(To be filled out in the EDPS' office)
REGISTER NUMBER: 1266

(To be filled out in the EDPS' office)

NOTIFICATION FOR PRIOR CHECKING

DATE OF SUBMISSION: 12/09/2014

CASE NUMBER: 2014-0871

INSTITUTION: EUROPEAN CENTRAL BANK

LEGAL BASIS: ARTICLE 27-5 OF THE REGULATION CE N° 45/2001([1])

INFORMATION TO BE GIVEN[2]

1/ NAME AND ADDRESS OF THE CONTROLLER

European Central Bank
Kaiserstrasse 29
60311 Frankfurt am Main
Germany

2/ ORGANISATIONAL PARTS OF THE INSTITUTION OR BODY ENTRUSTED WITH THE PROCESSING OF PERSONAL DATA

Directorate General Micro-Prudential Supervision IV (hereinafter **'DG-MS4'**);
Enforcement and Sanctions Division (hereinafter **'ESA'**).
Breach Reporting Unit (hereinafter **'BRU'**)

3/ NAME OF THE PROCESSING

Breach Reporting Mechanism (hereinafter **'BRM'**) or Breach Reporting Mechanism procedure.

4/ PURPOSE OR PURPOSES OF THE PROCESSING

According to Article 23 of Council Regulation (EU) No 1024/2013[3] (hereinafter **'SSM Regulation'**), the ECB is required to ensure that effective mechanisms are put in place for reporting

[1] OJ L 8, 12.01.2001.
[2] **Please attach all necessary backup documents**
[3] OJ L 287, 29.10.2013

of breaches of legal acts referred to in Article 4(3) of the SSM Regulation (hereinafter **'relevant Union law'**)[4]4 by credit institutions, financial holding companies or mixed financial holding companies or competent authorities in the participating member states by 4 November 2014. Even though the reference on competent authorities includes the ECB, the BRM is not a 'whistleblowing' mechanism. 'Whistleblowing' is understood as an internal reporting mechanism within an institution or a company. The BRM, however, is directed to the general public and thus, to anyone who has knowledge of a potential breach of relevant Union law. Even though the ECB is encouraging potential informants to disclose their identity, the ECB is aiming at offering an anonymous reporting option, too.

The BRM consist of two main parts. The first part is the reporting channel (i) and the second part is the internal procedure (ii) following the submission of a report of a potential breach of relevant Union law.

(i) Reporting channel: The ECB is aiming at obtaining a licence for a reporting platform (permanent solution). To obtain a licence for such platform, the ECB has to conduct a procurement procedure which can last up to several months. Since the ECB is obliged to have an effective reporting mechanism in place by 4 November 2014, the ECB has developed an interim solution that will be in operation from 4 November 2014 until the permanent solution can be used.

BRM Interim Solution:
The ECB is going to offer a web/online-form on the public ECB website for reporting of breaches as an interim solution. This web/online-form requires potential informants to fill in a questionnaire containing pre-defined questions on the potential breach, including a free text field. A potential informant will be asked to submit an e-mail address to the ECB, in order to establish a possibility to communicate on the submitted report. Once the informant has completed the form and submitted the report, an e-mail containing this information is automatically generated and sent to the BRU. From this point on, the internal procedures regarding the BRM are triggered. The draft of the web/online-form is attached as **Appendix I.**

BRM Permanent Solution:
A reporting platform is a web-based system which allows informants to file reports of potential breaches of relevant Union law to ECB anonymously. Furthermore, a reporting platform allows members of the BRU to establish a secure communication channel to the informant. A potential informant will complete a questionnaire containing pre-defined questions on the potential breach, including a free text field. It will also be possible to attach documents to a report of a breach. The informant decides if he registers for on-going communication or just submits the questionnaire. If an informant decides to register, a username and a password have to be chosen to gain access to an on-going communication account. The on-going communication will be conducted via messages from the BRU members containing more detailed follow up questions on the alleged breach of relevant Union law.

