Autorité de protection des données
Gegevensbeschermingsautoriteit

General Secretariat

Decision n° 05/2021 of 20 May 2021

Subject: Approval decision of the "Eu Data Protection Code of Conduct for Cloud Service Providers" by the General Secretariat of the Belgian Data Protection Authority (DOS-2018-07353)

The General Secretariat of the Belgian Data Protection Authority (hereinafter "Belgian DPA");

Having regard to article 40 of the EU General Data Protection Regulation 2016/679 ("GDPR"), the Belgian DPA shall approve the "EU Data Protection Code of Conduct for Cloud Service Providers" ("Eu Cloud COC" or "Code") submitted by Scope Europe provided that it meets the requirements set out under this Article;

Having regard to the Guidelines 01/2019 on codes of conduct and monitoring bodies (hereinafter "Guidelines 01/2019") adopted by the European Data Protection Board (hereinafter "EDPB") on 4 June 2019;

Having regard to Article 20.4 of the "Loi du 3 décembre 2017 portant création de l'Autorité de protection des données";

Having regard to article 12 of the internal rules of procedure of the Belgian DPA;

Considering that in accordance with the articles 40.7, 64.1(b) and 63 GDPR, the Belgian DPA has taken utmost account of the Opinion on the draft decision of the Belgian Supervisory Authority regarding the Eu Cloud COC adopted by the EDPB on 19 May 2021;

Adopts on 20 May 2021 the following decision:

I. Preliminary remarks

1. The Belgian DPA underlines the importance of codes of conduct as voluntary accountability tools to tailor data protection rules to the specificities of the processing of a sector. It also reaffirms its commitment to encourage associations and bodies representing a sector in developing codes of conduct.

2. In accordance with the cooperation procedure set out in section 8 of the Guidelines 1/2019, the Eu Cloud COC was reviewed by the Belgian DPA, as the code of conduct lead Authority, in collaboration with two co-reviewing supervisory authorities in accordance with articles 40.5, 55 and Recital 122 of the GDPR and Appendix 2 of the Guidelines 1/2019.

3. As stated in Recital 81 and article 28.5 of the GDPR, adherence of a processor to an approved code of conduct may be used as an element by which to demonstrate the sufficient guarantees as referred to in article 28.1 and 28.5 GDPR. The approval of this Code cannot be construed as any validation of the compliance of the members of the Code itself. As stated in article 41.4 of the GDPR, the provisions of the Code and the actions taken by the monitoring body are without prejudice to the prerogatives of the supervisory authorities.

II. Scope of the code of conduct

4. The Eu Cloud COC aims to contribute to the proper application of the GDPR, taking into account the specific features of the cloud computing sector. The primary objective of the Eu Cloud CoC consists of concretising the legal requirements of article 28 GDPR and the following relevant related articles of the GDPR: art. 5.1, art. 6, art. 27, art. 28.1, art. 28.2, art. 28.3, art. 28.4, art. 28.5, art. 28.9, art. 29, art. 30.2, art. 30.3, art. 30.4, art. 31, art. 32, art. 33, art. 37, art. 39.1 (b), art. 44, art. 45.1, art. 45 art. 46, art. 47).

5. The Eu Cloud CoC is intended to address all service types of the cloud market (e.g. IaaS, PaaS, SaaS) and creates a "baseline for implementation of GDPR" for these services. Its purpose is to provide practical guidance and define specific requirements for the cloud service providers ("CSPs"). The Code only applies to cloud services where the CSP is acting as a processor. It therefore does not apply to "business to consumer" (B2C) services or to any processing activities for which the CSP may act as a data controller.

6. The Eu Cloud CoC is not intended to provide appropriate safeguards for third country data transfers pursuant to 46.2 e) of the GDPR. Therefore, adherence to the Code is not intended to be a basis for permitting transfers of personal data to third countries as envisaged by article 40.3 GDPR. The Belgian DPA stresses, as stated in the code (Section 5.4 of the COC), that customers and CSPs, who will be

transferring personal data to a third country outside the European Economic Area ("EEA"), remain responsible to assess the individual appropriateness of implemented safeguards according to Chapter V of the GDPR.

III. Review of the Eu Cloud COC

7. The review of the Eu Cloud COC led to the conclusion that the Code complies with the requirements set out by article 40 of the GDPR, as well as Section 6 of the Guidelines 1/2019 and in particular that the code of conduct:

1. Meets a particular need of that sector or processing activity

8. The Eu Cloud COC contains both strict requirements particularizing the provisions of the GDPR mentioned in the "Scope of the code of conduct" section of the present decision and good practices currently followed by the sector.

