EUROPEAN CENTRAL BANK

EUROSYSTEM

Roman Schremser
Chief Compliance and Governance Officer

Ms Emily O'Reilly
European Ombudsman
1 avenue du Président Robert Schuman
CS 30403
F-67001 Strasbourg Cedex
EO@ombudsman.europa.eu

11 November 2021

**Subject: How EU institutions, bodies, offices and agencies record text and instant messages sent/received by staff members in their professional capacity (SI/4/2021/TE)**

Dear Ms O'Reilly,

Thank you for your letter of 30 June 2021 inviting the ECB to provide information on its rules and practices for the recording of text and instant messages.

Please find attached the ECB's reply to your survey.

We remain, of course, at your disposal should you require any further information.

Yours sincerely

[redacted]

Attachments

cc. Ms Tanja Ehnert

**Address**
European Central Bank
Sonnemannstrasse 20
60314 Frankfurt am Main
Germany

**Postal address**
European Central Bank
60640 Frankfurt am Main
Germany

Tel.: +49 69 1344 0
[redacted]
www.ecb.europa.eu

EUROPEAN CENTRAL BANK

EUROSYSTEM

**ECB-UNRESTRICTED**

**EUROPEAN OMBUDSMAN STRATEGIC INITIATIVE ON HOW EU INSTITUTIONS, BODIES, OFFICES AND AGENCIES RECORD TEXT AND INSTANT MESSAGES SENT/RECEIVED BY STAFF MEMBERS IN THEIR PROFESSIONAL CAPACITY – REPLY FROM THE EUROPEAN CENTRAL BANK (ECB)**

**Preliminary remarks**

The European Central Bank (ECB) has adopted **specific rules and processes for the management of ECB documents and information**. ECB documents and information are defined as any content - whatever its medium -, created or received, related to the ECB's policies, tasks, activities, or decisions.[1]

The rules for the sharing, keeping or destroying, and storing of ECB documents and information are set out in the ECB's Business Rulebook (BRB). The BRB states that *"[a]s soon as [ECB staff] create or receive ECB information, [they] have a responsibility to use and treat that information in accordance with the ECB's rules and procedures*" and "*in order to document the decisions it takes, the ECB should keep valuable ECB information that it created or received (records); however, not all ECB information needs to be preserved. Information saved in DARWIN is retained or destroyed in an automated manner*."

ECB information to be stored includes (i) evidence of business activities, decisions, transactions; (ii) information with future value, e.g. business, financial, legal, research and (iii) formal communication (between staff and external parties). Conversely, information should not be kept when (i) of short-term value; (ii) not required in the future; or consists of (iii) duplicates or copies, or (iv) drafts superseded by a final version.

Until recently, the ECB did not consider the use of text and instant messages for "business purpose", namely, for any activities that (directly or indirectly) enable the ECB to perform its tasks as provided for in the Union Treaties, the Statute of the ESCB and the SSM Regulation. In the course of 2020, while the majority of ECB staff was working remotely, the ECB introduced new tools, such as Signal and MS Teams, to facilitate communication and collaboration within the bank. However, all

[1] Decision ECB/2004/3 on public access to ECB documents defines ECB document as "*any content whatever its medium (written on paper or stored in electronic form or as a sound, visual or audiovisual recording) drawn up or held by the ECB and relating to its policies, activities or decisions, as well as documents originating from the European Monetary Institute (EMI) and from the Committee of Governors of the central banks of the Member States of the European Economic Community (Committee of Governors)*". The ECB's Business Rulebook defines ECB information as "*Any content created or received related to the policies, tasks, activities or decisions of the ECB (including the tasks performed in accordance with the Union Treaties, the Statute of the ESCB and the SSM Regulation)*".

information related to ECB tasks, activities and decisions continued to be exchanged via official ECB email messages and duly recorded in the ECB's record management system.

| | THE APPLICABLE RULES |
|---|---|
| 1 | **Does the ECB's record management decision cover text and instant messages, sent or received through professional and/or personal devices?** |
| | The BRB (chapter 3.5) lists the different IT and communications equipment and applications which can be used. It currently allows the use of Signal, Slack, Jabber and MS Teams, for the **communication of transitory information**, subject to the following restrictions:<br>• **Signal** is the only tool allowed for instant messaging on mobile phones for business purposes. It was approved in 2020 in response to the pandemic and increased teleworking. An intranet article contains the rules and recommendations for the use of Signal and recommends setting the deletion rule to one day. Since instant messages contain only transitory information, they do not need to be captured but should be deleted as soon as possible (attachment 2);<br>• **Slack** is allowed only exceptionally and for up to ECB-RESTRICTED information at a maximum. Staff are informed that Slack is not an ECB managed service and so no support is available at the ECB. In addition, users are asked to consider the tool as being in pilot mode, not meant to continue, that the content could be deleted at short notice and that there is no assurance of continuity of service. The default Slack retention policy applies with instant messages being retained only for the life of the associated workspace in Slack (attachments 3 and 4);<br>• **Jabber** is an internal ECB chat tool that can be used only from laptops for transitory information among ECB staff and not to record business decisions. It is being replaced by MS Teams and will be discontinued when the contract ends [attachment 5];<br>• **MS Teams** has just been introduced at the ECB and can also be used from mobile phones. Team chats are intended for transitory information and not to record business decisions. Use of the private chat function is restricted to ECB staff and cannot be extended to externals. Chat messages are deleted after one year. This guidance is contained in a governance document as well as in the relevant intranet pages (attachments 6 & 7).<br>Chat applications (e.g. WhatsApp, Telegram) are not allowed for the exchange of ECB information.<br>The new version of the BRB, to be finalised still in 2021, will include an explicit reference to the use of SMS, which is only allowed for up to ECB-UNRESTRICTED information. |
| 2 | **Does the ECB's record management decision set out criteria/principles for the recording of text and instant messages?** |
| | Since text and instant messages should only be used for the communication of short-lived and transitory information, these messages are considered by default non valuable business information. As a consequence, and also following data protection recommendations, a short |