(ii) Internal procedures following the receipt of a report:
The internal procedures following the receipt of a report are aiming at assessing whether a report received is relevant for the ECB or a National Competent Authority (hereinafter 'NCA') or not. It has to be stressed that the BRU is assessing only the relevance of a report and it is not investigating the breach itself. The investigation of alleged breaches will be conducted by other ECB business

[4] Article 4(3) first subparagraph SSM Regulation refers to "all relevant Union law". This term entails all relevant Regulations and Directives. If relevant Union law is composed of Directives, the ECB shall apply the national legislation transposing those Directives. Where the relevant Union law is composed of Regulations, and where currently those Regulations explicitly grant options for Member States, the ECB is required to apply also the national legislation exercising these options.

areas according to their regular supervisory tasks or by the NCAs.

Once a report is received via the reporting channel, a BRU member takes this report and the attached documents, transfers it manually to the ECB's Electronic Document and Records Management System (hereinafter '**DARWIN'**) and a BRU case file is created. Within a period of one month after the transfer to

DARWIN, the report and its attachments will be deleted from the reporting platform. The same procedure applies to each follow-up communication made via the reporting channel.

According to Article 36 of Regulation (EU) No 468/2014[5] (hereinafter **'SSM Framework Regulation'**), the ECB is obliged to treat a report of a breach of relevant Union law as a **protected report**, if it is made in good faith and if the informant has reasonable grounds for believing that the report will show breaches of relevant Union law.

The ECB has installed several confidentiality and data protection safeguards in the internal procedures following the receipt of a report. One measure is that only a special unit - the BRU - is competent to deal with the BRM and reports received via the BRM. The task of the BRU is to analyse received reports and to decide whether such report is relevant in regard to ECB's or an NCA's competences (relevance assessment phase). Another safeguard is that the BRU will not disclose personal data of a BRU case file except if there is a need to know for another ECB Business Area (hereinafter **'BA'**) or NCA. Furthermore, the identity of an informant who submitted a report in good faith is further protected by the fact that his identity will not be disclosed unless the informant provides an explicit consent or unless such a disclosure is required by a court order in the context of further investigations or subsequent judicial proceedings.

Within its competence to assess the relevance of a report, the BRU is authorised to consult with other BAs within the ECB. However, such consultation shall only include factual information and no personal data of an informant or an accused person or an involved person[6] shall be disclosed at this stage of the procedure.

Once the BRU has finished the relevance analysis, it will create a final note on its findings and forward the note to the competent ECB BA or NCA, if the report was deemed relevant.

The final note will include the all necessary documents and the personal data which need to be known by the recipient. If personal data are included in the note and thus forwarded to another ECB BA or an NCA, the BRU is not competent to inform the data subject itself since the BRU does not conduct the investigation of an alleged breach. Therefore, the investigating function shall be in the end competent to decide on the information of the relevant data subjects in accordance with Article 12 of Regulation (EC) No 45/2001 or by applying Article 20 of Regulation (EC) No 45/2001. Otherwise the investigation might be jeopardized.

After the report was assessed relevant for the ECB or an NCA, the BRU will assist the relevant ECB BAs or NCAs if they need to communicate with an informant via the BRM (messenger phase). The messenger phase shall not circumvent the confidentiality and data protection safeguards installed in the BRM procedure. Indeed, if for example an ECB BA requires more information from an informant and the BRU receives that information, the BRU will hand over personal data which are included in the new information to the requesting BA only on a need-to- know basis.

[5] OJ L 141, 14.05.2014.
[6] See the categories of data subjects in item 5.

(iii) Specifics concerning the submission of reports by *"other channels"*

The aforementioned reporting channel aims both to provide the most effective mechanism in order to receive reports of breaches from informants and to protect the personal data of data subjects concerned by these reports. For this purpose, the ECB will encourage potential informants to send reports using the aforementioned BRM and thus will not suggest on its website to submit reports by other means.

However, it cannot be ruled out that the ECB receives such reports by other channels. For that reason, the confidentiality and data protection safeguards described above have been adapted for the situations described below.

