EU Cloud CoC looks forward to closer collaboration with GAIA-X, offering contributions and support

In June 2020, Ministries of France and Germany announced that Europe's next generation cloud environment is entering its next level of design and development. Analysing current publications, the General Assembly of the EU Cloud Code of Conduct highly welcomes GAIA-X core principles, as both initiatives seem well aligned, already.

The EU Cloud Code of Conduct for Cloud Service Providers ("EU Cloud CoC" or "the Code") has been developing its code of conduct particularizing EU General Data Protection Regulation (GDPR) with rigorous requirements for years. Fostering trust, accountability, and consequently enabling Customers to perform their rights und GDPR as best as possible when using Cloud Services has been key since the earliest days of the Code. After numerous iterations incorporating feedback from different stakeholders, including latest remarks by supervisory authorities, the General Assembly is currently awaiting the pending approval pursuant Article 40 GDPR.

Following its publications, the GAIA-X foundation (in establishment) is striving to become an essential element of Europe's cloud environment. To reach its overarching goal, the GAIA-X community focusses on key issues such as data-sovereignty, IT security, data portability, and data protection and strives to implement trusted and rigorous procedures related to its onboarding and continuous compliance check, eventually ensuring that services GAIA-X compliant services meet GAIA-X standards and requirements aligned with European values.

> *The EU Cloud CoC is the only current publicly available code of conduct for cloud services that has pursued a robust and externally governed independent monitoring of adherent services.*
>
> Jonathan Sage, Government and Regulatory Affairs Executive, IBM, Chairman of the EU Cloud CoC General Assembly

EU Cloud Code of Conduct
c/o SCOPE Europe b.v.b.a./s.p.r.l.
Rue de la Science 14
1040 Brussels, Belgium

Info@scope-europe.eu
+32 2 609 5319

https://eucoc.cloud

To enable trust of customers, it will be crucial to follow common and well-recognized principles and procedures regarding its monitoring and enforcement of compliance. As GAIA-X community is striving for high standards, as well as the EU Cloud CoC, we now recognize a significant alignment in this regard: The EU Cloud CoC is also pleased that they already being mentioned as one initiative that is considered suitable for GAIA-X standards by which Cloud Service Providers may prove compliance with Art. 28 GDPR, once the Code will be approved.

Robust and recurring verification procedures

GAIA-X and EU Cloud CoC both will require each service that is being listed as compliant to undergo independent conformity assessments, thus differentiating themselves from other initiatives allowing mere self-assessments. As key benefit of the GAIA-X environment it is mentioned that every interested user shall be enabled to easily choose a trusted cloud service without being the necessity of having in-depth expertise in cloud computing. Whereas providers may even nowadays proclaim compliance with any framework they like, interested users may only trust such claims if being independently verified.

Conformity should not be assessed only once in time. Especially, if business and service models are as constantly evolving as withing cloud computing, a constant and recurring assessment is key. The EU Cloud CoC requires re-verification at least annually, as additional ad-hoc assessments are possible. GAIA-X community has not yet defined its expected maximum timeframe between each assessment, but it is already said that "*at a given interval, a re-evaluation has to be performed*". GAIA-X, as the EU Cloud CoC, also expects remedies and enforcement actions in case verification will be passed positively. E.g. "*if the criteria of the scheme do not continue to be met, the listing in the GAIA-X Catalogue can be suspended.*" It will be interesting whether GAIA-X foundation (in establishment) will also implement a mechanism by which one may file complaints and thus trigger conformity assessment of partaking providers, similar to the monitoring scheme of the EU Cloud CoC. Such a mechanism can be an effective measure to ensure thorough conformity.

> *Being subject to at least annual, external scrutiny in a Code of Conduct is really important; this helps optimise internal procedures and safeguards compliance. We expect stakeholders will recognise this and the value of independent verifications will rise.*
>
> Helmut Fallmann, Member of the Managing Board, Fabasoft, Member of the EU Cloud CoC General Assembly

Reference to existing standards

The EU Cloud CoC gathers, maps, and references relevant standards, initiatives and well-recognised good practices like ISO and C5 to its unique Controls and thus strives to ease the documentation of compliance. For the avoidance of doubt: it is subject to the Monitoring Body only to verify compliance, but provisions of current compliance with existing well-recognised standards may surely be taken into account.

The GAIA-X environment covers numerous areas of which data protection is only one. The GAIA-X community describes one of its upcoming key tasks as further gathering, analysing, and condensing existing standards. We are confident that the similarities in this approach, and the underlying goal of interoperability, will ease future alignments and cooperation between both initiatives.

Different levels of assurance respectively compliance

One year after GDPR, the EU Cybersecurity Act became effective, introducing three levels of assurance, basis, substantial and high. Also, GAIA-X community refers to this classification. Such a threefold approach is becoming a suitable and broadly adopted standard.

The current EU Cloud CoC addresses obligations deriving from the GDPR. In this regard its baseline requirements set a high bar for privacy. The EU Cloud CoC may enhance the code further to address other upcoming laws and standards, keeping the high level of data protection set by the GDPR. Regarding the EU Cybersecurity Act and GAIA-X standards and their provisions of different levels of assurance, there is already a certain alignment as the EU Cloud CoC provides three levels of compliance which can be easily adapted to a mechanism, reflecting the upcoming risk classification standard as promoted by the EU Cybersecurity Act and GAIA-X community. Such implementation, though not mandatory under GDPR, still perfectly correlate with GDPR's risk based approach and specific upcoming modules of the EU Cloud CoC.

