

Verification of Declaration of Adherence

Declaring Company: Fabasoft AG



EU
CLOUD
COC

Verification-ID 2021LVL03SCOPE016

Date of Approval May 2026

Valid until May 2027

Table of Contents

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

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 services

2.1 Fabasphere⁶

The Fabasphere is the new cloud-native home for documents and business processes. Based on the Fabasphere AI Core technology – consisting of the Fabasoft Cloud and Mindbreeze AI – the Fabasphere offers a connected ecosystem of solutions for a wide range of requirements.⁷

The Fabasphere brings together carefully curated solutions for different industries and use cases:

- Fabasoft Approve
- Fabasoft Boards
- Fabasoft Contracts
- Fabasoft DORA
- Fabasoft OneGov
- Fabasoft Talents
- Fabasoft Xpublisher

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 GDPR⁸.

¹ <https://eucoc.cloud>

² <https://eucoc.cloud/get-the-code>

³ <https://ec.europa.eu/digital-single-market/en/cloud-select-industry-group-code-conduct>

⁴ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046>

⁵ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679>

⁶ <https://www.fabasoft.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.

⁸ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679>

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 SRL⁹.

The Code has been officially approved in May 2021¹⁰. SCOPE Europe has been officially accredited as Monitoring Body in May 2021¹¹. 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 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 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

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://euococ.cloud/en/public-register/assessment-procedure/>

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 adherent 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 Mark¹³ and referring to the Public Register of the EU Cloud CoC¹⁴ to enable Customers to verify the validity of adherence.

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

4.1 Fact Finding

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

As this declaration is a renewal¹⁵, the Monitoring Body requested from Fabasoft a confirmation that there has been no material change to the applicable technical and organisational and contractual framework. The Monitoring Body also requested from Fabasoft 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

¹³ <https://eucoc.cloud/en/public-register/levels-of-compliance/>

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

¹⁵ You can access the Verification Report of previous year via the following link: [Fabasoft - Verification Report - 2025](#)

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.

Fabasoft 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 CoC¹⁶, the Monitoring Body analysed the responses and information provided by Fabasoft.

Fabasoft's declared services have been externally certified and audited. Fabasoft holds ISO 27001 and 27018 certificates, which are valid for the duration of the Declaration of Adherence, and the scope of registration includes all the declared services, as confirmed by the third party auditor. The declaration of adherence referred to the respective ISO certifications 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 Fabasoft which outlined how all the requirements of the Code were met by Fabasoft'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.B, 5.2.A, 5.2.B, 5.2.C, 5.2.F, 5.4.A, 5.4.B, 5.4.C, 5.4.D, 5.4.E, 5.4.F, 5.5.D, 5.5.E, 5.7.E, 5.8.B, 5.10.A, 5.10.B, 5.12.A, 5.12.D, 6.1.C – 6.2.G, 6.2.J – 6.2.O, 6.2.Q and 6.3.A.

¹⁶ <https://eucoc.cloud/en/about/about-eu-cloud-coc/applicable-procedures/>

4.3.2 Findings by the Monitoring Body

During the process of verification, Fabasoft consistently prepared the Declaration of Adherence well and thoroughly. Fabasoft'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.

As this is a Third Level of Compliance verification, responses to every Control were supported by third-party attestations and included a dedicated EU Cloud CoC related attestation report. The dedicated report ("Auditor's Report") was prepared thoroughly by a third-party auditor ("Auditor"). Requests for clarifications, additional and supporting information, as well as relevant samples were promptly dealt with by the Auditor. The Monitoring Body has had no reason, from a formal or material perspective, to doubt the appropriateness or suitability of the relevant Auditor's Report with respect to the understanding of the Code and relevant Controls.

Related to the Monitoring Body's requests (see section 4.1), Fabasoft 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, Fabasoft provided explicit confirmation that such Cloud Services belong to the same Cloud Service Family.

The Monitoring Body assessed Fabasoft's mechanisms for the transfer of personal data to third countries. The Auditor confirmed that Customer Personal Data was transferred within the European Union, with the exception of transfers to Switzerland, in the context of the declared services. The Auditor explained that for transfers to Switzerland, Fabasoft relies on Adequacy Decisions. The procedure implemented by the CSP to assess and monitor Adequacy Decisions was also described.

Furthermore, the procedures related to Customers' Audit Rights were assessed. The CSP makes certificates, attestations and reports readily available on its website. The Auditor's Report elaborated on Customer Audits being a standard part of the CSP's Data Processing Agreement ("DPA"). The DPA defines the audit request procedures (e.g., the notice period). The cost determination and allocation related to Customers' Audit Rights were also presented to the Monitoring Body. There was no indication that such costs are prohibitive or excessive.

The Auditor's Report included information on Fabasoft's data privacy team and its specific role. In the same vein, Fabasoft has designated a Data Protection Officer ("DPO") with competencies in accordance with Chapter IV, Section 4 GDPR. The contact details of the DPO have been communicated and made available through Fabasoft's website, where they are visible to Data Subjects and Customers.

Regarding requests from Supervisory Authorities, the Auditor's Report indicated that Fabasoft has implemented procedures to handle such requests in a diligent and timely manner. Relevant points of contact are involved, including the DPO. In addition to this, relevant teams are mobilised to inform the Customer, where legally permissible, when the CSP receives a request from a Supervisory Authority relating to Customer Personal Data.

The Auditor has confirmed that Fabasoft imposes a duty of confidentiality on its employees and contractors, which continues after the end of the respective agreements. Internal procedures and policies are put in place to ensure that personnel are aware of their confidentiality obligations and the consequences of non-adherence. In the same manner, Fabasoft ensures that all important information (such as information security) is provided to personnel at onboarding and throughout their employment.

As confirmed by the Auditor's Report, relevant policies and procedures have been established by Fabasoft to timely and adequately handle and report data breaches to the Customer without any undue delay. The CSP's incident process describes how security events are reported. The Auditor also indicated that the process includes how reported security incidents are assessed, categorised and prioritised. Relevant teams are involved to determine whether a security breach potentially resulted in a data breach. The obligation to report data breaches to the Customer is included in the CSP's contractual documents.

5 Conclusion

The information provided by Fabasoft and the third-party auditor was consistent. Where necessary, Fabasoft 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 CoC¹⁷ alongside this report.

In accordance with sections 3.4.1.3 and 3.4.2 and given the type of information provided by Fabasoft to support the compliance of its service, the Monitoring Body grants Fabasoft with a Third Level of Compliance.

¹⁷ <https://eucocloud.com/en/public-register/>

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 CoC¹⁸.

Verification-date: May 2026

Valid until: May 2027

Verification-ID: 2021LVL03SCOPE016

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