| | |
|---|---|
| | retention is either automatically implemented for (e.g. in the case of Teams) or staff is requested to delete messages as soon as possible (e.g. in the case of Signal) (see also Q1). |
| 3 | **Does the ECB's record management decision set out how text and instant messages should be recorded by staff members?** |
| | See Q 1 |
| | **IMPLEMENTATION OF THE APPLICABLE RULES** |
| 4 | **How is the record management decision, as regards text and instant messaging, implemented? For example, has the ECB issued relevant guidelines to staff or does it provide training on this matter to staff?** |
| | The ECB's rules as regards text an instant messaging are included in the BRB (see Q1). Regular training is provided by the competent business units; in particular<br>• all newcomers receive an induction training which, among others, covers the obligations, rules and restrictions for access to and exchange of ECB information and documents (including on the obligation to capture business information and the limitations to the use of equipment and applications);<br>• the Information Governance Division (DG-SE/IGO) delivers in addition ad-hoc presentations, provides guidance and offers personalised advice to users;<br>• the Digital Security Services Division (DG-IS/DSS) delivers a regular mandatory training on IT Security and also organises workshops and publishes intranet articles on important topics related to IT security;<br>• the introduction of new tools and applications is accompanied by training and information campaigns, for example, in the context of the roll-out of MS Teams, the Project Team provided information and Q&A sessions to all ECB staff. |
| 5 | **In practice, has the ECB recorded text and instant messages? If so, could the ECB please provide examples?** |
| | Given the ephemeral nature of the information exchanged via text and instant messages, such messages do not have to be recorded. |
| 6 | **Has the ECB already received requests for public access to text and/or instant messages or has the ECB identified text and/or instant messages as falling within the scope of an access to documents request? If so, could the ECB please give examples?** |
| | The ECB has not received requests for public access which explicitly or predictably covered text and/or instant messages, nor has the ECB identified text and/or instant messages as falling within the scope of a request for public access to ECB documents. |
| 7 | **When receiving public access requests which cover, explicitly or implicitly, text and/or instant messages, how does the ECB search for relevant 'documents'? Has the ECB put mechanisms in place (for instance, guidelines or instructions) to assist staff in searching for such 'documents'?** |
| | N/A |

Attachments:

1. Copy of the Business Rulebook – Chapter 3
2. Copy of Intranet article containing guidance for the use of Signal
3. Copy of Guidance on the use of Jabber
4. Copy of Slack web page on default retention policy
5. Extract from intranet FAQ on use of collaboration tools including Slack
6. Copy of MS Teams governance document
7. Copy of intranet guidance on MS Teams retention

# Business Rulebook

As adopted by the Executive Board on 03 December 2019*

Entry into force: 1 January 2020

Entry into force business travel rules: 1 March 2020

*Latest links added on 13 February 2020

# MANAGEMENT OF ECB INFORMATION

| Policy owner DIV/IGO | Main contact point Your RMS | Last update 01 January 2020 |
|---|---|---|

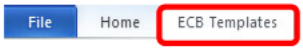
In order for the ECB, ESCB and SSM to function well, there must be a regular exchange of information and cooperation among them. At the same time, the information created or received by the ECB is often sensitive, and must be protected from unauthorised access and misuse.

To help ECB staff to make the best use of ECB information, meet their professional secrecy obligations and protect such information, they must follow the information management rules set out in this chapter.

## 1. Create ECB documents

As soon as you create or receive ECB information, you have a responsibility to use and treat that information in accordance with the ECB's rules and procedures.

### How do I create ECB documents?

- ✓ Use official ECB templates when available (accessible via the ECB templates tab in MS Word and PowerPoint). 

- ✓ Describe your folders and documents by adding metadata as provided in the Metadata Standard. In particular:
  - give your folders and documents titles that:
    - clearly describe their content;
    - do not contain sensitive information;
    - ensure they will be easily found;
    - distinguish them from similar folders/documents;
  - mark the document's status, e.g. DRAFT, FINAL or UPDATABLE, both within the document and in the title of the electronic file and update the status when it changes.
- ✓ Classify all ECB documents that you create according to their sensitivity as further specified in "How do I classify ECB information?".
- ✓ Give ECB documents containing sensitive information a marking from the List of ECB markings, when relevant to indicate:
  - why the content is sensitive, e.g. market-sensitive;
  - any restrictions on access, e.g. EB only;
  - predictable security classification changes, e.g. ECB-CONFIDENTIAL until approval then ECB-PUBLIC.

**More:** Guide on managing information at the ECB.
Consult your RMS for further support with creating documents.

***Think green!*** Think of the environment before printing and use electronic files whenever possible.

## 2. Classify ECB information

All ECB information must be classified by its author or, in the case of an external document, its recipient, according to its sensitivity. Classifying the document makes it clear who is allowed to access the information and to protect it from misuse or unauthorised access.

### How do I classify ECB information?

- ✓ Classify all ECB information you create or receive according to its sensitivity (i.e. the likely negative impact that its misuse could have as indicated in the ORM impact grading scale):

| If the likely negative impact in the event of misuse of information is | Classify information as |
|---|---|
| Very high | ECB-SECRET |
| High | ECB-CONFIDENTIAL |
| Medium | ECB-RESTRICTED |
| Low or negligible | ECB-UNRESTRICTED |
| None | ECB-PUBLIC |

- ✓ Classify collections of documents, e.g. a folder, a file or removable electronic media, at the level of the highest classification applied to an individual item in that collection.
- ✓ Classify ECB information as "ECB-SECRET" only with senior management approval.
- ✓ Reclassify ECB information if its sensitivity changes.
- ✓ If your business area has established a pre-approved classification for particular categories of information this classification should be used.

**Remember:** DIV/SEC and DIV/DM may reclassify documents submitted to their respective bodies after consulting the relevant business area.

**More:** Classification examples for ECB documents, for help with classifying your documents.
Desk aid for the ECB confidentiality regime
ECB confidentiality regime FAQ
Consult your RMS if you have any questions about classifying ECB information.

# 3. Store ECB information

All ECB information must be stored in one of the designated ECB information systems or storage units.

## Where do I store ECB information?

✓ Store ECB information you create or receive in a designated ECB information system:

| Type of ECB information / Information system | Business documents, including emails | Econometric packages | Data files | Databases | HR, accounting & other operational data | Personal documents including emails |
|---|---|---|---|---|---|---|
| **DARWIN enterprise workspace** | ✓ | | | | | |
| **Network drives (P, etc.)** | | ✓ | ✓ | ✓ | | |
| **Other corporate applications (IMAS, ISIS, statistical, market operations databases)** | | | ✓ | | ✓ | |
| **Outlook** | | | | | | ✓ |
| **DARWIN personal workspace/J drive** | | | | | | ✓ |

- ✓ Store ECB information on your ECB IT and communication equipment only if the ECB network is unavailable or if necessary in order to share the ECB information. Transfer ECB information back into the ECB network as soon as possible and delete local copies of ECB information.
- ✓ Store:
  - ECB-SECRET physical documents in a locked safe; and
  - ECB-CONFIDENTIAL and ECB-RESTRICTED physical documents and portable storage devices in a locked storage unit.

