THE FIRST GDPR EU-WIDE CODE OF CONDUCT APPROVED BY DATA PROTECTION AUTHORITIES

SERGIO GUIDA,
Independent Researcher, Sr. Data Governance & Privacy Mgr.

Keywords: *GDPR Code of Conduct, Cloud Service Providers, European data sovereignty.*
Category: *Legal area*

Every day we can see how, without user's trust, technology cannot express its full potential, with at the core of building trust a robust data protection standing.

Actually cloud computing provides significant benefits to both public and private sector in terms of cost, flexibility, efficiency, security and scalability, so it is crucial that customers develop a level of confidence in a Cloud Service Provider[1] (CSP), before they entrust them with their data and applications[2]. GDPR requires that the customers only use CSPs as processors that provide 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.

So the 'EU Data Protection Code of Conduct for Cloud Service Providers'[3] plays an important role, by setting out clear requirements and procedures to raise the level of data protection in cloud services, based on GDPR.

The EU Cloud Code of Conduct General Assembly has been working on the EU Cloud Code of Conduct for years, developing a Code version aligned to GDPR prior to submitting to the supervisory authorities.

---

[1] Cf. "A Cloud Service is any system that provides on-demand availability of computer system resources, e.g. data storage and computing power, without direct active management by the user". (..) Today, rather than owning their own computing infrastructure or data centers, companies can rent access to anything from applications to storage. What that means is that if you have a supplier that handles and processes your companies healthcare data for instance, they may in fact be storing and processing your information in the cloud, either by outsourcing services or in some cases using an internal cloud or "private cloud" that they developed themselves by implementing it within the organization's dedicated resources, and infrastructure using 'on-premises' services." (..) The basic concept behind the cloud is that the location of the service, and associated processes and assets such as the hardware and operating system(s) and/or applications on which it is running, are largely immaterial to the user. They may have a separate business unit that is a private cloud that is dedicated to serving the entire internal organization, they may use a 3rd party service like AWS or Azure and in some cases may use both. In any event they are servicing you from the cloud and you should expect that they have cloud specific controls like the CSA Cloud Control Matrix (CCM) to address the applicable scope of service and to mitigate the associated risks", as we can read in JOHN DI MARIA, Cloud Security Alliance, What is a Cloud Service Provider?, Blog Article Published 04/30/2020 in https://cloud security alliance.org/ blog/2020/04/30/what-is-a-cloud-service-provider/#~:text=Acloudserviceprovider2Cortootherbusinessesor individuals.

[2] Indeed, "the conspicuous lack of cloud-specific security certifications, in addition to the existing market fragmentation (scope, methodologies), hinder transparency and accountability in the provision of European cloud services. Both issues ultimately reflect on the level of customer's trustworthiness and adoption of cloud services in Europe. In an effort to solve some of the challenges depicted above, the EU Cybersecurity Act (EU CSA, approved in June 2019) in its Title III gives ENISA the mandate of defining and implementing a European security certification scheme for ICT products, processes and services for three different levels of assurance (low, substantial, and high). Being cloud computing one of the identified EU CSA priorities, Articles 54 (j) and 57 (9) propose the possibility of deploying a high-assurance, evidence-based and continuous certification of European cloud providers. Despite the evident benefits of EU CSA's principles for the European market and cloud customers, currently there are no concrete cloud certification frameworks nor tools for implementing any of those proposals", as we can read in LEIRE ORUE-ECHEVARRIA, JESUS LUNA GARCIA, CHRISTIAN BANSE, JUNCAL ALONSO, MEDINA: Improving Cloud Services trustworthiness through continuous audit based certification, TECNALIA in https://www.swforum.eu/sites/default/files/ 1stSwForumWs paper_3.pdf, page 2.

[3] Also known by its abbreviated name EU Cloud Code of Conduct, as we can read at the website https://eucoc.cloud/en/home/#:~:text=InthiscontexttheEU,cloudservicesbasedonGDPR.

This is a crucial added value of the Code, which, as a voluntary instrument but based on input by supervisory authorities and the Guidelines on Codes of Conduct and Monitoring Bodies by EDPB, has been designed to ensure a robust level of data protection and transparency, providing for an independent monitoring function, as well.

