ARTICLE 29 DATA PROTECTION WORKING PARTY

2588/15/EN
WP 232

Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing

Adopted on 22 September 2015

Summary

In this Opinion the Article 29 Working Party (WP29) analyses the Data Protection Code of Conduct for Cloud Service Providers (the Code), drafted by the Cloud Select Industry Group (C-SIG), a working group composed of representatives of the industry, that was submitted to the WP29 on 19 January 2015.

WP29 appreciates the effort put in by industry to draft this Code of Conduct. The code provides important guidance to cloud computing providers with regard to applicable data protection and privacy rules in Europe. Adherence to the code of conduct will contribute to greater transparency and legal certainty, for all parties involved.

However, the Working Party cannot formally approve the draft Code, since it does not always meet the minimal legal requirements, and the added value of this draft Code with respect to Directive 95/46/EC and national legislation is not always clear. Therefore, some substantial concerns remain. This Opinion analyses those aspects by highlighting points of concern, with a view to contributing to an adoption of the Code which would provide such added value.

In particular, the opinion addresses:

- the consequences of adhering to the Code: adherence will help companies demonstrate that they are accountable, but this does not prevent DPAs from exercising their enforcement powers;
- governance of the Code: the Code should elaborate on the transition towards the data protection regulation, the difference between self-assessment and third party certification and the powers of the governance body, in particular concerning deterrence mechanisms. In addition, the WP29 cannot be a member of the Steering Board;
- liability: the Code must prevent the adoption of terms of service that unduly limit obligations and responsibilities. The Code must specify (in an Annex) when the CSP is a co-controller, a controller or a processor, and allocate liabilities;
- transparency on the location(s) of the data processing;
- processing of special categories and sensitive data (such as financial or health data);
- applicability of the European definition of personal data;
- requirements for international transfers and law enforcement access requests;
- security measures and the level of detail on those measures;
- the right to conduct IT audits;
- the reference to data portability as a key right of users.

WP29 is encouraged by the progress made by C-SIG in developing the Code and supports the group in their efforts to finalise the Code by taking into account comments made in this opinion. C-SIG should therefore consider each of WP29's comments and recommendations for incorporation into a final version of the Code.

Table of contents

0. Introduction

The draft Data Protection Code of Conduct for Cloud Service Providers (CoC) drafted by the Cloud Select Industry Group (C-SIG) was formally submitted to the Article 29 Working Party (WP29) on 27 February 2014. The WP29 had summed up a first series of comments in a letter sent to the C-SIG in June 2014.

A new version of the Code taking into account a number of formal and substantial comments made in the letter was submitted to the WP29 on 21 January 2015.

Article 30(1) of Directive 95/46/EC provides that "the Working Party shall: (…) give an opinion on codes of conduct drawn up at Community level". In its Working Document on the procedure for the consideration of Community codes of conduct adopted on 10 September 1998 (WP13), the Working Party clarified that, when requested to issue such an opinion, it shall determine whether or not a submitted code of conduct:

- is in accordance with the data protection directives and, where relevant, the national provisions adopted pursuant to these directives;
- is of sufficient quality and internal consistency and provides sufficient added value to the directives and other applicable data protection legislation, specifically whether the draft code is sufficiently focused on the specific data protection questions and problems in the organisation or sector to which it is intended to apply and offers sufficiently clear solutions for these questions and problems.

In the current case, while the Code of conduct is certainly useful for cloud computing providers (CSPs), some concerns remain. This Opinion addresses those aspects, with a view to contributing to the adoption of the Code that could provide significant added value with respect to the data protection directive and national legislation.

1. Role of the Code of conduct in the perspective of the draft data protection regulation

While the Code should contribute to the proper implementation of the national provisions adopted pursuant to the current data protection directive (Article 27) and the WP29 assessment of the code will be based on the current legal framework, this assessment should also be considered in the light of the possible provisions of the draft general data protection regulation (GDPR) on codes of conduct.