## How do I store ECB information?

- ✓ Store related ECB information together.
- ✓ Do not duplicate ECB information in different folders; use shortcuts or collections instead.
- ✓ Store information without encryption, compression (zip), or password protection.
- ✓ Keep your personal documents separate from ECB information.
- ✓ Store business emails in the relevant folder in the DARWIN enterprise workspace and any personal emails in your personal DARWIN workspace, to avoid relevant emails being deleted by default after one year.

**More:** Check the DARWIN User Guide or consult your DARWIN key user about the use of DARWIN.
Consult your RMS if you have any questions about storing ECB information.
BRB - Protect ECB information

# 4. Access and share ECB information

To perform their tasks efficiently, ECB staff must share ECB information and collaborate. At the same time, ECB staff should safeguard sensitive information and protect it from unauthorised access.
This also applies with regard to inside information, in particular when it is market-sensitive. In addition to ECB staff being prohibited from using, or attempting to use, inside information to further their own or another's private interests, the ECB should not take advantage of market-sensitive inside information when deciding on the acquisition or disposal of financial instruments for the ECB in the management of its own resources. By

exercising particular caution when handling inside information, ECB staff assist in preventing insider trading and the unlawful disclosure of inside information.

## What ECB information may I access or share and with whom?

- ✓ Access or share ECB information for professional purposes only.
- ✓ Access or share ECB information only when the conditions for accessing or sharing are met. If necessary, obtain prior traceable approval before sharing:

| ECB CLASSIFICATION | Under what conditions may I access or share ECB information with an intended recipient | Whose prior traceable approval is required? | | |
|---|---|---|---|---|
| | | Within the ECB, ESCB, SSM | Outside the ESCB | Outside the SSM |
| **ECB-SECRET** | Strict "need-to-know" basis | Senior manager of the originator | EB member | DMB |
| **ECB-CONFIDENTIAL** | "Need-to-know" basis | Manager of the information owner | | |
| **ECB-RESTRICTED** | Within the ECB,ESCB, SSM: Legitimate interest | No approval required | | |
| | Outside the ECB, ESCB, SSM: "Need-to-know" basis | | Manager of the information owner | |
| **ECB-UNRESTRICTED** | Within the ECB, ESCB, SSM: No restriction | No approval required | | |
| | Outside the ECB, ESCB, SSM: Business purpose | | | |
| **ECB-PUBLIC** | No restriction | No approval required | | |

- ✓ When sharing sensitive information outside the ESCB/SSM, inform the intended recipient of the information's security classification and the need to protect the information.
- ✓ Register ECB-SECRET information that you plan on sharing in the Register of ECB-SECRET information taken out of ECB premises.

**Remember:** Forward all requests from the general public for ECB documents to the CGO.
Store all approvals for sharing ECB information together with the shared ECB information.
Before sharing ECB information, make sure that there is a legal basis for sharing. Contact the DPO if you intend to collect, store or share personal data to ensure compliance with the Data Protection Regulation.
If you have any doubts about sharing ECB-SECRET information originating outside the ECB, consult DIV/SEC or DIV/DM.
Request editing/proof-reading, and if necessary, translation of ECB documents prior to sharing them outside the Eurosystem, ESCB or SSM.

**More:**
ECB Decision on public access to ECB documents
ECB Decision on public access to European Central Bank documents in the possession of the national competent authorities
ECB Decision on disclosure of confidential information in the context of criminal investigations

Common rules and minimum standards for the treatment of sensitive ESCB and SSM information

**See also:** BRB - What ECB information can I access via the different IT and communication equipment?

## How can I share ECB information?

- ✓ Share electronic information by using DARWIN links.
- ✓ If using DARWIN links is technically not possible:
  - share ECB-SECRET information by PGP or similar encrypted email;
  - share ECB-CONFIDENTIAL and ECB-RESTRICTED information via an ECB-approved secure collaboration portal, encrypted email, or secure email (TLS).
- ✓ If using a secure collaboration portal, encrypted email, or secure email (TLS) is not possible, share ECB-CONFIDENTIAL and ECB-RESTRICTED information by means of an encrypted portable storage device provided by the ECB.
- ✓ Send physical documents classified as ECB-SECRET and ECB-CONFIDENTIAL in two sealed envelopes with a return address on both envelopes. The inner envelope must indicate the classification and markings, where necessary. These ECB documents must be delivered as follows:
  - ECB-SECRET documents: hand over personally to the intended recipient or send via courier in tamper-proof envelopes with return receipt requested;
  - ECB-CONFIDENTIAL documents: sent via internal or registered mail.

**See also:** BRB - What ECB information can I access via the different IT and communication equipment?

## What additional responsibilities do I have regarding inside information?

- ✓ Exercise particular caution when handling inside information by:
  - accessing and sharing inside information on a "need-to-know" basis, as approved or confirmed by your management;
  - not participating in the preparation or discussion of ECB investment decisions which could be influenced by any market-sensitive inside information of which you are aware;
  - letting recipients know about the specific responsibilities involved in receiving market-sensitive inside information, in particular the prohibition on insider trading and unlawful disclosure.
- ✓ As SCT/IMA staff if you come into the possession of market-sensitive inside information from the FRS, BoJ or PBC:
  - immediately report this to the HoD of DIV/BMI or the Deputy Director General of DG/M to whom DIV/BMI reports;
  - do not participate in the preparation or discussion of the tactical benchmark proposal.
- ✓ As a manager in DIV/BMI, only grant access to inside information to individuals for whom such information is necessary.
- ✓ As a manager in DG/M:
  - ensure that staff in possession of market-sensitive inside information do not participate in the preparation of decisions on the ECB's acquisition or disposal of financial instruments to which this information relates. In particular ensure that:

- euro denominated, non-monetary policy portfolios are managed passively, with the exception of cash management transactions and securities lending activities;
- market-sensitive inside information received at quadripartite meetings between the ECB, FRS, BoJ and PBC is not disclosed to those actively managing tactical benchmark portfolios;
- staff in possession of market-sensitive inside information from the FRS, BoJ or PBC do not participate in the preparation or discussion of the tactical benchmark proposal;

- freeze tactical benchmark activities for one month if SCT/IMA staff have conducted foreign exchange interventions in the US dollar and/or the Japanese yen shortly before an ICO meeting or if upcoming interventions are planned to take place at or before the date of the ICO meeting, and extend the freeze if exceptional circumstances continue.

