Opinion on a notification for Prior Checking received from the Data Protection Officer of the European Central Bank regarding the "Breach Reporting Mechanism (BRM)"

Brussels, 3 November 2014 (2014-0871)

1. Proceedings

On 12 September 2014, the European Data Protection Supervisor (**EDPS**) received a notification for prior checking under Article 27 of Regulation (EC) 45/2001[1] (the Regulation) relating to the processing of personal data in the Breach Reporting Mechanism (**BRM**) from the Data Protection Officer (**DPO**) of the European Central Bank (**ECB**).

Questions were raised on 17 September 2014, to which the ECB replied on 23 September 2014; on 17 October 2014, the ECB supplied additional clarifications in reply to questions asked on 15 October 2014. The draft Opinion was sent to the DPO for comments on 28 October 2014. The EDPS received a reply on 29 October 2014, with additional documentation being provided on 30 October 2014.

2. The facts

2.1. Description of the processing: incoming reports

According to Article 23 of Council Regulation (EU) 1024/2013 (the Single Supervisory Mechanism (SSM) Regulation)[2], the ECB should ensure that effective mechanisms for reporting breaches of the legislation referred to in Article 4(3) of the same Regulation are put in place.[3]

Article 23 of the SSM Regulation reads as follows:

> "*The ECB shall ensure that effective mechanisms are put in place for reporting of breaches by credit institutions, financial holding companies or mixed financial holding companies or competent authorities in the participating Member States of the legal acts referred to in Article 4(3) [all relevant Union law], including specific procedures for the receipt of reports of breaches and their follow-up. Such procedures shall be consistent with relevant Union legislation and shall ensure that the following principles are applied: appropriate protection for persons who report breaches, protection of personal data, and appropriate protection for the accused person*".

[1] OJ L 8 12.01.2001, p. 1-22.
[2] OJ L 287, 29.10.2013, p. 63-89.
[3] This Article refers broadly to "all relevant Union law". This includes a wide range of banking legislation, dealing with matters such as the authorisation of credit institutions, verifying the aptitude of high management staff and board members, robust governance arrangements, remuneration policies and practices, internal capital adequacy assessment processes, stress tests, publication requirements, liquidity requirements.

To fulfil this task, the ECB will provide the BRM, through which the Breach Reporting Unit (BRU) will assess incoming cases and further despatch them to the relevant business area of the ECB or the relevant NCA for them to conduct the investigation.

The ECB is the controller, while the practical processing will be carried out by the BRU in the Enforcement and Sanctions Division of Directorate-General Micro-Prudential Supervision IV (DGMS IV).

The BRM will allow informants to provide information on possible breaches of the legislation referred to in Article 4(3) of the SSM Regulation (SSM-related breaches), irrespective of whether they have been committed by supervised entities (i.e. credit institutions), national competent supervisory authorities (NCAs) or the ECB itself. While SSM-related breaches are the reason for this procedure, it cannot be excluded that non-SSM-related suspected breaches might be reported as well.

Information on breaches can be provided without providing contact details, if the informant so wishes.[4] The information will first be provided via a structured web form as an interim solution pending the implementation of a permanent solution (see also section 2.6 below).[5] When a report is received, it is transferred to the BRU and stored in a case file.

Personal data concerning the following categories of data subjects may be included in the BRU case file:

1) Persons who have provided information to the ECB (informants);
2) Persons suspected of breaching/having breached relevant Union law (accused persons);
3) Persons who may be involved in or are affected by the procedure and who are named in the information provided by the informant (persons involved);
4) Staff of ECB or NCA working on the file (staff);
5) Other persons who may appear in the information provided or the ECB case file, but have no relevance to the case (other persons).

The categories of personal data that may be processed relate to the content of the allegations, earlier contacts with NCAs, persons responsible for the alleged breach, information on where/how to find additional evidence etc. To this end, the ECB provides a web form collecting information, including free text fields. The permanent solution will also provide the possibility to upload attachments. In the interim solution, informants can provide further documents via electronic or physical mail.

2.2. Description of the processing: analysis and forwarding of reports

BRU does not conduct a investigation of the cases, but only assesses the relevance of the information provided and then decides on how to proceed with the case ("relevance assessment procedure"). The result of this assessment is documented in a final note:

1. Cases relevant for the ECB: BRU forwards relevant information within ECB
    a. If the case is relevant for the ECB's SSM-related tasks, the final note will be disclosed to the relevant business area(s) of the ECB[6];
    b. If the case does not concern a breach of relevant Union law, but is otherwise relevant for ECB's tasks (except as under d below), the final note is transferred

[4] In this case, the informant is provided with an automatically generated reference number that he/she may use to link further anonymous submissions to the initial report. Informants are however invited to provide an e-mail address for further communication.

