Verification of Declaration of Adherence

Declaring Company: NGA, an Alight company

Verification-ID	2020PV02SCOPE014
Date of Approval	December 2020
Valid until	December 2021

Table of Contents

1 Verification against v2.6 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 2.6 (**'v2.6'**)[2] as of March 2019.

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 v2.6 and its provisions has been aligned to the European General Data Protection Regulation (**'GDPR'**)[5].

The EU Cloud CoC already applies the same principles and procedures now, pending the endorsement of the Code and its official approval by supervisory authorities, cloud service providers are welcomed and invited to sign up their services under v2.6 of the EU Cloud CoC, to publicly underpin their efforts to comply with GDPR requirements.

2 List of declared services

2.1 hrX[6]

hrX is the proprietary product of NGA, an Alight company, and a cloud-based solution that is deeply integrated with cloud Human Capital Management platform, enabling the seamless and successful delivery of the services provided by Alight to its customers. It is a combination of solutions for integration, case management, payroll compliance, analytics, and employee engagement into a single suite of products which ensures that employees of Alight's customers are able to access information and the tools anywhere and on any device. hrX is composed of several modules such as Access, Analyze, Assist, Exchange and Pay.[7]

[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.ngahr.com/hr-services/cloud-services
[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.

2.2 XTend HR

XTend HR applications are NGA, an Alight company, SAP Cloud Platform Extensions built by NGA that integrate with standard HCM platforms, On Premise SAP HCM and SAP SuccessFactors Cloud to address specific business challenges requiring quick integration with the other systems. The apps provide among the other, visibility into the status of HR requests and workflows across a complex HCM landscape, provide employees with a single point of access and administration for the self-service management of their salary, rewards and benefits entitlements, allow HR and Payroll admins to monitor and manage complex HR processes, automate the transfer of data between the platform and any ID management system, create a one-step, end-to-end hiring process.[8]

2.3 euHReka

euHReka is a comprehensive preconfigured Human Capital Management solution powered by SAP and leveraging SAP's Payroll Control Center. Built on the concept of Business Process as a Service, **euHReka** blends an application layer with multi-country delivery capabilities and standardized workforce and payroll administration processes.

3 Verification Process - Background

V2.6 of the EU Cloud CoC has been developed against GDPR and hence provides mechanisms as required by Articles 40 and 41 GDPR[9]. Those mechanisms will apply pending the formal approval of the EU Cloud CoC and accreditation of the Monitoring Body.

3.1 Provisional Status of the Verification Process

The services concerned passed a provisional verification process by the Monitoring Body of the EU Cloud CoC, i.e. SCOPE Europe sprl/bvba[10].

This provisional verification process follows the same principles and procedures as the EU Cloud CoC will apply under its official approval and accreditation. 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.[11]

---

[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] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679
[10] https://scope-europe.eu
[11] https://eucoc.cloud/en/public-register/assessment-procedure/

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.

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 adhered as compliant and thereupon make them subject to continuous monitoring.

3.4.1 Levels of Compliance

V2.6 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 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 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.

3.5 Transparency about adherence

Each service adherent to the EU Cloud CoC must transparently communicate its adherence by both using the appropriate Compliance Mark[12] and refer to the Public Register of the EU Cloud CoC[13] to enable Customers to verify the validity of adherence.

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

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

4.1 Fact Finding

Following the declaration of adherence of NGA, an Alight company ('**Alight**'), the Monitoring Body provided Alight with a template, requesting Alight to detail its compliance with each of the Controls of the EU Cloud CoC. Additionally, the Monitoring Body requested an overview and reasoned response on the actual structure of the services declared adherent and why declared services are to be considered a "service family". A service family requires that all services rely on the same core infrastructure, with regard to hardware and software, and are embedded in the same contractual framework.

Alight promptly responded within the template. 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. Alight provided information illustrating the actual structure of the services declared adherent and describing the technical and contractual framework. Alight provided convincing responses that, as all services declared adherent are subject to the same technical framework and share to the extent relevant for the Code the same contractual framework. In detail, based on information provided by Alight, the Monitoring Body concluded that the declared Cloud Service(s) are comprised of several components that can be configured flexibly as per customer needs. However, whichever configuration the resultant service and available features are always delivered under the same legal and contractual framework, qualifying declared Cloud Services to be considered a "service family".

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[14], the Monitoring Body analysed the responses and information provided by Alight.

Alight services including those declared adherent are validly certified to comply with ISO27001:2013. Adequate statements and references were provided, and the certification status was considered regarding 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 indicate compliance.

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

As prescribed in 4.1, declared Cloud Service(s) comprise of several components. The technical architecture of such Cloud Service(s) follows common service architecture patterns, which may also include and integrate services and solutions provided by third-party commercial organisations. These components are thus part of the Cloud Service's provision and in scope of Alight's responsibility to ensure overall compliance of its Cloud Service(s). While these components are out of scope of the assessment performed by the Monitoring Body, we explicitly note that it is Alight's obligation to select appropriate components; however, management processes related to applicable third-party components are subject to the Code and will be verified.

