

Verification of Declaration of Adherence

Declaring Company: Figma, Inc.



EU
CLOUD
COC

Verification-ID	2022LVL02SCOPE4114
Date of Approval	August 2026
Valid until	August 2027

Table of Contents

1	Verification against v2.11 of the EU Cloud CoC	3
2	List of declared services	3
2.1	Figma Design	3
2.2	FigJam	4
2.3	Figma Slides	5
2.4	Figma Sites (Beta)	5
2.5	Figma Make	5
3	Verification Process - Background	6
3.1	Approval of the Code and Accreditation of the Monitoring Body	6
3.2	Principles of the Verification Process	6
3.3	Multiple Safeguards of Compliance	6
3.4	Process in Detail	7
3.4.1	Levels of Compliance	8
3.4.2	Final decision on the applicable Level of Compliance	9
3.5	Transparency about adherence	9
4	Assessment of declared services by Figma (see 2.)	9
4.1	Fact Finding	9
4.2	Selection of Controls for in-depth assessment	10
4.3	Examined Controls and related findings by the Monitoring Body	10
4.3.1	Examined Controls	10
4.3.2	Findings by the Monitoring Body	11
5	Conclusion	12
6	Validity	12
7	Appendix 1 – List of features	13

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’ or ‘Code’**)¹ in its version 2.11 (**‘v2.11’**)² as of December 2020.

Originally drafted by the Cloud Select Industry Group³ (**‘C-SIG’**) the EU Cloud CoC – at that time called C-SIG Code of Conduct on data protection for Cloud Service Providers (**‘CSPs’**) – was developed against Directive 95/46/EC⁴ 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 services⁶

2.1 Figma Design⁷

Figma offers a wide array of features that can be grouped into several key areas. Its **core design features** within the Figma Editor product includes advanced drawing tools, and support for components, styles, and interactive prototypes (e.g., auto layout, advanced animations, overlays). For **collaboration and communication**, Figma enables real-time teamwork with multiplayer support, on-canvas commenting, and shareable links (e.g., audio conversations, unlimited viewers, observation mode). The **prototyping and interactivity** tools allow designers to build dynamic prototypes with variables,, conditional logic, and branching (e.g., multiple actions, expressions, videos in prototypes). Figma’s **organization and team management** features help teams stay organized with unlimited teams, private projects, and custom workspaces (e.g., team libraries, shared fonts, default libraries by workspace).

For larger organizations, Figma provides robust **enterprise and security** options, including single sign-on (SSO), centralized content management, and network access restrictions (e.g., password protection, role assignment via SCIM, expiring public links). Developers can leverage **developer tools and integrations**, such as Figma for VS Code, REST APIs, and private plugins (e.g., webhooks, third-party

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 **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 www.figma.com

integrations, Dev Mode⁸). The platform also includes comprehensive **design system management** with centralized administration, team libraries, and design system analytics (e.g., plugin and widget management, default teams). Figma supports **file management and storage** with cross-platform access, unlimited file storage, and easy file transfers (e.g., Sketch import, team and project transfer). Lastly, Figma emphasizes **security and access controls** with features like link access controls, password protection, and network restrictions, while offering **support and administration** through its help center, onboarding planning, and dedicated account managers (e.g., activity logs, workspace administration).

- Figma Buzz (Beta)
- Figma Draw
- Dev Mode

2.2 FigJam

Figma's FigJam product offers a variety of features organized into several functional areas. Its **core collaboration tools** include diagramming tools, ready-made templates, and voting mechanisms to facilitate brainstorming and teamwork (e.g., code blocks, cursor chat, music player). For **engagement and interaction**, users can utilize widgets and plugins, engagement features like timers, and audio conversations to keep sessions dynamic (e.g., Asana & Jira widgets, voting, open sessions). FigJam's **customization and templates** allow teams to create custom templates, set custom color palettes, and export their work (e.g., ready-made templates, custom templates, exports).

To manage **security and access controls**, FigJam offers password protection, link access controls, and domain capture (e.g., guest access controls, expiring public links, network access restrictions). For larger organizations, FigJam includes **enterprise and administrative features** like single sign-on (SSO), centralized administration, and role assignment via SCIM (e.g., widget management, centralized content management, workspace management). Developers and admins can also benefit from **plugin and widget management**, including plugin management, widget management, and tools for centralized content administration. FigJam emphasizes **data security and compliance**, offering activity logs, activity logs API, and EU data hosting (e.g., idle session timeout, external content controls, expiring public links).

⁸ Dev Mode with its features VS Code extension, Private plugins, and Syncing or automating workflows via REST API.