And it is precisely on the basis of Article 40 of the GDPR that on 20 May 2021 the Belgian DPA approved the "EU Data Protection Code of Conduct for Cloud Service Providers" [4]submitted by Scope Europe[5] provided that it meets the requirements set out under that Article[6], "having regard to the 'Guidelines 01/2019 on codes of conduct and monitoring bodies' adopted by the European Data Protection Board on 4 June 2019[7]"and "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"[8].

This is the first time that a single initiative allows a cloud provider to establish precisely

- ✓ which requirements they should meet under the GDPR,
- ✓ which assurances they get from existing certifications and
- ✓ obtain the certainty that the gap between the GDPR and the certification is comprehensively filled.

In particular, this Code is an element pursuant to Article 28.5 GDPR whereby a CSP demonstrates sufficient guarantees by implementing appropriate technical and organizational measures in such a manner that processing will meet the requirements of the GDPR (including when engaging sub-processors)[9]. The EU Cloud Code of Conduct also addresses Article 28.2 and Article 28.3 GDPR[10] including the references, as far as applicable for the cloud processing industry.

---

[4] Cf. The General Secretariat of the BELGIAN DATA PROTECTION AUTHORITY, Decision n° 05/2021 of 20 May 2021, Approval decision of the "Eu Data Protection Code of Conduct for Cloud Service Providers" (AH-2018-0084) in https://www.dataprotectionauthority.be/publications/decision-n05-2021-of-20-may-2021.pdf.

[5] The EU Cloud Code owner is "Scope Europe", an association supporting the co-regulation of the information economy. It acts as a think tank to discuss and debate key issues in digital policy and provides an umbrella organization for a range of co-regulatory measures in the digital industry. SCOPE Europe was founded in February 2017 as a subsidiary of the German non-profit-organization SRIW e.V. (Selbstregulierung Informationswirtschaft - Self-Regulation Information Economy) at https://scope-europe.eu/en/projects/eu-cloud-code-of-conduct/.

[6] GDPR, Article 40(1): "The Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises."

[7] Cf. EUROPEAN DATA PROTECTION BOARD, Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 - version adopted after public consultation, 4 June 2019, available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-0_en.

[8] Cf. EUROPEAN DATA PROTECTION BOARD, Opinion 16/2021 on the draft decision of the Belgian Supervisory Authority regarding the "EU Data Protection Code of Conduct for Cloud Service Providers" submitted by Scope Europe, 20 May 2021 in https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-162021-draft-decision-belgian-supervisory_en.

[9] Cf. "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" in The General Secretariat of the BELGIAN DATA PROTECTION AUTHORITY, Decision n° 05/2021 of 20 May 2021, Approval decision of the "Eu Data Protection Code of Conduct for Cloud Service Providers" (AH-2018-0084) in https://www.dataprotectionauthority.be/publications/decision-n05-2021-of-20-may-2021.pdf, cit., page 2.

[10] In summary, under Article 28 of the GDPR, controllers must only appoint processors who can provide "sufficient guarantees" to meet the requirements of the GDPR. Processors must only act on the documented instructions of the controller and they can be held directly responsible for non-compliance with the GDPR obligations, or the instructions provided by the controller, and may be subject to administrative fines or other sanctions and liable to pay compensation to data subjects.

The Belgian data protection authority's approving the first transnational code of conduct in the EU, for cloud services

- is being creating a baseline for implementation of the GDPR for cloud providers of all types[11];

- comes at a time when the use of cloud providers, and particularly the issues of using US-based operators (including in Europe), is newly under scrutiny, in conjunction with 'Schrems 2'-related updates too[12].

And if, on the one hand, the code does not provide appropriate safeguards for third-country data transfers[13], on the other hand it remains more internationalist than the cloud strategy recently

[11] There are "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 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, as detailed in The General Secretariat of the BELGIAN DATA PROTECTION AUTHORITY, Decision n° 05/2021 of 20 May 2021, Approval decision of the "Eu Data Protection Code of Conduct for Cloud Service Providers" (AH-2018-0084) in https://www.dataprotectionauthority.be/publications/decision-n05-2021-of-20-may-2021.pdf, cit., pages 4-5.