When an informant submits a report without using the web/online-form but by sending e-mails, physical mails or telefaxes to a valid e-mail address, (postal) address or number respectively within the ECB, the e- mail, mail or telefax concerned is forwarded to the BRU, if the latter is not the direct recipient of these documents. Then, a BRU member scans the report, including all other potential related documents sent by the informant via the mail or telefax, and transfers them manually to **'DARWIN'** into a BRU case file which is created for this purpose. Afterwards, the BRU member assesses, on a case by case basis, whether the physical version of the report and, if any, other documents provided by the informant, need to be kept in a physical BRU case file created for this purpose[7] and stored in a locked cabinet located within the BRU area, or can be destroyed. If an e-mail was forwarded to the BRU, a BRU member creates a BRU case file and the information of the report is transferred manually into this file. The e-mail will be stored in the BRU case file, too. The retention period described in the item 13 is applicable to both physical and electronic versions of such reports.

When an informant submits an oral report by giving a call to a valid phone number within the ECB, the incoming call is transferred to the BRU, if this latter is not the direct receiver of the call. When one of the BRU members receives the call, he first suggests to the informant to submit his report using the BRM[8]. If the informant refuses, the BRU member then takes note of the oral report of the informant and asks for any further explanation required. After the call, the BRU member finalises the minutes of the call following a template, transfers the minutes manually to DARWIN into a BRU case file created for this purpose.

When an informant submitted an oral report during a meeting with the BRU, a BRU member writes the minutes of the meeting and transfers these minutes to DARWIN into a BRU case file created for this purpose. The BRU member is also in charge of the scanning of the potential related documents provided by the informant during the meeting and the following storage of these scans into the BRU case file in DARWIN. The BRU member also assesses if such documents need also to be kept after their scanning in a physical BRU case file which would be stored in a locked cabinet located within the BRU area or if it can be destroyed. The retention period described in the item 13 is applicable to both physical and electronic versions of such reports.

For more information on the BRM, please see the detailed "Description of the ECB Breach Reporting Mechanism", attached as **Annex 2 to the ECB Cover Letter**. In addition, please see the "Flowchart showing the Breach Reporting Mechanism procedure", attached as **Appendix I to Annex 2.**

Please note that the aforementioned legislation is attached as **Appendix III to this notification.**

[7] E.g. if the paper-based document is signed manually, handwritten.
[8] Such as suggestions shall also be done before the end of the call as a reminder.

5/ DESCRIPTION OF THE CATEGORY OR CATEGORIES OF DATA SUBJECTS

1) natural persons who have provided information to the ECB (informants);
2) natural persons who are or were suspected breaching relevant Union law (accused persons);
3) natural person who may be involved in or are affected by the procedure and who are named in the report (persons involved);
4) natural persons working for the ECB or an NCA who are working on ECB matters;
5) other persons whose personal data appears in the report or in the ECB case file but have no relevance to the case (other persons).

6/ DESCRIPTION OF THE DATA OR CATEGORIES OF DATA
(including, if applicable, special categories of data (Article 10) and/or origin of data)

1) identification data (surname, forename, nickname, day of birth, birthplace, street, postcode, city, country, telephone number, fax number, and e-mail address);
2) professional data: profession, organisation, function;
3) data on a potential breach of relevant Union law which may constitute an offence according to Article 10(5) of Regulation (EC) No 45/2001.
4) According to Article 10(1) of Regulation (EC) No 45/2001, data revealing e.g. racial or ethnic origin or political opinions[9] are not requested from informants and the ECB does not intend to process such data within the BRM. Nevertheless, if the ECB receives such data, the ECB will apply the defined confidentiality and data protection standards to those data.

7/ INFORMATION TO BE GIVEN TO DATA SUBJECTS

A link on the public ECB website will be offered to connect the potential informant to the BRM. In the website's section hosting the BRM, the ECB will provide a guidance note on how to use the system technically, on the consequences of abusing the system, on the competences of the ECB with regard to breaches of relevant Union law and on the applicable confidentiality and data protection regime. Furthermore, the ECB will provide a link to a Privacy Statement which will be available on the public ECB website. Before the potential informant is authorised to make a report, he will be asked to tick a mandatory box in order to provide an acknowledgement of the reading and understanding of the aforementioned information.