> *Initiatives like GAIA-X and the EU Cloud CoC will significantly shape cloud industry in Europe thus they will have to meet high standards and provide trusted verifications for those adherent. Involvement and exchange therefore are key, for businesses as well as other stakeholders and experts concerned to build*

future-proof but flexible frameworks that can be adopted by relevant sectors.

Corinna Schulze, Director, EU Government Affairs and Deputy Head of EU Representation Office, SAP, Member of the EU Cloud CoC General Assembly

Future-proof with sector-specific modules

Business models and user expectations are constantly evolving and changing. Also, regulators are ongoingly particularizing and adjusting requirements for distinct business sectors. Not a surprise that GAIA-X community and CSPCert, as a suggestion how to implement EU Cybersecurity Act, are considering it efficient and future-proof to define a common baseline whilst at the same time being accessible for additional sector specific modules. The EU Cloud CoC implements the very same logic: The General Assembly submitted its Code version defining an overarching baseline for the provisions of Cloud Services as processors pursuant Article 28 GDPR. However, the EU Cloud CoC is willing to address specific Customer and sector needs with dedicated modules to which Cloud Service may adhere additionally to the baseline requirements as set out in the latest version of the Code. By such modules, the EU Cloud CoC may also help defining a framework that enables CSPs and Customers to not only comply with GDPR but also other affecting regulations, as for example applicable in health, banking or governmental services.

Interoperability is of utmost importance to leverage burdens of conformity, as interoperability enables providers to adhere to more than one conformity framework and consequently services can be even more trusted by users. This also relates to the shifting provision of Cloud Services. It will be key to agree on consistent and broadly accepted new criteria to determine provider's responsibilities, and thus obligations. Static approaches like type of services will not be future proof.

Jörn Wittmann, Managing Director SCOPE Europe bvba, Monitoring Body of the EU Cloud CoC

Full coverage of cloud stack (XaaS)

The EU Cloud CoC, a Code that is addressing the full stack of Cloud Services, is following GAIA-X with highest interest, as also GAIA-X community is aiming to define a trusted environment for the full stack of cloud services (XaaS). Modern cloud services are, however, not relating to outdated but still commonly acknowledged categories of Infrastructure, Software or Platform as a Service anymore. GAIA-X publications even refer to enhancing models like “Infrastructure as Code”, clearly indicating that the conventional definition of IaaS services is not completely adoptable anymore and proving that barriers between types of Cloud Services are diminishing if not even vanishing. Models of shared responsibilities as defined by the EU Cloud CoC and GAIA-X standards will be the role model and driver in future.

Accessibility for Small and Medium-sized Enterprises (SME)

Different levels of assurance allow for accessibility of SMEs, as it is not required to acquire expensive certifications or audits. The basic level of assurance in GAIA-X environment and the Level of Compliance 1 of the EU Cloud CoC strive to ensure openness for SMEs. The EU Cloud CoC is requesting an evidence-based conformity assessment. GAIA-X publications have not provided a distinct terminology, yet, but promote that – especially in comparison to higher levels of assurance – GAIA-X’s basic follows similar mechanisms.

While the future structure of the GAIA-X entity is not clear yet, a proper mechanism to enable and accelerate trusted cloud computing for SME may be a staggered approach regarding fees and contributions as provided by the EU Cloud CoC.

> *Numerous experts from different backgrounds, have been contributing to the EU Cloud CoC to ensure the Code is following good practices and capable of meeting high expectations. Keeping continuous exchange also with external experts makes it possible to be ready for broad market adoption and reception and positively recognised by such ambitious initiatives as GAIA-X.*
>
> Nathaly Rey, Head of EMEA Data Protection & Compliance, Google Cloud, Member of the EU Cloud CoC General Assembly

Concluding, the EU Cloud very much appreciates that GAIA-X environment is opening itself to even more experts and European Member States, inviting them to contribute to a successful future European cloud environment. The EU Cloud CoC wants to emphasize that keeping the current approach, including accessibility, interoperability, balancing interests of different stakeholders, addressing dynamically the full stack of cloud services (XaaS), and last but not least always requesting continuous verification of compliance will be key to establish a coming European, broadly-endorsed standard.

As both initiatives are already aligned as they are, the EU Cloud CoC and its members are happy to offer assistance and contributions to the prosperous and future development of GAIA-X environment. Especially, as both initiatives are covering the full stack of cloud services, and GAIA-X community even going beyond in addressing even a single information as an asset, a cooperation in developing modern distinguishers to determine cloud providers responsibilities instead of old fashioned attributions to Infrastructure as a Servicer (IaaS), Software as a Service (SaaS), or even Platform as a Service (PaaS), appears worth an exchange the EU Cloud CoC's General assembly is willing to provide.

About the EU Cloud Code of Conduct

Cloud computing provides significant benefits to both public and private sector customers in terms of cost, flexibility, efficiency, security, and scalability. In order to secure the trust of cloud customers in Cloud Service Provider (CSPs), the EU Cloud Code of Conduct aims to help Cloud Providers on their path to GDPR compliance.

The EU Cloud Code of Conduct consists of requirements for CSPs that wish to adhere to the Code, plus a governance section that is designed to support the effective and transparent implementation, management, and evolution of the Code. The Code is a voluntary instrument, allowing a CSP to evaluate and demonstrate its adherence to the Code's requirements, either through self-evaluation and self-declaration of compliance and / or through third-party certification. The Code is developed to cover GDPR requirements for a Code of Conduct under GDPR and is being submitted to the appropriate Data Protection Authority.

The intention of the EU Cloud Code of Conduct is to make it easier for cloud customers (particularly small and medium enterprises and public entities) to determine whether certain cloud services are appropriate for their designated purpose. In addition, the transparency created by the Code will contribute to an environment of trust and create a high default level of data protection in the European cloud computing market.