

# Verification of Declaration of Adherence

Declaring Company: Tempo Acquisitions LLC t/a Alight



EU  
CLOUD  
COC

**Verification-ID** 2020LVL02SCOPE014

**Date of Approval** December 2022

**Valid until** December 2023

## Table of Contents

<b>1</b>	<b>Verification against v2.11 of the EU Cloud CoC</b>	<b>3</b>
<b>2</b>	<b>List of declared services</b>	<b>3</b>
2.1	hrX	3
2.2	XTend HR	3
2.3	EuHReka	4
<b>3</b>	<b>Verification Process - Background</b>	<b>4</b>
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	5
3.4	Process in Detail	5
3.4.1	Levels of Compliance	6
3.4.2	Final decision on the applicable Level of Compliance	7
3.5	Transparency about adherence	8
<b>4</b>	<b>Assessment of declared services by Tempo (see 2.)</b>	<b>8</b>
4.1	Fact Finding	8
4.2	Selection of Controls for in-depth assessment	8
4.3	Examined Controls and related findings by the Monitoring Body	9
4.3.1	Examined Controls	9
4.3.2	Findings by the Monitoring Body	9
<b>5</b>	<b>Conclusion</b>	<b>11</b>
<b>6</b>	<b>Validity</b>	<b>11</b>

## 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'**)<sup>1</sup> in its version 2.11 (**'v2.11'**)<sup>2</sup> as of December 2020.

Originally drafted by the Cloud Select Industry Group<sup>3</sup> (**'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<sup>4</sup> 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'**)<sup>5</sup>.

## 2 List of declared services

### 2.1 hrX<sup>6</sup>

hrX is 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.<sup>7</sup>

### 2.2 XTend HR

XTend HR applications are SAP Business Technology Platform Extensions built by Alight 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

---

<sup>1</sup> <https://eucoc.cloud>

<sup>2</sup> <https://eucoc.cloud/get-the-code>

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

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

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

<sup>6</sup> <https://www.alight.com/ngahr>

<sup>7</sup> **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.

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.<sup>8</sup>

## 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 payroll processes administration.<sup>9</sup>

## 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<sup>10</sup>.

### 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<sup>11</sup>.

The Code has been officially approved in May 2021<sup>12</sup>. SCOPE Europe has been officially accredited as Monitoring Body in May 2021<sup>13</sup>. 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.<sup>14</sup>

### 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

---

<sup>8</sup> **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.

<sup>9</sup> **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.

<sup>10</sup> <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679>

<sup>11</sup> <https://scope-europe.eu>

<sup>12</sup> <https://www.gegevensbeschermingsautoriteit.be/publications/decision-n05-2021-of-20-may-2021.pdf>

<sup>13</sup> <https://www.gegevensbeschermingsautoriteit.be/publications/decision-n-06-2021-of-20-may-2021.pdf>

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

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 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<sup>15</sup> and referring to the Public Register of the EU Cloud CoC<sup>16</sup> to enable Customers to verify the validity of adherence.

## 4 Assessment of declared services by Tempo (see 2.)

### 4.1 Fact Finding

Following the declaration of adherence of Tempo Acquisitions LLC t/a Alight (**Tempo**), the Monitoring Body provided Tempo with a template, requesting Tempo to detail its compliance with each of the Controls of the EU Cloud CoC.

As this declaration is a renewal<sup>17</sup>, the Monitoring Body requested from Tempo a confirmation that there has been no material change to the applicable technical, organisational and contractual framework. The Monitoring Body also requested from Tempo 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.

Tempo 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<sup>18</sup>, the Monitoring Body analysed the responses and information provided by Tempo.

