SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: Dropbox International Unlimited Company

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

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 being drafted by the Cloud Select Industry Group[3] (**'C-SIG'**) the EU Cloud CoC – at that time being called C-SIG Code of Conduct on data protection for Cloud Service Providers – the Code was developed against Directive 95/46/EC[4] and incorporates 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

Dropbox declares its suite[6] under the EU Cloud CoC, which comprised at the time of assessment of the following elements and features.

The service known as Dropbox Business 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 addition, customer administrators have a central console that provides visibility and control over user activity[7].

---

[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://dropbox.com
[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 Dropbox core features

- Storage
- Users
- Best-in-class sync technology
- Anytime, anywhere access
- Easy and secure sharing
- 256-bit AES and SSL/TLS encryption
- Content and accident protection
- Dropbox Backup
- File recovery and version history (180 days)
- Dropbox Rewind (180-day history)
- Remote device wipe
- Enable two-factor authentication (2FA)
- Document Watermarking
- Shared link controls
- Account transfer tool
- Enables HIPAA compliance
- Device approvals

2.2 Productivity and sharing tools

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

2.3 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

2.4 Support

- 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[8].

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[9].

The Code has been officially approved May 2021[10]. SCOPE Europe has been officially accredited as Monitoring Body May 2021[11]. 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.[12]

3.2 Principles of the Verification Process

Notwithstanding the powers of and requirements set-out by the supervisory authority pursuant 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; pro-actively 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.

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

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[9] https://scope-europe.eu
[10] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n05-2021-of-20-may-2021.pdf
[11] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n-06-2021-of-20-may-2021.pdf
[12] https://eucoc.cloud/en/public-register/assessment-procedure/

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 Control's Catalogue, to the Monitoring Body.

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

With regards to internationally recognized 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 request for 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 indications for 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 recognized 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 recognized 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 up to 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[13] and refer to the Public Register of the EU Cloud CoC[14] to enable Customers to verify the validity of adherence.

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

4.1 Fact Finding

Following the declaration of adherence of Dropbox International Unlimited Company ('**Dropbox**') regarding the Cloud Services as listed in Section 2, the Monitoring Body provided Dropbox with a template, requesting Dropbox to detail its compliance with each of the Controls of the EU Cloud CoC. Additionally, the Monitoring Body requested an overview and reasoned response on the actual structure of the services declared adherent and why declared services are to be considered a "service family". A service family requires that all services rely on the same core infrastructure, with regard to hardware and software, and are embedded in the same contractual framework.

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

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[15], the Monitoring Body analysed the responses and information provided by Dropbox.

4.3 Examined Controls and related findings by the Monitoring Body

4.3.1 Examined Controls

The Monitoring Body reviewed the initial submission from Dropbox which outlined how all the requirements of the Code were met by Dropbox 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.C, 5.1.H, 5.2.A, 5.2.B, 5.2.C, 5.2.E, 5.3.G, 5.4.E, 5.5.E, 5.6.A, 5.11.B, 5.12.G, 5.13.B and 5.14.E.

4.3.2 Findings by the Monitoring Body

First, the Monitoring Body wishes to highlight that Dropbox responded to the questionnaire detailed and in high quality. The Monitoring Body is considerably satisfied with precision of responses provided by Dropbox. Dropbox included appropriate and relevant references for each of its responses, answering to the control. Additionally, requests for clarification or additional, supporting information and / or evidence were promptly dealt with and always met the deadlines set by the Monitoring Body.

One area of assessment has been the cooperation and assistance by Dropbox in supporting Customers to comply with their obligations under GDPR. Dropbox implemented procedures by which Customers will receive relevant information and support to account for their Compliance with Article 28. Given the nature of the Cloud Service, the procedures and documentation have a strong focus on security related aspects as well as deletion and access of processed data. Besides this focus, Dropbox provides necessary and reasonable assistance in any other legally required aspects.

The Code also requires assistance in enabling Customers to respond to data subject requests. By the nature of the Cloud Service, Dropbox enables Customers with self-service options. The provided information and description of capabilities convincingly indicates that Customers can fully manage their data by means of self-service. Additionally, where needed, Dropbox will support Customers. Where

[15] https://eucoc.cloud/en/about/about-eu-cloud-coc/applicable-procedures/

Dropbox communicates and contractually agrees upon distinct periods for retaining data – e.g., version history of 180 days – internal procedures ensure that the capability will not be impacted adversely in the course of service development or maintenance.

Regarding third country transfers, Dropbox implemented safeguards as provided by Chapter V GDPR. Dropbox third country transfer management will allow Dropbox to promptly determine which transfers are impacted in case of need, e.g., if a safeguard needs adaptations or updates. Such an update was required and is being performed accordingly, after the new Standard Contractual Clauses, also referred to as Standard Data Protection clauses, were published by the European Commission in 2021.

Dropbox provides its Customers with multiple options for retrieving compliance related information. Customers may access several third-party attestations and certifications. Where needed, Customers may also request the possibility for an individual Customer Audit, without prohibitive or excessive limitations, including pricing.

In regards of data breaches, Dropbox has interlinked the security incident response and data breach incidents response procedures, allowing for timely responses by Dropbox, such as remedial actions but also notifications of relevant stakeholders.

Dropbox communicates its subprocessors to its Customers, allowing Customers to take informed decisions. Given the nature of the Cloud Service, Dropbox also defines the roles and responsibilities in the Cloud Service Agreement in a manner that an average Customers, who also may consult expert, can draw informed conclusion and will understand each party's role.

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[16] alongside this report.

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

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 11 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[17].

Verification-date: July 2022 **Valid until**: July 2023

Verification-ID: 2022LVL02SCOPE3114

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