9. The Code aims to create comparability between different data processing practices in the cloud industry and improves upon the state of the art for data protection in this sector.

10. The objective of the Eu Cloud COC is to help CSPs to demonstrate compliance with article 28 GDPR and to make it easier and more transparent for customers to analyze whether cloud services are appropriate for their use case and in line with article 28.1 and 28.5 GDPR. Article 28.1 GDPR provides that controllers shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject. Article 28.5 GDPR states that the adherence of a processor to an approved code of conduct may be used as an element by which to demonstrate sufficient guarantees as referred to in paragraphs 1 and 4 of article 28 GDPR.

2. Facilitates the effective application of the GDPR

11. The Eu Cloud COC brings added value to the provisions of the GDPR by providing guidance and imposing binding requirements to its member.

12. Those guidance and requirements relate to:

- The use of sub-processors, including the authorization (general or specific) given by the customer, and changes in sub-processors (Code, section 5.3);
- Auditing requirements, including the mechanisms and information that a CSP should make available to a customer in order to allow them to determine how the CSP complies with its obligations under data

protection law, under its cloud service agreement with the customer and under the Code (Code, section 5.5);

- Data subject rights, in particular to the obligation for the CSP to provide assistance to the customer in order to allow data subject rights to be exercised (Code, section 5.7 and section 5.10);
- The fact that any adhering CSP, even those not legally obliged to have a DPO, must have at least a "data protection point of contact" in order to assist the customer (COC, section 5.9);
- The inclusion of termination modalities, including the return or deletion of customer personal data upon termination of the cloud service agreement, (Code, section 5.14);
- The fact that any CSP participating to the Code must fulfill at least, the security objectives drafted on the basis of recognized standards such as ISO 27001, ISO 27701, SOC 2,C5. It must be underlined that formal certification against those standards is recommended but not required under the Code, in order to account for the interests of small and medium sized CSPs (Code, section 6). If the CSP decides to implement alternative measures than those established by the aforementioned standards, it shall provide reasoning and evidence to the monitoring body why those measures adequately replace the "controls" concerned (Code, section 6.1);
- The Code's enhanced transparency requirements. The Code clearly outlines information which must be made available to all customers, including on topics on which the GDPR does not impose transparency (Code, section 6.3; 7.2.5)

3. Specifies the application of the GDPR

13. The Code consists of a set of requirements that CSPs have to implement to comply with the Code.

14. Those requirements are supported by a "controls catalogue" helping to assess compliance with the requirements of the Code. The "controls catalogue" maps the requirements of the Code to auditable elements ("controls"), and also maps requirements of the Code to corresponding provisions of the GDPR and relevant international standards, thus facilitating its application and interpretation and enabling implementation, monitoring and where required auditing.

15. The "controls" are to be read in conjunction with the "control guidance" which gives advice on how to implement the "controls". The "control guidance", although not mandatory, compels a CSP which would decide to implement alternative measures to be compliant with the Code, to demonstrate that the alternative measures are not less protective than those being provided by the "control guidance".

16. All provisions of the Code and the "controls catalogue" are binding, wherever the provisions make use of "shall", "must" or "will". Some provisions should be regarded as guidance, setting examples of good practices and are denoted by the use of the terms "should" or "may".

4. Provide sufficient safeguards

17. In the course of its review and the approval procedure, the Belgian DPA has not identified any provision that could undermine the level of protection provided by the GDPR or any other applicable European data protection legislation. The Code also provides for safeguards in this respect:

- Regarding the definitions, the Code commits that "*any terminology used in this Code, which is defined by the GDPR (e.g. personal data, controller, processor, data subject, etc.) shall have the meaning and interpretation as defined in accordance with that regulation*" (Code, section 2);
- Regarding the right to audit of article 28.1(h) of the GDPR, the Code states that the customer can exercise his right to audit at any time and the Code prohibits explicitly CSPs from effectively limiting this right (Code, section 5.5). Furthermore, regarding the repartition of the cost of audits between the customer and the CSP, the Code states that "*The CSP and the Customer may specify any arrangements in relation to the cost allocation for audits in the Cloud Services Agreement, provided that such arrangements are reasonable and reflect the realistic cost of the audit, consequently are not excessive or prohibitive. In the absence of any arrangements in relation to the costs and cost allocation, the costs shall be borne by the party requesting the audit; to the extent CSP is defining those costs, they still must not be excessive or prohibitive*" (Code, section 5.5.6);
- Regarding the right to complaint, the Eu Cloud COC allows customers, any CSPs, and data subjects to file a complaint before the monitoring body in case of alleged infringement to the Code. Such complaints can also be filed anonymously (Code, section 7.8.2). In addition, the Code establishes that, as a rule, such complaints can be submitted free of any costs. Only to prevent manifestly unfounded or excessive complaints, the monitoring body may charge a fee or refuse to act on the complaint (Code, section 7.8.3.1).