In light of the above, the Code would benefit from further specifications on mechanisms which can ensure a smooth transition towards the new regulatory environment.

In particular, the future GDPR includes several provisions *[on controllership, status of processors, codes of conduct (Art. 38), certifications (Art. 39), powers and functions of DPAs (in particular the One-Stop-Shop mechanism)]* that will have a significant impact on both controllers and processors. The Code establishes a Steering Board which is required to propose changes to the Code and work on new developments (7.1) but the mechanisms currently envisaged to that effect are worded very broadly.

The Code should clearly state that adherence does not make a CSP immune to change in the EU law. In particular, any CSP who would adhere to the Code before a modification in

the EU legislation is implemented in the Code would have to assure that he complies to the new legislation, even if it implies new or conflicting obligations regarding the Code.

2. Code of conduct and enforcement actions by DPAs

CSPs adhering to the Code certainly intend to use this means to mitigate the risk of formal enforcement procedures (specifically the imposition of sanctions) by the EU DPAs. Such a concern is legitimate in the light of the future powers likely to be granted to DPAs under the future regulation.

Adherence to the Code ensures no automatic protection against possible interventions or actions by the competent (DPAs (or other authorities) in the course of their supervision and enforcement activities.

While making this point clear, WP29 encourages CSPs to adhere to such codes of conduct. Complying with the requirements of such codes will help these CSPs demonstrate that they are accountable with regard to data protection rules, which will definitely have a positive impact in the context of those supervision and enforcement activities.

3. Governance of the Code

A prominent section of the code is devoted to the implementation of a governance structure set up with the scope of assessing the condition of adherence and the supervision on the adoption of the code by industry players. These aspects may indirectly impact the level of data protection guarantees to data subjects.

First of all, **the role of the WP29 needs to be clarified (7.1) since it may not participate in the governance structure of the code**. WP29 was set up under Directive 95/46/EC, as an advisory body of the European Commission, with the scope (among others) to examine any question covering the application of the Directive in order to contribute to its uniform application. One of the main prerogatives of the WP29 is that it acts independently. From this standpoint, any involvement of the WP29 in the governance structure, as proposed by the Code, seems to fall outside the scope or the mandate of the WP29, and may generate, in such a way, a conflict of interests among its components (the national DPAs) with the supervisory role that they have at national level vis-à-vis the players of the cloud industry.

The WP29 acknowledges the delicate phase of transition between legal frameworks within which the Code applies. For this reason, **it appears necessary to set up a transition management strategy, supervised by a real governance structure in place, allowing the code to be valid and effectively adopted throughout the transition and once the new Regulation is adopted.** In this perspective, some discrepancies between the implementation time of the code and the entry into force of the governance structure should be addressed in the current formulation and solved (e.g. 7.1 p. 35).

The conditions for adherence to the Code are based either on self-assessments or on third party certifications. However, these two conditions provide different levels of assurance. In that respect, several points should be clarified in the Code:

- **the Code does not provide a clear commitment for a more stringent approach by the Competent Bodies[1], in case of self-assessment.** The possibility of (re-)assessment by Competent Bodies in case of adherence based on self-assessment should be correctly framed. In this sense, it would be appropriate to define a more active role of the governance structure.

- In case of a certification-driven assessment, **it should be made clearer that certifications eligible for certification-based adherence must be cloud-specific** and cover not only the security but also all the personal data protection principles as defined in the EU legal framework.

- WP29 welcomes that the Code specifies different possible compliance marks for different adherence schemes (7.4). Nevertheless, the language should be amended to **make it unambiguous that compliance marks for self-assessed CSP and marks for certified CSP will be different.**

Finally, **the Code should clarify the powers of the governance body, specifically concerning the selection of deterrence mechanisms**, or the conditions and the procedure to be followed in order to assess, on a regular basis, the validity of the adherence requisites, and to decide upon the revocation of such previously granted status of adherence (7.2, 7.3, 7.4, 7.5).