**Remember:** In addition to the prohibition under the Staff Rules, insider trading constitutes a criminal offence, which is punishable under national criminal law.

## 5. Protect ECB information

ECB information requires special protection, both on and off the ECB's premises. This means that sensitive information may only be accessed, discussed or temporarily stored using specific IT and communication equipment.

### What ECB information can I access via the different IT and communications equipment and applications?

✓ When accessing, discussing or temporarily storing ECB information, use IT and communication equipment as follows:

| ECB CLASSIFICATION | | ECB laptop or desktop computer | ECB phone, smartphone or tablet | ECB encrypted portable storage device | Private IT and communication equipment |
|---|---|---|---|---|---|
| ECB-SECRET | Discuss | Encrypted laptops only | Encrypted landline phones only | No | |
| | Access | | No | | |
| | Temporary storage | With explicit line manager permission and on encrypted laptops only | No | | |
| ECB-CONFIDENTIAL | Discuss | Yes | Yes | For needed time period | No |
| | Access | | In the business workspace | | Via Citrix |
| | Temporary storage | | | | No |
| ECB-RESTRICTED | Discuss | Yes | Yes | For needed time period | Yes |
| | Access | | In the business workspace | | Via Citrix |
| | Temporary storage | | | | No |
| ECB-UNRESTRICTED | Access | Yes | Yes | For needed time period | Yes |
| | Discuss | | | | |
| | Temporary storage | | | | |

✓ As soon as possible store all ECB information that you temporarily stored on your IT and communication equipment in the appropriate ECB information system and delete the local copy.

✓ When accessing, discussing or temporarily storing ECB information, use as first option the applications currently approved by the ECB and marked in **green** in the table below and use applications as follows:

| | ECB-SECRET | | ECB-CONFIDENTIAL | | ECB-RESTRICTED | | ECB-UNRESTRICTED | |
|---|---|---|---|---|---|---|---|---|
| | Access/ discuss | Storage | Access/ discuss | Storage | Access/ discuss | Storage | Access/ discuss | Storage |
| **Cisco WebEx** | No | | Via encrypted mode | | Yes | | Yes | |
| **Cisco Jabber** | No | | No | | Yes | | Yes | |
| **Brainloop (Virtual Data Room)** | No | | For needed time period | | For needed time period | | For needed time period | |
| **Slack team collaboration tool** | No | | No | | Yes, in channels with restricted access | | Yes | |
| **Cloud services for file sharing** | No | | No | | No | | For exceptional business reasons for needed time period | |
| **Web services for language translation (e.g. Google Translate)** | No | | No | | No | | Yes | |
| **Video/call/chat applications (e.g. Whatsapp, Telegram)** | No | | No | | No | | No | |
| **Public/commercial Doc-reader App downloadable in the personal workspace** | No | | No | | No | | Yes | |

**Remember:** Store ECB information on your ECB IT and communication equipment only if the ECB network is unavailable or if necessary in order to share the ECB information. Transfer ECB information back into the ECB network as soon as possible and delete local copies of ECB information.

## How do I protect ECB information on and off the ECB's premises?

✓ Do not leave sensitive ECB information unattended.

✓ When off the ECB's premises do not leave non-public ECB information or ECB IT and communication equipment unattended.

✓ Only take non-public ECB information off the ECB's premises if required for business purposes. In addition:

- for ECB-SECRET information – obtain prior approval from a senior manager (information owner) and register it in DARWIN under the Register of ECB-SECRET information taken out of ECB premises;
- for ECB-CONFIDENTIAL information – obtain prior approval from a HoD.

✓ If travelling to countries with a high espionage risk:
- never take ECB-SECRET information;
- only take ECB-CONFIDENTIAL information if absolutely necessary and after having registered it in the Register of ECB-CONFIDENTIAL documents taken to countries with a high risk of espionage.

✓ Be careful when accessing or discussing sensitive information in public:
- never access or discuss ECB-SECRET information;
- avoid accessing or discussing ECB-CONFIDENTIAL and ECB-RESTRICTED information. If unavoidable, protect it against "shoulder surfing" and ensure that you are not overheard.

**Remember:** ECB IT and communication equipment may only be used in line with the ECB's acceptable use policy in the BRB chapter on IT and communication equipment.
Immediately notify your management and the DG/IS Service Desk when you know or suspect that sensitive information or ECB IT and communication equipment have been compromised, stolen or lost.

When permanently leaving the ECB, you may only take copies of documents with senior management approval. Executive and SB members require a proposal by the CGO and approval of the EB. Staff and EB/SB members may not take any ECB-SECRET information when they leave.

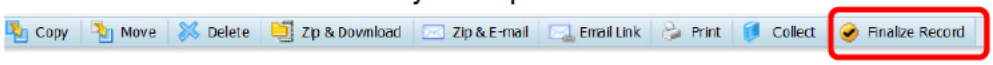
## 6. Keep or destroy ECB information

In order to document the decisions it takes, the ECB should keep valuable ECB information that it created or received (records); however, not all ECB information needs to be preserved. Information saved in DARWIN is retained or destroyed in an automated manner.

### How do I decide which information to keep or destroy?

| *KEEP (records)* | *DESTROY (non-records)* |
|---|---|
| ○ **evidence of business activities, decisions, transactions**<br>○ **information with future value, e.g. business, financial, legal, research**<br>○ **formal communication (between staff and external parties)** | ○ information of short-term value<br>○ information not required in the future<br>○ duplicates or copies<br>○ drafts superseded by a final version |

✓ Finalise the following records in DARWIN:
- final or approved documents, including business emails created or received by the ECB;
- folders once an ECB task or activity is completed.




✓ Transfer the following records to the archives as soon as they are signed, using the dedicated workflow:
- original contracts, agreements or memoranda of understanding with third parties;
- legal acts;
- summary proceedings and minutes of the decision-making bodies, the SB, the ESRB or ESCB and SSM Committees.

✓ Transfer physical records with a retention period of 10 years or longer to the archives within five years of the end of the activity using the dedicated workflow.

- ✓ Destroy information once it has reached its retention period as set out in the ECB Filing and Retention Plan.

**More:** Consult your RMS if you have any questions about keeping or destroying ECB information. Guidance on the transfer of physical files to the ECB's archives.

**See also:** Schedule A of the ECB Filing and Retention Plan explaining what ECB documents you can destroy.

### How do I destroy ECB information?

- ✓ For ECB-SECRET paper documents, use a cross-cut shredder.
- ✓ For ECB-CONFIDENTIAL and ECB-RESTRICTED paper documents, use a locked confidential waste container.
- ✓ For digital media containing sensitive information, use the special containers in the ECB printing centre.