18. Finally, the Code underlines in section 7.3 that: "*verified adherence of Cloud Services to the Code does not absolve any CSP from having to comply with the GDPR, and/or applicable EU Member State data protection law, nor does it protect CSPs from possible interventions or actions by supervisory authorities in the course of their supervision and enforcement activities with regards to the adherent Cloud Service. GDPR and applicable Member State Law will always prevail over the Code*".

5. Provides mechanisms which allow for effective oversight

19. A code of conduct requires the implementation of suitable mechanisms to ensure that its rules are appropriately monitored and that efficient and meaningful enforcement measures are put in place to ensure full compliance. A code of conduct specifically needs to identify and propose structures and procedures which provide for effective monitoring and enforcement of infringements.

20. The Eu Cloud COC ensures that its rules will be followed through the following mechanisms:

- 5.1) Monitoring of the Code (initial, recurring and ad-hoc);
- 5.2) Complaint mechanism; and
- 5.3) Sanctions.

5.1 Monitoring of the Code

21. The monitoring of the accredited monitoring body is based on an evidence-based conformity assessment (interviews and document reviews) performed by the monitoring body. If the evidence is insufficient to demonstrate compliance, appears to be false, or is inconsistent, the monitoring body shall request additional information and can request substantiation by independent reports (Code, section 7.5.6).

22. Three cumulative types of monitoring are carried out by the monitoring body: "initial", "recurring" and "ad hoc".

5.1.1 "Initial" monitoring of the Code

23. The monitoring body will carry out an "initial" assessment which will examine if the service of a CSP which signs up to the Code through a "Declaration of Adherence" complies with the Code.

24. It is important to underline that the monitoring body will not assert a cloud service's compliance with the Code, as long as the monitoring body is not convincingly satisfied by the provided evidence that the cloud service demonstrates compliance.

25. The Code requires an evidence-based conformity assessment for all CSPs and every CSP will be subject to checks by the monitoring body. However, the Code supports three different methods of checking conformity of the CSPs which translate into three different levels of compliance marks (Code, section 7.6). The different levels of compliance are related to the level of substantiation being provided by the CSPs to the monitoring body. It is up to the CSP to indicate the level of compliance it seeks. The final decision as to whether the CSP meets the requirement of the sought-after level rests on the monitoring body (Code, section 7.6.3). Those three different methods to demonstrate compliance with the Code have been put in place in order to supports SME providers who have the internal know-how to provide cloud services and high levels of data protection, but who do not necessarily have a readily available budget for third party certifications and audits; such CSPs can use the first level of compliance. At the same time, the Code also empowers CSPs to leverage the authority of credible already undergone third-party certifications and audits at levels two and three.

26. Those three methods of checking conformity are the following:

- Level 1 - the CSP has to perform an internal review of its conformity itself, by documenting the measures it has implemented in order to prove compliance with the requirements of the Code. It then provides

this information to the monitoring body, along with a formal declaration that its services adhere to the requirements of the Code. The monitoring body actively verifies that the cloud service complies with the Code, on the basis of the provided evidence. It assesses the completeness of the evidence as well as its credibility: if the evidence provided appears to be unusual or any doubts arise, the monitoring body will ask follow-up questions, and the CSP will not be published as adhering to the Code until appropriate clarifications have been obtained (Code, section 7.6.2.1);

- Level 2 - In addition to the evidence requirements of the first level a CSP can choose to additionally provide complementary evidence of compliance from independent third-parties, such as certificates and audit reports which the CSP has obtained, possibly even before applying to join the Code. While no certificate or audit report currently covers all requirements or "controls" of the Code, it is possible through the "controls catalogue" for the monitoring body to determine which "controls" have been externally and independently audited. While the monitoring body will still conduct a thorough and independent verification of compliance with all requirements of the Code, all provided evidence originating from the third party such as certificates and audit reports provide additional assurance depth scrutiny. For the avoidance of doubt: this does not prevent the monitoring body to perform a full in-depth assessment, at all times (Code, section 7.6.2.2);
- Level 3 - A third level of assurance is attained when compliance with every part of the Code (i.e. to every "control", not just a set of "controls" as under the second level) is fully demonstrated by independent third-party certificates and audits, which the CSP has undergone with regard to the cloud service declared adherent and which are based upon internationally recognized standards. In other words, evidence of compliance is provided and checked comprehensively by the CSP, by the third party, and by the monitoring body. This level does not either prevent the monitoring body to perform a full in-depth assessment, at all times (Code, section 7.6.2.3).

