Autorité de protection des données
Gegevensbeschermingsautoriteit

General Secretariat

Decision n° 06/2021 of 20 May 2021

Subject: accreditation of the "Scope Europe" for the monitoring of the "Eu Cloud Code of Conduct" (DOS -2019-03289)

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

Having regard to article 41 and 57(1)(q) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("GDPR");

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 Opinion 02/2020 on the Belgian DPA's draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR adopted on 28 January 2020 by the EDPB;

Having regard to article 20 of the "Loi du 3 décembre 2017 portant création de l'Autorité de protection des données";

Having regard to article 15 of the internal rules of procedure of the Belgian DPA;

Having regard to Decision of the General Secretariat n° 01/2020 on the accreditation requirements for code of conduct monitoring bodies of 24 September 2020 (hereinafter' Decision of the General Secretariat n° 01/2020);

Having regard to Decision of the General Secretariat n° 04/2021 on the approval of the "EU Data Protection Code of Conduct for Cloud Service Providers";

Adopts on 20 May 2021 the following decision:

I. Preliminary remarks

1. Scope Europe (hereinafter "the applicant") submitted an application to be accredited as a monitoring body for the Eu Cloud code of conduct (hereinafter "Eu Cloud COC") on the 24th of August 2020. Upon request of the Belgian DPA, the applicant submitted a revised application including additional documentation on the 26th of April 2021.

2. In accordance with the articles 40 and 41 GDPR and the Guidelines 01/2019, §27, a code of conduct which involves processing activities of private, non-public authorities or bodies must be monitored by an accredited monitoring body.

3. The competence to accredit a monitoring body in charge of monitoring a transnational code of conduct according to article 57(1)(q) GDPR is granted to the data protection authority which is in charge of approving the transnational code of conduct. Under the criteria listed in Appendix 2 of the Guidelines 01/2019, the Belgian DPA was deemed competent to carry out the review the Eu Cloud COC which led to the approval of the aforementioned code by decision of the General Secretariat n° 04/2021. By way of consequence, the Belgian DPA is also competent to assess the application for accreditation of the proposed monitoring body for the Eu Cloud COC.

4. The applicant's submission has been assessed against the accreditation requirements as set out in Decision of the General Secretariat n° 01/2020.

II. Assessment of the application for accreditation

1. Independence and impartiality

Legal and decision-making procedure

5. The applicant is a Belgian limited liability corporation established at Wetenschapsstraat 14, 1040 Brussel in Belgium. The applicant's main shareholder is Selbstregulierung Informationswirtschaft e.V.(SRIW), which is established at Albrechtstraße 10B, 10117 Berlin in Germany.

6. The applicant has demonstrated the implementation of appropriate safeguards to ensure that the Monitoring Body will operate independently from the decision making of SRIW so that any decisions made by the board of SRIW or its members do not influence the activity of the Monitoring Body of the applicant:

   - The current and future members of the Eu Cloud COC are not members nor shareholders of Scope Europe;

- Code members which want to adhere to the Eu Cloud COC will have a contractual agreement with the applicant related to the provisioning of monitoring services which will prevent them from having any undue influence on the performance of the monitoring tasks by the applicant;

- Any personnel of the monitoring body, regardless of its role or hierarchy, is given in its labor contract the right to reject decisions that may inappropriately influence decisions of the Monitoring Body. Such rejection shall not lead to any direct or indirect disadvantages for the employee concerned;

- The establishment of a 'Head of Monitoring' which is in charge of ensuring that this independence is preserved and must be involved in all decisions related to the monitoring tasks of the applicant.

Financial

7. The Monitoring body is financed through the contributions of the code members. The applicant ensures the financial sustainability of its operations by charging basic fees and service-based fees. Recurring basic fees ensure the general operation and administration of the applicant, whereas service-based fees are charged to (potential) code members for distinct services related to monitoring tasks. The applicant demonstrated that the calculation of the basic and service-based fee ensures a sustainable performance of the monitoring tasks.

8. To prevent financial pressure by a code member, the applicant has introduced adequate termination periods preventing monitored companies to inappropriately influence the Monitoring Body by threating to terminate the monitoring services immediately. Furthermore the applicant requires pre-payment for certain services and has established a commonly agreed pricelist that should not be negotiated with the code members.