**Remember:** Documents finalised as records in DARWIN are automatically kept and deleted in line with the ECB Filing and Retention Plan. DG/SE/IGO oversees all destruction of physical ECB records.
From July 2022, emails older than one year that have not been saved to DARWIN will be deleted from Outlook.

## 7. Responsibilities of DARWIN key users

DARWIN key users are staff members nominated by their management to help their business area deliver its information management responsibilities.

### What additional responsibilities do I have as a DARWIN key user?

- ✓ Maintain DARWIN folder structures within your area of responsibility.
- ✓ Administer membership of the DARWIN access groups managed within your area of responsibility, and provide access to DARWIN documents owned within your area of responsibility based on managerial decision.
- ✓ Provide advice and support to DARWIN users and raise awareness about DARWIN.
- ✓ Perform regular reconciliations in respect of access groups and access rights managed within your area of responsibility and report the results to your management.
- ✓ Support the implementation of the corrective actions identified in the DARWIN monitoring reports.
- ✓ Keep up to date on ECB Information Management and DARWIN developments e.g. by attending key user meetings.
- ✓ Attend DARWIN key user refresher training every three years and after an absence of more than 12 months.

**More:** DARWIN key user profile

# 8. Information management-related responsibilities of managers

Managers are responsible for awareness of and adherence to the ECB information management rules within their teams, in particular the protection of sensitive information by managing access to such information. Access rights should be granted based on the role of the ECB or non-ECB staff (role-based access) and should aim to strike the right balance between sharing when possible and protecting when necessary.

## What additional information management-related responsibilities do I have as a manager?

- ✓ As a manager:
  - approve, as information owner, the sharing of:
    - ECB-RESTRICTED information;
    - ECB-CONFIDENTIAL information within the ECB, ESCB, and the SSM;
  - on a yearly basis:
    - approve changes to groups and their composition, and
    - carry out the role certification;
  - on a yearly basis, verify and approve (reconcile) access rights to ECB-CONFIDENTIAL and ECB-RESTRICTED information within your area of responsibility;
  - make non-public information available to non-ECB staff only after you have checked that:
    - they have contractually agreed to the "House rules of the European Central Bank for external staff";
    - they have been informed of their responsibilities under the confidentiality regime and have signed a confidentiality declaration;
  - authorise access rights for non-ECB staff to ECB-CONFIDENTIAL information only after you have established their need to know and after they have received security clearance;
  - with the support of your RMS, identify vital records and ensure that they will be available during a crisis.
- ✓ As a HoD:
  - approve, as information owner, the sharing of ECB-CONFIDENTIAL information outside the ESCB/SSM;
  - approve the removal of non-public information from the ECB once you have established the business purpose.
- ✓ As a senior manager:
  - approve, and verify on a quarterly basis ECB-SECRET clearances for your business area's staff;
  - establish whether intended recipients need to know about ECB-SECRET information originating in your business area and authorise their access accordingly;
  - approve the temporary removal, from the ECB's premises, of ECB-SECRET information originating in your business area;
  - authorise the destruction of documents from your business area in accordance with the ECB Filing and Retention Plan.

# Need to send Instant Messages? Use Signal, not WhatsApp!

Given the high number of us working remotely, Signal has been approved as an additional instant messaging tool on mobile devices for efficient communication.

With the majority of us working remotely, it is essential to make communication between colleagues as simple as possible. While WebEx and Jabber should remain your preferred communication tool, and DARWIN your main document repository system of ECB information, you may – as of now – also use **Signal** as a tool for instant messaging and calls on your ECB or private mobile phone to discuss up to ECB-RESTRICTED information. Please use only Signal on your mobile phone, because it is end-to-end encrypted, which means that the messages you send and the calls you make can only be read or heard by your intended recipients, and thus it adequately protects ECB information. Do not use WhatsApp or other instant messaging tools to share ECB information!

**How can I install Signal?**

To install Signal, please go through the following steps:

1. Make sure to use a sufficiently recent operating system version on your mobile phone (at least iOS 10.0 on iPhones, or at least Android 8.0 (Oreo) or later on Android devices). If your private mobile phone uses an operating system older than the above, the installation of Signal will still be possible, but it should not be used for the exchange of ECB information, given that the operating system might be prone to severe security vulnerabilities.
2. Download Signal from the official market store – Apple Store or Google Play Store – and open Signal. The application is free of charge.
3. Follow the on-screen instructions to complete the registration process, i.e. entering your phone number and the verification code sent via SMS. You can allow access to your contacts.

**How can I use Signal?**

After registering your phone number, you can start communicating securely with other Signal users. Read here how to send a message.

You may use Signal on your private or ECB mobile phone, but not the Signal Desktop application.

All business-related conversations should be deleted as soon as possible. Signal gives you the possibility to set and manage disappearing messages after a specific time. We strongly recommend you to set the message timer to one day maximum. Read here how to do it on both Android and iOS devices.

You are not allowed to share files via Signal.

Please note that, as all publically available Apps that can be downloaded in the personal workspace of your ECB iPhones or in your private device, Signal is not subject to specific support from DG-IS. Therefore, the DG-IS Service Desk will not be able to assist if you experience usage difficulties.

**How do I know a contact is using Signal?**

- On iOS, Signal contacts stored in your phone's contact list will be shown as someone you can start a conversation with.
- On Android, when looking at your contact list within Signal, a blue letter in the outside column will indicate it is a Signal contact.

People who already know your number and already have you in their contact list can see that you joined Signal.

**How secure is Signal?**

Signal is designed to never collect or store any sensitive information; messages and calls cannot be accessed by the application owner or other third parties. In terms of privacy, all data is stored locally on your phone: the Signal service provider does not know your contacts and does not share your phone number with anyone.

With the introduction of Signal, the ECB follows the EU Commission who recently has suggested their staff to start using Signal as well.

For more information, visit and read on Signal's website:

- support page: https://support.signal.org/hc/en-us
- the technical information in the blog post
- some common security questions

If the use of Signal is successful, the Business Rulebook will be updated accordingly to introduce Signal permanently.

Menu

# Workspace administration

Learn how to manage your Slack workspace or Enterprise Grid org.

## Customize message and file retention

By default, Slack will retain all messages and files for the lifetime of your workspace. If you'd like, you can adjust your retention settings to automatically delete messages and files after a set amount of time. You can also allow members to edit the message retention settings for individual channels and direct messages (DMs).