4. Concrete case scenarios relating to the processing of sensitive categories of data or carried out for specific categories of controllers

The Code currently makes no reference to specific scenarios in the cloud.

Even if it can certainly not be an all-encompassing exercise referring to all possible case scenarios, **the Code should refer to some very relevant cases where CSPs offer cloud services dedicated to the processing of sensitive data,** whether in the legal sense (e.g. cloud services for health data, for instance) or in the common language (for instance cloud services related to financial services). As such services are developing rapidly in number, scope and pervasiveness, so do the data protection risks generated by the processing of sensitive data in the cloud. They thus generate significant concerns for both professional and individual users.

Nevertheless, the Code makes no reference to such situations, if only to provide that, without prejudice to national laws, such processing commonly requires "additional safeguards".

5. Information about the location of processing

The issue of location of data was raised in June 2014 in the letter of the WP29 to the C-SIG concerning the previous version of the Code. The letter explicitly mentioned that "*Foremost, the obligation of information CSPs are in charge of should be specified and strengthened. In particular, specific and easy-to-access information will be required concerning data location that is to say more specific information than just countries where the data will be 'processed', subprocessed and/or transferred to or by whom the data will be processed*."

[1] that review and approve Declarations of Adherence by cloud providers

The current version of the Code does not mention, nor ensure, that the controller can have information about the precise locations where the processing takes place[2].

However, in some Member States, the national implementation of Directive 95/46/EC includes provisions which oblige the controller to actively supervise, monitor, and if necessary inspect the processing and security measures in place, in case the processing is handed over to processors. The controller can only fulfill these obligations if it has precise information on the addresses of all locations where the processing takes place by the CSP and subprocessors, if any. Furthermore, it should be provided in advance with any change in those addresses.

In order to contribute to the proper implementation of the national provisions of some Member States, the Code needs to become specific on information about the addresses of the locations where processing takes place. For security reasons, only a general location may be provided before entering into the contract. This general description should, at least, allow the controller to identify the applicable laws and, whenever data are sent outside of the EU, to inform the data subject. As soon as a contract is signed between the controller and the CSP acting as a processor, specific addresses should be easily accessible, at any time, to the controller and the DPA.

6. The notion of personal data

While the Code refers to the notions of data controllers and processors, to date, it does not make any reference to the notion of personal data. This choice seems to stem from the fact that, as the code provides, "*a CSP acting as a data processor typically does not identify the personal data on their service, in particular when the CSP is not entitled under the service agreement to identify such personal data, or when the customer has deployed tools such as data encryption which prevent the CSP from identifying the personal data on their service*".

To start with, while such a sentence might be relevant for PaaS/IaaS, the possibility of identification is frequent in SaaS. Thus, the sentence should be amended so as not to rule out the possibility of identification by CSPs in practice.

Also, **WP29 would like to confirm the EU definition of personal data to be applied to the Code. Such a reference could be articulated with a reference to the notion of anonymisation which is currently absent from the Code.** The high standards required by WP29 in its opinion on anonymisation could be mentioned, as well as the fact that **in case any reference to pseudonymisation is made, it can only be considered as a security measure and not as a means to enable CSPs or customers to be exempted from their responsibilities under data protection law.**

7. International transfers and law enforcement access requests

The current draft of the Code is only superficial on the matter of law enforcement or government access requests. Yet, as stated in the WP29 opinion 05/2012 on cloud computing, this issue is a major one in relation to data protection and cloud computing.

[2] According to article 27(1) of Directive 95/46/EC, codes of conduct are intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to the directive.

WP29 specifically insists on its specific requirements on the issue of transfers or disclosures of data to non EU authorities, based on its interpretation of the proposed Article 43A in the GDPR. The inclusion of such requirements in the draft code would also match its expectations that a code of conduct exceeds the mere compliance to the law[3].