Another area decided to be of relevance for the Initial Assessment has been third country transfers and whether measures regarding safeguards of such transfers are implemented accordingly, also taking into account that the European Court of Justice issued its decision in the so-called "Schrems II" ruling during the period in which the Cloud Services were assessed.

4.3 Examined Controls and related findings by the Monitoring Body

4.3.1 Examined Controls

The Monitoring Body reviewed the initial submission from Alight which outlined how all of the requirements of the Code were met by Alight 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. For this level of review almost all Controls were selected. This does not indicate any reservations of the Monitoring Body regarding the CPS's compliance, but Alight's Cloud Service provision has a very distinct, and individualised setup per Customer. Therefor the Monitoring Body needed to add a specific layer to its verification process that is not necessary where e.g. the Cloud Service provision follows a more generalist approach.

Additionally, samples were requested regarding Controls:

5.1.A, 5.2.C, 5.12.A

Based on the information provided by Alight, follow-up requests were issued, for further detail on implemented measures related to Controls and respective information provided for. All follow-up responses satisfied the requests made.

For avoidance of doubt: As indicated and explained earlier, the number of follow-up requests do not reflect in any case the quality of service provided, or in any case reflect the quality of compliance of the service.

4.3.2 Findings by the Monitoring Body

The assessment's main focus was to understand the procedures safeguarding that each Customer will be provided a Cloud Service set up in a manner that is compliant with the Code, both contractually and technically. As Alight offers highly individualised setups it was necessary to understand the existence and effectiveness of an overarching management process ensuring that such individualisation is capable to safeguard Code compliance at a minimum. Alight convincingly described its internal procedures, safeguarding that each contract comprises of a defined minimum set of relevant provisions and that individualisations will not take adverse effects, underpinned by the provision of respective samples of both the procedures and Cloud Service Agreement templates. Internal procedures also safeguard that regardless of a Customers configuration the same level of internal controls apply regarding data protection and IT security.

Consequently, another key aspect of the verification has been how Customers are being enabled to adequately respond to data subject rights related requests. Alight services several entry points for Customers to address data subject rights related requests; all entry points are linked to the same standardised procedures regardless if it was raised in the context of Alight's public-facing website, or by Customers of the declared Cloud Service. Customers may raise data subject rights related requests through their dedicated account managers, the self-service customer portal, or by phone/e-mail, the latter ensuring that trusted contacts established in the contract are observed. Alight provided detailed material how data subject rights related requests are processed, including internal timelines ensuring that regulatory timelines are respected, where applicable.

Due to the individual setup another area of interest during this verification has been the handling of data breaches. Alight provided detailed internal procedures mandating internal timelines, including safeguards ensuring compliance with regulatory deadlines.

Regarding adequate subprocessor handling Alight transparently communicates a schedule in their contractual framework detailing the processes and guarantees given to Customers. Hence sufficient information is available to Customers in the pre-contractual phase. Alight notifies Customers with reasonable lead time; Customers are able to object to any changes related so subprocessors, triggering a process to resolve objections amicably.

Section 6, in line with the general procedures as described above was only covered regarding appropriate interlinks of the IT Security Management System with data protection related dimensions, as the principal existence of adequate controls was already underpinned with Alight current and valid ISO 27001:2013 certification.

The Monitoring Body assessed whether measures regarding safeguards of third country transfers were implemented accordingly, especially as the European Court of Justice issued its decision in the so-called “Schrems II” ruling during the period in which the Cloud Services were assessed. Alight sufficiently and convincingly reported how Customers were notified about changes related to the so-called “Schrems II” ruling, where applicable. Alight also reported that transfers of personal data are no longer safeguarded solely with the EU-U.S. Privacy Shield, but other means such as Standard Contractual Clauses. Furthermore, Alight‘s responses convincingly assured that (at the time of the assessment), Alight did not receive any official request from a Supervisory Authority to suspend data transfers and agreed to provide notification to the Monitoring Body if Alight receives any such request.

Also, the Monitoring Body assessed in more detail compliance with requirements relating to confidentiality. Requirements related to the confidentiality of the processing, e.g. were verified as the confidentiality template agreement was assessed, verifying that provisions related to appropriate confidentiality obligations for employees and subcontractors prior, during and after engaging in relevant data processing activities are met.

5 Conclusion

Given answers by Alight were consistent. Where necessary Alight 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[15] alongside this report.

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

6 Validity

This verification is valid for one year. The full report consists of 12 pages in total, whereof this is the last page closing with the Verification-ID. Please refer to the table of contents at the top of this report to verify, that the copy you are reading is complete, if you have not received the copy of this report via the Public Register of the EU Cloud CoC[16].

Verification-date: December 2020 **Valid until**: December 2021

Verification-ID: 2020PV02SCOPE014

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