### What you need to know

- Message and file deletion is permanent. Adjust these settings with care.
- Deletions run once a day, so making changes can result in data being deleted shortly after a policy has been set.
- Retention settings will apply to all messages and files, including ones that are pinned or saved.
- On the Enterprise Grid plan, you can set a policy for retention settings that will apply to every workspace in your organizations.

**Note:** If a request to export data from all channels and conversations has been approved in your workspace or Enterprise Grid org, custom retention settings will be reset to keep all files.

## Adjust message retention settings

You can choose from three different options when setting message retention for conversations. Keep in mind that your retention settings will impact what you see in an export file.

- **Keep everything**
  Slack will keep all messages and track message edits and deletions.
- **Keep all messages, but don't track revisions**
  Slack will keep all messages, but will not track message edits or deletions.
- **Delete messages and their revisions after...**
  Slack will delete messages following the custom time frame you choose.

> **Note:** If admins or members are allowed to edit retention settings for individual conversations, those settings will override the workspace or org-wide settings.

Pro and Business+ plans  Enterprise Grid plan

## Allow conversation-specific retention settings

Workspace Owners and Org Owners can allow people to override retention settings and edit message retention for individual conversations with the following options:

- **Admin overrides** allow admins on the Business+ and Enterprise Grid plans to edit message retention for public and private channels with channel management tools.
- **Member overrides** allow members on all plans to set their own message retention period for private channels and direct messages they're a part of.

Pro and Business+ plans  Enterprise Grid plan

## Adjust file retention settings

When configuring your file retention settings, there are two options to choose from:

- **Keep all files**
  Slack will keep all shared files for the lifetime of your workspace.
- **Keep all files, only for a set number of days**
  Slack will permanently delete files (snippets, posts, uploaded files, and those shared via third-party apps like Dropbox or Google Drive) older than the number of days you choose.

**Note:** Files shared via apps like Dropbox or Google Drive remain stored in the service they originate from. Deleting them from Slack won't impact the original files.

Pro and Business+ plans  Enterprise Grid plans

**Note:** It's not currently possible to set file retention settings for specific conversations.

**Who can use this feature?**

- **Workspace Owners** and **Org Owners**
- Available on **paid plans**

Yes, thanks!  Not really

**Can I use alternative collaboration tools to Webex e.g. Zoom, Slack etc. for business purposes?**

**Webex is the recommended and preferred tool to remotely discuss up to ECB-CONFIDENTIAL information, when using Webex Meetings in End-To-End Encryption mode** (Read on How to create an encrypted Webex meeting)

Only if you cannot use Webex, are you allowed to use Slack to discuss up to ECB-UNRESTRICTED information. Please note that Slack is not an ECB Service; this means that DG-IS Service Desk is not trained to support you in case of need, and the provider is free to change, restrict, or modify its usage anytime. You should also be particularly careful when using restricted channels via Slack; even though the access is only by invitation and password protected, new joiners will be able to see previous conversations, with a potential risk of information disclosure.

Other software freely available for teleconferencing, like **Skype for Business, should be avoided**. They cannot guarantee the adequate level of security and data protection that is required for handling ECB and personal information.

Zoom has now been re-enabled on ECB laptops to attend externally organised trainings and conferences and to discuss non-sensitive ECB information only, find more information here.

EUROPEAN CENTRAL BANK

EUROSYSTEM

DG-SE/IMS

**ECB-UNRESTRICTED**

Information Management Expert

21 July 2015

**UPDATABLE**

# Guidance on the use of the Instant Messaging function of Cisco Jabber

## 1. Use of the Instant Messaging Function of Cisco Jabber

Cisco Jabber is an add-on tool to enhance the user's experience of his/her ECB desk phone. In addition to a callers list, it also provides an instant messaging tool that is very suitable for the exchange of short-lived information and informal discussions.

It is not a suitable tool to document and record policies, activities and decisions. For such purposes you must continue to draft, save and finalize such information in DARWIN.

The Instant Messaging function can be used in two different ways:

- To exchange text messages using the chat window: recommended for informal exchanges and short-lived business information, and
- to *send a screen-capture:* recommended for informal exchanges, trouble-shooting and short-lived business information

## 2. Capturing business relevant information in DARWIN

According to the BPH, "Information created or received in the course of ECB business, whether electronically or physically, must be captured in the designated ECB information systems so that it can be accessed for reasons of business need, continuity and accountability". If business relevant information is erroneously exchanged via a Jabber conversation, the author must capture it in an e-mail or any other appropriate format and save it in the relevant workspace in DARWIN.

## 3. Retention and deletion of conversations

Remember, that once you initiate a conversation in Jabber you cannot delete it, either fully or any part of it. For each chat contact, Jabber keeps the last 99 messages; once this number is reached the oldest message will be automatically deleted. Deleted messages cannot be recovered.

## 4. Do’s and Don’ts

**Do use Jabber:**

- ✓ for informal conversations
- ✓ for short-lived business-related information
- ✓ to quickly send links to documents in DARWIN

**Do not use Jabber:**

- x for information with a long-term business value
- x to communicate sensitive ECB information (ECB-RESTRICTED, ECB-CONFIDENTIAL or ECB-SECRET)
- x “Send a file” option to exchange documents containing business-related information (business documents should only be saved in DARWIN).

EUROPEAN CENTRAL BANK

EUROSYSTEM

**ECB-UNRESTRICTED**

## DG-SE/IGO/IGP

# Governance of MS Teams at the ECB

[redacted]
Information Management Expert

**UPDATABLE**
DARWIN ID: 290598044
4 December 2020

# VERSION HISTORY

**Author:** [redacted] DG-SE/IGO

**Object ID:** 290598044

**Version history** (A printed version of this document is an uncontrolled copy. See DARWIN for all controlled versions.)

| Date | Contributor's Name | Revision Description |
|---|---|---|
| 30 Sep 2020 | [redacted] | Release draft 1.0 |
| 6 Nov 2020 | [redacted] | Release draft 2.0 |
| 17 Nov 2020 | [redacted] | Release draft 3.0 – Guest access removed to annex. Annex on BRB removed. Include Miro Governance. |
| 4 Dec 2020 | [redacted] | Final release before Pilot – References updated. Document set to UPDATABLE |
| 14 Dec 2020 | [redacted] | Removing references to Planner and WebEx. Cosmetic changes. |

## Table of contents

# Governance of MS Teams

## 1. Purpose of Teams

Microsoft (MS) Teams serves multiple purposes, including allowing users to chat and make calls with seamless integration with MS Outlook and to facilitate collaboration in context, e.g. in a project, a Committee, a Joint Supervisory Team or for ad-hoc collaboration. It is also a binding element which allows diverse applications and services (messaging, meetings, calls, DARWIN, digital whiteboards) to be used within the same context and user interface.

MS Teams will be used to collaborate with other users within the boundaries defined by the Business Rulebook and in conjunction with other ECB systems such DARWIN, ASTRA[1] and the Intranet.

Use of terms in this document:

- *MS Teams* will be used to refer to the application;
- *Chat* will be used to refer to the private chat functionality one to one or one to many (second icon from the top);
- *Team(s)* will be used to refer to a Team workspace created in MS Teams (third icon from the top);
- *Team channel* will be used to refer to the channels created inside a Team;
- *Calls* will be used to refer to the communication functionalities of MS Teams, namely Call and Video Call (5th icon from the top);
- *MS Team meetings* will be used to refer to meetings scheduled using the Calendar functionality (4th icon from the top) or the MS Outlook integration.


This document assumes the following configuration settings:

- Simple integration with DARWIN
- Guest access is not allowed

[1] ASTRA is the platform used by the European Central Bank (ECB) to exchange documents with external (i.e. non-ESCB/SSM) institutions and partners

# 2. Roles and responsibilities in MS Teams

## 2.1 ECB users

All ECB users can use MS Teams functionalities across Business Areas and can request the creation of a Team via the IGAM Portal (https://igam.ecb.de).

Any ECB user can create Chats to discuss information with other users or several users, use the Calls functionalities and schedule MS Teams meetings (meetings can be scheduled with both ECB and non-ECB users, just using the email address of the participants).

## 2.2 Non-ECB users

In MS Teams there are two modalities of access for non-ECB users, each modality has different features.

External access

External access allows an entire external domain (e.g. a whole central bank, institution or company) to find, call, chat, and set up meetings in Teams. The list of domains to be federated will be pre-defined and additional domains can be added on a case by case basis via normal IT change[2]. In this case, communication with external users would be limited to chats and meetings (i.e. not possible to be members of a Team).

Guest access

Guest access provides the possibility for non-ECB users to be invited to collaborate in Teams and channels. Due to security concerns by default new Teams will be created with **no guest access**. Guest access is under further investigation and might be introduced in subsequent releases[3].

ECB users can be invited as Guests in the MS Teams tenant of other institutions. When collaborating in non-ECB systems, ECB users should be particularly aware of the limitations to share information set out in Section 3.4 of the Business Rulebook[4].

[2] This feature is not active yet

[3] Annex 1 details the use cases under investigation

[4] Business Rulebook (BRB.3.4) available at:
https://intranet.ecb.europa.eu/Interact/Pages/Content/Document.aspx?id=3414

# 3. Team creation

## 3.1 Team request

Any ECB user can request via IGAM portal (https://igam.ecb.de) the creation of a Team using a request workflow. The requestor will select the division or service owner and provide a number of elements that define the Team:

- **Description of the Team**
- **Confidentiality classification** (maximum level of sensitivity of information exchanged in the Team)
- **Definition of Team** as public (anybody can join) or private (users need to be invited). Public teams should only be requested for sharing up to ECB-UNRESTRICTED information.
- **Guest access** (by default no Guest access until use cases are clarified, see section 2.2 above)
- **Link to DARWIN workspace** in which documents will be saved (ideally this should trigger the creation of a tab in the team that links to that workspace)
- **Applicable template** (a number of templates will be offered for different pre-defined use cases)
- **Owning organisation**: the division, section or service that will be responsible to approve/review the access.

## 3.2 Request for access

ECB users can request access to a Team via the IGAM portal (https://igam.ecb.de) (IGAM>Request Access>Request for Self).

## 3.3 Team ownership and approval

The owning organisation will be defined in the request to create a Team. The following responsibilities will be performed by this role:

- Verify and approve membership, including the follow-up process of recertification of membership;
- Update Team name and description;

- Request the deletion of a Team.

The approval of a Team is done by the approver group of the owning organisation in the IGAM portal

### 3.4 Naming and organisation of Teams

A Team must have a meaningful name that describes the business activity the Team is involved in. Duplication of names should be avoided. In order to facilitate future management, the title should give certain indication about the activity and ownership (e.g. Business Area).

Teams have the same name as the underlying group created in IGAM with the following naming convention:

| | | | | |
|---|---|---|---|---|
| **<tenant>**<br><br>TEAM | - | **<Service Short>**<br><br>Divisions, sections, committees | - | **<description short>**<br><br>Free text, no space, no dash, only alphanumeric and underscore allowed |

e.g. TEAM-IOS-TEAMS2020_Project

Team names are automatically built with the information from the request form.

### 3.5 Defining Team templates

Templates will be defined for different use cases so that standard elements are predefined following the table below:

| TEAM | APPROVAL | CONFIDENTIALITY | MEMBERSHIP | GUESTS | APPS |
|---|---|---|---|---|---|
| Type of team | Approval of owning organisation | Maximum retention | Private/Public | Not allowed | ☐ OneNote<br>☐ Website<br>☐ Miro |

### 3.6 Creation and use of channels

Members of the Team can create channels. Only public channels - that can be seen by all the members of the Team - will be allowed. Private channels are disabled as they are not compliant with ECB retention rules and policies. If there is a need for restricted access a separate Team or a Chat group could be used.

### 3.7 Apps available in Teams

The following apps will be integrated in MS Teams:

- OneNote

Third-party apps:

- Miro (Digital Whiteboard)

## 4. What type of information can be shared?

Business information up to ECB-CONFIDENTIAL can be shared within MS Teams chats and Team channels, and orally in meetings. The rules for accessing and sharing information contained in Section 3.4 of the Business Rulebook[5] also apply to exchanges of information via Teams, chats and meetings (e.g. If necessary, obtain prior traceable approval before sharing).

MS Teams chats, Team channels and meetings should not be used for the sharing of personal data (including special categories of data[6]).

### 4.1 Sharing documents in MS Teams

The standard way of sharing documents in MS Teams is by sharing links to documents in DARWIN, in line with the Business Rulebook, BRB 3.3[7]. Users can temporarily share documents as part of a Team channel conversation or in a Chat (e.g. initial sharing of early draft, sharing of a document for a quick check and to allow co-editing of the document). In order to avoid the creation of new silos and repositories, documents in Chats and Teams are considered as convenience copies and as such subject to a 7 days retention period counting form the creation date. Documents that have a longer business value must be stored in DARWIN where they will be managed according to the relevant policies.

### 4.2 SharePoint and OneDrive

SharePoint and OneDrive for Business are used in the background of MS Teams to store documents exchanged in Teams (SharePoint) and in Chats (OneDrive for Business). In order to avoid the creation

[5] Business Rulebook (BRB.3.4) available at: https://intranet.ecb.europa.eu/Interact/Pages/Content/Document.aspx?id=3414

[6] Regulation (EU) 2018/1725 (EUDPR) sets forth the rules applicable to the processing of personal data by EU institutions, bodies, offices and agencies which are in line with the high data protection standards established in the GDPR.

[7] Business Rulebook (BRB.3.3) available at: https://intranet.ecb.europa.eu/Interact/Pages/Content/Document.aspx?id=3413

of parallel repositories, both systems will only be accessible from Teams. In line with the above a retention of 7 days will be applied to any documents that are stored in those locations.

### 4.3 Integration with DARWIN

Integration with DARWIN (simple integration) uses the standard add Website app in MS Teams. In this way Teams can be connected to one or several DARWIN workspaces or documents adding the DARWIN URL. The URLs are shown as tabs (see figure below) and can be opened by clicking on them.


From the tab users are able to perform basic DARWIN functionalities like browsing, open and edit documents, copy links, etc.

## 5. Expiration and retirement of MS Teams

Teams are regularly monitored so that unused teams are retired (archived and/or deleted). An overview of active Teams and their owners should be available to IGO for follow up actions.

The owning organisation will have to confirm every year that the Team is still in use and that membership is correct (recertification).

If a Team has not been used for a year it will be archived (with prior notification to the owning organisation). Once a Team is archived it will be retained for 6 months and then deleted with all its content.

In the view of monitoring this process, regular reports on deleted/to be deleted Teams and adequate reporting capabilities should be available to DG-SE/IGO.

## 6. Retention of MS Teams

The standard retention is different for different elements in Teams:

- Team conversations and chats: deletion after 1 year
- Documents uploaded to a Team channel (stored in SharePoint): deletion after 7 days
- Documents uploaded to a chat (stored in OneDrive for Business): deletion after 7 days
- Team is archived after 1 year inactive and deleted after 6 months.

## 7. Support and maintenance of Teams

[pending definition of the operating model and business ownership]

In this section we will define the roles that will be in charge of providing support to users with functional questions on how to use the system and also who is going to maintain the Teams, i.e. ensure that unused Teams are either archived or deleted and that owners have done the regular recertification/reconciliation of Teams and groups, retention is correctly applied and executed, etc.

Drawing reports on owner and member changes, recertifications and renewal activities logged in the system, user access, user activities, tasks and approvals will be relevant for this function.

Guidance on use of Teams is available for users in the dedicated intranet page.

## 8. Miro – Digital Whiteboard

Miro is an online collaborative whiteboard platform integrated with MS Teams to allow Teams to collaborate and be more creative.

Information up to ECB-CONFIDENTIAL can be created and shared in Miro.

It is the responsibility of the Whiteboard owner to control that the right users have access to the right information according to the rules for accessing and sharing information contained in Section 3.4 of the Business Rulebook[8]. The owner is also responsible for capturing the relevant content of the whiteboards in DARWIN and delete it as soon as it is no longer needed in Miro.

Miro whiteboards should not be used for the sharing of personal data (including special categories of data[9]).

[8] Business Rulebook (BRB.3.4 https://intranet.ecb.europa.eu/Interact/Pages/Content/Document.aspx?id=3414

[9] Regulation (EU) 2018/1725 (EUDPR) sets forth the rules applicable to the processing of personal data by EU institutions, bodies, offices and agencies which are in line with the high data protection standards established in the GDPR.

**Annex 1:**

Currently there are concerns on whether Guest users would be properly authenticated to access ECB systems. For that purpose it has been decided to further investigate and test the different use cases that are summarised in the table below (Table 1).

| Use case | Access to DARWIN | Access to ASTRA | Maximum Confidentiality | IAM account possible |
|---|---|---|---|---|
| ESCB collaboration | Yes | Not needed | ECB-CONFIDENTIAL | Yes |
| SSM collaboration | Yes | Not needed | ECB-CONFIDENTIAL | Yes |
| Users outside ESCB/SSM (third parties) | No | Possible | ECB-CONFIDENTIAL | No |

**Table 1**

Elements to investigate and test:

- Ensure that Guest access has management approval
- Disable sharing of documents with externals (as documents should be shared via ASTRA links only)
- Guest access must comply with the confidentiality rules in the Business Rulebook and ESCB/SSM access management policies
- Define responsibility of owners towards Guest access and tools needed for compliance
- Recertification of access
- GDPR requirements that might arise from Data Protection Assessment

# How long will your information be kept in MS Teams

Learn more about retention in MS Teams

- **Files:** 7 days from date of upload
- **Teams and Team channels:** archived after 1 year of inactivity. Deleted 6 months after archived.
- **Conversations in Teams**: 1 year - please be aware that anyone joining your team will be able to read messages of up to the last 12 months.
- **Chats (1:1, group):** 1 year

What should you do if you need to keep something for a longer period?

**Save to DARWIN** any information that is relevant for a longer period.

| FILE PATH | FILE NAME | ITEM TYPE | DATA ID | VERSION | STATUS | DETAILS |
|---|---|---|---|---|---|---|
| | Attachment 1 - Copy of Business Rulebook - Chapter 3.pdf | Document | 344753716 | 1 | Succeeded | |
| | Attachment 2 - Copy of intranet article - Need to send Instant Messages - Use Signal, not WhatsApp - ECB intranet.pdf | Document | 343478038 | 1 | Succeeded | |
| | Attachment 3 - Customize message and file retention Slack.pdf | Document | 346321646 | 1 | Succeeded | |
| | Attachment 4 - Extract from Intranet article on use of Slack.pdf | Document | 346385507 | 1 | Succeeded | |
| | Attachment 5 - Copy of Guidance on the use of the Instant Messaging function of Cisco Jabber - UPDATABLE.pdf | Document | 344793050 | 1 | Succeeded | |
| | Attachment 6 - Copy of 2020-11 - Governance of MS Teams - UPDATABLE.pdf | Document | 344696897 | 1 | Succeeded | |
| | Attachment 7 - How long will your information be kept in MS Teams - ECB intranet.pdf | Document | 344697129 | 1 | Succeeded | |
| | EO 2021 03 ECB reply - survey on recording of text and instant messages.pdf | Document | 355125533 | 1 | Succeeded | |