Verification of Declaration of Adherence

Declaring Company: Figma Inc.

Verification-ID	2022LVL02SCOPE4114
Date of Approval	August 2022
Valid until	August 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 – 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

Figma declared its two Cloud Services, i.e., Figma Design and FigJam, adherent to the EU Cloud CoC. Each is provided in different pricing and feature schemes, being Starter, Professional, Organization and Enterprise. Figma Design and FigJam (collectively, the "Figma Platform") are design tools for use

[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

in internal business operations. From a GDPR perspective, the following features were in scope of the assessment:[6]

2.1 Figma Design[7]

Figma Design is a cloud based design solution used for creating, sharing, prototyping and collaborating on digital assets e.g. websites, applications. It is an internal use tool that is most commonly utilised in a user experience or user interface context. From a GDPR perspective, the following features were in scope of the assessment:[8]

- Figma Editor
- Figma Advanced Drawing Tools
- File storage
- Version History
- PDF, PNG, JPG, SVG export
- Multiplayer
- On-canvas commenting
- Audio Conversations
- Cursor Chat
- Webhooks
- Plugins and widgets[9]
- Private Plugins and widgets[10]
- Centralized administration
- Centralized content management
- Plugin and widget management[11]
- Workspace administration
- Activity logs
- Password protection
- Link access controls
- Domain capture
- Single sign-on (SSO)
- Password protection required
- Guest access controls
- Default roles
- Default teams
- Role assignment via SCIM

[6] **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.
[7] https://figma.com
[8] **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.
[9] **NOTE**: In scope is only the appropriate architectural implementation. The report does not give any indication if a distinct plugin or widget is compliant with the Code, unless explicitly stated.
[10] **NOTE:** The assessment may only cover the elements provided by the CSP. To the extent Customers develop their own capabilities or have significant influence on the actual configuration, this is explicitly out of scope of any finding by the Monitoring Body.
[11] **NOTE**: In scope is only the appropriate architectural implementation. The report does not give any indication if a distinct plugin or widget is compliant with the Code, unless explicitly stated.

2.2 FigJam[12]

FigJam is a cloud based virtual whiteboard tool that allows users to brainstorm, collaborate and organize ideas in a shared digital environment.[13]

- Exports
- Cursor Chat
- Audio Conversations
- Centralized administration
- Centralized content management
- Plugin management[14]
- Widget Management[15]
- Workspace management
- Activity logs
- Password protection
- Link access controls
- Domain capture
- Single sign-on (SSO)
- Guest access controls
- Default roles
- Default teams
- Role assignment via SCIM
- Open sessions

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[16].

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[17].

[12] https://figma.com
[13] **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.
[14] **NOTE**: In scope is only the appropriate architectural implementation. The report does not give any indication if a distinct plugin is compliant with the Code, unless explicitly stated.
[15] **NOTE**: In scope is only the appropriate architectural implementation. The report does not give any indication if a distinct widget is compliant with the Code, unless explicitly stated.
[16] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[17] https://scope-europe.eu

The Code has been officially approved May 2021[18]. SCOPE Europe has been officially accredited as Monitoring Body May 2021[19]. 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.[20]

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 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.

[18] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n05-2021-of-20-may-2021.pdf
[19] https://www.gegevensbeschermingsautoriteit.be/publications/decision-n-06-2021-of-20-may-2021.pdf
[20] https://eucoc.cloud/en/public-register/assessment-procedure/

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 consid-

ered 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[21] and refer to the Public Register of the EU Cloud CoC[22] to enable Customers to verify the validity of adherence.

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

4.1 Fact Finding

Following the declaration of adherence of Figma Inc. ('**Figma**'), the Monitoring Body provided Figma with a template, requesting Figma 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.

Figma promptly responded to any inquiries by the Monitoring Body. Information provided by Figma comprised of references and a 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.

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[23], the Monitoring Body analysed the responses and information provided by Figma.

---

[21] https://eucoc.cloud/en/public-register/levels-of-compliance/
[22] https://eucoc.cloud/en/public-register/
[23] https://eucoc.cloud/en/about/about-eu-cloud-coc/applicable-procedures/

Figma declared Cloud Services have been externally certified and audited, e.g., Figma hold current SOC 2 and ISO 27001 reports and certificates. The declaration of adherence referred to the respective ISO 27001 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 did verify the certification and references.

4.3 Examined Controls and related findings by the Monitoring Body

4.3.1 Examined Controls

The Monitoring Body reviewed the initial submission from Figma which outlined how all the requirements of the Code were met by Figma 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.C, 5.1.D, 5.1.F, 5.2.B, 5.2.C, 5.2.E to G, 5.3.C, 5.3.D, 5.4.A to C, 5.4.E, 5.5.D, 5.5.E, 5.6.A, 5.7.B, 5.7.D, 5.7.F, 5.8.A, 5.8.B, 5.9.A, 5.9.B, 5.10.A, 5.10.B, 5.11.A to C, 5.12.C to F, 5.14.A, 5.14.B, 5.14.E, 6.1.A, 6.1.C, 6.1.D.

4.3.2 Findings by the Monitoring Body

During the process of verification, Figma consistently prepared the Declaration of Adherence well and thoroughly. Figma provided requested information without hesitation and promptly clarified its responses, where needed, meeting any set deadlines. The information provided never created any impression of intentional non-transparency.

Generally, it must be noted that a significant share of the assessment and related follow-ups were aiming for clarifications. The specific type of the Cloud Services adherent relates to a mainly indirect processing of Customer Personal Data. Regardless, appropriate measures must be implemented to comply with the Code. The specifics resulting from the nature of the Cloud Services required an increased understanding of the Monitoring Body of the conceptual approaches by Figma.

Given the nature of Cloud Services, one area of focus was the assistance of Customers. Generally, Figma provides self-service capabilities. This includes specifically means of deletion and export. However, where additional capabilities are required under GDPR, Customers will either be enabled for self-service, or, where necessary, may reach out to Figma to request additional reasonable assistance. In this context, Figma also implemented procedures to adequately react where data subject rights will be concerned or where supervisory authorities may reach out to Figma.

Figma implemented a subprocessor management program. This includes diligent assessments and processes to ensure that the provided level of data protection by Figma will remain throughout the processing chain.

To the extent third-country transfers are concerned, Figma implemented respective procedures, ensuring that transfers are subject to at least one safeguard pursuant Chapter V GDPR. Figma also has implemented measures allowing Figma to identify transfers subject to a specific safeguard, enabling Figma to react in due time in case of need. In this context also the records of processing activities will provide useful information.

GDPR provides Customers with a Customer Audit Right, thus the Code provides for distinct safeguards. In case of need, Figma's Customers may request individual audits. Such audits will follow a common procedure. To the extent related costs might be imposed on the Customer, there was no indication that such costs will be unduly excessive or prohibitive.

An internal training programme is maintained, enabling Figma employees and contractors to adequately perform their duties. Such trainings will raise awareness by Figma employees and contractors in respect of data protection and related internal policies and procedures, as well as relevant contractual and legal obligations.

5 Conclusion

The information provided by Figma were consistent. Where necessary Figma 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[24] alongside this report.

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

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

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[25].

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

Verification-ID: 2022LVL02SCOPE4114

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