Opinion 17/2021 on the draft decision of the French Supervisory Authority regarding the European code of conduct submitted by the Cloud Infrastructure Service Providers (CISPE)

Adopted on 19 May 2021

Adopted

Table of contents

The European Data Protection Board

Having regard to Article 63, Article 64(1)(b) and Article 40 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 (hereinafter "GDPR"),

Having regard to the European Economic Area (hereinafter "EEA") Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

Having regard to Articles 10 and 22 of its Rules of Procedure.

Whereas:

(1) Member States, Supervisory Authorities, the European Data Protection Board and the European Commission shall encourage the drawing up of codes of conduct (hereinafter "code") to contribute to the proper application of the GDPR[2].

(2) The main role of the European Data Protection Board (hereinafter "the EDPB") is to ensure the consistent application of the GDPR when a supervisory authority (hereinafter "SA") intends to approve a code of conduct that related to processing activities in several Member States (hereinafter "transnational code") pursuant to article 40.7 GDPR and to the Board's "Guidelines 1/2019 on Codes of Conduct and Monitoring bodies under Regulation 2016/679" (hereinafter the "Guidelines").

(3) The EDPB welcomes and acknowledges the efforts made by the associations and others bodies representing categories of controllers or processors to elaborate codes of conduct which are practical and potentially cost-effective tools to ensure greater consistency among a sector and foster the right to privacy and data protection of data subjects by increasing transparency.

(4) This opinion aims to ensure the consistent application of the GDPR, including by the SAs, controllers and processors and to highlight the core elements which each code of conduct has to develop.

(5) Taking into account the specific characteristics of the sector concerned, each code of conduct should be addressed individually and is without prejudice of the assessment of any other code of conduct. The EDPB recalls that Codes represent an opportunity to establish a set of rules which contribute to the proper application of the GDPR in a practical, transparent and potentially cost-effective manner that takes on board the specificities for a particular sector and/or its processing activities.

(6) The EDPB underlines that codes of conduct are voluntary accountability tools, and that the adherence to a code does not prevent DPAs from exercising their enforcement power and prerogatives.

[1] References to "Member States" made throughout this opinion should be understood as references to "EEA Member States".
[2] Article 40(1) of the GDPR

(7) The present code is not a code of conduct according to article 46(2)(e) meant for international transfers of personal data and therefore does not provide appropriate safeguards within the framework of transfers of personal data to third countries or international organisations under the terms referred to in point (e) of article 46 (2). Indeed, any transfer of personal data to a third country or to an international organisation shall take place only if the provisions of chapter V of the GDPR are respected.

(8) The opinion of the EDPB shall be adopted, pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure, within eight weeks after the Chair has decided that the file is complete.

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. In accordance with the cooperation procedure as set out in the guidelines on codes of conduct[3], the code of conduct of CISPE ("CISPE Code" or "Code") was reviewed by the French Supervisory Authority as the Competent Supervisory Authority (hereinafter the "CompSA").

2. The CISPE Code has been reviewed according to the procedures set up by the EDPB.

3. The FR SA has submitted its draft decision regarding the draft CISPE Code, requesting an opinion of the EDPB pursuant to Article 64(1)(b) GDPR on 29 February 2021. The decision on the completeness of the file was taken on 31 March 2021.

2 ASSESSMENT

2.1 The Code of conduct meets the needs of the sector

2.1.1 Presentation of the sector

4. Cloud computing consists of a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space.

5. The CISPE Code aims to contribute to the proper application of the GDPR, taking into account the specific features of the cloud computing sector.

6. The term "cloud computing" covers a variety of very distinct service provision models such as Cloud Infrastructure as a Service Cloud ("IaaS"), Cloud Software as a Service ("SaaS") and Cloud Platform as a Service ("PaaS"). The term "IaaS" describes a situation in which a provider leases a technological infrastructure, i.e. virtual remote servers the end-user can rely upon in accordance with mechanisms and arrangements such as to make it simple, effective as well as beneficial to replace the corporate IT systems at the company's premises and/or use the leased infrastructure alongside the corporate systems. When providing "SaaS", a provider delivers, via the web, various application services and makes them available to end-users. These services are often meant to replace conventional applications to be installed by users on their local systems; accordingly, users are ultimately meant to outsource their data to the individual provider. When providing "PaaS", a provider offers solutions for

[3] Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/676 adopted by the EDPB on 4 June 2019.

the advanced development and hosting of applications. These services are usually addressed to market players that use them to develop and host proprietary application-based solutions to meet in-house requirements and/or to provide services to third parties.

2.1.2 The code owner as a representative organisation

7. Codes of conduct must be submitted for approval to the supervisory authority which is competent in accordance with article 55 of the GDPR. In case of transnational codes, when identifying the competent SA, some factors could be taken into account, for example, the location of the largest density of the processing activity or the location of the code owner's headquarters.[4]

8. The Cloud Infrastructure Service Providers (CISPE) is a non-profit association established in Belgium.

9. The code owner has identified the French supervisory authority as the competent supervisory authority for the purposes of seeking approval of the CISPE Code. The code owner has justified his choice in the code of conduct based on several criteria such as the establishment of several CISPE members in France or the establishment of officers of CISPE including the treasurer and the chairman's companies in France.