[12] Cf. "After more than six months, Schrems II is still proving to be difficult to manage for many organizations across the world. In 2021, Schrems II – the landmark data privacy verdict issued in July 2020 – continues to prevent businesses from carrying out basic data transfers to non-EU countries. What's more, in a context of unprecedented home working and the adoption of public cloud platforms, the implications of Schrems II have become more complex as the world has adapted to the conditions enforced by the COVID-19 pandemic. And, with the news that the UK is set to leave GDPR following Brexit, guidance around data protection in Europe has never been more unclear.(..) With the COVID-19 pandemic forcing millions around the world to work from home, the business world has had to adapt in order to survive these new, often complex conditions. In turn, public cloud platforms, such as Microsoft Azure and Amazon Web Services, have become almost indispensable to businesses. This trend is set to continue, with researchers predicting that worldwide end-user spending on public cloud services will grow 18.4% in 2021. In monetary terms, total spending will rise to a total of $304.9 billion, up from $257.5 billion in 2020.
However, in the context of Schrems II, remote working and the adoption of cloud services has added another layer of complexity to the equation. For example, if a European organization was looking to store customer data on servers based in a non-EU country, any data transfer to these servers would have to undergo an individual risk assessment to ensure it is compliant with GDPR. With security and data protection already being a key priority when using public cloud platforms, the additional complexities emanating from Schrems II offers a tough challenge for Chief Technology Officers (CTOs) to handle", as remarked in SEBASTIEN CANO, What is Schrems II and how does it affect your data protection in 2021?- Thales Digital Identity & Security Blog, Posted on 29 April 2021 in https://dis-blog.thalesgroup.com/security/2021/04/29/what-is-schrems-ii-and-how-does-it-affect-your-data-protection-in-2021/.

[13] Cf. "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", as remarked in The General Secretariat of the BELGIAN DATA PROTECTION AUTHORITY, Decision n° 05/2021 of 20 May 2021, Approval decision of the "Eu Data Protection Code of Conduct for Cloud Service Providers" (AH-2018-0084) in https://www.dataprotectionauthority.be/ publications/decision-n05-2021-of-20-may-2021.pdf, cit., page 3.

released by France[14], which seeks to keep data within French borders, as a last step towards European data sovereignty[15].

The Code consists of a set of requirements that CSPs have to implement to comply with: those requirements are supported by a "controls catalogue" helping to assess compliance with the requirements of the Code[16].

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[17].

The 'controls' are to be read in conjunction with the "control guidance" which give advice on how to implement the 'controls'[18]. "The Code 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. The EDPB welcomes the use of this kind of tool"[19].

---

[14] Cf. "the Government has developed a strategy based on 3 pillars: the trusted cloud label which will allow French companies and administrations to benefit from the best services offered by the Cloud (collaborative office suites, videoconferencing tools, etc.) while ensuring the best protection for their data; the "Cloud at the center" policy of the administration to resolutely accelerate the digital transformation of the public service; an ambitious industrial strategy, included in the framework of 'France Relance', which will allow French and European sovereignty to be established, supporting the construction of new Cloud tools", as stated in GOUVERNEMENT DE LA REPUBLIQUE FRANÇAISE, Communique de Presse 17 mai 2021 N° 1002, Le Gouvernement annonce sa stratégie nationale pour le Cloud, in https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=B32CFA9B-74D2-411D-A501-82041939FC67&filename=1002-LeGouvernementannoncesastrategienationalepourleCloud.pdf, page 1.

[15] Cf. "To make the most out of the data we produce, we also need to enable the deployment of EU data spaces in key public and private sectors. Only by integrating data and network technologies at European scale can we attain the next generation of resilient and competitive cloud offering. But we must act rapidly and together", as stated in the JOINT DECLARATION BY 25 EU MEMBER STATES 'Building the next generation cloud for businesses and the public sector in the EU', available at https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=70089, page 3.