Also, as described in previous opinions[4], the Code should specify that**,**

- a processor shall communicate any legally binding request for disclosure of the personal data by a law enforcement authority to the controller unless otherwise prohibited,

-and **in any case, transfers of personal data by a processor to any public authority cannot be massive, disproportionate and indiscriminate in a manner that it would go beyond what is necessary in a democratic society.**

Finally, CSPs must be reminded that for international transfers of data also, they should act strictly within the remit of the instructions received from the customer. The CSP may cease to be considered as a processor, with all its consequences especially in terms of liability, in cases where the actions taken by the CSP exceeds by far the normal capacities of a data processor in view of its supposed absence of autonomy with respect to the instructions of the controller. This may be the case, for example, where CSPs autonomously organise international transfers of data to respond to a law enforcement authority or state security's requests without seeking any involvement of the respective controllers[5].

8. Liability

The Code does not elaborate sufficiently on the liability regime applicable to the parties in case of breach of their data protection obligations.

WP29 Opinion 05/2012 on Cloud Computing underlined that it is important to clarify the role of each and every party in order to establish their specific obligations with regard to data protection legislation and to allocate responsibility for possible breach of these rules. Doing so would help preventing possible gaps whereby some obligations or rights stemming from the data protection legislation are not ensured by any of the parties[6]. Also, the proposed Article 26(4) of the future GDPR[7] should lead cloud services providers to provide more clarity on their obligations and liability in such cases. In this respect, **the Code must prevent the adoption of terms of services that are to the disadvantage of the clients by unduly limiting cloud providers' obligations and liability and restricting clients' rights.**[8]

The allocation of responsibilities between commercial parties is a matter of concern to individuals whenever it may have a negative impact on them. The Code must therefore

[3] see WP 13
[4] See WP 204 rev.01 - Explanatory Document on the Processor Binding Corporate Rules
[5] See p11 of Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)
[6] It is all the more important given that there may be different levels of controllership and situations in which a provider of cloud services may be considered either as a joint controller or as a controller in their own right depending on concrete circumstances.
[7] which provides that the processor who processes personal data other than as instructed by the controller shall be considered to be a controller
[8] See EDPS Opinion on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", 16 November 2012, p.5.

specify that whatever this allocation of responsibilities, it should not deprive individuals from their rights or from the possibility to obtain compensation for a possible damage incurred by them. In particular, in case of co-controllership, the different roles and responsibilities relating to data processing should be clearly allocated between CSP and customer, so as to facilitate the exercise of their rights by data subjects. Also, the liability regime applicable to customers and CSPs, respectively, as well as possible sub-processors, in addition to the Services Agreement, would need to be set out more clearly (as mentioned in Section 5.1, for instance). This namely relates to the handling of data subjects' complaints/requests (5.8). **Therefore, Annex C should specify what areas of the processing are managed by the CSP as a co-controller, controller or processor, and should provide information on the allocation of liability between the CSP and its customer.**

In addition, Article 77 of the future GDPR envisages a presumptive joint controllership and several liability regimes, whereby a controller or processor may be exempted from this liability if he demonstrates that he is not responsible for the damage. Such a presumption of liability can therefore be rebutted by any actor involved in the processing operation, without prejudice to recourse actions of the controller vis-à-vis the processor in case the latter cannot prove not to be liable for the specific damage. This draft framework is actually in line with the stance taken by the WP29 in particular in its opinion on cloud computing and sub-processing (WP196, p. 9-10). In that opinion, emphasis was placed on the need for a clear allocation of responsibilities among the different actors and for introducing specific safeguards also with regard to data subjects. Such safeguards could namely be third-party beneficiary rights modeled after those of standard contractual clauses applied to controller-to-processor relationships.

WP29 recommends expanding this section of the Code, with a specific care of the handling of data subjects' complaints/requests (5.8) and the need for CSP to cooperate with customers to that effect.

The provisions of the Code that hold specific benefits to individuals could also be specifically mentioned as directly enforceable by them, and it should be specified that the liability regime applicable to the parties should be one of the EU Member States exclusively.