[5] This is the only suggested way of filing reports. However, it cannot be excluded that the ECB might receive reports in other ways, e.g. by postal letter. In these cases, the information is transferred to BRU for handling in the relevance assessment procedure. Reports via phone will be redirected to BRU, who will first suggest using the web form or the permanent solution, once ready; if the prospective informant declines this suggestion, BRU will take note of the report.

[6] E.g. the relevant joint supervisory team in DGMS I or II.

to the ECB's coordination function for the determination of and onward transfer to the relevant ECB business area;

c. If the case concerns both SSM-related aspects and non-SSM-related aspects, BRU and the coordination function will decide on the follow-up on a case-by-case basis; the case will be forwarded to the relevant ECB business area(s). If the different aspects of the case can be split, they will be;
d. If the case concerns professional misconduct of an employee of the ECB or a NCA, the ECB's Directorate Internal Audit (D-IA) will be notified.
    i. if the case concerns an ECB staff member, D-IA will handle the case according to its rules on administrative inquiries and disciplinary proceedings[7];
    ii. If the case appears to be symptomatic of a systemic risk, D-IA will refer it to the Internal Auditors Committee (IAC) in SSM composition, including the relevant NCA;
    iii. If the case concerns an NCA staff member working for a Joint Supervisory Team (JST), [and the ECB is not competent to follow up on this matter, the BRU will notify the informant of its lack of competence[8]]

2. Cases relevant for NCAs: BRU forwards relevant information to NCAs
    a. Alleged breach of relevant Union law by less significant entity[9] (i.e. SSM-related): the case will be forwarded to the relevant NCA;
    b. Alleged criminal offence: whenever the ECB, in carrying out its tasks under the SSM Regulation, has reason to suspect that a criminal offence may have been committed, the matter will be referred to the relevant NCA with the advice to refer it to the competent authorities for investigation and possible prosecution; this may also be used when the BRU considers that a report was not made in good faith;
3. If the case is not relevant for any of the above categories, it will be closed.

These possibilities fall into three groups: SSM-related (1.a, parts of 1.c, parts of 1.d., 2) and non SSM-related (1.b, parts of 1.c, 1.d and, possibly, 2(b), see below point 3.6.2) and clearly irrelevant cases.

For SSM-related cases ("protected reports"), the final note to be transferred to the relevant NCA will not reveal the identity of informants unless they have provided prior explicit consent (the ECB announced that the final web form will ask prospective informants "*Do you consent to the ECB forwarding your personal data to NCAs if relevant for the follow up procedure on your report?*"). As an exception to this rule, their personal data might be disclosed to national authorities where required by a court order in the context of follow-up investigations or where required for judicial proceedings. For SSM-related cases relevant for the ECB, the final note forwarded to the recipient within the ECB may include the name of the informant where deemed necessary by BRU.

In the other cases (non-SSM-related), the identity of the informant may be revealed to the recipient, either within the ECB or in an NCA, on a need-to-know-basis.

Irrelevant cases will not be further forwarded by the BRU.

In all cases, personal data of other categories of data subjects may be included in the final note where necessary. For the category of "other persons", the ECB, as a rule, includes their

[7] See EDPS case 2005-0290.

[[8] The ECB informed the EDPS that its approach to this situation has changed compared to the initial notification.]

[9] The criteria for determining whether a supervised entity is significant or less significant are set out in Article 6(4) of the SSM Regulation.

personal data in the note if they are not affected by the procedure; this is assessed on an ad-hoc basis.

Concerning possible transfers to third countries or international organisations, cooperation agreements entered into by NCAs before the ECB takes over their SSM-related tasks will continue to apply, and the ECB may join them, or conclude new cooperation agreements.

If, following the forwarding of the final note, the NCA or ECB business area in charge of the following investigation needs further information from the informant, the BRU will act as a messenger between the parties, relaying requests to the informant (where he/she has provided contact details) and relaying his/her replies back. Additional personal data contained in the informant's replies will only be further transferred to the relevant ECB business area/NCA on a need-to-know basis.

When the investigation conducted by the recipient (NCA or other ECB business area) is finished, BRU is informed about this and about the outcome.

2.3. Information to data subjects

Informants will be shown and requested to acknowledge having read and understood a privacy statement before submitting their report. Other categories of data subject will not be informed by BRU.

If personal data are transferred to another ECB business area or NCA(s), the recipient is reminded of the rules on informing data subjects about the processing of personal data not collected from them, with reference to Article 12 of the Regulation.[10]

2.4. Rights of access and rectification

The ECB applies the standard procedure as per its implementing rules on data protection.[11] Requests are to be submitted in writing to the controller, who shall grant access under Article 13 of the Regulation within three months.