2.3 Figma Slides

Figma Slides extends the collaborative power of Figma into presentations, combining design flexibility with real-time teamwork. Its core creation tools let teams build slide decks using familiar design elements—frames, auto layout, and components—while enabling seamless collaboration through live cursors, comments, and co-editing. For engagement, Slides offers features like interactive polls, reactions, alignment scales, and embedded prototypes to make presentations dynamic and participatory. Customization options allow users to design branded templates, apply team libraries, and export decks directly from the Figma environment. Security and access controls mirror Figma’s core platform, including link permissions and workspace roles, while enterprise features such as SSO, SCIM provisioning, and content governance support large organizations. Slides runs within Figma’s secure cloud infrastructure, leveraging the same governance, data protection, and compliance standards as Figma Design and FigJam.

2.4 Figma Sites (Beta)

Figma Sites brings website design, prototyping, and publishing together in one unified workflow. Teams can design responsive sites using Figma’s familiar tools—components, auto layout, and shared libraries—then publish directly to the web without leaving the platform. Interactive elements such as hover effects, scrolling animations, and embedded code make it easy to create modern, engaging experiences. With customizable templates, component reusability, and brand libraries, Sites supports consistent, scalable web creation across teams. Enterprise users benefit from centralized management, version control, and shared permissions, ensuring design consistency across global sites. Sites is part of Figma’s secure cloud infrastructure, leveraging the same governance, data protection, and compliance standards as Figma Design and FigJam.

2.5 Figma Make

Figma Make turns ideas into interactive prototypes and code, bridging design and development. Users can describe what they want in natural language or upload assets, and Make generates functional layouts, components, and front-end code in real time. Make can also host the websites that are created through the prompting process. Collaboration remains central—teams can co-edit, test flows, and refine outputs directly in Figma. Customization options include AI-assisted layout generation, reusable design systems, and export to frameworks like React. For enterprises, Make streamlines prototype-to-production workflows and enforces design-system consistency under existing security and access controls. Make is part of Figma’s secure cloud infrastructure, leveraging the same governance, data protection, and compliance standards as Figma Design and FigJam.

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 GDPR⁹.

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 SRL¹⁰.

The Code has been officially approved in May 2021¹¹. SCOPE Europe has been officially accredited as Monitoring Body in May 2021¹². 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.

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

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/>

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 Mark¹⁴ and referring to the Public Register of the EU Cloud CoC¹⁵ 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.

As this declaration is a renewal¹⁶, the Monitoring Body requested from Figma a confirmation that there has been no material change to the applicable technical and organisational and contractual

¹⁴ <https://eucoc.cloud/en/public-register/levels-of-compliance/>

¹⁵ <https://eucoc.cloud/en/public-register/>

¹⁶ You can access the Verification Report of previous year via the following link: [Figma - Verification Report - \(2025\)](#)

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 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 CoC¹⁷, the Monitoring Body analysed the responses and information provided by Figma.

Figma's declared services have been externally certified and audited. Figma holds an ISO 27001 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 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

¹⁷ <https://eucoc.cloud/en/about/about-eu-cloud-coc/applicable-procedures/>

review were: 5.1.A, 5.1.E, 5.2.A, 5.2.B, 5.2.C, 5.2.G, 5.3.B, 5.3.D, 5.3.E, 5.4.A, 5.5.B, 5.5.C, 5.5.E, 5.7.B, 5.7.C, 5.7.F, 5.8.A, 5.10.A, 5.11.B, 5.13.A, 5.14.A, 5.14.B and 6.1.C.

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 first area of assessment has been the enablement of Customers. Customers are provided with self-service functionalities to handle their Data Subjects Requests. Such functionalities allow them to access, export, modify and delete Customer Personal Data. Figma confirmed that where Customers may need more information or support not already covered by the self-service functionalities, Customers may reach out via dedicated channels.

The procedures related to Customers' Audit Rights were also assessed. The assessment focused on Figma's methodology to determine the costs of audits, as well as the possibility for Customers to request additional evidence of compliance. Figma provided the Monitoring Body with an overview of its methodology to determine the costs of audits. As indicated by Figma, Customers are also provided with the relevant communication channels to request additional evidence of compliance, beyond exercising their audit rights.

Figma's records of processing activities ("ROPA") built another area of focus. Based on the information provided, Figma maintains a ROPA in its capacity as Processor, which includes the relevant information as per Art. 30.2 GDPR. The relevant communication channels for Customers to provide the information in relation to the completion and relevancy of the ROPA were confirmed by Figma.

In the context of determining whether a representative pursuant Art. 27 GDPR must be appointed or whether the CSP is established in a Member State of the European Union, Figma indicated that it is established in the United States and confirmed having designated a representative in accordance with Art. 27 GDPR. In a similar vein, the CSP indicated having designated a Data Protection Officer ("DPO"). The contact of the DPO has been communicated through the CSP's Trust Center.