9. Security

Protecting personal data includes ensuring IT security. WP29 recommends taking this into account in the structure and content of the Code, where security aspects are not to be considered on top of personal data protection but are essential parts of it.

A data processor must act "only on instructions from the controller" (art.17(3)) and should therefore configure its role as a mere leverage in the hands of the controller, with no involvement in the semantics of the processing and no margin of maneuver for any sort of further processing[9]. This principle should be mirrored in the technical interfaces through which the controllers and the cloud provider acting only as a processor interact. Roles and responsibilities should therefore be clearly defined in the Code.

[9] According to the WP29's Opinion 1/2010 on the concepts of "controller" and "processor", however, "delegation may still imply a certain degree of discretion about how to best serve the controller's interests, allowing the processor to choose the most suitable technical and organizational means "

In addition, security measures and audit capabilities should be arranged in such a way to take into account the specificities and the risks inherent to the various emerging paradigms for cloud services, namely Infrastructure as a service (IaaS), Platform as a service (PaaS) and Software as a service (SaaS), where an increasing level of privacy risk is envisaged due to their inherent specificities.

The Code states that "*a key objective of the security section is for the CSP to enable the customer to perform a security risk assessment and data protection impact assessment*". This is indeed necessary for the controller (the customer) to set up security measures which, according to Art. 17 of the Directive, are "*appropriate to the risks represented by the processing and the nature of the data to be protected*".

To this purpose, it is indeed fundamental that the CSP provides the customer with "*a sufficient level of detail on the security measures implemented by the CSP*". This, though, should also be complemented by a **sufficient level of information on the threats on and vulnerabilities of the CSP service and infrastructure and on the risk management decisions taken by the CSP.** If it is not the case, the background for the customer to perform its own data protection risk management would not be adequate. Nevertheless, when providing such information, account should be taken of the confidentiality needs of the CSP for security and business reasons.

The Code imposes also on the CSP a duty to perform a risk assessment "*to ensure that the right of personal data protection is guaranteed to the data subject"*. **The CSP should consider establishing different levels of protection depending on the "*processing and the nature of the data to be protected*" and to advertise them publicly when offering their services.** This would mitigate the lack of sufficient information on threats, vulnerabilities and overall risk management from the CSP to the prospective customer.

WP29 acknowledges and welcomes the existence of a set of minimum security objectives. Nevertheless, they are generically formulated and thus, in case of a security self-assessment, they may not provide sufficient guarantees of a solid security management. These objectives and their formulation could be further matched against those listed in existing security standards and best practices. For example, even though a risk management approach is present in the Code, no clear security objective exists that refers to it. WP29 further recommends framing those security objectives in the context of a broader set of data protection objectives.

"Demonstration keys" are considered as possible alternatives although they are not equivalent and give different level of assurance. For example, in section 6.1 it is written that the "*CSP shall specify the technical, physical and organizational measures in place to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized use, modification, disclosure or access and against all other unlawful forms of processing*". Providing "*a copy of the certificate or attestation providing evidences of the successful completion of an independent third party audit*" does not necessarily include that information.

Finally, the WP29 would like to stress that ISO/IEC 27018 is a catalogue of best practices for cloud providers acting as processors. It describes a list of controls to improve privacy. This standard is only a good collection of non-compulsory, non-exhaustive and non-maximalist controls that may be implemented. Thus ISO/IEC 27018 is not built to be used as a standalone document for certification. It can be used in conjunction with ISO/IEC 27001 which allows a certification. ISO/IEC 27001 does not take into account the specificities of the protection of

privacy such as impacts on the individuals, but it ensures a high level of protection of information in the organization's interest. The addition of good practices based on ISO/IEC 27018 may therefore help to ensure that privacy is better taken into account but it does not prove that privacy risks are taken into account. ISO/IEC 27018 should ideally be used only after assessing the risks on the privacy of the persons concerned, in order to treat them in a proportionate way. For now, no published standard describes the way to conduct this process. Ongoing work at the ISO may help to fill this gap in the next few years.