---

<sup>15</sup> <https://eucoc.cloud/en/public-register/levels-of-compliance/>

<sup>16</sup> <https://eucoc.cloud/en/public-register/>

<sup>17</sup> You can access the Verification Report(s) of previous year(s) via the following link(s): [Report 2021](#)

<sup>18</sup> <https://eucoc.cloud/en/about/about-eu-cloud-coc/applicable-procedures/>



Tempo's declared services have been externally certified and audited. Tempo holds 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 Tempo which outlined how all the requirements of the Code were met by Tempo'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.E], [5.2.E], [5.2.F], [5.2.G], [5.4.C], [5.4.E], [5.5.E], [5.7.E], [5.7.F], [5.8.A], [5.11.B], [5.12.A], [5.12.C], [5.12.D], [5.12.E], [5.14.A] and [5.14.B].

#### **4.3.2 Findings by the Monitoring Body**

Related to the Monitoring Body's requests (see section 4.1), Tempo indicated that no relevant changes to the Cloud Service Family were applied in regards of the implemented technical, organisational and contractual frameworks.

Tempo underwent a corporate restructure since the latest assessment. The contractual framework has been updated accordingly. The Monitoring Body, therefore, put in additional efforts to understand the consequences of such restructuring and extended the scope of its assessment.

Tempo presented the Monitoring Body with its (new) contractual framework, which includes a Framework Service Agreement (FSA) and a Data Protection Agreement (DPA). Responsibilities of Tempo, as data processor and the Customer as data controller are clearly defined in the DPA. In addition to its agreements, Tempo has established documented procedures to assist Customers to comply with their obligations under Article 28 of the GDPR.

The Monitoring Body assessed Tempo's procedures and alternative options provided to Customers relating to the engagement and rejection of subprocessors. Tempo provided the Monitoring Body with

a paraphrasing of its implemented measures which ensures that Customers provide their written authorisation to Tempo prior to engaging subprocessors and that Customers have the right to object to the appointment of new subprocessors by providing a written notice to Tempo of their rejection.

In the same vein, Tempo has put in place a program to ensure that subprocessors engaged provide sufficient guarantees of compliance with the GDPR throughout the life of the agreement with Tempo. The program includes the development and implementation of standard processes to verify Subprocessors' compliance with data protection laws, among others. A list of subprocessors is also made available to Customers through Tempo's website, as duly indicated in the DPA.

Another area of focus was around the transfer of Customer Personal Data to third countries. Tempo indicated safeguarding such transfers, at a minimum, by Standard Contractual Clauses (SCCs). In case other safeguards are adopted – in addition to the SCCs – their validity and adequate implementation is monitored as well. In addition to this, Tempo indicated having fully transitioned to the new SCCs.

The Monitoring Body also assessed Customers' Audit Rights. Tempo sends annual reports and certification to its Customers. Customers' Audit Rights are a standard part of Tempo's DPA and specifics are included in a relevant Statement of Work. Tempo's costs determination and allocation related to Customers' Audit Rights was also presented to the Monitoring Body.

Tempo presented policies and procedures allowing to maintain an up-to-date and accurate Records of Processing Activities (ROPA) carried out on behalf of Customers. In addition to this, the relevant communication channels for Customers providing the relevant information in relation to the completion and relevancy of the ROPA were confirmed by Tempo.

Relevant policies and procedures have been established by Tempo to timely and adequately report data breaches to the Customer without any undue delay. Tempo confirmed such internal timeline to the Monitoring Body.

Another area of focus was around the retrieval and destruction of Customer Personal Data, which is ensured by Tempo at the written request of the Customer or at the end of the agreement. While certain Customers have the capability to retrieve or delete Customer Personal Data through self-service features, other Customers need to provide Tempo with a written request. In that case, Tempo ensures that Customer Personal Data is also returned and permanently destroyed by its chain of subprocessors engaged as well.

## 5 Conclusion

The information provided by Tempo were consistent. Where necessary, Tempo 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<sup>19</sup> alongside this report.

In accordance with sections 3.4.1.2 and 3.4.2 and given the type of information provided by Tempo to support the compliance of its service, the Monitoring Body grants Tempo with a Second Level of Compliance.

## 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 CoC<sup>20</sup>.

**Verification-date:** December 2022

**Valid until:** December 2023

**Verification-ID:** 2020LVL02SCOPE014

---

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

<sup>20</sup> <https://eucooc.cloud/en/public-register/>