EBA/DC/2021/377

EBA Regular Use

Decision of the European Banking Authority

of 23 April 2021

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 European Banking Authority

The Management Board

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

Having regard to Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 establishing a European Supervisory Authority (European Banking Authority), amending Decision No 716/2009/EC and repealing Commission Decision 2009/78/EC[2], in particular Article 47(1) and 71 thereof,

Whereas:

(1) The European Banking Authority ('EBA') carries out its activities in accordance with Regulation (EU) No 1093/2010 as may be further amended, repealed or replaced.

(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

1. OJ L 295, 21.11.2018, p. 39.
1. OJ L331, 15.12.2010, p. 12.

internal rules to be adopted by the EBA, where these are not based on legal acts adopted on the basis of the Treaties.

(3) Where the EBA 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.

(4) The EBA processes several categories of personal data, including 'objective' data (such as identification data, contact data, professional data, administrative details, data received from specific sources, electronic communications and traffic data) and/or 'subjective' data (related to the case such as reasoning, behavioural and conduct data and data related to or brought forward in connection with the subject matter of the procedure or activity.

(5) The EBA, represented by its Executive Director, acts as the data controller irrespective of further delegations of the controller role within the EBA to reflect operational responsibilities for specific personal data processing operations.

(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 records and privacy statements of the EBA.

(7) For the exercise of its missions, the EBA is bound to respect to the maximum extent possible, the fundamental rights of the 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 enshrined in Regulation (EU) 2018/1725.

(8) However, the EBA may be obliged to restrict the information to data subjects or other data subject rights to protect, in particular, the confidentiality and effectiveness of 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.

(9) Within the framework of its administrative functioning, the EBA may conduct a number of investigations, such as administrative inquiries, disciplinary proceedings, preliminary activities related to financial fraud, investigations relating to whistleblowing or harassment cases, internal audits, investigations performed by the Data Protection Officer (DPO) or ethics investigations, ICT investigations, information security investigations and activities performed in the context of security risks and incidents management. In addition, for the exercise of its missions, the EBA may conduct investigations relating to potential breaches of Union law, settlement of disagreements between competent authorities, mediation conducted between competent authorities as well as investigations related to the prevention and countering of money laundering and of terrorist financing, inquiries related to consumer protection and financial activities in order to assess potential threats to the integrity of financial markets or the stability of the financial system in the Union.

(10) The internal rules should apply to all processing operations carried out by the EBA in the performance of the above investigations. They should also apply to processing operations carried out prior to the opening of the investigations referred to above, during these investigations and during the monitoring of the follow-up to the outcome of these investigations. It should also include assistance, coordination and/or cooperation requested from the EBA by national authorities and international organisations in the context of their own administrative investigations.

(11) Before making use of the restrictions foreseen in these internal rules, the EBA should consider whether any of the exemptions laid down in Regulation (EU) 2018/1725 applies. In the cases where restrictions under these internal rules apply, the EBA has to explain why these restrictions are strictly necessary and proportionate in a democratic society and respect the essence of the fundamental rights and freedoms.

(12) The EBA should monitor if the conditions that justify the restriction continue to apply and lift the restriction when they no longer apply.

(13) The Controller should inform the Data Protection Officer when restricting the application of certain data subjects' rights under this Decision, when extending such restriction and when the restriction is lifted,

Has decided as follows:

Article 1 – Subject matter and scope

1. This Decision lays down internal rules relating to the conditions under which the EBA in the framework of the activities set out in paragraphs 2 to 5 may restrict the application of the rights enshrined in Articles 14 to 21, and 35, as well as Article 4 thereof, following Article 25 of Regulation (EU) 2018/1725. These restrictions are without prejudice to the exemptions to data subject rights provided in Regulation (EU) 2018/1725.

2. Within the framework of the administrative functioning of the EBA, the restrictions foreseen in paragraph 1 apply to the processing of personal data by the EBA for the purpose of:

   (a) administrative inquiries and disciplinary proceedings, in accordance with Article 25(1) point (f) of Regulation (EU) 2018/1725;

   (b) processing irregularities in liaison with the European Anti-Fraud Office (OLAF), in accordance with Article 25(1) points (b) or (f) of Regulation (EU) 2018/1725;

   (c) processing whistleblowing cases, (formal and informal) harassment cases as well as internal and external complaints, in accordance with Article 25(1) point (f) of Regulation (EU) 2018/1725;

(d) internal audits, ethics investigations, inquiries, proceedings and investigations performed by the Data Protection Officer ('the DPO') in line with Article 25(1) points (f) or (g) or Article 45(2) of Regulation (EU) 2018/1725;

(e) ICT investigations, information security investigations and activities performed in the context of security risks and incidents management, handled internally or with external involvement, in accordance with Article 25(1) point (d) of the Regulation (EU) 2018/1725.