10. In accordance with Article 40 (2) GDPR, a code of conduct has to be prepared by associations or others bodies representing categories of controllers or processors (code owners). Because the code owner has a major role in ensuring consistency and harmonization of practices within the sector concerned by the code, it has to demonstrate to the CompSA that it is an effective representative organization. As such, as stated in the Guidelines, the code owner should be capable of understanding the needs of their members and define the processing activity or sector to which the code is intended to apply.[5]

11. Recital 99 GDPR advises to consult during the process of drawing up a Code of Conduct with relevant stakeholders. The CISPE Code has been prepared through a collaborative process between the CISPE members, all of whom are cloud infrastructure service providers (hereinafter "CISPs") providing cloud infrastructure services to European customers. CISPE is intended to represent CISPs and includes representatives from market leading CISPs offering services throughout Europe, across many EU member states. All relevant stakeholders have been consulted and asked to approve the CISPE code of conduct. In this way, the Code provides a summary of stakeholder's consultations.

12. The code owner has demonstrated in the draft Code that it is an effective representative body, capable of understanding the needs of their members.

2.1.3 Processing Scope

13. The CISPE Code applies to the specific features of processing by IaaS providers. It seeks to bring clarity as to what GDPR means in practice when applied to IaaS providers, and what are the actual measures which CISPs will take to ensure compliance with GDPR. The Code requirements set out the GDPR principles which CISPs, as data processors, must respect. It therefore does not apply to "business to consumer" (B2C) services or for any processing activities for which the CISP may act as a data controller. However, the code is also relevant for consumers who will get additional guarantees of compliance when entrusting with their personal data a company which uses a processor which adheres to the Code.[6]

[4] See Appendix 2 to the Guidelines.
[5] See para. 22 Guidelines.
[6] It shall be noted, that the adherence of a processor to the Code of Conduct does not entail an automatic recognition of compliance of the processing carried out by such processor nor waives the responsibility of the

2.1.4 Territorial scope

14. The scope of the CISPE Code is transnational and is intended to apply across the EEA, as per article 40 (7) GDPR. The CISPE Code has identified all European Union and European Economic Area supervisory authorities as concerned SAs.

2.2 The code of conduct facilitates the effective application of the GDPR

15. The Guidelines precise that Codes will need to specify the practical application of the GDPR and accurately reflect the nature of the processing activity or sector. They should be able to provide clear industry specific improvements in terms of compliance with data protection law. A code shall not just re-state the GDPR. Instead, it should aim to codify how compliance to GDPR can be achieved in a specific, practical and precise manner.[7] Furthermore, the code has to provide sufficient appropriate safeguards to mitigate the risk around data processing and the right and freedoms of individuals.[8]

16. The CISPE Code contains both strict requirements particularizing the provisions of the GDPR mentioned in the "Processing Scope" section of the present Opinion and good practices currently followed by the sector. The CISPE Code helps CISPs to understand clearly what their obligations are under the GDPR, facilitates best practice compliance by IaaS providers and improves upon the state of the art for data protection in the Cloud sector

2.2.1 The code as a practical tool

17. The Code seeks to bring clarity as to what GDPR means in practice when applied to IaaS providers, and what are the actual measures which CISPs will take to ensure compliance with GDPR. The CISPE Code describes the rights and obligations of adhering CISPs on the basis of key principles of GDPR such as purpose limitations, data subject rights, transfers, security, auditing, liability, etc.

2.2.2 Matrix of requirements

18. The Code consists of a set of requirements that CISPs have to implement to comply with the Code.

19. The Codes develops requirements which are unambiguous, concrete, attainable and enforceable. All the requirements are consolidated in a control framework, which ensures transparency for all Code's members and data subjects and facilitates its application and interpretation, enabling implementation, monitoring and where required auditing. The EDPB welcomes the use of this kind of tool.

2.2.3 Binding nature of the Code

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

2.2.4 The Code provides sufficient safeguards

21. In line with the Guidelines,[9] a code of conduct must provide sufficient safeguards while being adequately focused on particular data protection areas and issues in the specific sector to which it applies ("added value"). The CISPE Code provides sufficient safeguards by, for instance adopting the

---

controller to ensure compliance for all the processing operations carried out on its behalf. In this particular case, the EDPB recalls that the Code of Conduct won't apply to all the processing operations carried out on behalf of the controller, but only to the elements of Article 28 GDPR and related relevant articles. In addition, it shall be recalled that, in this case, the monitoring of the CISPE Code of Conduct is based on a service-level approach. Thus, members of the Code might not adhere to the Code with regard to all the elements of all their processing activities, but they can declare which of their services are to be considered compliant with the Code.

[7] Para 36-37 of the Guidelines.

[8] Para 39 of the Guidelines.

