SCOPE EUROPE

# Verification of Declaration of Adherence

## Declaring Company: Fabasoft AG

EU CLOUD COC

| | |
|---|---|
| **Verification-ID** | 2021LVL03SCOPE016 |
| **Date of Approval** | May2021 |
| **Valid until** | May2022 |

# Table of Contents

# 1 Verification against v2.11 of the EU Cloud CoC

This Declaration of Adherence was against the *European Data Protection Code of Conduct for Cloud Service Providers* (**'EU Cloud CoC'**)[1] in its version 2.11 (**'v2.11'**)[2] as of December 2020.

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

## 2.1 Fabasoft Cloud[6]

As overarching service "Fabasoft Cloud" entails the products and solutions "Fabasoft Business Process Cloud", "Fabasoft Approve" and "Fabasoft Contracts".

Fabasoft Cloud offers customers the option to save and manage data on the IT infrastructure operated by Fabasoft to use a software product that is integrated into the service. The Cloud Service Fabasoft Cloud is the technical platform for the solutions and products operated in it, such as Fabasoft Business Process Cloud, Fabasoft Approve or Fabasoft Contracts.[7]

# 3 Verification Process - Background

V2.11 of the EU Cloud CoC has been developed against GDPR and hence provides mechanisms as required by Articles 40 and 41 GDPR[8].

---

[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/en/products
[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 sprl/bvba[9].

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

## 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 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.

---

[9] https://scope-europe.eu
[10] 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 both that over a due period every Control will be subject to scrutiny by the Monitoring Body and aspects of increased attention as indicated e.g., by media reports, publications and actions of supervisory authorities are covered.

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 adherent as compliant and thereupon make 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 and 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 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[11] and refer to the Public Register of the EU Cloud CoC[12] to enable Customers to verify the validity of adherence.

# 4 Assessment of declared service 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. Additionally, the Monitoring Body requested the list of the products and solutions covered by the overarching service as well as an overview and reasoned response on the actual structure/connection of the products and solutions with the service.

Fabasoft promptly responded within the template. The information provided consisted exclusively of references to third-party reports or a free text answer where an EU Cloud CoC control was not applicable to Fabasoft. For each EU Cloud CoC control applicable to Fabasoft, Fabasoft indicated the corresponding Fabasoft's internal controls which have been assessed by a third-party auditor. Four third-party certificates were provided alongside the template by Fabasoft.

Fabasoft provided information explaining the correlation between the service, products, and solutions. Fabasoft communicated the list of products and solutions covered by the service.

[11] https://eucoc.cloud/en/public-register/levels-of-compliance/
[12] https://eucoc.cloud/en/public-register/

## 4.2 Selection of Controls for in-depth assessment

Following the provisions of the Code and the Assessment Procedure applicable to the EU Cloud CoC[13], the Monitoring Body analysed the responses and information provided by Fabasoft.

Fabasoft Cloud declared service has been externally certified and audited. In that regard, Fabasoft Cloud holds current SOC 2, BSI C5, ISO 27001 (including ISO 27018), and a dedicated individual EU CoC Section (Data Protection) report.

The EU CoC Section (Data Protection) report has been conducted in conformity with Austrian Standards for independent assurance engagements (KFS/PG 13) and in accordance with the International Standard on Assurance Engagements (ISAE 3000) applicable to such engagements. The assessment has been conducted by a well-known international audit provider.

As provided by the Code, the Monitoring Body may consider third-party certifications and audits. Accordingly, the Monitoring Body did verify the certifications and references. The Monitoring Body has examined the scope and wording of the controls specified by Fabasoft and the outcome of the test procedures performed by the third-party auditor.

## 4.3 Examined Controls and related findings by the Monitoring Body

### 4.3.1 Examined Controls

The Monitoring Body reviewed the initial submission from Fabasoft which outlined how the requirements of the Code are met by Fabasoft 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. The controls selected for this level of review were: 5.1.A, 5.1.B, 5.1.F, 5.1.G, 5.1.H, 5.2.D, 5.3.A, 5.3.G, 5.4.A, 5.4.B, 5.4.C, 5.4.D, 5.4.E, 5.4.F, 5.5.E, 5.5.F, 5.6.A, 5.7.A, 5.7.B, 5.12.G, 5.13.A, 6.1.A and 6.3.A.

Based on the information provided by Fabasoft, a follow-up request was made, for further detail on implemented measures related to Controls and respective information provided for: 5.3.G, 5.4.A, 5.4.C, 5.4.D, 5.4.E and 5.4.F.

### 4.3.2 Findings by the Monitoring Body

The process of verification by the Monitoring Body has been eased by the upstream preparation of Fabasoft. Fabasoft completed the template in a precise and diligent manner. References to Fabasoft's

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

internal controls provided within the template allowed the Monitoring Body to promptly and easily find the relevant information. Additionally, requests for clarification or additional, supporting information were rapidly dealt with and always met the deadlines set by the Monitoring Body.

Fabasoft provided independent third-party certificates and audits to support the compliance of Fabasoft Cloud in total covering every Control of the EU Cloud CoC.

The Monitoring Body may rely on such external reports and certifications, if those meet the criteria as set out in the Code. In that regard, the four reports communicated by Fabasoft apply to Fabasoft Cloud, are valid and have assessed and sufficiently reported compliance with the mapped controls of the third-party certification or audit concerned. In light of the aforementioned, the Monitoring Body had strong indications allowing the Monitoring Body to rely on those reports.

Whilst the Code provides clear indication in Section 6 which standards are considered to provide a level of protection that is no less protective than the Code's requirements, the Monitoring Body took additional efforts to ensure that the provided ISAE 3000 report covering Section 5 was conducted with the same level of scrutiny and understanding of the Code as if it would have been conducted by the Monitoring Body. Therefore, the Monitoring Body analysed the certifications and took samples for which the Monitoring Body examined the scope and wording of the controls specified by Fabasoft and the outcome of the test procedures performed by the third-party auditor. The Monitoring Body considered for each of the samples that the scope and wording of the Fabasoft's internal control mirrored the corresponding EU Cloud CoC control. Taking into account the result of the test performed by the third-party auditor, the Monitoring Body considered there is no reasonable doubt regarding the accuracy of the conformity attestation related to the controls.

Fabasoft indicated that, as a matter of principle, Fabasoft does not transfer any data to a third country within the default scope of the Cloud Service but only subject to a separate express order of its Customers. Upon request Fabasoft clarified that in the event of a specific order, such request will result into an individual agreement either governing the Customer to be responsible for safeguarding third-country transfers or, Fabasoft will perform an ad hoc assessment to adequately safeguard such transfers.

After taking several samples, especially related to the ISAE 3000 individual report's covered controls, the Monitoring Body has no reason to doubt the appropriate performance of such third-party attestation, neither from a formal perspective nor from a material perspective, e.g., that a significantly diverse understanding of the Code has been applied.

# 5 Conclusion

Given answers by Fabasoft were consistent. Where necessary Fabasoft gave additional information or clarified the given information appropriately.

The Monitoring Body therefore verifies the service as compliant with the EU Cloud CoC based on the performed assessment as prescribed in 1. The service will be listed in the Public Register of the EU Cloud CoC[14] 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.

# 6 Validity

This verification is valid for one year. The full report consists of 10 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[15].

**Verification-date**: May 2021 **Valid until**: May 2022

**Verification-ID**: 2021LVL03SCOPE016

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