The main principle is that personal data stored in an BRU case file are not disclosed from such file, except if there is a need-to-know for another ECB BA or an NCA, or if there is another legal obligation to do so. Only one BRU member is assigned to a BRU case: thus, this member is competent to access to the BRU case file and the respective data and to assess the relevance of the report. Nonetheless, the Head of the BRU is competent to assign more BRU members to a case if it is necessary or to replace a competent BRU member by another one. As long as personal data are kept in the BRU file, the accused person or involved person will not be informed that the personal data are stored in the BRU file.

If the information in the report is considered relevant for the ECB or an NCA and a further investigation of the matter is recommended by the BRU, it may include relevant personal data in its final note and forward them to the competent ECB BA or NCA. Furthermore, also the competent investigating unit can request the disclosure of personal data on a strict need-to-know basis in

[9] Other data concerned: religious or philosophical beliefs, trade-union membership, and of data concerning health or sex life, are prohibited.

accordance with their competences.

Anytime, when the BRU discloses personal data from a BRU file, it has to remind the receiving ECB BA or NCA to inform the data subject according to Article 12 of Regulation (EC) No 45/2001 or to apply the exemptions and restrictions foreseen in Article 20 of Regulation (EC) No 45/2001.

For the full text of the Privacy Statement, see **Appendix II.**

8/ PROCEDURES TO GRANT RIGHTS OF DATA SUBJECTS
(Rights of access, to rectify, to block, to erase, to object)

Article 9 of the decision ECB/2007/1 applies in this regard **(Appendix III).**

9/ AUTOMATED / MANUAL PROCESSING OPERATION

The personal data which is submitted by an informant to the BRU via the interim solution or via the permanent solution is entered manually by the members of the BRU into the relevant template which is stored in DARWIN. If another ECB BA receives a report of a potential breach of relevant Union law, the report will be forwarded to the BRU which will then enter the information manually into the system. In summary, the BRM is characterised by both automated and manual means of processing.

10/ STORAGE MEDIA OF DATA

The personal data to be processed within the mentioned BRM procedure will be stored in DARWIN.

With regard to the interim solution, the BRU will receive an e-mail containing the information which was inserted in the web/online-form by the informant. Once a member of the BRU has stored the report manually in DARWIN, the aforementioned e-mail will be transferred to DARWIN too and then deleted from the BRU's single user's Outlook e-mail account within a period of one month. However, it has to be mentioned that any e-mail the ECB receives is recoverable due to the ECB back-up system for another 13 months following the deletion from a single user's e-mail account. This fact does comply with the applied retention periods as mentioned below in item 13.

With regard to the permanent solution, the ECB will include in the terms of tender that it must be possible for the ECB to delete information on the reporting platform permanently and not recoverably.

Received paper-based documents are scanned and transferred to DARWIN. When the physical versions of such documents are kept, the latter are stored in locked cabinets located within the BRU area.

11/ LEGAL BASIS AND LAWFULNESS OF THE PROCESSING OPERATION

Articles 127(6) of the Treaty on the Functioning of the European Union; 4(3) and 23 of the SSM Regulation; 36 to 38 and 136 of the SSM Framework Regulation.

Please note that the aforementioned legislation is attached as **Appendix III.**

12/ THE RECIPIENTS OR CATEGORIES OF RECIPIENT TO WHOM THE DATA MIGHT BE DISCLOSED

The ECB BA and NCA staff members who are involved in the processing operation need to have knowledge about certain types of personal data in order to perform their tasks. Namely:

- If the report is relevant for the ECB's SSM related tasks[10], the data might be disclosed to the relevant competent BAs, especially the Joint Supervisory Teams (hereinafter 'JSTs') in case it is necessary for the purpose of carrying out the on-going supervision of significant supervised entities or for other BAs within the SSM for the carrying out of their supervisory tasks;

- If the report is relevant for an NCA,[11] the report will be forwarded to the NCA;

If the report does not imply an alleged breach of relevant Union law, but affects internal or external tasks (except tasks regarding potential professional misconduct by an employee of the ECB or an NCA) of the ECB which are non SSM related, the report is transferred to the coordination function within the ECB in order for the coordination function to determine the competent BA(s) in such a case and to forward the report to the competent BA(s).

