DECISION (EU) 2021/1486 OF THE EUROPEAN CENTRAL BANK

of 7 September 2021

adopting internal rules concerning restrictions of rights of data subjects in connection with the European Central Bank's tasks relating to the prudential supervision of credit institutions (ECB/2021/42)

THE EXECUTIVE BOARD OF THE EUROPEAN CENTRAL BANK,

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

Having regard to the Statute of the European System of Central Banks and of the European Central Bank, and in particular Article 11.6 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 ([1]), and in particular Article 25 thereof,

Whereas:

(1) The European Central Bank (ECB) carries out its tasks in accordance with the Treaties and Council Regulation (EU) No 1024/2013 ([2]).

(2) In accordance with Article 45(3) of Regulation (EU) 2018/1725, Decision (EU) 2020/655 of the European Central Bank (ECB/2020/28) ([3]) sets out the general rules implementing Regulation (EU) 2018/1725 as regards the ECB. In particular, it specifies the rules relating to the appointment and role of the data protection officer of the ECB (DPO), including the DPO's tasks, duties and powers.

(3) In exercising the tasks conferred on the ECB, the ECB and in particular the organisational unit concerned acts as data controller in so far as it determines, alone or jointly with others, the purposes and means of the processing of personal data.

(4) Pursuant to Article 4(1) of Regulation (EU) No 1024/2013, the ECB is exclusively competent to carry out, for supervisory purposes, and with a view to ensuring the safety and soundness of credit institutions and the stability of the financial system, specific tasks in relation to all credit institutions established in the Member States participating in the Single Supervisory Mechanism (SSM).

(5) In carrying out these specific tasks, the ECB processes several categories of information that may be related to an identified or identifiable natural person such as identification data, contact data, professional data, financial or administrative details, data received from specific sources, data on electronic communication and electronic traffic data, criminal records, a description of financial and non-financial interests, details of relationships of an individual or their close relatives to supervised entities or to members of the management body of supervised entities, and data relating to the position for which an individual has been or may be appointed. Personal data could also form part of an assessment including an assessment conducted: for the purposes of the authorisation of a credit institution, the withdrawal of the authorisation of a credit institution and a qualifying holding procedure; in relation to the right of establishment for a significant supervised entity; to determine whether fit and proper requirements are met; in relation to a significant supervised entity's remuneration policies and regarding credits by such an entity to its own senior officials and persons related to these officials; and in relation to allegations related to potential breaches of the legal acts referred to in Article 4(3) of Regulation (EU) No 1024/2013.

([1]) OJ L 295, 21.11.2018, p. 39.

([2]) Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions (OJ L 287, 29.10.2013, p. 63).

([3]) Decision (EU) 2020/655 of the European Central Bank of 5 May 2020 adopting implementing rules concerning data protection at the European Central Bank and repealing Decision ECB/2007/1 (ECB/2020/28) (OJ L 152, 15.5.2020, p. 13).

(6) The aim of the ECB in performing these specific tasks is to pursue important objectives of general public interest of the Union. For this reason, the performance of such tasks should be safeguarded as contemplated by Regulation (EU) 2018/1725, in particular by Article 25(1)(c) and (g) thereof. In particular in performing such tasks, the ECB acts in the general public interest of the Union as a public authority entrusted with carrying out, for supervisory purposes, specific tasks in relation to all credit institutions established in the Member States participating in the SSM. Such tasks include monitoring, inspection or regulatory functions connected with the exercise of official authority related to the prudential supervision of credit institutions.

(7) In this context, it is appropriate to specify the grounds on which the ECB may restrict the rights of data subjects in relation to data obtained in the performance of its supervisory tasks pursuant to Regulation (EU) No 1024/2013.

(8) In accordance with Article 25(1) of Regulation (EU) 2018/1725, restrictions of the application of Articles 14 to 22, 35 and 36 and, in so far as its provisions correspond to the rights and obligations provided for in Articles 14 to 22, Article 4 of that Regulation should be set out in internal rules or legal acts adopted on the basis of the Treaties. Accordingly, the ECB should set out the rules under which it may restrict the rights of data subjects in the performance of its supervisory tasks.