2.5. Conservation periods

The conservation periods in the BRU case files are 5 years from the closing of the BRU case[12] for SSM-related cases, or 14 months from closure for non-SSM-related cases.

2.6. Technical implementation

[…]

3. Legal analysis

3.1. Prior checking

The processing of personal data in the BRM is performed by a Union institution. Furthermore, the processing is done through automatic means. Therefore, Regulation No 45/2001 is applicable.

Article 27 of the Regulation subjects to prior checking by the EDPS processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. Article 27 (2) of the Regulation contains a list of

[10] One exception is if public statements, e.g. by politicians are included in the report and it might be necessary to reproduce them in the final note to provide context; in this case, the recipient would not be reminded of the need to inform this person.

[11] https://www.ecb.europa.eu/ecb/legal/pdf/l_11620070504en00640067.pdf.

[12] The date of closure is defined as the day following approval of final note on the relevance assessment procedure. In case criminal proceedings are started in a Member State following the receipt of information from BRU, the conservation period will be suspended for the duration of these proceedings.

processing operations that are likely to present such risks, including under point (a) the processing of data related to suspected offences, under point (b) processing intended to evaluate personal aspects relating to the data subject, including his or her conduct, and under point (d) processing operations intended to exclude persons from rights, benefits or contracts.

Points (a) and (d) above were indicated by the ECB in its notification as reasons for prior checking.

The BRM itself does not lead to excluding persons from rights, benefits or contracts. It is true that the procedures following the transfer may lead to such consequences, but the BRM is not *intended to* directly lead to such outcomes.[13] It therefore does not fall under point (d) of Article 27(2).

However, as the BRM will process personal data related to (suspected) offences, it is subject to prior checking under Article 27(2)(a).

Additionally, while the BRU will not carry out a full investigation, it will conduct an initial evaluation of accused persons' conduct during the relevance assessment procedure, triggering Article 27(2)(b).

The notification of the DPO was received on 12 September 2014. According to Article 27(4) the present Opinion must be delivered within a period of two months, not counting suspensions for requests for further information. The case was suspended for information from 17 September 2014 to 23 September 2014 and for comments of the DPO from 28 October to 29 October 2014. The EDPS shall thus render its Opinion before 21 November 2014.

3.2. Lawfulness of the processing

The lawfulness of processing has to be based on one of the grounds in Article 5 of the Regulation. According to Article 5(a), processing that is "necessary for performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof" is lawful.

Article 23 of the SSM Regulation, quoted above in section 2.1 clearly entrusts the ECB with providing the BRM for reporting breaches of banking legislation. This is further specified in Regulation (EU) 468/2014 (the SSM Framework Regulation)[14]:

Article 36:

> "*Any person, in good faith, may submit a report directly to the ECB if that person has reasonable grounds for believing that the report will show breaches of the legal acts referred to in Article 4(3) of the SSM Regulation by credit institutions, financial holding companies, mixed financial holding companies or competent authorities (including the ECB itself).".*

Article 37:

> "1.*Where a person makes a report in good faith about alleged breaches of the legal acts referred to in Article 4(3) of the SSM Regulation by supervised entities or competent authorities, the report shall be treated as a protected report.*
>
> *2. All personal data concerning both the person who makes a protected report and the person who is allegedly responsible for a breach shall be protected in compliance with the applicable Union data protection framework.*

[13] For cases of Article 27(2)(d), see e.g. EDPS cases 2010-0426, 2012-0724 to -0726, 2013-0340.
[14] OJ L 141, 14.05.2014, p. 1–50.

> *3. The ECB shall not reveal the identity of a person who has made a protected report without first obtaining that person's explicit consent, unless such disclosure is required by a court order in the context of further investigations or subsequent judicial proceedings.".*

It should be noted that Article 37(2) quoted above has mainly declaratory character: as the ECB is the controller for the BRM, the processing of personal data in it falls under the Regulation. In this respect, non-protected reports (Non SSM related file) will also have to be treated in accordance with the Regulation.

Article 136:

> "*Where, in carrying out its tasks under the SSM Regulation, the ECB has reason to suspect that a criminal offence may have been committed, it shall request the relevant NCA to refer the matter to the appropriate authorities for investigation and possible criminal prosecution, in accordance with national law.".*

According to Article 38 of the SSM Framework Regulation, the ECB "shall assess all reports relating to significant supervised entities" as well as "reports relating to less significant supervised entities in respect of breaches of ECB regulations or decisions".

The BRU may thus lawfully process personal data under Article 5(a) of the Regulation for SSM-related purposes.

As the ECB indicated in the notification, it cannot be excluded that the BRM will also be used to report other issues which do not relate to the SSM, but which might still be relevant for the ECB. It should be noted that the purpose of the BRM as established under the SSM Regulation is to provide a reporting channel for SSM-related breaches. This purpose should be made clear to prospective informants, including reference to other reporting channels where appropriate (see also sections 3.4 and 3.7.1 below), to ensure that the BRM will be used only for SSM-related breaches.

If the ECB then still exceptionally receives reports which are not relevant for the SSM, but which might be relevant for other parts of the ECB (e.g. information on non-SSM related serious professional misconduct), then they may - after the relevance assessment - be forwarded to the relevant part of the ECB, provided the ECB has a legal basis to further process the report, e.g. under its disciplinary rules.[15]

If on the other hand, the ECB wants to create reporting channels for other, non-SSM-related issues, then it should provide a clear legal basis for doing so. This would be a different purpose than for the BRM as established under Article 23 of the SSM Regulation. As under Article 4(1)(b) of the Regulation, the purpose(s) of processing operations have to be among other specific and explicit, the BRM should serve its purpose as established by the SSM Regulation. Reporting channels for other issues would need to be based on other legal bases.

3.3. Processing of special categories of data

The BRM will process personal data related to suspected offences (i.e. the allegations made by informants), one of the categories of Article 10. Due to their sensitivity, the processing of such data is subject to specific rules.

According to Article 10(5) of the Regulation, data related to (suspected) offences may only be processed "*if authorised by the Treaties [...] or other legal instruments adopted on the basis thereof*".

[15] The alternative would be to return the material to the informant with an indication of the appropriate ECB recipient. This would not be good administrative behaviour.

Article 23 of the SSM Regulation and Article 36 of the SSM Framework Regulation (both quoted above) entrust the ECB with providing a mechanism to report breaches of relevant Union law and thus authorise the processing of personal data related to (suspected) offences in the sense of Article 10(5). Similarly to the discussion above on lawfulness, this covers the SSM-related aspects of the BRM.

The ECB also indicated that it could not be excluded that informants might include other special categories of data in the free text fields of the web form. It should be noted that the form does not request this kind of data; any such processing would thus be incidental.

3.4. Data Quality

According to Article 4(1)(c) of the Regulation, data must be adequate, relevant and non excessive in relation to the purposes for which collected and/or further processed. They must also be accurate and where necessary kept up to data (Article 4(1)(d)).

In the context of breach reporting, the notion of accuracy relates to the fact that certain statements have been made, not whether their content is true or not. The investigation of the allegations is not to be carried out by the BRU, but by the relevant recipient, e.g. a Joint Supervisory Team or DG-IA.

The data fields in the breach reporting form do not seem to be excessive for the purpose of reporting SSM-related breaches. However, it cannot be excluded that informants include clearly irrelevant information in their reports or use the BRM to report on issues that may have no relation to the SSM.

In order to avoid this, the ECB should **clearly explain which kinds of breaches the BRM is meant for and which kind of information is needed before prospective informants submit their reports.** This information should be clearly given to prospective informants. In order to avoid reports irrelevant for the BRM being sent through the BRM, **this information should also include references to other established reporting channels for different kinds of issues**. Ensuring that the purpose of the BRM is specific and explicit will help respecting the data quality principle (see also section 3.2 above).

If information clearly irrelevant for BRM is submitted, it should be deleted without delay (see also section 3.5 below).[16]

3.5. Conservation of data

As a general principle, personal data must not be kept in a form which permits identification of data of data subjects for longer than is necessary for the purpose for which the data are collected and/or further processed. (Article 4(1)(e)).

The conservation periods are 14 months following closure for non-SSM-related cases and 5 years from closure for SSM-related cases.

The ECB justifies the 5 years conservation period by reference to its power to impose administrative penalties on supervised entities under Article 130 of the SSM Framework Regulation, which is subject to a limitation of 5 years following the breach. In case criminal proceedings are started in a Member State following the receipt of information from BRU, the conservation period will be suspended for the duration of these proceedings.

The ECB justifies the 14 month period for non-SSM-related cases with two arguments. The first one is that its coordination function and other business areas need a certain amount of

[16] WP 29 Opinion 1/2006, p. 12, see section 3.5 below.

time to follow up on the final note transferred by the BRU. The second is that the ECB's IT system keeps backups of all systems for a period of 13 months. This second period also applies to reports which are clearly irrelevant for the BRM.