10. Right to audit

As a rule of principle, this right to audit should be generally guaranteed and not strictly limited to the case where the CSP has not been certified by an independent body. Indeed, Directive 95/46/EC provides that:

- the controller must ensure that all the data quality requirements in art. 6(1) are complied with (article 6(2)),

- the processor shall act only on instructions from the controller (articles 16 and 17(3)).

The duty of supervision which lies on the controller is the premise of the right that is granted to them to correctly exercise their control on the activities put in place by the processor. This right should be exercised by any controller, irrespective of its economic power, skill or technical capabilities.

This means that as a prerequisite for an effective supervision of cloud provider data processing, a number of Key Performance Indicators (KPI) on their activity should be abided by the industry. A controller can be effectively accountable if he can demonstrate in a measurable way that he has complied with the EU data protection obligations. If the link is missing between the accountability obligation on data controllers and the measurability of the processing put in place by cloud providers based on the instructions received by the controller (and this is particularly relevant when a great unbalance exists between the two) the accountability obligation cannot be properly fulfilled.

The right to audit can then be laid down in order to cover various phases of the processing, and to address the specificities of the risks attached to the processing or the nature of the processed data, and it can range from the right to audit the location of the servers where data are processed and stored, to the right to audit the logic (the algorithms) which are used throughout the various steps envisaged for the whole processing, to the right to audit the security measures put in place by the processor.

WP29 favorably hails the implementation of standards for cloud computing, especially related to data interoperability, portability and security, and encourages the industry to adopt internationally agreed solutions for these areas as a requisite of adherence to the Code. Also, every possible effort should be put in place in order to implement interfaces between the processors systems and the controller application, so to facilitate a smooth exercise of the audit capabilities realized by the cloud providers.

These possibilities should be clearly reflected in the Code, which should include use cases where roles and responsibilities are defined together with the audit capabilities that the cloud providers will make available.

11. User's rights

Currently, most cloud providers do not make use of standard data formats and service interfaces facilitating interoperability and portability between different cloud providers. If a cloud client decides to migrate from one cloud provider to another, a lack of interoperability may result in the impossibility or at least difficulties to transfer the client's (personal) data to the new cloud provider[10]. The same holds true for services that the client developed on a platform offered by the original cloud provider (PaaS).

While section 5.8 of the Code provides for cooperation in good faith of the CSP to protect the data subject's rights, those rights are listed only as: the right to access their personal data, to have it corrected and to have it deleted in a timely and efficient manner. The only reference to data portability is currently in the transparency form of the Annex A. As the Code aims at helping "to anticipate the data protection reform", **a reference to portability would contribute to the Code's sustainability.**

Finally, concerning the relationship with the data subject, WP29 draws the C-SIG's attention to article 10 of Directive[11] 95/46/EC.

Consequently, **the Code would benefit from the addition of a clause that would clearly remind CSP that they should, depending on the context, either provide adequate information to the data subject or cooperate in good faith with their customer to enable him to properly inform data subjects.**

12. Conclusion

WP29 is encouraged by the progress made by C-SIG in developing the Code and supports the group in their efforts to finalise the Code by taking into account comments made in this opinion and previous correspondence.

WP29 recognises the value that such a Code can provide to the cloud computing industry and it does assist data controllers in assessing a CSP and a particular cloud computing product or service. However, in its current form there are still a number of significant gaps which should be addressed before the Code is finalised.

WP29 therefore recommends that C-SIG consider each of WP29's comments and recommendations for incorporation into a final version of the Code.

---

[10] This is also known as vendor lock-in

[11] "*Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:*
(a) the identity of the controller and of his representative, if any;
(b) the purposes of the processing for which the data are intended;
(c) any further information such as
- the recipients or categories of recipients of the data,
- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
- the existence of the right of access to and the right to rectify the data concerning him
in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject."