SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: Dropbox International Unlimited Company

Verification-ID	2022LVL02SCOPE3114
Date of Approval	July 2023
Valid until	July 2024

Table of Contents

1 Verification against v2.11 of the EU Cloud CoC

This Declaration of Adherence was against the *European Data Protection Code of Conduct for Cloud Service Providers* (**'EU Cloud CoC'**)[1] in its version 2.11 (**'v2.11'**)[2] as of December 2020.

Originally drafted by the Cloud Select Industry Group[3] (**'C-SIG'**) the EU Cloud CoC – at that time called C-SIG Code of Conduct on data protection for Cloud Service Providers – was developed against Directive 95/46/EC[4] and incorporated feedback by the European Commission as well as Working Party 29. Following an extensive revision of earlier versions of Code and further developing the substance of the Code (v2.11) and its provisions has been aligned to the European General Data Protection Regulation (**'GDPR'**)[5].

2 List of declared services

2.1 Dropbox Teams[6]

Dropbox declares its suite under the EU Cloud CoC, which comprised at the time of assessment of the following elements and features.

The service known as Dropbox Teams is comprised of the Standard, Advanced, Enterprise, and Education plans for teams. This service is a productivity platform that offers collaboration features, such as file sync and share, version history, deletion recovery, live support, and a suite of administrator features for better control, visibility, and management. Dropbox Education is designed specifically for the needs of higher education institutions. Dropbox Paper is a feature available in all teams' plans.

A common set of control processes applies across all Dropbox products. The Standard, Advanced, Enterprise, and Education Dropbox plans provide cloud storage, file synchronization, and collaboration capabilities to organizations around the world. Users can collaborate in, store, and share files and Paper docs seamlessly, as well as access important information from any supported operating system or device. The service is designed to keep users' data safe, confidential, and available. In

[1] https://eucoc.cloud
[2] https://eucoc.cloud/get-the-code
[3] https://ec.europa.eu/digital-single-market/en/cloud-select-industry-group-code-conduct
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[6] https://www.dropbox.com

addition, customer administrators have a central console that provides visibility and control over user activity. [7]

2.1.1 Dropbox core features

- Storage
- Users
- Best-in-class sync technology
- Anytime, anywhere access
- Easy and secure sharing
- 256-bit AES and SSL/TLS encryption

2.1.2 Content and accident protection

- Dropbox Backup
- File recovery and version history (180 days)
- Dropbox Rewind (180-day history)
- Shared link controls
- External sharing controls and reporting
- Data classification
- Ransomware detection and recovery
- Alerts and notifications
- Dropbox Passwords
- Account Tool Transfer
- Remote device wipe
- Enable Multifactor Authentication
- Watermarking
- Enables HIPAA compliance
- Device approvals

2.1.3 Productivity and sharing tools

- Dropbox Paper
- Dropbox Capture
- Dropbox Replay
- Dropbox Transfer
- File locking
- Integrated cloud content
- Branded sharing
- Web previews and comments
- PDF editing
- Plus button
- File requests
- Full text search
- Viewer history

2.1.4 Team Management

- Admin console
- Multi-team admin login
- Centralized billing
- Company-managed groups
- Unlimited API access to security platform partners
- Unlimited API access to productivity platform partners
- 1 billion API calls/month for data transport partners
- Tiered admin roles
- Sign in as user
- Audit logs with file event tracking
- Single sign-on (SSO) integrations
- Invite enforcement

[7] **NOTE**: The content for the service description has been provided by the CSP and does not reflect any opinion of or assessment by the Monitoring Body.

2.1.5 Support[8]

- Priority email support
- Live chat support
- Phone support during business hours

3 Verification Process - Background

V2.11 of the EU Cloud CoC has been developed against GDPR and hence provides mechanisms as required by Articles 40 and 41 GDPR[9].

3.1 Approval of the Code and Accreditation of the Monitoring Body

The services concerned passed the verification process by the Monitoring Body of the EU Cloud CoC, i.e., SCOPE Europe sprl/bvba[10].

The Code has been officially approved in May 2021[11]. SCOPE Europe has been officially accredited as Monitoring Body in May 2021[12]. The robust and complex procedures and mechanisms can be reviewed by any third-party in detail at the website of the EU Cloud CoC alongside a short summary thereof.[13]

3.2 Principles of the Verification Process

Notwithstanding the powers of and requirements set out by the supervisory authority pursuant to Article 41 GDPR, the Monitoring Body will assess whether a Cloud Service, that has been declared adherent to the Code, is compliant with the requirements of the Code - especially as laid down in the Controls Catalogue. Unless otherwise provided by the Code, the Monitoring Body's assessment process will be based on an evidence-based conformity assessment, based on interviews and document reviews; proactively performed by the Monitoring Body.

To the extent the Monitoring Body is not satisfied with the evidence provided by a CSP with regards to the Cloud Service to be declared adherent to the Code, the Monitoring Body will request additional information. Where the information provided by the CSP appears to be inconsistent or false, the Monitoring Body will - as necessary - request substantiation by independent reports.

---

[8] **NOTE:** These elements were listed for the purpose of completeness. However, it is considered that such elements are provided by the CSP in its role as Controller, thus falling out of scope of the Code.
[9] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[10] https://scope-europe.eu
[11] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n05-2021-of-20-may-2021.pdf
[12] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n-06-2021-of-20-may-2021.pdf
[13] https://eucoc.cloud/en/public-register/assessment-procedure/

3.3 Multiple Safeguards of Compliance

Compliance of adherent services is safeguarded by the interaction of several mechanisms, i.e., continuous, rigorous, and independent monitoring, an independent complaints' handling process, and finally any CSP declaring services adherent is subject to substantial remedies and penalties in case of any infringement.

3.4 Process in Detail

It is expected that, prior to any assessment of the Monitoring Body, each CSP assesses its compliance internally. When declaring its service(s) adherent to the EU Cloud CoC, each CSP must elaborate its compliance with each of the Controls as provided by the Code considering the Control Guidance, as provided by the Controls Catalogue, to the Monitoring Body.

The CSP may do so either by referencing existing third-party audits or certifications, their respective reports and by free text responses. Additionally, the CSP will have to provide a general overview of the functionalities, technical, organisational and contractual frameworks of the service(s) declared adherent.

With regards to internationally recognised standards, the Monitoring Body will consider the mapping as provided by the Controls Catalogue. However, the Monitoring Body will verify whether (a) any third-party certification or audit provided by the CSP applies to the Cloud Service concerned, (b) such third-party certification or audit provided by the CSP is valid, (c) such third-party certification or audit has assessed and sufficiently reported compliance with the mapped controls of the third-party certification or audit concerned. Provided that the aforementioned criteria are met, the Monitoring Body may consider such third-party certifications or audits as sufficient evidence for the compliance with the Code.

Within Initial Assessments, the Monitoring Body selects an appropriate share of Controls that will undergo in-depth scrutiny, e.g., by sample-taking and requesting further, detailed information including potentially confidential information. Within any other Recurring Assessment, the Monitoring Body will select an appropriate share of Controls provided that over a due period every Control will be subject to scrutiny by the Monitoring Body. Where applicable, aspects of current attention at the time of assessment shall be covered too, e.g., where such aspects were indicated in media reports, publications or actions of supervisory authorities.

If the responses of the CSP satisfy the Monitoring Body, especially if responses are consistent and of appropriate quality and level of detail, reflecting the requirements of the Controls and indicating appropriate implementation by the Control Guidance, then, the Monitoring Body verifies the service(s) declared adhered as compliant and thereupon, makes them subject to continuous monitoring.

3.4.1 Levels of Compliance

V2.11 of the Code provides three different levels of Compliance. The different levels of compliance relate only to the levels of evidence that are submitted to the Monitoring Body. There is, however, no difference in terms of which parts of the Code are covered, since adherent Cloud Services have to comply with all provisions of the Code and their respective Controls.

3.4.1.1 First Level of Compliance

The CSP has performed an internal review and documented its implemented measures proving compliance with the requirements of the Code with regard to the declared Cloud Service and confirms that the Cloud Service fully complies with the requirements set out in this Code and further specified in the Controls Catalogue. The Monitoring Body verifies that the Cloud Service complies with the Code by information originating from the CSP.

3.4.1.2 Second Level of Compliance

Additional to the "First Level of Compliance", Compliance with the Code is partially supported by independent third-party certificates and audits, which the CSP has undergone with specific relevance to the Cloud Service declared adherent and which were based upon internationally recognised standards procedures. Any such third-party certificates and audits that covered controls similar to this Code, but not less protective, are considered in the verification process of the Monitoring Body. Each third-party certificates and audits that were considered in the verification process by the Monitoring Body shall be referred in the Monitoring Body's report of verification, provided that the findings of such certificates were sufficiently and convincingly reported and documented towards the Monitoring Body and only to the extent such certificates and audits are in line with the Code. The CSP must notify the Monitoring Body if there are any changes to the provided certificates or audits.

The Controls Catalogue may give guidance on third-party certificates and audits that are equivalent to certain Controls in terms of providing evidence of complying with the Code.

