DECISION OF THE SINGLE RESOLUTION BOARD

of 18 September 2019

on internal rules concerning restrictions of certain rights of data subjects in relation to processing of personal data in the framework of internal security incident investigations carried out by the Single Resolution Board (SRB/ES/2019/34)

THE SINGLE RESOLUTION BOARD,

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

Having regard to Regulation (EU) No 806/2014 of the European Parliament and of the Council of 15 July 2014 establishing uniform rules and a uniform procedure for the resolution of credit institutions and certain investment firms in the framework of a Single Resolution Mechanism and a Single Resolution Fund and amending Regulation (EU) No 1093/2010 ([1]) and in particular, Articles 42, Article 43(5), Articles 50(3), 56(1)-(3), 61, 63 and 64 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 ([2]),

Having regard to the consultation with the European Data Protection Supervisor,

Whereas:

(1) The Single Resolution Board ('**SRB**') fulfils the tasks of a resolution authority as part of the Single Resolution Mechanism (**'SRM'**) in accordance with Regulation (EU) No 806/2014. The SRB's mission is to ensure an orderly resolution of failing banks with minimum impact on the real economy, the financial system, and the public finances of the participating MS and beyond.

(2) The SRB can process personal data for the various systems installed at the SRB premises (video-surveillance, access control, visitors log books). This information is strictly collected for security & safety reasons (e.g. to keep track of how many people are in the building for evacuation purposes, both in line with EC's security decisions), to prevent, detect and document any security incident that occurs inside the buildings or surrounding areas.

(3) The SRB, here represented by the SRB Head of Unit Corporate Services and ICT, processes several categories of personal data, and particularly identification data, contact data, professional data. The personal data are stored in a secured electronic environment which prevents unlawful access or transfer of data to persons who do not have a need to know. The personal data processed are retained in accordance with the EC rules on retention of data. At the end of the retention period, the collected information including personal data is deleted in accordance with the maximum agreed period: visitors log books: 6 months, video surveillance system: 30 days, access control system: 2 months.

(4) The internal rules should apply to all processing operations carried out by the SRB in the performance of its activities for the security & safety matters, for the prevention, detection or investigation of security incidents, protection of the agency's staff, property and information and the SRB's visitors.

(5) The internal rules should apply to processing operations carried out during internal security incident investigations, as well as during the monitoring of the follow-up to the outcome of these investigations. The internal rules should apply to processing operations which form part of the activities linked to the SRB Security/Facilities' sector. It should also include assistance and cooperation provided by the SRB Security/Facilities to national authorities, Belgian Law forces, OLAF, the Emergency services and international organisations outside of its administrative investigations;

(6) The SRB has to give justifications explaining why the restrictions are strictly necessary and proportionate in a democratic society and respect the essence of the fundamental rights and freedoms;

([1]) OJ L 225, 30.7.2014, p. 1.
([2]) OJ L 295, 21.11.2018, p. 39.

(7) Within this framework SRB 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 access and rectification, right to erasure, data portability etc. as enshrined in Regulation (EU) 2018/1725;

(8) However, the SRB may be obliged to defer the information to data subject and other data subject's rights to protect, in particular, its own security incident investigations involving the data from the video surveillance or access control systems.

(9) The SRB may thus defer the information for the purpose of protecting the security incident investigations;

(10) The SRB should lift the restriction as soon as and as far as the conditions that justify the restriction no longer apply;

(11) The SRB should monitor the restricting conditions on a regular basis, every six months and revise where needed;

(12) The SRB should consult the DPO during the revisions.

HAS ADOPTED THIS DECISION:

Article 1

Subject matter and scope

1. This Decision lays down internal rules relating to the conditions under which the SRB in the framework of internal security incident investigations, may restrict the application of the rights enshrined in Articles 14 to 21, 35, as well as Article 4 thereof, following Article 25 of the Regulation (EU) 2018/1725.

2. This Decision applies to the processing operation(s) of personal data by the SRB for the purpose of conducting internal security incident investigations, as well as during the monitoring of the follow-up to the outcome of these investigations.

3. The categories of data concerned are hard data (administrative details, telephone, private address, electronic communications, and traffic data and/or soft data (appraisals, opening of inquiries, reports on preliminary investigations) etc.

4. Subject to the conditions set out in this Decision, the restrictions may apply to the following rights: access, rectification, erasure and portability rights, rights of information, confidentiality of communication, and principles of the data processing operation provided that they relate to a right.

Article 2

Specification of the controller and safeguards

1. The safeguards in place to avoid data breaches, leakages or unauthorised disclosure are the following: restriction of access rights to electronic folders and to the functional mailbox for submission of complaints, cupboards secured with keys, and specific training of the persons handling the information on confidentiality.

2. The controller of these processing operations is the SRB, here represented by the SRB Head of Unit Corporate Services and ICT.

3. The personal data collected are stored and retained in accordance with the EC rules on retention of data and in accordance with the Belgian law of 21/3/2007 (governing the installation and use of surveillance cameras). The retention period respects the principle of retention no longer than necessary for the fulfilment of the purpose of the processing operation, and eventually, to allow judicial or administrative disputes.

Article 3

Restrictions

1. In accordance with Article 25(1) of Regulation (EU) No 2018/1725, any restriction shall only be applied to safeguard:

— 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;

— the internal security of Union institutions and bodies, including of their electronic communications networks;

— the protection of judicial proceedings;

— the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

— the protection of the data subject or the rights and freedoms of others;

2. Any restriction shall be necessary and proportionate in a democratic society and respect the essence of the fundamental rights and freedoms.

3. A necessity and proportionality test shall be carried out based on the present internal rules. It shall be documented through an internal assessment note for accountability purposes on a case by case basis.

4. Restrictions shall be duly monitored and a periodical revision shall be done every six months.

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

6. The risk to the rights and freedoms of the data subject is the temporary limitation of the effective exercise of the data subject's rights, inter alia, to information, erasure or defence, as guaranteed by the Regulation (EU) 2018/1725. These risks shall be taken into account in the scope of the necessity and proportionality test mentioned under paragraph 3 of this Article.

Article 4

Involvement of the Data Protection Officer

1. The SRB shall, throughout the restriction procedure and without undue delay, inform the Data Protection Officer of the SRB ('the DPO') whenever it restricts the application of data subjects' rights in accordance with this Decision. It shall provide access to the record and the assessment of the necessity and proportionality of the restriction.

2. The DPO may request the controller in writing to review the application of the restrictions. The SRB shall inform the DPO in writing about the outcome of the requested review and when the restriction is lifted.

Article 5

Provision of information to data subject

1. The SRB shall include in the data protection notices published on its intranet and website 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.

2. Additionally, the SRB shall inform individually data subjects on their rights concerning present or future restrictions without undue delay and in a written form, without prejudice of the following paragraph.

3. Data subjects shall be informed on the principal reasons on which the application of a restriction is based and of their right to lodge a complaint before the European Data Protection Supervisor.

Article 6

Right of access by data subject

1. 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 SRB shall limit its assessment of the request to such personal data only.

2. Where the SRB restricts, wholly or partly, the right of access, referred to in Article 17 of Regulation (EU) 2018/1725, it shall take the following steps:

(a) 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;

(b) 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 providing access would jeopardise the purpose of the SRB's investigative activities or of restrictions applied pursuant to Article 2(3), or would adversely affect the rights and freedoms of other data subjects.

The provision of information referred to in point (a) may be deferred, omitted or denied in accordance with Article 25(8) of Regulation (EU) 2018/1725.

3. The record referred to in point (b) of paragraph 2 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 25(7) of Regulation (EU) 2018/1725 shall apply.

Article 7

Right of rectification, erasure and restriction of processing

Where the SRB restricts, wholly or partly, the application of the right to rectification, erasure or restriction of processing, referred to in Articles 18, 19(1) and 20(1) of Regulation (EU) 2018/1725, it shall take the steps set out in Article 6(2) of this Decision and register the record in accordance with Article 6(3) thereof.

Article 8

Communication of a personal data breach to the data subject

Where the SRB restricts the communication of a personal data breach to the data subject, referred to in Article 35 of Regulation (EU) 2018/1725, it shall record and register the reasons for the restriction in accordance with Article 3(3) of this Decision. Article 3(4) of this Decision shall apply.

Article 9

Entry into force

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

Done at Brussels, 18 September 2019.

For the Single Resolution Board
Elke KÖNIG
The Chair