procedures.
- (12) Where the S2R JU considers to apply a restriction, the risk to the rights and freedoms of the data subject shall be weighed, in particular, against the risk to the rights and freedoms of other data subjects and the risk of cancelling the effect of the S2R JU's investigations or procedures for example by destroying evidence. The risks to the rights and freedoms of the data subject concern primarily, but are not limited to, reputational risks and risks to the right of defence and the right to be heard.
- (13) The S2R JU may thus restrict the information for the purposes of protecting the investigation, and the fundamental rights and freedoms of other data subjects.
- (14) The S2R JU should periodically monitor that the conditions justifying the restriction apply, and lift the restriction as far as they no longer apply.
- (15) The Controller should inform the Data Protection Officer at the moment of deferral and during the revisions,

HAS ADOPTED THIS DECISION:

Article 1

Subject matter and scope

1. This Decision lays down rules relating to the conditions under which the S2R JU in the framework of its procedures set out paragraph 2 may restrict the application of the rights enshrined in Articles 14 to 21, 35 and 36, as well as Article 4 thereof, following Article 25 of Regulation (EU) 2018/1725.

2. Within the framework of the administrative functioning of the S2R JU, this Decision applies to the processing operations on personal data by the Programme Office for the purposes of conducting administrative inquiries, disciplinary proceedings, preliminary activities related to cases of potential irregularities reported to OLAF, processing whistleblowing cases, (formal and informal) procedures of harassment, processing internal and external complaints, conducting internal audits, investigations carried out by the Data Protection Officer in line with Article 45(2) of Regulation (EU) 2018/1725 and (IT) security investigations handled internally or with external involvement (e.g. CERT-EU).

3. The categories of data concerned include identification data, contact data, professional data, administrative details, data received from specific sources, electronic communications and traffic data, and data related to the case, such as reasoning, behavioural data, appraisals, performance and conduct data and data related to or brought forward in connection with the subject matter of the procedure or activity.

4. Where the S2R JU performs its duties with respect to data subject's rights under Regulation (EU) 2018/1725, it shall consider whether any of the exemptions laid down in that Regulation apply.

Article 2

Specification of the controller

The controller of the processing operations is the S2R JU, represented by its Executive Director.

Article 3

Specification of safeguards

1. The S2R JU shall put in place the following safeguards aimed at preventing abuse or unlawful access or transfer of personal data:

- (a) Paper documents shall be kept in secured cupboards and only accessible to authorized staff;
- (b) All electronic data shall be stored in a secure IT application according to the S2R JU's security standards, as well as in specific electronic folders accessible only to authorised staff. Appropriate levels of access shall be granted individually;
- (c) The database shall be password-protected under a single sign-on system and connected automatically to the user's ID and password, including 'pseudonymisation' and/or 'encryption' when appropriate. Replacing users is strictly prohibited. E-records shall be held securely to safeguard the confidentiality and privacy of the data therein;
- (d) All persons having access to the data are bound by the obligation of confidentiality.

2. In accordance with Article 6(3), the safeguards referred to in paragraph 1 should be subject to a periodic review.

3. The retention period of the personal data referred to in Article 1(3) is indicated in its respective data protection notices, privacy statements or records referred to in Article 7(1). The retention period shall in any event not be longer than necessary and appropriate for the purposes for which the data are processed ⁽⁵⁾.

Article 4

Grounds for restrictions

1. Any restriction shall only be applied by the S2R JU to safeguard:

- (a) the national security, public security or defence of the Member States;
- (b) the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

⁽⁵⁾ S2R retention policy is based in retention of files in the Commission regulated by the Common retention list, a regulatory document (the last version is SEC(2019)900) in the form of a retention schedule that establishes the retention periods for the different types of Commission files.