3. Within the exercise of the EBA's missions, the restrictions foreseen in paragraph 1 apply to the processing of personal data by the EBA for the purpose of any of the following:

(a) investigations of potential breaches of Union law pursuant to Article 17 of Regulation (EU) No 1093/2010;

(b) inquiries and proceedings related to consumer protection and financial activities in order to assess potential threats to the integrity of financial markets or the stability of the financial system in the Union pursuant to Articles 9 and 22 of Regulation (EU) No 1093/2010;

(c) proceedings related to the settlement of disagreements between competent authorities pursuant to Article 19 of Regulation (EU) No 1093/2010 and legislative acts referred to in Article 1(2) of that Regulation;

(d) proceedings related to non-binding mediation carried out by the EBA pursuant to Article 31(2)(c) of Regulation (EU) No 1093/2010 and legislative acts referred to in Article 1(2) of that Regulation (EU);

(e) investigations related to the prevention and countering of money laundering and of terrorist financing pursuant to Article 9b of Regulation (EU) No 1093/2010 and legislative acts referred to in Article 1(2) of that Regulation.

4. In addition, these restrictions apply to assistance, coordination and/or cooperation provided by the EBA to competent authorities as defined in Article 4 point (2) of Regulation (EU) No 1093/2010, including third country authorities, and international organisations in the context of the investigations conducted for the exercise of their statutory missions.

5. The restrictions referred to in paragraph 1 also apply to processing operations carried out prior to the opening of the investigations or other administrative enquiries referred to in paragraphs 2 to 4, during these investigations and during the monitoring of the follow-up to the outcome of these investigations.

6. This Decision applies to any category of personal data processed in the context of the activities set out in paragraphs 2 to 5.

7. Subject to the conditions set out in this Decision the restrictions may apply to the following rights: provision of information to data subjects, right of access, rectification, erasure, restriction of processing and communication of a personal data breach to the data subject.

Article 2 - Controller in charge of investigations and applicable safeguards

1. The safeguards in place to prevent abuse or unlawful access or transfer in the context of the investigations referred to in Article 1 are the following:

   (a) paper documents shall be kept in locked cupboards which are only accessible to authorized staff members on a need-to know basis. The security system of the premises, internal record management policies, staff training and audits shall also be in place to ensure proper safeguards;

   (b) electronic files shall be managed with the EBA's approved devices, information systems, applications and storage media resources. The data shall be stored in a secure electronic environment which is designed and maintained to prevent accidental or unlawful destruction, loss, alteration, transfer, unauthorized disclosure of, or access to, personal data to internal and external partners who are not authorized to have access to such data. The EBA's document management system applications shall be used to organise, find, share, maintain and protect the EBA's electronic data. Authorised EBA staff shall only be granted access to electronic data based on a need to know basis;

   (c) databases and electronic files shall be password-protected under a single sign-on system and connected automatically to the user's ID and password. Replacing users is strictly prohibited. Electronic records shall be held securely to safeguard the confidentiality and privacy of the data therein;

   (d) all persons having access to the data shall be bound by the obligation of confidentiality and shall sign a document acknowledging that obligation and the requirements set out in this paragraph.

2. The Controller of the processing operations is the EBA, represented by its Executive Director. Data subjects shall be informed of the delegated controller by way of the data protection records published on the website of the EBA.

3. The retention period of the personal data processed shall be no longer than necessary and appropriate for the purposes for which the data are processed. The retention period shall be specified in the data protection records and privacy statements referred to in Article 5(1).

4. Where the EBA considers applying 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 EBA'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.

Article 3 - Restrictions

1. Pursuant to Article 25(1) of Regulation (EU) 2018/1725, any restriction shall only be applied by the EBA to safeguard:

   (a) 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, in particular in relation to the processing operations under Article 1(2) point (b) of this Decision;

   (b) 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 in particular in relation to the processing operations under Article 1(3) of this Decision;

   (c) the internal security of Union institutions and bodies, including of their electronic communications networks, in particular in relation to the processing operation under Article 1(2) point (c) of this Decision;

   (d) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions, in particular in relation to the processing operations under Article 1(2) points (a) and (c) of this Decision;

   (e) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) and (b), in particular in relation to the processing operations under Article 1(2) point (d) of this Decision;

   (f) the protection of the data subject or the rights and freedoms of others.

2. As a specific application of the purposes described in paragraph 1 above, the EBA may apply restrictions in relation to personal data exchanged with Commission services or other Union institutions, bodies, agencies and offices, competent authorities of Member States or third countries or international organisations, if one or more of the following circumstances occurs:

   (a) where the exercise of those rights and obligations could be restricted by Commission services or other Union institutions, bodies, agencies and offices 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;

   (b) where the exercise of those rights and obligations could be restricted by competent authorities of Member States on the basis of acts referred to in Article 23 of Regulation

(EU) 2016/679 of the European Parliament and of the Council, 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;

(c) where the exercise of those rights and obligations would jeopardise the EBA's cooperation with third country or international organisations in the conduct of its tasks or of the tasks of the third country or international organisations.

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

3. Any restriction 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.

4. If the application of restriction is considered, a necessity and proportionality test shall be carried out based on the present rules. It shall be documented through an internal assessment note for accountability purposes on a case by case basis.