(9) Whilst this Decision sets out the rules under which the ECB may restrict the rights of data subjects in the performance of its supervisory tasks, the Executive Board intends to adopt a separate decision adopting internal rules concerning the restriction of those rights when the ECB processes personal data in connection with its internal functioning.

(10) The ECB may be able to apply an exception in accordance with Regulation (EU) 2018/1725 which makes the need to consider a restriction unnecessary including in particular those set out in Articles 15(4), 16(5), 19(3) and 35(3) of that Regulation. For processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, the ECB may be able to apply an exception set out in point (b) of Article 16(5) or point (d) of Article 19(3) of Regulation (EU) 2018/1725.

(11) The exercise of the rights of data subjects referred to in Articles 17, 18, 20, 21, 22 and 23 of Regulation (EU) 2018/1725 may render impossible or seriously impair the achievement of certain purposes including, as applicable, archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. Therefore this Decision should provide for a derogation from those rights in accordance with Article 25(3) or (4) of Regulation (EU) 2018/1725, subject to appropriate safeguards.

(12) The ECB should justify why such restrictions of data subjects' rights are strictly necessary and proportionate in a democratic society to safeguard the objectives pursued in the exercise of its official authority and the functions connected to it, and how the ECB respects the essence of fundamental rights and freedoms whilst imposing any such restriction.

(13) Within this framework the ECB is bound to respect, to the maximum extent possible, the fundamental rights of data subjects, 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 provided for in Regulation (EU) 2018/1725.

(14) However, the ECB may be obliged to restrict the information provided to data subjects and the rights of data subjects to protect the performance of its supervisory tasks, in particular its own investigations and procedures, the investigations and procedures of other public authorities and the fundamental rights and freedoms of other persons related to its investigations or other procedures.

(15) The ECB should lift a restriction which has already been applied to the extent it is no longer needed.

(16) The ECB's DPO should review the application of restrictions with a view to ensuring compliance with this Decision and with Regulation (EU) 2018/1725.

(17) The European Data Protection Supervisor was consulted in accordance with Article 41(2) of Regulation (EU) 2018/1725 and delivered an opinion on 12 March 2021,

HAS ADOPTED THIS DECISION:

Article 1

Subject matter and scope

1. This Decision sets out rules relating to the restriction of the rights of data subjects by the ECB when conducting personal data processing activities as recorded in the central register in the performance of its supervisory tasks pursuant to Regulation (EU) No 1024/2013.

2. The rights of data subjects which may be restricted are specified in the following Articles of Regulation (EU) 2018/1725:

(a) Article 14 (transparent information, communication and modalities for the exercise of the rights of the data subject);

(b) Article 15 (information to be provided where personal data are collected from the data subject);

(c) Article 16 (information to be provided where personal data have not been obtained from the data subject);

(d) Article 17 (right of access by the data subject);

(e) Article 18 (right to rectification);

(f) Article 19 (right to erasure ('right to be forgotten'));

(g) Article 20 (right to restriction of processing);

(h) Article 21 (notification obligation regarding rectification or erasure of personal data or restriction of processing);

(i) Article 22 (right to data portability);

(j) Article 35 (communication of a personal data breach to the data subject);

(k) Article 36 (confidentiality of electronic communications);

(l) Article 4 in so far as its provisions correspond to the rights and obligations provided for in Articles 14 to 22 of Regulation (EU) 2018/1725.

Article 2

Definitions

For the purposes of this Decision, the following definitions apply:

(1) 'processing' means processing as defined in point (3) of Article 3 of Regulation (EU) 2018/1725;

(2) 'personal data' means personal data as defined in point (1) of Article 3 of Regulation (EU) 2018/1725;

(3) 'data subject' means an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(4) 'central register' means the publicly available repository of all personal data processing activities conducted at the ECB which is kept by the ECB's DPO and referred to in Article 9 of Decision (EU) 2020/655 (ECB/2020/28);

(5) 'controller' means the ECB, and in particular the competent organisational unit within the ECB which, alone or jointly with others, determines the purposes and means of the processing of personal data and which is responsible for the processing operation.

(6) 'Union institutions and bodies' means Union institutions and bodies as defined in point (10) of Article 3 of Regulation (EU) 2018/1725.