However, to those Controls that the CSP has not provided any equivalent third-party certificate or audit, the Monitoring Body verifies that the Cloud Service complies with the Code by information originating from the CSP.

The Monitoring Body may refuse application of Second Level of Compliance if third-party certificates and audit reports, that are recognised by the Monitoring Body in the verification process concerned, are not covering an adequate share of Controls of this Code; such adequate share shall be subject to the discretion of the Monitoring Body, considering e.g., the share related to the overall amount of Controls of the Code or whether a full Section or topic is being covered.

3.4.1.3 Third Level of Compliance

Identical to the "Second Level of Compliance" but Compliance is fully supported by independent third-party certificates and audits, which the CSP has undergone with regard to the Cloud Service declared adherent and which were based upon internationally recognised standards.

To the extent a CSP refers to individual reports, such as ISAE-3000 reports, the CSP shall ensure that such reports provide sufficient and assessable information and details on the actual measures implemented by the CSP regarding the Cloud Service concerned. The Monitoring Body shall, if considered necessary, in consultation with the Steering Board, define further requirements on such individual reports, such as accreditation and training for auditors against the provisions and requirements of this Code.

3.4.2 Final decision on the applicable Level of Compliance

When declaring its Cloud Service adherent, the CSP indicates the Level of Compliance it is seeking to achieve. Any final decision, whether a CSP is meeting the requirements of a specific Level of Compliance is at the sole discretion of the Monitoring Body.

3.5 Transparency about adherence

Each service adherent to the EU Cloud CoC must transparently communicate its adherence by both using the appropriate Compliance Mark[14] and referring to the Public Register of the EU Cloud CoC[15] to enable Customers to verify the validity of adherence.

[14] https://eucoc.cloud/en/public-register/levels-of-compliance/
[15] https://eucoc.cloud/en/public-register/

4 Assessment of declared services by Dropbox (see 2.)

4.1 Fact Finding

Following the declaration of adherence of Dropbox International Unlimited Company ('**Dropbox**'), the Monitoring Body provided Dropbox with a template, requesting Dropbox to detail its compliance with each of the Controls of the EU Cloud CoC.

As this declaration is a renewal[16], the Monitoring Body requested from Dropbox a confirmation that there has been no material change to the applicable technical and organisational and contractual framework. The Monitoring Body also requested from Dropbox a comparison of the declared Cloud Services of last year and this year as well as to explicitly indicate any Cloud Services that are no longer included in the Declaration of Adherence and, where applicable, provide the Monitoring Body with adequate reasons. To the extent the list of Cloud Services was extended, the Monitoring Body requested a confirmation, that any such additional Cloud Services are subject to the same technical, organisational and contractual framework as the original Cloud Services.

Dropbox promptly responded to the templates. Information provided consisted of references and list of actual measures meeting the requirements of each Control, a free text answer describing their measures, and a reference to third party audits and certifications, where applicable. This information was completed by the confirmations requested by the Monitoring Body as well as a detailed comparison of the declared Cloud Services between last year and this year verification highlighting the changes and the reasons for them.

4.2 Selection of Controls for in-depth assessment

Following the provisions of the Code and the Assessment Procedure applicable to the EU Cloud CoC[17], the Monitoring Body analysed the responses and information provided by Dropbox.

Dropbox's declared services have been externally certified and audited. Dropbox holds an ISO certificate, which is valid for the duration of the Declaration of Adherence, and the scope of registration includes all the declared services. The declaration of adherence referred to the respective ISO certification within the responses to Section 6 of the Code (IT Security). As provided by the Code, the Monitoring Body may consider third-party certifications and audits. Accordingly, the Monitoring Body

[16] You can access the Verification Report(s) of previous year(s) via the following link(s): Report 2022
[17] https://eucoc.cloud/en/about/about-eu-cloud-coc/applicable-procedures/

verified the certification and references. Further in-depth checks were not performed, as provided third-party certifications adequately indicated compliance.

4.3 Examined Controls and related findings by the Monitoring Body

4.3.1 Examined Controls

The Monitoring Body reviewed the submission from Dropbox which outlined how all the requirements of the Code were met by Dropbox's implemented measures. In line with the Monitoring Body's process outlined in Section 3.4, the Monitoring Body selected a subset of Controls from the Code for in-depth scrutiny. In-depth scrutiny reflects sample taking and follow-up questions, whilst the latter may address requests for clarifications or more detailed information. The Controls selected for this level of review were: 5.1.A, 5.1.D, 5.1.E, 5.2.C, 5.2.E, 5.3.D, 5.3.E, 5.4.A, 5.4.C, 5.4.E, 5.5.E, 5.7.A, 5.7.B, 5.7.F, 5.8.A, 5.11.B and 6.1.C.

