SCOPE EUROPE

Verification of Declaration of Adherence

Declaring Company: Figma Inc.

Verification-ID	2022LVL02SCOPE4114
Date of Approval	August 2023
Valid until	August 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].

[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

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 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. [8]

2.1.1 Design features

- Version history
- Figma Editor
- Advanced drawing tools
- Auto layout
- Plugins and widgets[9]
- Unlimited file storage
- Cross platform
- Sketch import
- PDF, PNG, JPG, SVG export

2.1.2 Collaboration

- Multiplayer
- Unlimited viewers
- Shareable links
- On-canvas commenting
- Observation mode
- Private projects
- Custom workspaces
- Prototype sharing permissions
- Audio conversations
- Team and project transfer
- Unlimited teams
- Branching and merging

2.1.3 Prototyping

- Interactive prototypes
- Videos in prototypes

[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://www.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.

- Overlays
- Transitions
- Advanced animations
- Set variable
- Conditional logic
- Multiple actions
- Expressions

2.1.4 Design systems

- Variables
- Components
- Styles
- Modes
- Team libraries
- Organization-wide design systems
- Shared fonts
- Design system analytics
- Default libraries by workspace
- REST API for variables

2.1.5 Development

- Dev Mode
- Figma for VS Code

2.1.6 Developer platform

- REST APIs
- Third-party integrations
- Private plugins and widgets [10]
- Live embeds
- Webhooks

2.1.7 Admin & security

- Password protection
- Plugin and widget management[11]
- Centralized administration
- Domain capture
- Link access controls
- Centralized content management
- Single sign-on (SSO)
- Activity logs
- Workspace administration
- Guest access controls
- EU data hosting
- Default roles
- Default teams
- Role assignment via SCIM
- Password protection required
- Team creation controls
- Network access restrictions
- External content controls
- Activity logs API
- Windows Installer
- Idle session timeout

---

[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.

- Expiring public links

2.1.8 Support[12]

- Figma Support Forum
- Figma Help Center
- Onboarding planning and support
- Dedicated account manager

2.2 FigJam[13]

FigJam is a cloud based virtual whiteboard tool that allows users to brainstorm, collaborate and organize ideas in a shared digital environment[14]

2.2.1 FigJam features

- Code blocks
- Templates
- Exports
- Timer
- Widgets and plugins[15]
- Engagement features
- Cursor chat
- Ready-made templates
- Diagramming tools
- Music player
- Tables
- Asana & Jira widgets[16]
- Audio conversations
- Open sessions
- Voting
- Custom templates
- Custom color palettes

2.2.2 Admin & security

- Password protection
- Plugin management[17]
- Centralized administration
- Single sign-on (SSO)
- Widget management[18]
- Domain capture
- Link access controls
- Centralized content management
- Activity logs

---

[12] **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.
[13] https://www.figma.com
[14] **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
[15] **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.
[16] **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.
[17] **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.
[18] **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.

- Workspace management
- Guest access controls
- Role assignment via SCIM
- Team creation controls
- Network access restrictions
- External content controls
- Expiring public links
- Default roles
- Activity logs API
- Idle session timeout
- EU data hosting

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[19].

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[20].

The Code has been officially approved in May 2021[21]. SCOPE Europe has been officially accredited as Monitoring Body in May 2021[22]. 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.[23]

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

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

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 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[24] and referring to the Public Register of the EU Cloud CoC[25] to enable Customers to verify the validity of adherence.

[24] https://eucoc.cloud/en/public-register/levels-of-compliance/
[25] https://eucoc.cloud/en/public-register/

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.

As this declaration is a renewal[26], the Monitoring Body requested from Figma a confirmation that there has been no material change to the applicable technical and organisational and contractual framework. The Monitoring Body also requested from Figma 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.

Figma 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 two 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[27], the Monitoring Body analysed the responses and information provided by Figma.

Figma's declared services have been externally certified and audited. Figma holds SOC 2 and ISO 27001 report and 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 27001 certification within the responses to Section 6 of the Code (IT Security). As

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

provided by the Code, the Monitoring Body may consider third-party certifications and audits. Accordingly, the Monitoring Body 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 Figma which outlined how all the requirements of the Code were met by Figma'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.C, 5.1.D, 5.1.E, 5.2.B, 5.2.C, 5.2.E, 5.2.F, 5.2.G, 5.3.C, 5.3.D, 5.4.A, 5.5.A, 5.5.C, 5.5.E, 5.7.A, 5.7.B, 5.7.F, 5.10.A, 5.10.B, 5.11.B, 5.11.C, 5.13.A, 5.13.B, 5.14.B, 5.14.E, 5.14.F, 6.1.C, 6.2.P.

4.3.2 Findings by the Monitoring Body

During the process of verification, Figma consistently prepared the Declaration of Adherence well and thoroughly. Figma'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), Figma 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, Figma provided explicit confirmation that such Cloud Services belong to the same Cloud Service Family.

The Monitoring Body focused on the assistance provided to the Customers. Based on the information provided and assessed Figma provides Customers with relevant GDPR compliance information and third-party attestations, and documentation by means of a Trust Center, however access to confidential information is provided only under non-disclosure agreement. Likewise, Figma provides Customers with further assistance in exercising their data protection obligations or any additional support by making available a dedicated support email. Alternatively, the Product Support team may be contacted by Customers.

Figma indicated to offer to its Customers a deletion self-service capability. In order to access or retrieve Customer personal Data Customers may reach out via dedicated communication channels to

Figma, where relevant assistance would be provided. In this vein, requested data is provided in industry standard format. Additional information regarding formats and mechanisms to retrieve data may be further requested by the Customers via dedicated communication channels. Moreover, Figma maintains internal procedures to adequately fulfil data subject right requests and respond to requests by a supervisory authority. Customers are entitled to receive relevant notification of supervisory authorities' requests, as provided by the EU Cloud CoC.

Third country transfers have been in the scope of the assessment of the Monitoring Body. Figma has referred to implemented safeguards as provided by Chapter V GDPR, as it relies on the Standard Contractual Clauses (SCCs) as the third-country transfer mechanism. Additionally, Figma has indicated that legal and compliance teams continuously evaluate Figma's international data transfers to ensure compliance with applicable data privacy laws.

Another area of the assessment has been Figma's subprocessor management program. Figma referred to implemented relevant internal policies and procedures to ensure that only subprocessors that provide sufficient guarantees of compliance with the GDPR may be engaged. Moreover, Figma indicated that at onboarding subprocessors undergo legal, security and compliance due diligence. Figma makes its subprocessors' list publicly available and indicated that it maintains Customer notification mechanism to provide information as to the changes of subprocessors, allowing Customers to make informed decisions and take effective measures prior changes are implemented.

To the extent Customer Audit Rights are concerned, subject to appropriate confidentiality requirements, Figma ensures to provide Customer with relevant third-party certifications and reports. Further, Customers are enabled to request individual audits and Customer Audit Rights are included as standard part of the Figma's Data Processing Addendum. To the extent Figma determines that the Customer should bear the cost of the audit, there was no indication that such costs will be unduly excessive or prohibitive.

Figma confirmed maintaining an internal training program, which includes annual review of the information security policy and security and privacy training, which is obligatory for the employees and contractors. Furthermore, employees undergo role specific privacy training as relevant for their role and job function. Figma limits employees' access to the Customer Personal Data and provides dedicated trainings to ensure that Customer Personal Data is not being processed by employees for any purpose unless specifically instructed by the Customer.

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[28] 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.

6 Validity

This verification is valid for one year. The full report consists of 15 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[29].

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

Verification-ID: 2022LVL02SCOPE4114

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