27. Those three different levels of conformity checks reflect in three different "compliance marks". For the sake of transparency and clarity for customers and data subjects, the "compliance marks" shall be used in combination with a unique "Verification- ID" assigned by the monitoring body and where technically possible, the "compliance mark" shall link to the public register of the Code; otherwise the CSP shall provide at least a footnote explaining the safeguards entailed by the respective "compliance mark" and a reference to the public register (Code, section 7.6.4).

5.1.2 "Recurring" monitoring of the Code

28. The monitoring body will conduct at least annual checks of all adhering CSPs taking random samples of "controls" to ensure that the asserted compliance information is still complete. Each individual annual revision does not cover all requirements of the Code; however, over successive reviews, all requirements of the Code will be covered. Notwithstanding the aforementioned, the adherent cloud service must

comply with all requirements of the Code at all times and the monitoring body may at all times perform a full assessment (Code, section 7.7.1).

29. CSPs are required to update information in relation to their services provided to the monitoring body to ensure that the information available for the monitoring body always remains fully up to date and accurate. Not submitting the compulsory annual, renewal of a declaration of adherence is considered as infringement of the Code to the extent the CSP has not terminated its adherence consistent with the provisions of this Code and the procedures established by the Monitoring Body (Code, section 7.7.1).

5.1.3 "Ad hoc" monitoring of the Code

30. The compliance shall also be reviewed on an "ad-hoc" basis by the monitoring body if "*any significant changes occur to adherent Cloud Services*" or "*in reaction to a Customer complaint, an adverse media report or anonymous feedback about a CSP which has declared a Cloud Service adherent to the Code*" (Code, section 7.7.1).

5.2 Complaints mechanism

31. If the monitoring body receives complaints (for instance, by third parties, customers, competing CSPs, data subjects), the complaints panel, an independent board within the monitoring body that is not bound by instructions of any kind, decides on the respective merits of the complaint. Such complaint can also be filed anonymously. In case a complaint is found to be valid, this panel can impose sanctions on to CSP (Code, section 7.8.2).

5.3 Sanctions

32. The monitoring body can impose sanctions on the code members. Those sanctions range from non-public but formal reprimand to temporary or permanent revocation from the Code. The monitoring body commits to inform the supervisory authority about any related actions taken (Code, section 7.9).

33. The Belgian DPA reminds that sanctions imposed by the monitoring body are without prejudice to the sanctions from competent authorities as foreseen in case of breaches of the GDPR and/or other legal acts in accordance 41.4 of the GDPR.

6. Has designated a monitoring body

34. A draft code also needs to identify an appropriate body which has at its disposal mechanisms to enable that body to provide for the effective monitoring of compliance with the code

35. The Code and the Code owner have appointed "Scope Europe" as monitoring body in accordance with article 41 of the GDPR.

36. This monitoring body will have to be accredited by the Belgian DPA and therefore will have to demonstrate that it fulfills the requirements imposed by article 41 of the GDPR. This monitoring body will be in charge of ensuring compliance of the members of the Code with the provisions of the Eu Cloud COC and taking actions including sanctions in case of infringement to the provisions of the Eu Cloud COC. If and to the extent the Code or a "control" leaves room for interpretation, e.g. where it requires reasonable assistance, the Monitoring Body shall provide the final conclusive decision, whether the Code's requirement is being complied with (Code, section 7.5.3).

DECIDES AS FOLLOWS:

37. Taking into account the aforementioned considerations the Belgian DPA decides that the Eu Cloud COC submitted by Scope Europe fulfills the requirement set out in article 40 of the GDPR and the Guidelines 1/2019 and hereby approves the Eu Cloud COC.

38. This Decision will be published on the Belgian DPA's website and the Code will be communicated to the EDPB in accordance with article 40.11 of the GDPR.

David Stevens

Director of the General Secretariat