In this respect, it should be noted that the backups of the IT systems are done on a general level for all ECB IT systems and serves a different purpose (business continuity) than the BRM itself. What is considered here is the administrative retention period for the purpose of the functioning of the BRM. In the production system, reports should not be kept for longer than they are needed. For irrelevant reports, there seems to be no need for further storage following the ascertainment of their status. Such reports should be deleted without delay after their status as irrelevant has been ascertained.[17]

In the light of this, the ECB should both reduce the general conservation period for non-SSM related reports and establish a specific, shorter period for cases clearly irrelevant for BRM.[18]

3.6. Transfer of data

Transfers of personal data from the BRM may occur in three different ways:

1. Internally within the ECB (follow-up possibility 1 described in section 2.2 above): Article 7 of the Regulation applies;
2. To NCAs (follow-up possibility 2 described in section 2.2 above): Article 8 of the Regulation applies;
3. Possibly to third countries or international organisations: Article 9 applies.

The first two cases are the main intention of the BRM; the third case may happen in particular cases.

In all cases, personal data should as a rule only be transferred if this is necessary. For example, information on persons not relevant to the allegations made should not be transferred.

3.6.1. Transfers under Article 7

Article 7 allows transfers of personal data within and between Union institutions if they are "necessary for the legitimate performance of tasks covered by the competence of the recipient".

As described in section 2.2 above, there are three cases in which personal data from the BRM might be transferred internally within the ECB:

a. If the case is relevant for the ECB's SSM-related tasks, the final note might be disclosed to the relevant business area of the ECB.

   The ECB exercises direct supervisory tasks under Article 4 of the SSM Regulation. Transfers for these purposes thus appear to be covered under Article 7. Whether a case falls within the ECB's SSM-related tasks will need to be analysed in the light of the circumstances of the particular case; similarly, not all personal data provided in the informant's report might be relevant for this purpose - only relevant data should be transferred;

[17] See also Article 29 Working Party Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime, WP 117, page 12; available here: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp117_en.pdf.
[18] WP 29 Opinion 1/2006, p. 12.

b. If the case does not concern a breach of relevant Union law, but is otherwise relevant for the ECB's tasks (except as under point c) below), the final note is transferred to the ECB's coordination function for determining and onward transfer to the relevant ECB business area;

   In this case, it needs to be assessed whether the transfer is necessary for the legitimate performance of the recipients' tasks. Only those personal data necessary for these tasks should be transferred.

c. If the report concerns professional misconduct of an employee of the ECB or a NCA, the ECB's Directorate Internal Audit (D-IA) will be notified.

   Concerning alleged professional misconduct of ECB employees D-IA is, in accordance with internal ECB rules, in charge of administrative inquiries and disciplinary proceedings. Information on professional misconduct which could give rise to such procedures, if available to the ECB, should be forwarded to the relevant parts of D-IA, again subject to the caveat that only those personal data necessary for the investigation should be transferred.

   If the alleged misconduct of an NCA employee appears to be symptomatic of a systemic risk, D-IA will refer it to the Internal Auditors Committee (IAC) in SSM composition, including the relevant NCA.

   The IAC's mandate states that it "assists on matters related to the Single Supervisory Mechanism". This vague provision does not clearly establish the specific tasks of the IAC in this area. The ECB should **provide further information on the specific role of the IAC in this context in order to establish how far transfers are necessary for the legitimate performance of the tasks covered by the IAC's competence. Transfers should only occur if this necessity and competence can be demonstrated.**

In all cases, it should be noted that the ECB interprets the rule that it "shall not reveal the identity of a person who has made a protected report without first obtaining that person's explicit consent" in Article 37(3) of the SSM Framework Regulation as only prohibiting revealing the identity to recipients outside the ECB. On the other hand, for internal transfers, as described above, the ECB stated that the identity of the informant may be included where necessary. Given that the aim of this provision is to protect the informant against reprisals or other adverse consequences, even internal disclosures should be avoided whenever possible, both for SSM- related and non-SSM-related reports. To this end, **the criteria used for deciding whether the identity of an informant will be revealed internally should be defined and documented. Their application in concrete cases should be documented as well.**

3.6.2. Transfers under Article 8

Article 8(a) allows transfers to recipients subject to national legislation implementing Directive 95/46/EC (as is the case for NCAs) "if the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority". In case a transfer is initiated by the sender (i.e. the ECB), this assessment has to be made by the sender.

Cases deemed as relevant for NCAs by the BRU prima facie fall under this provision: NCAs' tasks in investigating breaches as developed in Union law[19] are carried out in the public interest. It should be noted that the transfer of the final note to NCAs will not include the identity of informants for SSM-related cases unless they have provided explicit prior consent.

[19] Here: legislation referred to in Article 4(3) of the SSM Regulation.

It is for BRU to restrict the personal data transferred to the minimum amount necessary for the purpose of the transfer.