Article 3

Application of restrictions

1. The controller may restrict the rights referred to in Article 1(2) to safeguard the interests and objectives referred to in Article 25(1) of Regulation (EU) 2018/1725, in particular where the exercise of those rights would jeopardise or otherwise adversely affect:

(a) the performance of the ECB's supervisory tasks under Regulation (EU) No 1024/2013, including the proper functioning of the supervisory system;

(b) the safety and soundness of credit institutions and the stability of the financial system within the Union and each Member State;

(c) the effectiveness of the reporting of breaches in accordance with Article 23 of Regulation (EU) No 1024/2013.

2. To safeguard the interests and objectives referred to in Article 25(1) of Regulation (EU) 2018/1725, the controller may restrict the rights referred to in Article 1(2) in relation to personal data obtained from other Union institutions and bodies and competent authorities of Member States or third countries or international organisations, in any of the following circumstances:

(a) where the exercise of those rights could be restricted by other Union institutions and bodies, from which the personal data was obtained, 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 and bodies;

(b) where the exercise of those rights could be restricted by the competent authorities of Member States, from which the personal data was obtained, on the basis of acts referred to in Article 23 of Regulation (EU) 2016/679 of the European Parliament and of the Council ([4]), 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 ([5]);

(c) where the exercise of those rights could jeopardise or otherwise adversely affect the ECB's cooperation with third countries or international organisations, from which the information was obtained, in the conduct of its tasks, unless the ECB's interest in cooperation is overridden by the interests or fundamental rights and freedoms of the data subjects.

([4]) 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).

([5]) 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).

3. Before applying a restriction in the circumstances referred to in paragraphs 2(a) and (b), the controller shall:

(a) take note of arrangements concluded with the relevant Union institutions and bodies or the competent authorities of Member States; and

(b) consult with the relevant Union institutions and bodies or the competent authorities of Member States unless it is clear to the controller that the application of that restriction is provided for by one of the acts or measures referred to in paragraphs 2(a) and (b).

4. The controller may only apply a restriction where on a case-by-case assessment it concludes that the restriction:

(a) is necessary and proportionate taking into account the risks to the rights and freedoms of the data subject; and

(b) respects the essence of the fundamental rights and freedoms in a democratic society.

5. The controller shall document its assessment in an internal assessment note which shall include the legal basis, the reasons for the restriction, the rights of the data subjects that are restricted, the data subjects affected, the necessity and proportionality of the restriction and the likely duration of the restriction.

6. A decision to restrict the rights of a data subject pursuant to this Decision to be taken by the controller shall be made at the level of the relevant business area head or deputy head in whose business area the main processing operation involving the personal data is carried out.

Article 4

Derogations

1. For processing for scientific or historical research purposes or statistical purposes, the controller may apply derogations in accordance with Article 25(3) of Regulation (EU) 2018/1725. To that end, the controller may derogate from the rights referred to in Articles 17, 18, 20 and 23 of Regulation (EU) 2018/1725 in accordance with the conditions provided for in Article 25(3) of that Regulation.

2. For processing for archiving purposes in the public interest, the controller may apply derogations in accordance with Article 25(4) of Regulation (EU) 2018/1725. To that end, the controller may derogate from the rights referred to in Articles 17, 18, 20, 21, 22 and 23 of Regulation (EU) 2018/1725 in accordance with the conditions provided for in Article 25(4) of that Regulation.

3. Such derogations shall be subject to appropriate safeguards in accordance with Article 13 of Regulation (EU) 2018/1725 and Article 8 of this Decision.

Article 5

Provision of general information on restrictions

The controller shall provide general information on the potential restriction of data subject rights as follows:

(a) the controller shall specify the rights which may be restricted, the reasons for restriction and the potential duration;

(b) the controller shall include the information referred to in point (a) in its data protection notices, privacy statements and records of processing activities as referred to in Article 31 of Regulation (EU) 2018/1725.

Article 6

Restriction of right of access by data subjects, right to rectification, right of erasure or restriction of processing

1. Where the controller restricts, wholly or partially, the right of access, the right to rectification, the right of erasure or the right to restriction of processing, respectively referred to in Articles 17, 18, 19(1) and 20(1) of Regulation (EU) 2018/1725, it shall, within the period referred to in Article 11(5) of Decision (EU) 2020/655 (ECB/2020/28), inform the data subject concerned, in its written reply to the request, of the restriction applied, the principal reasons for the restriction and 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.