[16] Cf. "In order to ensure that the Monitoring Body and supervisory authorities can verify that requirements of this Code are met by the Cloud Services declared adherent, requirements of this Code have been translated into controls. Each control is given a unique identifier (Control-ID) of the pattern Section Subsection Letter, e.g. 5.1.A. For each Control, where appropriate, there is also a guidance ("Control Guidance"). This Control Guidance is a selection of best practices on how the Control can be implemented by CSPs declaring a Cloud Service adherent to this Code. The Control Guidance is not mandatory, however, if CSPs implement alternative measures, they cannot be less protective than those being provided by the Control Guidance. For the avoidance of doubt: Wherever the Code and this Controls Catalogue makes use of the terms "shall" and "must", a CSP is obliged to implement the respective provision in order to be compliant with the Code; even if the respective provision is not translated directly into a Control. Wherever the Controls Catalogue makes use of the terms "should", "may" or "can", examples and recommendations are introduced. It is worth noting that even in cases of nonbinding provisions indicated by such terms, the examples and recommendations establish good practices and if the CSP chooses an alternative implementation, in order to be compliant with the Code, the respective implementation must be as effective and no less protective than the given guidance. In case binding requirements of the Controls Catalogue and any part of the Code may be conflicting in order to reach compliance, the Code prevails", as disclosed in EU CLOUD CODE OF CONDUCT, ANNEX A CONTROLS CATALOGUE, Version: 2.11 Publication Date December 2020, page 2.

[17] Cf. "Controls of Section 5 have been referenced to internationally recognized standards where relevant, including ISO/IEC 27001:2013, ISO/IEC 27018:2019, ISO/IEC 27701:2019, SOC 2, and Cloud Computing Compliance Controls Catalog ("C5"), in order to provide CSPs with best practices of similar areas which might act as reference and starting point when implementing specific data protection related measures. Please note: GDPR mapping is considered a starting point which GDPR provisions relate to the Control; GDPR mapping is not intended to provide an exhaustive and binding reference of which GDPR provision is being thoroughly particularized. Consequently, compliance with the respective Controls does not necessarily relate to an exhaustive compliance with the provided GDPR provisions", ibidem, page 3.

[18] Cf. EUROPEAN DATA PROTECTION BOARD, Opinion 16/2021 on the draft decision of the Belgian Supervisory Authority regarding the "EU Data Protection Code of Conduct for Cloud Service Providers" submitted by Scope Europe, 20 May 2021 in https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-162021-draft-decision-belgian-supervisory_en, cit, page 6.

[19] Ibidem, page 7.

As with all GDPR rules, there is no 'one-size-fits-all', but the code it's also designed to be accessible and relevant for providers of all sizes, through a three-level compliance framework[20].

David Stevens, Chairman of the Belgian Data Protection Authority, the lead data protection authority for the Code of Conduct, said: "The approval of the EU Cloud CoC was achieved through narrow collaboration within the European Data Protection Board and is an important step towards a harmonized interpretation and application of the GDPR in a crucial sector for the digital economy. I hope that this first experience in approving a transnational code of conduct will mark the beginning of the development of more transnational codes of conduct to foster compliance for companies, harmonization for sectoral organizations and transparency for data subjects"[21].

Agnieszka Bruyère, Vice-President, IBM Cloud, IBM EMEA, said:

"The major contribution of this Code of Conduct will be to make GDPR readiness easy to verify. This is great news for users and public entities across Europe, who will find it easier to assess the services on offer and capitalize on the possibilities offered by cloud computing"[22]

---

[20] Cf. "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 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).

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)", as stated in The General Secretariat of the BELGIAN DATA PROTECTION AUTHORITY, Decision n° 05/2021 of 20 May 2021, Approval decision of the "Eu Data Protection Code of Conduct for Cloud Service Providers" (AH-2018-0084) in https://www.dataprotectionauthority.be/ publications/decision-n05-2021-of-20-may-2021.pdf, cit., pages 6-7.

[21] As reported in THE BELGIAN DATA PROTECTION AUTHORITY, Press releases, The BE DPA approves its first European code of conduct, 20 May 2021 in https://www.dataprotectionauthority.be/citizen/the-be-dpa-approves-its-first-european-code-of-conduct.