- (c) other important objectives of general public interest of the Union or of a Member State, in particular the objectives of the common foreign and security policy of the Union or an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;
- (d) the internal security of Union institutions and bodies, including of their electronic communications networks;
- (e) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
- (f) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (c);
- (g) the protection of the data subject or the rights and freedoms of others;
- (h) the enforcement of civil law claims.

2. As a specific application of the purposes described in paragraph 1 above, the S2R JU may apply restrictions in the following circumstances:

- (a) in relation to personal data exchanged with Commission services or other Union institutions, bodies, agencies and offices;
 - where such Commission service, Union institution, body or agency, is entitled to restrict the exercise of the listed rights on the basis of other acts provided for in Article 25 of Regulation (EU) 2018/1725 or in accordance with Chapter IX of that Regulation or with the founding acts of other Union institutions, bodies, agencies and offices,
 - where the purpose of such a restriction by that Commission service, Union institution, body or agency would be jeopardised were the S2R JU not to apply an equivalent restriction in respect of the same personal data;
- (b) in relation to personal data exchanged with competent authorities of Member States;
 - where such competent authorities of Member States are entitled to restrict the exercise of the listed rights on the basis of acts referred to in Article 23 of Regulation (EU) 2016/679 of the European Parliament and of the Council ⁽⁶⁾, or under national measures transposing Articles 13(3), 15(3) or 16(3) of Directive (EU) 2016/680 of the European Parliament and of the Council ⁽⁷⁾,
 - where the purpose of such a restriction by that competent authority would be jeopardised were the S2R JU not to apply an equivalent restriction in respect of the same personal data;
- (c) in relation to personal data exchanged with third countries or international organisations, where there is clear evidence that the exercise of those rights and obligations is likely to jeopardise the S2R JU's cooperation with third countries or international organisations in the conduct of its tasks.

Before applying restrictions in the circumstances referred to in points (a) and (b) of the first subparagraph, the S2R JU shall consult the relevant Commission services, Union institutions, bodies, agencies, offices or the competent authorities of Member States unless it is clear to the S2R JU that the application of a restriction is provided for by one of the acts referred to in those points.

Article 5

Restrictions and rights of data subjects

1. In duly justified cases and under the conditions stipulated in this decision, the following rights may be restricted by the controller in the context of the processing operations listed in Article 1(2) and paragraph 2 below where necessary and proportionate:

- (a) The right to information;
- (b) The right of access;

⁽⁶⁾ 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).

⁽⁷⁾ Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

- (c) The right of rectification, erasure and restriction of processing;
 - (d) The right to communication of a personal data breach to the data subject;
 - (e) The right to confidentiality of electronic communications.
2. In duly justified cases and in order to safeguard the purposes mentioned in article 4(1), restrictions may be applied by the controller in the context of the following processing operations referred to in Article 1(2):
- (a) the performance of administrative inquiries and disciplinary proceedings;
 - (b) preliminary activities related to cases of potential irregularities reported to OLAF;
 - (c) whistleblowing procedures;
 - (d) (formal and informal) procedures for cases of harassment;
 - (e) processing internal and external complaints;
 - (f) internal audits;
 - (g) the investigations carried out by the Data Protection Officer in line with Article 45(2) of Regulation (EU) 2018/1725;
 - (h) (IT) security investigations handled internally or with external involvement (e.g. CERT-EU);
 - (i) within the frame of the grant management or procurement procedure, after the closing date of the submission of the calls for proposals or the application of tenders.
3. In the context of procedure for cases of harassment, the rights referred to in paragraph 1 may be limited under the same conditions, with the exception of the right to communication of a personal data breach to the data subject referred to in point (d) of paragraph 1.
4. In the context of grant management or procurement procedure, the rights referred to in paragraph 1 may be limited under the same conditions, with the exception of the right of rectification, erasure and restriction of processing referred to in point (c) of paragraph 1.
5. In duly justified cases and under the conditions stipulated in this decision, the right of rectification, erasure and restriction of processing may be restricted by the controller, with the exceptions provided for in paragraph 3 and 4.
6. Where the S2R JU restricts, wholly or partly, the application of the rights referred to in paragraphs 1, 3,4 and 5, it shall take the steps set out in Articles 6 and 7 of this Decision.
7. Where data subjects request access to their personal data processed in the context of one or more specific cases or to a particular processing operation, in accordance with Article 17 of Regulation (EU) 2018/1725, the S2R JU shall limit its assessment of the request to such personal data only.