[9] See para 36 of the Guidelines.

same terminology as the one used in the GDPR and providing complaint mechanism to data subjects. In terms of added value, the code provides guidance adapted to the sector on, among others, security measures, auditing requirements, data subject rights and transparency requirement.

2.2.5 The Code as an accountability tool

22. The objective of the CISPE Code is to help CISPs to demonstrate compliance with article 28 GDPR and make it easier and more transparent for customers to analyze whether cloud services are appropriate for their use case in line with article 28.1 GDPR which 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 and article 28.5 GDPR which 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.

2.3 The code of conduct provides effective mechanisms for monitoring compliance with a code

23. As per Article 40(4) of the GDPR and the Guidelines,[10] a code 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 specifically needs to identify and propose structures and procedures which provide for effective monitoring and enforcement of infringements.

2.3.1 Adherence to the Code

24. The code has to detail an adhesion mechanism.

25. An effective adhesion mechanism has to develop a process divided on three phases which coincide with the code of conduct "lifetime". During the first phase, the mechanism must precise that the code members must comply with all the Code requirements and that the monitoring body will assess the eligibility of candidate to the code. In a second phase, the mechanism shall describe how that monitoring is carried out on an ongoing basis and in a third phase on ad hoc basis.[11] The CISPE Code develops an adhesion mechanism which fulfills the three phases of monitoring.

2.3.2 The monitoring of the Code

26. The Guidelines indicate that a code will also need 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.[12] As per Article 41 (1) GDPR, the monitoring body identified by the Code has to be accredited by the CompSA[13] Consequently, the CompSA will act as a single point of contact with the code owner and the monitoring body.

27. The CISPE Code has appointed several external monitoring bodies in accordance with article 41 of the GDPR. These monitoring bodies will be in charge of ensuring compliance of the members of the Code with the provisions of the CISPE Code and taking actions including sanctions in case of infringement to

[10] See para 40 of the Guidelines.
[11] Para 70 of the Guidelines.
[12] Para 40 of the Guidelines.
[13] In accordance with the consistency mechanism referred to in Article 63 of the GDPR, the EDPB adopted an Opinion 3/2020 on the France data protection supervisory authority draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR on 28 January 2020. The monitoring bodies designated by the code owner of the CISPE code of conduct will have to be accredited by the French SA and therefore will have to demonstrate that they fulfil the requirements imposed by article 41 of the GDPR.

the provisions of the CISPE Code. Decisions taken by these monitoring bodies relating to their monitoring functions (for instance regarding the interpretation of the Code's rules) shall not be submitted to another entity for approval. Indeed, these monitoring bodies have to be independent in their mission.

28. The EDPB acknowledges that the CISPE Code contains a mechanism which enables the monitoring bodies to carry out their monitoring functions, as per article 40 (4) of the GDPR.

29. Finally, the EDPB recalls that the code of conduct will not be operational before the designated monitoring body is accredited.[14]

2.3.3 Sanctions

30. In accordance with article 40 (4) of the GDPR and the Guidelines, without prejudice to the tasks and powers of the competent supervisory authority, the monitoring body designated by the code owner shall, subject to appropriate safeguards, take appropriate action in cases of infringement of the code by a controller or processor. Those sanctions range from non-public but formal reprimand to temporary or permanent revocation from the Code. The monitoring body commits to inform the competent supervisory authority about any related actions taken.

31. To ensure transparency to code members, the code shall include a list of corrective measures which must be applied by the monitoring body. For this purpose, the CISPE Code develops an enforcement framework which determines the appropriate sanction to be followed by the monitoring bodies.

2.3.4 The review of the code

32. As per article 40 (2) of the GDPR and the Guidelines, the code sets out an appropriate review mechanism to ensure that the code remains relevant to legal and technical standard. In particular, section 7.3 of the CISPE Code provides that a regular review of the Code to reflect legal, technological or operational changes and best practices shall take place when appropriate.

3 CONCLUSIONS / RECOMMENDATIONS

33. By way of conclusion, the EDPB considers that the draft code complies with the GDPR, since the CISPE code of conduct fulfills the requirements imposed by Article 40 and 41 GDPR.

34. Finally, the EDPB also recalls the provisions contained within Article 40 (5) GDPR, in case of amendment or extension of the CISPE code of conduct, the CompSA will have to submit the modified version to the EDPB in accordance with the procedures outlines in the guidelines approved by the EDPB.

4 FINAL REMARKS

35. This opinion is addressed to the FR SA and will be made public pursuant to Article 64(5)(b) GDPR.

36. According to Article 64(7) and (8) GDPR, the FR SA shall communicate its response to this opinion to the Chair within two weeks after receiving the opinion.

37. Pursuant to Article 70(1)(y) GDPR, the FR SA shall communicate the final decision to the EDPB for inclusion in the register of decisions which have been subject to the consistency mechanism.

[14] Where several monitoring bodies are designated by the code, the accreditation of one of them is sufficient to provide to the code of conduct a binding nature.

38. As per Article 40 (8) GDPR, the Board shall submit this opinion to the European Commission.

For the European Data Protection Board

The Chair

(Andrea Jelinek)