[22] As we can read in SCOPE EUROPE, The EU Cloud Code of Conduct becomes first GDPR code of conduct to receive green light from data protection authorities , 05/20/2021 in https://sriw.de/index.php?id=525&L=1&tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Baction%5D=detail&tx_news_pi1%5Bnews%5D=647&cHash=1856d62d134bba4050a8b579da0ddb67.

In parallel to the approval of the Code of Conduct, SCOPE Europe has been officially accredited as the monitoring body tasked with overseeing the Code of Conduct[23]. This means it meets the requirements in the GDPR concerning independence, expertise and established procedures for monitoring compliance[24].

Notably "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 (Code, section 7.9)"[25].

Finally, the EU Cloud Code of Conduct emerges as the first tool to receive official approval by Data Protection Authorities to ensure and prove GDPR compliance for all service types of cloud computing.

"The EU Cloud Code provides sufficient safeguards by, for instance adopting the same terminology as the one used in the GDPR (Code, section 2) and providing complaint mechanism to data subjects (Code, section 7.8.2). 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"[26].

Definitely, the intention of the EU Cloud Code of Conduct is to make it easier for cloud customers (particularly small and medium enterprises and public entities) to determine whether cloud services they are interested in are appropriate for their designated purpose.

Moreover, the transparency created by the approved Code will contribute to an environment of trust and to build a high 'default level' of data protection in the European cloud computing market[27]

---

[23] Cf. The General Secretariat of the Belgian Data Protection Authority, Decision n° 06/2021 of 20 May 2021, Accreditation of the "Scope Europe" for the monitoring of the "Eu Cloud Code of Conduct" (DOS -2019-03289) in https://www.dataprotectionauthority.be/publications/decision-n-06-2021-of-20-may-2021.pdf.

[24] Cf. "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). (..) Three cumulative types of monitoring are carried out by the monitoring body: 'initial', 'recurring' and 'ad hoc'.", as stated in The General Secretariat of the BELGIAN DATA PROTECTION AUTHORITY, Decision n° 05/2021 of 20 May 2021, Approval decision of the "Eu Data Protection Code of Conduct for Cloud Service Providers" (AH-2018-0084) in https://www.dataprotectionauthority.be/publications/decision-n05-2021-of-20-may-2021.pdf, cit., page 3.

[25] Cf. EUROPEAN DATA PROTECTION BOARD, Opinion 16/2021 on the draft decision of the Belgian Supervisory Authority regarding the "EU Data Protection Code of Conduct for Cloud Service Providers" submitted by Scope Europe, 20 May 2021 in https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-162021-draft-decision-belgian-supervisory_en, cit., page 9.

[26] Cf. EUROPEAN DATA PROTECTION BOARD, Opinion 16/2021 on the draft decision of the Belgian Supervisory Authority regarding the "EU Data Protection Code of Conduct for Cloud Service Providers" submitted by Scope Europe, 20 May 2021 in https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-162021-draft-decision-belgian-supervisory_en, cit., page 7.

[27] Cf. "Europe Cloud Computing market is projected to surpass USD 75 billion by 2026. The market growth is attributed to the steady uptake of cloud computing platforms to lower IT infrastructure procurement and maintenance costs and rapid expansion of global cloud vendors within the European countries. (..)he retail sector will witness a significant surge in the adoption of cloud computing due to the growing use of the IaaS model to handle website traffic and deliver seamless shopping experience through mobile platforms. The retail industry is rapidly adopting cloud computing technology to leverage customer data for enhanced business intelligence. Technologies, such as interconnected Point-of-Sales (POS) and centralized invoicing through the cloud platform, are assisting retail enterprises in delivering better customer service", as reported in MARKET INSIGHT REPORTS, Press Release, Europe Cloud Computing Market – Detailed Analysis of Current Industry Figures with Forecasts Growth By 2026 Published March 15, 2021, in https://www.marketwatch.com/press-release/europe-cloud-computing-market-detailed-analysis-of-current-industry-figures-with-forecasts-growth-by-2026-2021-03-15?tesla=y.

Source: The Belgian Data Protection Authority, Press releases > The BE DPA approves its first European code of conduct.

Link: https://www.dataprotectionauthority.be/citizen/the-be-dpa-approves-its-first-european-code-of-conduct.