In terms of subprocessor management, Figma has put in place a procedure to ensure that subprocessors engaged provide sufficient guarantees of compliance with the GDPR throughout the life of the agreement with Figma. This procedure ensures that verification of the subprocessors good standing and implementation of GDPR, and as well security measures, both at onboarding and periodically. A list of subprocessors is made available to Customers through Figma's website. In the same manner, Figma has a defined mechanism to notify Customers of changes in subprocessors. The timeline for the Customers to object to the appointment of new subprocessors and/or to exercise an alternative option was confirmed by the CSP.

5 Conclusion

The information provided by Figma was 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 CoC¹⁸ 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 16 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 CoC¹⁹.

Verification-date: August 2026

Valid until: August 2027

Verification-ID: 2022LVL02SCOPE4114

¹⁸ <https://eucoc.cloud/en/public-register/>

¹⁹ <https://eucoc.cloud/en/public-register/>

7 Appendix 1 – List of features²⁰

Figma Design - features

- Components
- Figma Editor
- Auto layout
- Advanced drawing tools
- Styles
- Interactive prototypes
- Advanced animations
- Transitions
- Overlays
- Video in prototypes
- Responsive prototyping viewer
- UI Kits
- Inspect in design files
- Community templates
- Variables
- MCP support
- Variable modes
- Annotations
- Team libraries
- Design productivity tools (AI)
- Multiple actions
- Advanced prototyping
- Conditional logic
- Expressions
- Prototype sharing permissions
- Shared fonts
- Branching and merging
- In-app Library Analytics
- Organization-wide design systems
- Default libraries by workspace
- Approved libraries

Figma Draw - features

- Draw tools
- Enhanced vector editing
- Custom brushes
- Visual effects
- More stroke mechanics
- Text on a path
- Transforms

Dev Mode - features

- MCP support
- View annotations and measurements
- Code Connect
- Advanced inspection

²⁰ **NOTE:** The list is provided solely for transparency and completeness purposes and does not reflect any opinion of or assessment by the Monitoring

Body, as in scope is only the appropriate architectural implementation unless explicitly stated otherwise.

- Improved handoff experience
- Compare changes
- Component playground
- Dev resources
- Asset export
- Plugins
- VS Code extension

FigJam - features

- Engagement features
- Music player
- Timer
- Tables
- Code blocks
- Diagramming tools
- Summarize (AI)
- Generate (AI)
- Sort (AI)
- Voting
- Open sessions
- Advanced shapes
- Advanced diagramming
- Custom color palettes
- Custom templates
- MCP support
- Custom color palettes

Figma Slides - features

- Add interactive prototypes
- Live interactions
- Transitions
- Offline presentations
- Import / Export to PowerPoint
- Adjust content tone (AI)
- Draft presenter notes (AI)
- Slide outline from FigJam (AI)
- Figma Design libraries
- YouTube embeds
- Real-time presenter notes
- Custom templates

Figma Make - features

- Prompt the model
- Attach designs
- Add backend support
- Push to GitHub
- MCP support
- Publish via Figma Community
- Library styling context

Figma Buzz (Beta) - features

- Templates from Figma
- Free-form editing and design elements
- Brand template publishing
- Focused editing

Figma Sites (Beta) - features

- Blocks and embeds
- Breakpoints
- Interactions
- Code layers
- Publishing

Platform²¹

- AI Credits
- Multiplayer
- Unlimited viewers
- Comments
- Spotlight
- Observation mode
- Shareable links
- Exports
- Unlimited file storage
- File import
- Cursor chat
- Version history
- MCP server
- Private projects
- Team and project transfer
- Audio conversations
- Image editing tools (AI)
- Visual search (AI)
- Text tools (AI)
- Unlimited teams
- Custom workspaces

Admin²¹

- Centralized administration
- Centralized content management
- Workspace administration
- Team creation controls
- Default teams
- Inspect panel administration

Extensibility²¹

- REST APIs
- Plugins and widgets
- Third-party integrations
- Live embeds

²¹ **NOTE:** These features are integrated within the product suite (Cloud Service Family).

- Webhooks
- Private plugins and widgets
- Plugin management
- REST API with Dev Mode

- REST API for variables
- Library Analytics API (beta)
- Activity logs API
- Plugin and widget analytics

Security²¹

- Password protection
- Single sign-on (SSO)
- Domain capture
- Activity logs
- Link access controls
- Plugin and widget management
- Role assignment via SCIM

- Guest access controls
- Password protection required
- External content controls
- Idle session timeout
- Expiring public links
- EU data hosting