- If the report contains information on potential professional misconduct by an employee of the ECB or an NCA, the ECB Directorate Internal Audit (hereinafter 'D-IA') in accordance with its mandate under the applicable regulations will be notified by the BRU. The BRU and the D-IA are going to consult on how to proceed further in such a situation. If e.g. in addition to being relevant for D-IA such a report is also relevant for non SSM related tasks of the ECB, the BRU and the D/IA can agree on forwarding the information or (non-sensitive) parts of the information to the coordination function in order for them to forward the information to the competent BA(s). This decision is made on a case by case basis.

Personal data might be also disclosed to national authorities if such disclosure is required by a court order in the context of further investigations or subsequent judicial proceedings as stated in Article 37(3) of the SSM Framework Regulation.

For more information on the BRM, please see the detailed "Description of the ECB Breach Reporting Mechanism", attached as **Annex 2 to the ECB Cover Letter**. In addition, please see the "Flowchart showing the Breach Reporting Mechanism procedure", attached as **Appendix I to Annex 2.**

Please note that the aforementioned legislation is attached as **Appendix III.**

13/ RETENTION POLICY OF (CATEGORIES OF) PERSONAL DATA

A) The data in BRU case files are stored for five years after closing[12] the BRU file. The same retention period applies to paper files. The reason for this five year period is that the ECB's power to

[10] If a report contains allegations on (i) an alleged breach of relevant Union law by a significant supervised entity or (ii) an alleged breach of ECB regulations or decisions by a significant or less significant supervised entity or (iii) an alleged breach of relevant Union law by an NCA, it is deemed relevant for the ECB.

[11] If the information relates (i) to an alleged breach of relevant Union law by a less significant supervised entity, or (ii) contains information which gives reasons for the ECB to suspect that a criminal offence may have been committed. The latter case (iii) applies also if the BRU is of the opinion that a report was not made in good faith since such behaviour may constitute a criminal offence in Member States.

impose administrative penalties on supervised entities is subject to a limitation period of five years according to Article 130(1) SSM Framework Regulation.

If the ECB or an NCA is launching administrative proceedings or if criminal proceedings are initiated in a Member State upon the information received via the BRU, the above mentioned retention periods for BRU case files are suspended until the closure of such proceedings.

B) If the information contained in a report was considered not relevant for ECB's SSM related tasks and/or not relevant for an NCA, the BRU case files are stored for a period of 14 months after closing such a BRU case file.

The reason for this 14 months period is that the coordination function needs an appropriate amount of time in order to assess which ECB BA is competent. Subsequently, the competent ECB BA that receives the information will need an appropriate amount of time, too, in order to determine e.g. whether it needs more information from the informant on the report he submitted and whether it needs to contact this informant via the BRM. The same need for time applies in cases in which D/IA (in accordance with its mandate under the applicable regulations) must be involved by the BRU as such report contains information on potential professional misconduct by an employee of the ECB or an NCA.

In addition to this, there is also a technical reason to apply a retention period of 14 months for BRU case files containing non SSM related information: Regarding the Interim solution, the e-mail containing the information which was inserted in the web-form by the informant will be transferred to DARWIN and deleted from the BRU's single user's Outlook e-mail account within a period of one month. The e-mail will be deleted from the back-up server 13 months following the deletion from the BRU single user's Outlook e-mail account. Apart from the interim solution and once the permanent solution is in operation, and as outlined above, the BRU will also assess reports which were received via a valid ECB e-mail address. Therefore, the technical reason also applies once the permanent solution is put into operation.

Because of the above stated reasons, the ECB considers a retention period of 14 months for BRU case files regarding reports that are not relevant for SSM related tasks and that are not relevant for an NCA appropriate and necessary.

If, after closing a BRU case file, further communication with the informant via the BRM is needed, any request for information which is made by the BRU to the informant via the BRM will suspend the abovementioned retention period until the closure of such internal procedure.

13 A/ TIME LIMIT TO BLOCK/ERASE ON JUSTIFIED LEGITIMATE REQUEST FROM THE DATA SUBJECTS *(Please, specify the time limits for every category, if applicable)*

Not applicable.

[12] The point in time on which a case is deemed to be closed is the day following the approval of the final note of BRU on the relevance assessment procedure.

14/ HISTORICAL, STATISTICAL OR SCIENTIFIC PURPOSES
(*If you store data for longer periods than mentioned above, please specify, if applicable, why the data must be kept under a form which permits identification)*

According to Article 38(7) of the SSM Framework Regulation the ECB shall provide in its annual report information on the reports received in abridged or aggregated for, such that individual supervised entities or persons cannot be identified.

Please note that the aforementioned legislation is attached as **Appendix III.**

15/ PROPOSED TRANSFERS OF DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

According to Article 152 of the SSM Framework Regulation, the ECB has to respect the existing cooperation arrangements – including arrangements providing for exchanges of information – with other authorities entered into by NCAs prior to 4th November that cover at least in part tasks transferred to the ECB by the SSM Regulation. However, according to Article 55 of the Directive 2013/36/EU[13] (hereinafter **'CRDIV'**), the information disclosed should be subject to a guarantee that equivalent professional secrecy requirements are complied with.

The ECB will comply with the provisions of Article 9 of the Regulation 45/2001, and will not transfer data to third countries or international organisations if an adequate level of protection of such data is not ensured in the country of the recipient or within the recipient international organisation, without prejudice to the derogations as provided for in Article 9(6).

Please note that the aforementioned legislation is attached as **Appendix III.**

16/ THE PROCESSING OPERATION PRESENTS SPECIFIC RISK WHICH JUSTIFIES PRIOR CHECKING *(Please describe)*

AS FORESEEN IN:

☒ Article 27.2.(a)
(Processing of data relating to health and to suspected offences, offences, criminal convictions or security measures,)

According to Article 23 of the SSM Regulation, the ECB has to 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 Member States (including ECB) of relevant Union law. A report of a breach of relevant Union law can trigger administrative sanctions procedures by the ECB or NCAs or even criminal procedures by NCAs. Therefore, the BRM procedure has to be considered processing data relating to suspected offences or offences according to Article 27.2.(a).

☐ Article 27.2.(b)
(Processing operations intended to evaluate personal aspects relating to the data subject,)

No such processing operations intended.

☐ Article 27.2.(c)

[13] OJ L 176, 27.6.2013.

(Processing operations allowing linkages not provided for pursuant to national or Community legislation between data processed for different purposes,)

☒ Article 27.2.(d)
(Processing operations for the purpose of excluding individuals from a right, benefit or contract)

The information received via the BRM could ultimately lead to sanctions or other measures on natural and legal persons because of a breach of relevant Union law. Following such procedures, natural persons employed with supervised entities or competent authorities could face detrimental consequences which could ultimately lead to the termination of their employment contracts. Furthermore, information received via the BRM could lead to criminal investigations and criminal convictions, too.

☐ Other (general concept in Article 27.1)

17/ COMMENTS

We herein attach the following documents:

Appendix I: Draft of the web-form for the interim solution;
Appendix II: Privacy statement for the BRM;
Appendix III: Relevant applicable legislation.

PLACE AND DATE: FRANKFURT AM MAIN, GERMANY, 12 SEPTEMBER 2014

DATA PROTECTION OFFICER: FREDERICK MALFRÈRE

INSTITUTION OR BODY: EUROPEAN CENTRAL BANK