2. The controller shall keep the internal assessment note referred to in Article 3(5) and, where applicable, the documents containing underlying factual and legal elements and make these available to the European Data Protection Supervisor on request.

3. The controller may defer, omit or deny the provision of information concerning the reasons for the restriction referred to in paragraph 1 for as long as that provision of information would undermine the purpose of the restriction. As soon as the controller determines that providing the information no longer undermines the purpose of the restriction, the controller shall provide that information to the data subject.

Article 7

Duration of restrictions

1. The controller shall lift a restriction as soon as the circumstances that justified that restriction no longer apply.

2. Where the controller lifts a restriction pursuant to paragraph 1, the controller shall promptly:

(a) to the extent it has not already done so, inform the data subject of the principal reasons on which the application of a restriction was based;

(b) inform the data subject of his or her right to lodge a complaint with the European Data Protection Supervisor or to seek a judicial remedy before the Court of Justice of the European Union;

(c) grant the data subject the right that was subject to the restriction that has been lifted.

3. The controller shall reassess every six months the need to maintain a restriction applied pursuant to this Decision and shall document its reassessment in an internal assessment note.

Article 8

Safeguards

The ECB shall apply organisational and technical safeguards as set out in the Annex to prevent abuse or unlawful access or transfer.

Article 9

Review by the data protection officer

1. Where the controller restricts the application of a data subject's rights, it must continuously involve the DPO. In particular, the following shall apply:

(a) the controller shall, without undue delay, consult the DPO;

(b) on the DPO's request, the controller shall provide the DPO with access to any documents containing underlying factual and legal elements, including the internal assessment note referred to in Article 3(5);

(c) the controller shall document how the DPO was involved including relevant information that was shared, in particular the date of its first consultation as referred to in point (a);

(d) the DPO may request the controller to review the restriction;

(e) the controller shall inform the DPO in writing of the outcome of the review requested without undue delay and in any case before any restriction is applied.

2. The controller shall inform the DPO when the restriction has been lifted.

Article 10

Entry into force

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

Done at Frankfurt am Main, 7 September 2021.

The President of the ECB
Christine LAGARDE

ANNEX

Organisational and technical safeguards at the ECB to prevent abuse or unlawful access or transfer include:

(a) as regard persons:

(i) all persons who have access to non-public ECB information being responsible for knowing and applying the ECB's policy and rules on the management and confidentiality of information;

(ii) a security clearance process which ensures that only vetted and authorised persons have access to the ECB premises and its non-public information;

(iii) IT, information and physical security awareness measures;

(iv) trainings which are regularly held for members of staff and external service providers;

(v) members of staff of the ECB being subject to strict rules of professional secrecy set out in the ECB Conditions of Employment and Staff Rules, the breach of which gives rise to disciplinary sanctions;

(vi) rules and obligations governing external service providers' or contractors' access to non-public ECB information which are set out in contractual arrangements;

(vii) access controls including security zoning which are enforced ensuring that access of persons to ECB non-public information is authorised and restricted based on business needs and security requirements;

(b) as regard processes:

(i) processes being in place to ensure the controlled implementation, operation and maintenance of IT applications supporting the ECB's business;

(ii) using IT applications for the ECB's business which comply with the ECB's security standards;

(iii) having a comprehensive physical security programme in operation which continuously assesses security threats and encompasses physical security measures to ensure an adequate level of protection;

(c) as regard technology:

(i) all electronic data being stored in IT applications complying with the ECB's security standards and thus being protected against unauthorised access or alteration;

(ii) IT applications being implemented, operated and maintained at a level of security commensurate to the IT applications' confidentiality, integrity and availability needs, which are based on business impact analyses;

(iii) the level of security of IT applications being regularly validated through technical and non-technical security assessments;

(iv) access to ECB non-public information being granted in accordance with the need-to-know principle, and privileged access being strictly limited and tightly controlled;

(v) controls being implemented to detect and follow up on actual and potential security breaches.