Article 136 of the SSM Framework Regulation specifically states "[w]here, in carrying out its tasks under the SSM Regulation, the ECB has reason to suspect that a criminal offence may have been committed, it shall request the relevant NCA to refer the matter to the appropriate authorities for investigation and possible criminal prosecution, in accordance with national law". This concerns the cases described above as follow-up possibility 2.b. This provision is very wide. It can be interpreted to mean every possible criminal offence of which the ECB learns in exercising its tasks in the SSM. For the BRM - which is provided as part of the ECB's tasks in the SSM - a report about a totally unrelated suspected criminal offence (e.g. assault) could theoretically fall under this provision.[20] This would appear to be overly broad, as the *ratio legis* seems to aim at providing efficient reporting of SSM-related criminal offences. Again, the transfer of personal data to the NCA for this purpose should be limited to the amount necessary for this purpose.

Since NCAs are subject to the respective national implementation of Directive 95/46/EC, and not to Regulation (EC) 45/2001, the **reminder**[21] to them when transferring the final note **should be adapted accordingly with a reference to national legislation implementing Article 11 of Directive 95/46/EC.**

3.6.3. Transfers under Article 9

Article 9 lays down the specific rules for transfers of personal data to recipients who are not bound by national implementation of Directive 95/46/EC. Such transfers may be allowed if the recipient third country or international organisation provides adequate protection (Article 9(1) to (5)), in the case of several derogations (Article 9(6)), or when authorised by the EDPS (Article 9(7)).

According to Article 152 of the SSM Framework Regulation, existing cooperation agreements entered into by an NCA prior to 4 November 2014 relating to tasks (at least partly) covered under the SSM shall continue to apply. The ECB may decide to participate in such agreements in accordance with the procedures of the arrangement in question or may establish new cooperation agreements. The ECB has announced that it would participate in many of these agreements. In case the ECB plans to establish cooperation agreements on its own, it announced that it would consult the EDPS under Article 28(1), where necessary.[22]

If the ECB is to transfer personal data to third countries, **Article 9 of the Regulation needs to be complied with.**

3.7. Information to data subjects

Articles 11 and 12 of the Regulation impose certain information obligations on controllers; these differ depending on whether the data have been collected directly from the data subject (Article 11) or from another source (Article 12). In the first case, data subject are to be informed at the time of collection; in the second case, at the latest at the time of the first disclosure to a third party, where envisaged. For the BRM, informants are in an Article 11 situation when submitting the report. The other categories of data subjects (see the facts section above) are in an Article 12 situation.

[20] Outside the BRM, this would also cover all possible criminal offences of which the ECB learns e.g. during inspections, whether they are related to banking supervision or not.
[21] See section 2.3 above.
[22] See also EDPS Position Paper on the transfer of personal data to third countries and international organisations by EU institutions and bodies, 14 July 2014: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Papers/14-07-14_transfer_third_countries_EN.pdf.

3.7.1. Information to the data subject: informants and content of the privacy statement

The ECB will provide information on the BRM website, including a privacy statement, whose text has been provided to the EDPS. Prospective informants will be asked to tick a box acknowledging having read and understood the privacy statement before providing any information.

According to Article 37(3) of the SSM Framework Regulation, "the ECB shall not reveal the identity of a person who has made a protected report without first obtaining that person's explicit consent". The final web form to be used for submitting reports will ask "Do you consent to the ECB revealing your identity?". In order to ensure that this consent is fully informed, the ECB should **provide additional information on what this consent entails - notably in which cases and to whom the informant's identity could be revealed.**[23] Similarly, the **distinction between reports protected under Article 37 SSM Framework Regulation** (those related to the ECB's or NCAs' SSM-related tasks) **and other reports should be further clarified in the privacy statement**. Without further information, data subjects might legitimately expect that this protection applies to all reports, not only those protected under Article 37 SSM Framework Regulation.

The privacy statement does not mention the possible transfers to third countries (see section 3.6.3 above). Under Articles 11(1)(c) and 12(1)(d), data subjects need to be informed about the "recipients or categories of recipients of data". Therefore, **information on possible transfers to third countries/international organisations should be mentioned** in the privacy statement.

The text of the privacy statement **should be improved by clearly providing direct contact information for the controller**, e.g. a functional mailbox for the BRU.

3.7.2. Information to the data subject: other categories of data subjects

According to the ECB, accused persons, persons involved and other persons will not be informed under Article 12 by the BRU.

In principle, they have to be informed individually as well. However, Article 12(2) contains some limitations to the scope of information obligations. Additionally, there may be cases in which Article 20 may be used to restrict the right of information. These Articles are thus analysed below.