4.3.2 Findings by the Monitoring Body

During the process of verification, Dropbox consistently prepared the Declaration of Adherence well and thoroughly. Dropbox's responses were detailed and never created any impression of intentional non-transparency. Requests for clarification, additional and supporting information, as well as relevant samples were promptly dealt with and always met the deadlines set by the Monitoring Body.

Related to the Monitoring Body's requests (see section 4.1), Dropbox indicated that no relevant changes to the Cloud Service Family were applied in regards of the implemented technical, organisational and contractual framework. Where additional Cloud Services were added, Dropbox provided explicit confirmation that such Cloud Services belong to the same Cloud Service Family.

An area of focus was built around subprocessor management. As provided towards the Monitoring Body, Dropbox obtains written authorisation of the Customer prior to the processing of Customer Personal Data. Dropbox has a defined mechanism to notify Customers of the changes in subprocessors. The timelines for exercising an alternative option, as well as the means to do so were confirmed by Dropbox's contractual documents. The good standing of subprocessors, as well as the technical and organisational measures implemented by them are verified by Dropbox. In the same vein, flow-down mechanisms are implemented and this includes contractual obligations of subprocessors to adhere to the same standards of data processing as the Dropbox.

The Monitoring Body also assessed Customers' Audit Rights. Dropbox indicated to having adopted a staggered approach, which ensures that existing audit reports and certifications are provided to Customers at a first step, either upon request or if publicly available, on the Dropbox Trust Center. As a

second step, if ever the Customer is of opinion that further information is needed, the Customer is able to provide written questions on the audit reports to Dropbox. As a last step Customers are able perform an audit on Dropbox's premises. In addition to this, Dropbox provided the Monitoring Body with an overview of the methodology to determine the costs of an audit. Contractual obligations ensure that an estimate of costs related to an audit is provided to Customers before such costs are incurred.

The Code requires CSPs to assist Customers to respond to data subject requests. Dropbox confirmed providing Customers with self-service functionalities to enable them to respond to data subject requests. Likewise, where Customers may require additional support, Dropbox also offers to support Customers in this respect. Further to this, Dropbox affirmed having documented procedures to assist the Customer in fulfilling data subject requests, which include offering additional support to Customer, where required.

Dropbox's records of processing activities ('ROPA') built another area of focus. Based on the sample provided, the Monitoring Body was able to verify that Dropbox maintains a ROPA in its capacity as Processor, which includes the relevant information as per Article 30.2 GDPR. The relevant communication channels for Customers to provide the relevant information in relation to the completion and relevancy of the ROPA were confirmed by Dropbox.

Procedures to deal with requests from Supervisory Authorities were assessed. Dropbox's contractual documents confirmed Dropbox's contractual obligations to notify Customers, where legally permissible. In addition to this, Dropbox referred to an internal procedure operationalising requests received from regulators, including requests from Supervisory Authorities, which includes the steps taken by Dropbox to deal with the respective requests internally and any potential internal escalations, as well as actions.

The provided information also underpinned that Dropbox imposes a duty of confidentiality on its employees and contractors alike, which continue after the end of the respective agreements. Internal procedures are put in place to ensure that personnel are aware of their confidentiality obligations. In the same vein, Dropbox ensures security and privacy trainings for all its employees, at onboarding and annually thereafter. Additional training is also provided to employees, as relevant for their role and job function.

5 Conclusion

The information provided by Dropbox were consistent. Where necessary, Dropbox gave additional information or clarified their given information appropriately.

The Monitoring Body therefore verifies the services as compliant with the EU Cloud CoC based on the performed assessment as prescribed in 1. The service(s) will be listed in the Public Register of the EU Cloud CoC[18] alongside this report.

In accordance with sections 3.4.1.2 and 3.4.2 and given the type of information provided by Dropbox to support the compliance of its service, the Monitoring Body grants Dropbox with a Second Level of Compliance.

6 Validity

This verification is valid for one year. The full report consists of 12 pages in total, whereof this is the last page closing with the Verification-ID. Please refer to the table of contents at the top of this report to verify that the copy you are reading is complete, if you have not received the copy of this report via the Public Register of the EU Cloud CoC[19].

Verification-date: July 2023 **Valid until**: July 2024

Verification-ID: 2022LVL02SCOPE3114

[18] https://eucoc.cloud/en/public-register/
[19] https://eucoc.cloud/en/public-register/