5. Restrictions shall be lifted as soon as the circumstances that justify them no longer apply. 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.

Article 4 - Review by the Data Protection Officer

1. The Controller shall, without undue delay, inform the DPO whenever the Controller intends to restrict the application of data subjects' rights, or extends the restriction, in accordance with this Decision. The Controller shall provide the DPO access to the internal note containing the assessment of the necessity and proportionality of the restriction as well as, where applicable, underlying factual and legal elements and document the date of informing the DPO.

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 Controller shall inform the DPO when the restriction has been lifted.

4. The Controller shall document the involvement of the DPO along the different steps of the process, starting with the date of informing the DPO.

5. The internal note, and, where applicable, underlying factual and legal elements shall be made available to the European Data Protection Supervisor on request.

Article 5 - Provision of information to data subject

1. The EBA shall publish on its website data protection records that inform all data subjects of its activities involving processing of personal data, including information relating to the potential restriction of data subject rights pursuant to Article 3 of this Decision. The information shall cover which rights may be restricted, the grounds on which restrictions may be applied, and their potential duration.

2. The EBA shall individually notify all data subjects, whom it considers persons concerned by the investigation or inquiry, of the data protection record of the specific processing operations concerned, without undue delay and in a written form.

3. In duly justified cases and under the conditions stipulated in this decision, the EBA may restrict, wholly or partly, the provision of information to the data subjects referred to in paragraph 2. In this case, it shall document in an internal note the reasons for the restriction, the legal ground in accordance with Article 3 of this Decision, including an assessment of the necessity and proportionality of the restriction.

4. The restriction referred to in paragraph 3 shall continue to apply as long as the reasons justifying it remain applicable.

   Where the reasons for the restriction no longer apply, the EBA shall notify the data subject concerned of the relevant data protection record and the principal reasons for the restriction. This notification can be combined with an invitation to make submission on the findings of the investigation or inquiry underway, as part of the exercise of the rights of defence of the data subject concerned. At the same time, the EBA shall inform the data subject concerned of the right of lodging a complaint with the European Data Protection Supervisor at any time or of seeking a judicial remedy in the Court of Justice of the European Union.

   The EBA shall review the application of the restriction every six months from its adoption and at the closure of the relevant inquiry or investigation.

Article 6 - Right of access by data subject

1. Further to a data subject request, the EBA may restrict, wholly or partly, the right of this data subject to obtain confirmation as to whether or not personal data concerning him or her are being processed by the EBA in the context of an investigation or inquiry referred to in Article 1 of this Decision, and where that is the case, the right of access to this data and other information referred to in Article 17 of Regulation (EU) 2018/1725.

2. Where the EBA restricts the right of access, it shall inform the data subject concerned, in its reply to the request, 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.

3. The provision of information referred to in paragraph 2 may be deferred, omitted or denied if it would cancel the effect of the restriction imposed in accordance with Article 25(8) of Regulation (EU) 2018/1725. Where this is the case, the EBA shall document in an internal assessment note the reasons for the restriction, including an assessment of the necessity, proportionality of the restriction and its duration.

4. The EBA shall review the application of the restriction every six months from its adoption and at the closure of the relevant inquiry or investigation.

Article 7 - Right of rectification, erasure and restriction of processing

1. Further to a data subject request, the EBA may, in the context of an investigation or inquiry referred to in Article 1 of this Decision, restricts, wholly or partly, the right of this data subject to obtain rectification of personal data related to him or her, to erase or to restrict processing of his or her personal data as provided for in Articles 18, 19 and 20 of Regulation (EU) 2018/1725.

2. Where the EBA restricts the application of the right to rectification, erasure or restriction of processing referred to above, it shall take the steps set out in Articles 6(2) and document it in accordance with Article 6(3).

3. The EBA shall review the application of the restriction every six months from its adoption and at the closure of the relevant inquiry or investigation.

Article 8 - Communication of a personal data breach to the data subject

1. The EBA shall communicate a personal data breach to the data subject concerned without undue delay when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons as provided for in Article 35 of Regulation (EU) 2018/1725.

2. In duly justified cases and under the conditions stipulated in this decision, the EBA may restrict, wholly or partly, the provision of information to the data subjects referred to in paragraph 1 of this Article. In this case, it shall document in an internal note the reasons for the restriction, the legal ground in accordance with Article 3 of this Decision, including an assessment of the necessity and proportionality of the restriction.

3. The restriction referred to in paragraph 2 shall continue to apply as long as the reasons justifying it remain applicable.

   Where the reasons for the restriction no longer apply, the EBA shall communicate the personal data breach to the data subject concerned and inform the data subject of the principal reasons for the restriction. At the same time, the EBA shall inform the data subject concerned of the right of lodging a complaint with the European Data Protection Supervisor at any time or of seeking a judicial remedy in the Court of Justice of the European Union.

   The EBA shall review the application of the restriction every six months from its adoption and at the closure of the relevant inquiry or investigation.

Article 9 - 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 Paris, 23 April 2021

José Manuel Campa
Chairperson

For the Management Board