Article 12(2) excludes certain situations from the scope of the obligation to inform.[24] Controllers do not have to provide information under Article 12 where:

- "provision of such information proves impossible or would involve a disproportionate effort"

  This exception aims at cases in which the personal data of the data subject do not allow contacting him/her, e.g. because no address or other means of contact are known.[25] In such situations, the controller is usually not obliged to conduct further research to reach the data subject. Depending on the amount of information provided by the informant, this may apply to some categories of other data subjects mentioned in the reports submitted. It cannot, however, be assumed to be the case as a rule.

- "recording or disclosure is expressly laid down by Community law"

[23] This could be done either in the privacy statement, or in the web form for submitting information itself.
[24] While paragraph 2 specifically refers to scientific, historic and statistical reasons, its application is not limited to those cases.
[25] See e.g. EDPS case 2010-0426.

This exception applies to cases in which there is a clear obligation in Community (now Union) law to record or disclose information not collected from the data subject. The fact that the ECB is obliged by Union law to provide the BRM does not suffice to trigger this exemption: it is only the existence of a procedure that is mandatory, not the recording or disclosure of data relating to specific data subjects.[26]

For both cases, the controller should then provide appropriate safeguards after consultation with the EDPS.

Where these exemptions do not apply, such information may be delayed under Article 12 until the time of the first disclosure to a third party, where envisaged. As the BRM is meant to provide a reporting channel and to then further distribute incoming reports to the relevant recipients, such disclosure is envisaged as part of the procedure. The obligation to inform thus applies at the latest in the moment of onward transfer to an NCA or a different ECB Business Area. At this point in time, the ECB has to inform other categories of data subjects, unless it can apply a restriction under Article 20 of the Regulation.

If there is no exception from the scope of the right of information under Article 12 that applies, then several provisions of Article 20(1) of the Regulation might justify restricting its application where necessary for safeguarding the:

1. "prevention, investigation, detection and prosecution of criminal offences" (point (a))

   This exception might be used where the alleged breaches have the status of criminal offences and informing the data subject at this stage would prejudice the investigation. The EDPS has interpreted the term "offences" in a wide manner to also include information related to disciplinary matters;[27]

2. "important economic or financial interest of a Member State or of the European Communities" (point (b))

   This exception might be used where the alleged breaches could have such an impact.

3. "the protection of the data subject or of rights and freedoms of others" (point (c))

   This exception might be used to not inform the person accused about the identity of the informant ("source of the data", see Article 12(1)(f)(iv)).

4. "a monitoring, inspection or regulatory task connected, even occasionally, with the exercise of official authority in the cases referred to in (a) and (b)" (point (e))

   This is ancillary to points (a) and (b) above.

Under Article 20(3), the principal reasons for these restrictions have to be communicated to the data subject. Article 20(5) allows deferring this information if providing it would deprive the restriction of its effect. However, any use of these exceptions must only occur on a case-by-case basis; blanket restrictions are not possible. The use of restrictions has to be justified and documented.

As has been shown, there may be cases in which *some* data subjects other than informants may either fall under the limitations of the scope of the right to information under Article 12(2), or might be in situations where the ECB would be entitled to restrict this right under Article 20. However, this cannot be assumed at the policy level that *all* such data subjects (such as accused persons or witnesses) will fall into one of these cases. **The BRU's approach**

[26] One exception is the obligation to inform NCAs of cases concerning possible criminal offences for further referral to the competent authorities under Article-38(2) of the SSM Framework Regulation. However, this does not cover the other aspects of the processing.

[27] By analogy to Article 13(1)(d) of Directive 95/46/EC, which includes "breaches of ethics for regulated profession".

of not informing data subjects other than informants as a matter of policy thus does not appear to be compliant with Articles 12 and 20.[28] It should also be noted that being informed about the processing is a necessary precondition for exercising their other data subject rights. While there may very well be cases in which restrictions may be justified, this cannot be assumed to be the case on a policy level.

The reminder to recipients of the final note to inform the data subject under Article 12 of the Regulation is a safeguard, but not sufficient on its own. It should above all be noted that the reminder refers to informing the data subject about the processing by the recipient as the subsequent controller, not to the processing in the BRM. Where the information to be provided by this new controller under the legislation applicable to it does not include an indication of the origin of the data[29], this would not cover the full scope of the right to information concerning the processing of personal data in the BRM under Article 12 of the Regulation.

In principle, when Article 12(1) applies, the ECB has to provide the complete list of items in that Article to the data subject, including the origin of the data. As it is likely that premature provision of this information could prejudice the investigation carried out by the recipient, the ECB may -on a case-by-case basis- use the restrictions in Article 20. When these no longer apply, the data subject will have to be informed. When this will be the case depends on the state of the investigation carried out by the recipient. This recipient is the best-placed party to assess when this is the case.