Organisational

9. The monitoring body is divided in three distinct units: the Assessment Unit, the Complaints Committee and the Administrative Unit. The applicant has established mechanisms to ensure that all staff involved in the performance of monitoring tasks is subject to strict confidentiality obligations and should disclose possible conflicts of interest. The applicant has committed to evaluate on an annual basis to what extent its structure can be improved to ensure that the need-to-know principle is being respected and that conflicts of interest will not arise from the fact that information is unduly shared between staff of different departments or units. The use of a ticket-system with logs that cannot be unduly altered, enables the applicant to oversee that information barriers are complied with internally.

10. The applicant's has demonstrated that the monitoring body can freely choose, direct and manage its own personnel without any direct or indirect influence by the Eu Cloud COC code owner, code members or any other party that might have an interests in the decision-making activities of the Monitoring Body. The Head

of Monitoring shall be consulted in all decisions relating to its personnel to ensure that there is no adverse effect on the performance of the monitoring tasks.

Accountability

11. All relevant actions taken in the performance of the monitoring tasks (such as the handling of declarations of adherence or complaints) will be registered through a ticket-system which shall ensure the audit-proof handling of all cases. The ticket-system properly documents all activities related to the monitoring tasks.

12. In addition, the applicant has implemented procedural rules that oblige personnel to document all relevant decisions that are related to the general accreditation requirements of the monitoring body. Furthermore, the applicant will train its staff in relation to the implementation of article 41 GDPR and the documentation obligations as described above, including the indicators to recognize possible undue influence or effects on impartiality.

2. <u>Absence of conflict of interest</u>

13. The contractual arrangements in the labor contract of the monitoring body staff guarantee that employees are not simultaneously employed (full-or part-time and compensated and non-compensated) by one of the code members. In addition, employees who previously worked for a code member are not allowed to assess their former employing company for a period of three years.

14. In addition, the applicant has implemented transparency procedures to detect and resolve internal conflicts of interest. These rules prevent an employee from assessing his or her own performance and ensure that no individual shall perform both the assessment of the declaration of adherence and the complaints handling with regard to the same code member or service.

15. If a conflict of interest occurs, the employee has the obligation to report it to its hierarchy and will be re-assigned in a way minimizing the potential inappropriate influence.

3. <u>Expertise</u>

16. The applicant has adequately demonstrated that the monitoring body as a whole has sufficient expertise (certifications, degrees or professional experience) in data protection, the cloud sector which is covered by the Eu Cloud COC and auditing. The background, qualifications and experience of the monitoring body staff notably cover:
    - Certifications as a data protection officer and data protection auditor;
    - Expert legal knowledge in the domain of data protection legislation;
    - Academic degrees in law and experience as a practicing lawyer;
    - Certification and auditing expertise, in particular in the domain of IT-security.

17. Furthermore, the applicant will set up internal training, provide for internal guidelines and adhere to a four-eyes-policy (which ensures that every document is reviewed by another staff member) to ensure that each decision is based on the overall expertise of the monitoring body.

4. Established procedures and structure

18. The members of the Eu Cloud COC will be monitored by the applicant through three types of assessments (initial, recurring and ad hoc). The monitoring body will carry out an "initial" assessment which will examine if the service for which a code member signs up to the Eu Cloud COC through a "Declaration of Adherence" complies with the Code. The monitoring body will conduct recurring, at least annual checks of all adhering code members by taking random samples of "controls" to ensure that the asserted compliance information is still complete. Last but not least, 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 code member which has declared a Cloud Service adherent to the Code. The three types of assessments are described in further detail in section III.5 of the Decision of the General Secretariat n° 04/2021.

19. The applicant has demonstrated that the monitoring body is composed of an adequate number of staff to ensure that it is able to carry out its monitoring functions and assessments appropriately.

20. The assessments will be carried out against the controls and related guidance which are included in the Eu Cloud COC as approved by the Decision of the General Secretariat n° 04/2021.

21. Once a cloud service has been verified compliant with the code, the service will be listed in a public register including only Cloud Services that have been verified compliant.

22. In case the Assessment Unit considers a Cloud Service to be infringing the Code, the Assessment Unit will have to notify the Complaints Committee which is responsible for the determination of appropriate remedies and sanctions. The Complaints Committee shall select from possible sanctions and remedies as provided by the Eu Cloud COC.