Article 6

Necessity and proportionality of restrictions

1. Any restriction based on Article 4 shall be necessary and proportionate taking into account the risks to the rights and freedoms of data subjects and respect the essence of the fundamental rights and freedoms in a democratic society.
2. If the application of restriction is considered, a necessity and proportionality test shall be carried out based on the present rules. The test shall also be conducted within the framework of the periodic review, following assessment of whether the factual and legal reasons for a restriction still apply. It shall be documented through an internal assessment note for accountability purposes on a case-by-case basis.
3. Restrictions shall be temporary. They shall continue to apply as long as the reasons justifying them remain applicable. In particular, where it is considered that the exercise of the restricted right would no longer cancel the effect of the restriction imposed or adversely affect the rights or freedoms of other data subjects.

The S2R JU shall review the application of the restriction every six months from its adoption and at the closure of the relevant inquiry, procedure or investigation. Thereafter, the controller shall monitor the need to maintain any restriction every six months.

4. Where the S2R JU applies, wholly or partly, the restrictions based on Article 4 of this Decision, it shall record the reasons for the restriction, the legal ground in accordance with paragraph 1 above, including an assessment of the necessity and proportionality of the restriction.

The record and, where applicable, the documents containing underlying factual and legal elements shall be registered. They shall be made available to the European Data Protection Supervisor on request.

Article 7

Obligation to inform

1. The S2R JU shall include in the data protection notices, privacy statements or records in the sense of Article 31 of Regulation (EU) 2018/1725, published on its website and/or on the intranet informing data subjects of their rights in the framework of a given procedure, information relating to the potential restriction of these rights. The information shall cover which rights may be restricted, the reasons and the potential duration.

Without prejudice to the provisions of Article 6(4), the S2R JU, where proportionate, shall also inform individually all data subjects, which are considered persons concerned in the specific processing operation, of their rights concerning present or future restrictions without undue delay and in a written form.

2. Where the S2R JU restricts, wholly or partly, the rights laid out in Article 5, it shall inform the data subject concerned of the restriction applied and of the principal reasons thereof, and of the possibility of lodging a complaint with the European Data Protection Supervisor or of seeking a judicial remedy in the Court of Justice of the European Union;

The provision of information referred to in paragraph 2 above may be deferred, omitted or denied if it would cancel the effect of the restriction in accordance with Article 25(8) of Regulation (EU) 2018/1725.

Article 8

Review by the Data Protection Officer

1. The S2R JU shall, without undue delay, inform the Data Protection Officer of the S2R JU ('the DPO') whenever the controller restricts the application of data subjects' rights, or extends the restriction, in accordance with this Decision. The controller shall provide the DPO access to the record containing the assessment of the necessity and proportionality of the restriction and document the date of informing the DPO in the record.

2. The DPO may request the controller in writing to review the application of the restrictions. The controller shall inform the DPO in writing about the outcome of the requested review.

3. The DPO shall be involved throughout the procedure. The controller shall inform the DPO when the restriction has been lifted.

Article 9

Entry into force

This Decision shall enter into force on the twentieth day following its publication in the *Official Journal of the European Union*.

Done at Brussels, 26 March 2020.

For the Governing Board of the S2R JU
Henrik HOLOLEI
The Chairperson

ISSN 1977-0677 (electronic edition)
ISSN 1725-2555 (paper edition)



Publications Office of the European Union
2985 Luxembourg
LUXEMBOURG

EN