As a pragmatic solution, the EDPS recommends **instructing recipients not only to inform data subjects about their own processing under Article 12, but also to include a link to the ECB's privacy statement for the BRM,** thus ensuring that data subjects other than informants are appropriately informed about the ECB's processing operations.[30]

3.8. Rights of access and rectification

Under Article 13 and 14 of the Regulation, data subjects have the right to access their personal data and to have inaccurate data rectified. These rights may be restricted under the conditions set out in Article 20 of the Regulation.

The ECB will grant the rights of access and rectification in accordance with its implementing rules on data protection.

In the notification form, the ECB did not indicate any intended use of restrictions to the rights of access and rectification. It should however be noted that Article 20(1)(c) of the Regulation (here: rights of third persons) is relevant for access requests by data subjects other than informants: for protected reports, there is a specific obligation of confidentiality on the ECB; also for other reports, it may be necessary to restrict the right of access to ensure the

[28] See also, by analogy, Article 29 Working Party Opinion 1/2006, page 13: " In particular, the reported employee must be informed about: [1] the entity responsible for the whistle blowing scheme, [2] the facts he is accused of, [3] the departments or services which might receive the report within his own company or in other entities or companies of the group of which the company is part, and [4] how to exercise his rights of access and rectification".

[29] For recipients subject to the Regulation, this is required by Article 12(1)(f)(iv); while this requirement is not mentioned in Article 11 of Directive 95/46/EC, only some national data protection legislation imposes similar obligations, see. e.g. section 7.1.c.ii of the UK's Data Protection Act (http://www.legislation.gov.uk/ukpga/1998/29/part/II) and Article 5(4) of the Spanish Data Protection Act (http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/LOPD_consolidada.pdf) .

[30] The alternative would be to request recipients to inform BRU when they no longer see the need for a restriction, so that BRU could then proceed to inform data subjects on its own. This would create additional administrative burden compared to the recommended solution.

protection of the informant, as (except in the case of malicious false statements), the accused person should not obtain the name of the informant using the right of access.[31]

Such restrictions should only be used on a case-by-case basis. If they are used to defer access, Article 20(3) to (5) of the Regulation apply.

3.9. Processors

Article 23 of the Regulation sets out the applicable rules for subcontracting the processing of personal data to processors. Requirements include the need for a written (or equivalent) contract which shall state that the processor shall only act on instruction from the controller as well as security requirements.

In the interim solution, the BRM will be hosted by the ECB, while for the permanent solution, the ECB plans to use a subcontractor.

For this permanent solution, the ECB will have to take all the necessary steps to ensure compliance with Article 23. Given the sensitivity of the personal data to be processed in the BRM, special attention should be paid to the security measures to be implemented by the contractor.[32] As soon as the safeguards and security measures for the permanent solution will be defined, the ECB should inform the EDPS about these (see also section 3.10 below).

3.10. Security measures

[...]

4. Conclusion:

There is no reason to believe that there is a breach of the provisions of Regulation 45/2001 providing the recommendations indicated in bold in this Opinion are fully taken into account. To summarise, the ECB should:

- clearly explain which kinds of breaches the BRM is meant for and which kind of information is needed before prospective informants submit their reports. This information should be clearly visible to prospective informants. In order to avoid reports irrelevant for BRM being sent through the BRM, this information could also include references to other established reporting channels for different kinds of issues;
- reduce the general conservation period and establish a specific, shorter period for cases clearly irrelevant for the BRM; provide further information on the specific role of the IAC in the context of misconduct of NCA employees symptomatic of systemic risk in order to establish in how far transfers are necessary for the legitimate performance of the tasks covered by the IAC's competence. Transfers should only occur if this necessity and competence can be demonstrated;
- define and document the criteria used for deciding whether the identity of an informant will be revealed internally; document their application in concrete cases;
- for transfers of the final note to NCAs, adapt the reminder on information to data subjects with a reference to national legislation implementing Article 11 of Directive 95/46/EC;

[31] See also Article 29 Working Party Opinion 1/2006, p. 14.
[32] See also Article 29 Working Party Opinion 1/2006, p. 16.

- ensure that Article 9 of the Regulation is complied with when transferring personal data to third countries/international organisations;
- provide additional information to prospective informants about what consenting to the disclosure of their identity entails, notably in which cases and to whom it could be revealed;
- improve the privacy statement by:
    - further clarifying the different levels of protections for reports relating to the SSM ("protected reports") and other reports;
    - mentioning possible transfers to third countries/international organisations;
    - providing a direct contact point for the BRU;
- instruct recipients not only to inform data subjects about their own processing under operations, but also to include a link to the ECB's privacy statement for the BRM;

[…]

Please report back to the EDPS on these recommendations within three months of the date of this Opinion.

Done at Brussels, 3 November 2014

(signed)

Giovanni BUTTARELLI