5. Complaints and Sanctions

23. The applicant has put in place procedures to introduce complaints against a code member for any alleged infringement of the Eu Cloud COC. The procedures stipulate that complaints shall be processed in due time. Whether a complaint is fit for decision shall – by default – be determined within a maximum of eight weeks, else the Complaints Committee shall be notified accordingly. If and to the extent that final decision cannot be reached within three months, the complainant shall be notified accordingly, providing reasons, such as complexity of the complaints or that the complaint was not ready for decisions at the time of reception.

24. Through contractual agreements with the code members, the applicant is being granted power to enforce its decisions in case of infringement of the code.

25. The Eu Cloud COC allows for the following measures against a member:
    - A non-public but formal reprimand;
    - A announcement of the non-compliance, including facts and reasoning;
    - A temporary or permanent revocation of the verification of compliance with the code of conduct related to the Cloud Service concerned;
    - A temporary or permanent revocation of the verification of compliance with the code of conduct related to all Cloud Services of the code member;
    - A temporary or permanent revocation of membership in the General Assembly.

26. If the measures taken by the monitoring body are not sufficient to end the infringement, the monitoring body will take remedies which may result into a request for additional reports and on-premise assessments.

27. The relevant procedures that set out how complaints should be introduced and how they will be assessed, will be made public by the monitoring body on its website. In addition, the applicant has set up a mechanism to clearly communicate the adherence of a code member to the Eu Cloud COC to enable complainants to file complaints. In particular this is ensured by:
    - a publicly available and accurate list of adherent code members and/or services (Public Register);
    - a compliance marks transparently communicating the verified compliance with the Eu Cloud COC.

6. Communication

28. The applicant commits to communicate to the Belgian DPA on an annual basis a monitoring report containing the following information:
    - The general development of the Eu Cloud COC e.g. increases or decreases related to membership, total number of services declared adherent, etc.;
    - The number of declarations of adherence received, processed and renewed within the last 12 months;
    - The number of complaints received, regardless of their outcome; and
    - A general overview of relevant decisions.

    The applicant shall provide any additional information required upon request of the Belgian DPA.

29. All relevant documentation required by the Belgian DPA to assess the proper functioning and performance of the applicant shall be kept for a period of 5 years.

30. In addition to this annual communication, the applicant will:
    - communicate without undue delay any action taken against a code member;
    - notify complaints that could not be resolved due to lack of cooperation of a code member;

- notify any significant changes regarding the structure and procedures of the Monitoring Body which could affect its ability to perform its function impartially, independently and effectively.

31. The applicant ensures that interested parties shall have access to all relevant documents to determine scope and guarantees provided by the Eu Cloud COC. This shall be reached by making publicly available at least:
    - the Eu Cloud COC
    - the applicable procedures of the Monitoring Body (General, Assessment, Complaints);
    - the list of applicable remedies and sanctions;
    - the competent supervisory authority of the Eu Cloud COC and the applicant.

7. Review Mechanisms

32. The applicant has set up a procedure to monitor and document changes to the legal framework, including changes in its interpretation triggered by public guidelines, decisions of public authorities or court decisions. Such changes will be notified to the code owner and the Belgian DPA whenever they could result in potential conflicts with provisions of the Eu Cloud COC that are otherwise unambiguous.

8. Legal status and organizational structure

33. As set out in paragraph 5 of this decision, the applicant is a limited liability corporation that is registered and established in Belgium and subject to Belgian law. Therefore, the applicant has the appropriate legal standing to be held accountable for its actions and is capable of being fined as required per article 83.4.c) GDPR.

34. The applicant commits expressively to comply with all relevant legislation and in particular with the provisions of GDPR.

9. Subcontractors

35. The applicant commits that any subcontractor will satisfy all relevant requirements in particular requirements regarding: independence, impartiality, absence of conflict of interest, expertise, commitment to comply with all relevant legislation and in particular the provisions of the GDPR.

36. Scope Europe remains liable and responsible for all activities sub-contracted.

DECIDES AS FOLLOWS:

37. Having regard to the fact that the applicant has demonstrated the fulfillment of all requirements set out in the Decision of the General Secretariat n° 01/2020, the Belgian DPA grants the accreditation to the applicant to act as the monitoring body in the sense of article 41.2 GDPR in charge of monitoring the Eu Cloud COC.

38. In accordance with article 41.5 GDPR the applicant will retain its accreditation status unless the outcome of a review conducted by the Belgian DPA concludes that the requirements for accreditation are no longer met.

David Stevens

Director of the General Secretariat